INFORMATION SECURITY & DATA PROTECTION

Cyber security, object Storage, biometria, difesa globale e intelligence per un business always-on

EDIZIONE 2018

Giuseppe Saccardi - Gaetano Di Blasio - Riccardo Florio

Reportec

INFORMATION SECURITY

&

DATA PROTECTION

Prevenzione dalle minacce, risposta gli incidenti, protezione degli endpoint
Dallo object storage alla biometria, alla intelligence per una difesa globale per la salvaguardia del business

Giuseppe Saccardi - Gaetano Di Blasio - Riccardo Florio

Reportec

Avvertenze

 Va notato che le informazioni contenute possono cambiare senza preavviso; le informazioni contenute sono reputate essere corrette e affidabili anche se non sono garantite. La descrizione delle tecnologie non implica un suggerimento all'uso dell'una o dell'altra così come il parere espresso su alcuni argomenti da parte di Reportec è puramente personale. La vastità dell'argomento affrontato e la sua rapida evoluzione possono avere portato a inaccuratezze di cui Reportec non si ritiene responsabile, pur avendo espletato i possibili controlli sulla correttezza delle informazioni medesime; il libro non rappresenta una presa di posizione a favore di una o l'altra delle tecnologie, standard o prodotti ivi riportati né garantisce che le architetture, apparati, prodotti hardware e software siano stati personalmente verificati nelle funzionalità espresse; le descrizioni delle architetture, delle piattaforme, dei servizi e dei dati aziendali sono stati elaborati in base alle informazioni fornite dalle aziende, con le quali gli stessi sono stati analizzati e ridiscussi.

www.reportec.it

SOMMARIO

1 – RESILIENZA, GOVERNANCE E INCIDENT RESPONSE

Contrastare i "pericoli" online è necessario, ma la pressione degli attacchi è tale da rendere praticamente inevitabile il subire una violazione alla sicurezza. Occorre una strategia per mitigare il rischio e cavalcare l'onda della "Digital Technology", permettendo al contempo di superare gli incidenti e ripristinare la piena operatività aziendale.

Ora e sempre resilienza

Il cyber crime è letteralmente fuori controllo: per quante poche e piccole battaglie di riescano a vincere , la guerra sembra persa e l'unica consolazione per le truppe dei "white hat" è di riuscire a diffondere il "verbo" della resilienza. Suona come una resa incondizionata, ma in realtà è una strategia vincente, che, unita ai progressi legati all'artificial intellingence, dà grande speranza.

Secondo il rapporto Clusit 2018 i danni registrati complessivamente a livello globale hanno superato nel 2017 i 500 miliardi di dollari, colpendo oltre un miliardo di persone e questa è una stima per difetto, considerando che sono ancora molti quelli che non si accorgono di aver subito danni. È, infatti, ancora possibile sostenere, come ripetono gli esperti del Clusit da anni e affermò nel 2016 l'allora Ceo di Cisco, John Chambers: "Le aziende si dividono in due categorie: quelle che hanno subito una violazione della sicurezza informatica e quelle che hanno subito una violazione della sicurezza informatica, ma ancora non lo sanno".

La consapevolezza del problema sta effettivamente crescendo, proprio perché aumentando il numero degli attacchi e di conseguenza quello delle vittime, si diffonde la conoscenza, ma non migliora automaticamente la situazione, perché manca la formazione adeguata a evitare il ripetersi della violazione subita.

La diffusione della digital transformation non fa che aumentare il rischio, esponendo una superficie di attacco sempre maggiore. Non esiste più un perimetro aziendale definibile, basti pensare allo smart working, sempre più di "moda", che comporta però l'utilizzo di tecnologie mobili, cloud e social, senza una distinzione netta tra uso lavorativo e domestico della tecnologia.

In sostanza, nessuno è al sicuro, però in tanti, soprattutto in Italia, un paese di naviganti, poeti, inventori e "furbi" patentati", continuano a credere di non essere un bersaglio appetibile e, immancabilmente il/la titolare di turno chiede: "Perché dovrebbero attaccare proprio noi? Siamo piccoli". Infatti non è che attacchino proprio loro, è che attaccano tutti attraverso attacchi automatici che già nel 2016 pesavano per il 98%, secondo i dati registrati sulla rete Fastweb. Oggi la situazione peggiora con la crescita di tecnologie machine learning: come per le molti casi la tecnologia, sviluppata per scopi leciti e lodevoli, viene utilizzata per commettere reati e fare del male.

Uno scenario drammatico

Gli attacchi gravi a livello mondiale, analizzati dagli autori del rapporto Clusit, sono stati 1.127, con un incremento del 240% rispetto al 2011, anno in cui è stata pubblicata la prima edizione del rapporto e con un più 7% rispetto all'anno precedente.
Un 21% degli attacchi gravi registrati nel 2017 è stato giudicato "critico", sempre dagli esperti del Clusit. Negli anni quest'ultimi hanno modificato la valutazione di criticità di un attacco. Fino al 2014, per esempio, venivano considerati gravi i defacement dei siti governativi, tipica azione da hacktivist, cioè attivisti contrarie alle politiche di una o un'altra istituzione. Il danno era soprattutto d'immagine, ma l'indifferenza dell'opinione pubblica di fronti a tali episodi ha permesso di, un certo senso declassificare questi attacchi.
Tuttavia, l'ignavia imperante si registra anche di fronte situazioni poco chiare che hanno serie ripercussioni sui cittadini e le istituzioni. È sconcertante il silenzio su episodi che, sostengono presso il Clusit, palesano un vero e proprio “cambiamento di fase” nel livello di cyber-insicurezza globale. Attività di propaganda sui social architettate grazie a kit disponibili nel dark Web rappresentano rischi gravissimi, colpendo cittadini, istituzioni, governi durante elezioni, con ripercussioni sul fronte della geopolitica e della finanza.
Certamente sono in corso "guerre" tra nazioni incruenti, in termini di vittime umane, ma pronte a cambiare i destini di molte popolazioni.
Tutto ciò rimane in sordina anche perché l'attività principale resta quella del cyber criminali, interessati essenzialmente al denaro. Da questo punto di vista, la tendenza principale resta quella legata ai ramsonware, cioè le estorsioni con richieste di riscatto, le cui campagne si basano essenzialmente su criteri quantitativi: risulta infatti più efficace sferrare un attacco di massa, chiedendo cifre relativamente basse, piuttosto che cercare target più "difficili" e protetti, come le grandi imprese. In questo modo si tende a ridurre l'impatto mediatico e abbassare l'attenzione delle forze dell'ordine.
In ogni caso, viene calcolata in 180 miliardi di dollari la perdita di denaro diretta da parte dei normali cittadini.

Sussiste, peraltro, anche la crescita degli attacchi mirati, che possono rientrare tanto nella categoria del cyber spionaggio, i cui danni economici sono difficili da calcolare, quanto in quella delle frodi economiche. In questo caso, le cifre che vengono sottratte a un'impresa, tipicamente attraverso attacchi di email/business process compromise, sono ingenti. Gli attacchi cosiddetti BEC (Business Email Compromise) hanno inferto grandi perdite finanziarie. Si tratta delle false email, confezionate con cura e spesso precedute da un'accurata fase di raccolta dati per colpire al momento giusto. Tipico è il caso della falsa email spedita dal Ceo al Cfo con una richiesta di effettuare un bonifico urgente. Qui la sicurezza è anche una questione di processi e di cultura aziendale. Analogamente, esistono anche attacchi Business Process Compromise, che cercano di sfruttare appunto i processi, in genere del reparto finanziario, modificandoli, possibilmente tramite le vulnerabilità della supply chain (la catena di fornitura). Sono stati devastanti per Target nel 2014, ma richiedono una pianificazione a lungo termine e maggiore lavoro, quindi meno utilizzate.
Secondo l'analisi del Clusit, gli attacchi mirati sono cresciti del 353%, estendendosi anche a imprese medie e piccole. Gli attacchi sono più aggressivi e, sostengono gli autori del rapporto, prescindendo sempre più da limiti territoriali e tipologia di bersaglio per massimizzare il danno inflitto alle vittime il proprio risultato economico.
La tipologia delle vittime nel 2017 è stata così rappresentata nei vari settori: Research / Education (+29%), Software / Hardware Vendors (+21%), Banking & Finance (+11%) e Healthcare (+10%).

La situazione italiana e il GDPR

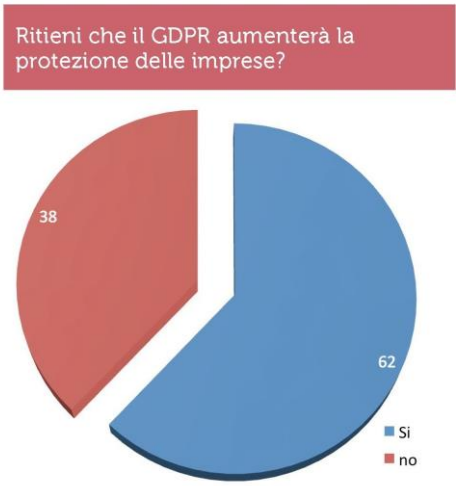
Ancora il rapporto Clusit propone una stima dell'impatto che l'insicurezza comporta dal punto di vista economico in Italia, valutata sul confronto con i dati provenienti da altri Paesi, quali USA e Regno Unito: la perdita così calcolata ammonterebbe a circa 10 miliardi di euro.

1. Resilienza, Governance e incident response

Viene sottolineato da Andrea Zapparoli Manzoni, menbro del consiglio direttivo del Clusit e uno degli autori del rapporto, che si trattai un valore dieci volte superiore a quello degli attuali investimenti in sicurezza informatica, appena sotto il miliardo di euro.

L'imminente scadenza del GDPR, che è stato varato nell'aprile del 2016 e prevede l'entrata in vigore il 25 maggio 2018 potrebbe contribuire a innalzare gli investimenti, ma la sensazione presso gli addetti ai lavori è che si ridurrà all'ultimo momento.

Lo conferma anche una recente inchiesta svolta dalla redazione di Reportec.

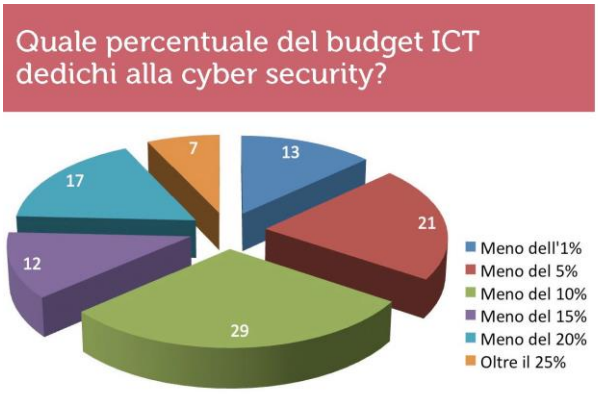


Guardando il lato positivo, possiamo osservare una crescita di attenzione nei confronti della sicurezza. Attacchi devastanti come WannaCry dello scorso anno e altri episodi legati alle estorsioni con il ramsonware hanno portato in televisione e sui tanti canali d'informazione il problema della sicurezza informatica. Sembra tuttavia prevalere la vecchia logica del "tanto a me non capita" , visto i livelli bassi d'investimento in sicurezza.

Un'inchiesta della nostra redazione ha sondato il tema della conformità al regolamento europeo e quello della spesa per la struttura dedicata alla sicurezza informatica.

I risultati sono deludenti: Il 76% delle imprese che hanno risposto al nostro sondaggio o che abbiamo intervistato direttamente, spendono meno del 10% in sicurezza informatica, cioè meno dello stretto necessario, stando alle valutazioni

effettuate dagli esperti del Gartner. Questi ultimi, infatti, ritengono che la suddetta quota occorra solo per la gestione ordinaria della sicurezza, come ci riporta Davide Del Vecchio, membro del consiglio direttivo del Clusit. In altre parole potrebbe bastare a chi ha già messo in piedi una strategia per la security. Nella realtà, però, le imprese italiane sono ancora molto indietro, come sostengono molti analisti e come viene confermato dal nostro sondaggio.



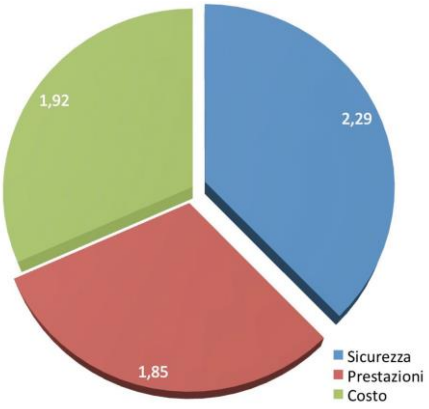
Sono ben il 79% le imprese italiane che ammettono di non essere pronte per il GDPR (General Data Protection Regulation). Una normativa che è stata varata dall'Unione Europea nell'aprile del 2016 ed è entrata in vigore il 25 maggio dello stesso anno, fissando al 25 maggio del 2018 la data in cui avrà efficacia. In altre parole sono stati concessi due anni di tempo per mettersi in regola con la normativa.

Sono rimasti poco più di quattro mesi, ma le imprese italiane non sono ancora pronte, almeno stando a una nostra inchiesta, realizzata sulla base di alcune interviste dirette e, soprattutto, un sondaggio cui hanno partecipato oltre 200 addetti ai lavori.

Sondaggio che, ci teniamo a precisare, non ha alcun presupposto statistico, non trattandosi di un campione significativo, né in termini numerici né quale

rappresentanza dell'universo di specialisti ICT, security manager e business manager (le tre tipologie di intervistati da noi contattati).
Peraltro, i risultati ottenuti, costituiscono una base di riflessione che ci permette d'integrare le opinioni espresse da numerosi esperti, sia in seno a società di ricerca qualificate, sia presso vendor del settore ICT, specializzati in sicurezza.
In sostanza, dunque sono poco più del 20% le imprese che si sentono a posto con la nuova normativa ed è probabile che si tratti perlopiù delle più grandi o, in particolare, delle banche e delle società di telecomunicazioni, già soggette a regole stringenti imposte sia dall'attuale normativa italiana sulla privacy sia da normative internazionali. Aziende che avevano poco o nulla da aggiungere per essere conformi al GDPR.
Sappiamo bene che in Italia siamo abituati a ridurci all'ultimo momento, ma non sempre poi ci riescono le ciambelle col buco
Purtroppo in molti hanno ritenuto il 25 maggio 2018, come la data in cui cominciare a realizzare il piano per la sicurezza e adeguarsi alle nuove norme. Di fatto, invece, è il giorno in cui potrebbero arrivare le prime ispezioni.
Molti degli esperti con cui abbiamo parlato sono convinti che la corsa alla compliance partirà veramente solo dopo che fioccheranno le prime multe.
Ricordiamo, infatti, che mentre banche e telco da tempo erano tenute a informare di eventuali violazioni, dal 25 maggio toccherà farlo a tutti e sono in tanti a non accorgersi di un attacco andato a buon fine se non dopo settimane o mesi.
Un aspetto importante è la possibilità di "scaricare" parte della responsabilità a una società esterna. Un vantaggio per chi già utilizza servizi di terze parti per la sicurezza, cioè il 38% dei rispondenti al nostro sondaggio, che hanno dichiarato di esternalizzare almeno in parte la gestione della sicurezza.
Questo dato mostra un'opportunità importante per tutti: sia per le imprese del settore, che possono ampliare i propri servizi aumentando l'offerta di managed security service (o MSS) sia per le aziende della domanda, che possono concentrarsi sul proprio core business, delegando agli esperti le onerose e delicate operazioni di protezione dei dati. È evidente che il tutto dovrà reggersi grazie a un rapporto di fiducia, una vera e propria partnership tra chi finora ha "semplicemente" venduto soluzioni, come firewall e antivirus e chi fino a ieri si limitava a installare del software e dei dispositivi.

Sul fronte della fiducia, la nostra inchiesta mostra un buon grado di maturità, rappresentato, a nostro avviso, dal punteggio più alto ottenuto dalla sicurezza nella scelta di un cloud provider, laddove il costo è l'ultima delle preoccupazioni.



Il passaggio appena descritto potrebbe non riguardare solo la sicurezza e invece estendersi ad altri servizi informatici, secondo la logica "dell'as a service" introdotta dal cloud. Le imprese del canale ICT possono trovare crescenti benefici per il loro business dalla trasformazione in managed service provider, di cui la sicurezza è solo la punta dell'iceberg.

Alla fine, per un imprenditore si tratta di trovare il partner giusto che sappia fare il proprio mestiere, per concentrarsi sulle attività principali. Ciò non impedisce di conservare un reparto interno dedicato all'informatica e alla sua sicurezza, ma deve sussistere una motivazione forte, quale potrebbe essere lo sviluppo innovativo.

Sempre più la digitalizzazione sta portando "intelligenza" nelle operazioni industriali. È il fenomeno dell'Internet of Things. Le imprese devono e possono sfruttare le nuove tecnologie e le capacità di connessione e integrazione per ottimizzare i processi a tutti i livelli. In sintesi, il "vecchio" reparto IT" mai prima d'ora può guadagnare un ruolo di primo piano in azienda, facendo diventare il CED il motore dell'innovazione aziendale.

L'adozione del cloud è in crescita, rallentata solo dalla necessità di salvaguardare investimenti pregressi e dalla vecchia abitudine italiana di aspettare che l'esperienza dei primi consolidi i processi a garanzia del successo.

Secondo quanto emerge dalla nostra inchiesta, la maggior parte di chi usa il cloud lo fa con attenzione: il punteggio più alto per le priorità viene infatti assegnato alla sicurezza, con un 2,9 rispetto a massimo di 3, o, quantomeno alla sensazione di sicurezza che il cloud provider scelto è riuscito a trasmettere. Al secondo posto, ma quasi a pari merito c'è il costo, che arriva a 1,92, appena sopra all'1,85 assegnato alle prestazioni.

Non abbiamo approfondito le ragioni di questo voto, anche se la senzazione è che il cloud oggi viva principalmente di servizi storage ed è ovvia la preoccupazione per la sicurezza dei dati, mentre le prestazioni vengono fatidicamente accettate in funzione della banda a disposizione.

Il GDPR e le nuove regole dell'Unione Europea

Il campo della sicurezza vede un'Europa comunitaria molto attiva e il contenzioso che per anni l'ha vista contrapposta agli Stati Uniti in termini di riservatezza dei dati dei cittadini europei residenti su data center situati negli USA ne è la evidente dimostrazione.
Quello di definire in modo preciso la riservatezza dei dati è solo uno dei filoni di interesse comunitario quando si tratta di sicurezza. Un altro filone riguarda la proprietà dei dati stessi. Al termine di un lavoro durato tre anni e con un percorso burocratico non del tutto completato, è tuttavia stato emanato dall'Unione Europea il testo della legge sulla protezione dei dati personali (General Data Protection Regulation – GDPR) che sancisce il diritto alla privacy dei cittadini.
Non mancherà di creare qualche problema alle imprese, che dovranno rapidamente adeguarsi alle nuove regole. L'aspetto chiave è che viene stabilito che i dati personali appartengono agli individui e non alle imprese.
Il framework rappresentato dal GDPR sostituirà i regolamenti dei singoli paesi e per molti risulterà più restrittivo delle normative esistenti. Potrebbe non essere il caso dell'Italia, che è piuttosto all'avanguardia sul fronte delle norme in proposito di proprietà dati e privacy.
Qualche problema, come evidenziato, potrebbe però derivare da tempi di attuazione troppo stringenti. Alcuni esperti ritengono infatti che il mondo del business non sia pronto per recepire i complessi cambiamenti legali che il nuovo regolamento impone, con le ripercussioni in termini di compliance, auditing e rischio di un aumento di cause/ricorsi.
Le imprese che gestiscono un numero significativo di dati sensibili saranno tenute a nominare un data protection officer. Lo stesso se monitorizzano il comportamento di numerosi consumatori.
Di fatto, si richiede e si impone alle aziende un'attenzione maggiore alla sicurezza (con i relativi oneri economici da sostenere). Inoltre, si sancisce che i

dati appartengono all'individuo, ma se ne permette anche l'utilizzo, purché l'individuo ne dia esplicito consenso.
È una limitazione per molti paesi comunitari, ma non per l'Italia, che già ha adottato questa politica da tempo.
Il nuovo regolamento prevede che dalla data di pubblicazione i Paesi interessati abbiano due anni di tempo per adeguarsi alla nuova normativa.
Un'analisi del tema e dei suoi effetti è stata fatta da GetSolution, una società che si occupa di Privacy Law e di sicurezza dei sistemi informativi, svolgendo progetti molto complessi presso clienti di medie e grandi dimensioni, sia italiani che internazionali. I maggiori cambiamenti evidenziati comprendono:

- Le responsabilità che ha l'incaricato del trattamento riferito oggi come "responsabile del trattamento" rispetto a quelle attuali.
- La possibilità da parte dell'incaricato del trattamento di subappaltare attività a un fornitore solamente a seguito dell'ottenimento dell'autorizzazione da parte del Responsabile del Trattamento (il Titolare del Trattamento).
- La valutazione d'impatto (analisi dei rischi) come base sulla quale costruire la sicurezza delle informazioni attraverso l'implementazione di contromisure di sicurezza tecnologiche, procedurali e fisiche
- Le procedure di Data Breach da implementare in modo efficace ed efficiente, in quanto non solo è necessario notificare la violazione dei dati personali all'autorità di controllo competente, ma nel caso in cui la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il responsabile del trattamento (il Titolare) deve comunicare tale violazione all'interessato.
- La possibilità da parte dell'interessato di chiedere al Responsabile del Trattamento e/o all'incaricato del Trattamento il risarcimento dei danni materiali e immateriali.
- Le sanzioni di carattere amministrativo, .
- La figura del Data Protection Officer e cioè il responsabile della protezione dei dati, figura che corrisponde al "Privacy Officer" attuale con però responsabilità certamente maggiori.

Per quanto concerne la valutazione di impatto va osservato che. è richiesta in particolare nel caso di una valutazione sistematica e globale di aspetti personali

relativi a persone fisiche basata sul trattamento automatizzato (profilazione compresa), nel trattamento su larga scala di categorie particolari di dati o di dati relativi a condanne penali e a reati di cui all'articolo 9 bis, nel caso di sorveglianza sistematica di una zona accessibile al pubblico.

Attenzione ai termini, evidenzia la società di ricerca. La precisazione "in particolare" riportata nel comma 2 dell'articolo n. 33 non vuol dire che è obbligatoria solo nei 3 suddetti casi. È da intendersi che è obbligatoria per tutti anche perché nell'art. 30 che parla della Sicurezza del Trattamento, il Responsabile del Trattamento come anche l'incaricato del trattamento, devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio.

In sostanza, si rende necessaria l'analisi dei rischi che permetta di definire le adeguate contromisure di sicurezza tecniche e organizzative al fine di garantire la sicurezza del trattamento

Come evidenziato le aziende avranno due anni dalla pubblicazione del regolamento per implementare gli adempimenti previsti. Cosa fare? Quello che la società di consulenza suggerisce è:

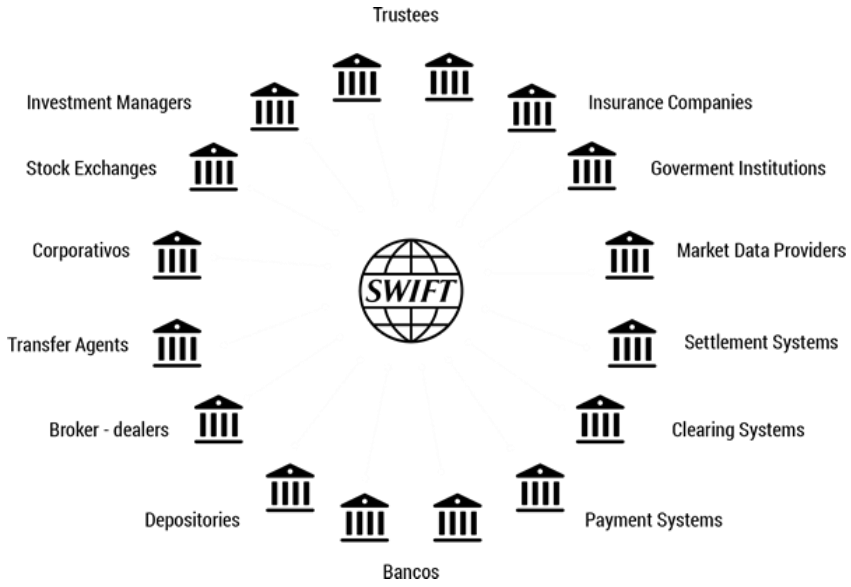
- Attendere che l'Autorità di Controllo Italiana dia indicazioni in merito all'approccio da adottare relativamente all'implementazione degli adempimenti.
- Rivolgersi se privi di specifici esperti aziendali a una società di consulenza esperta in ambito "Privacy" che possa affiancare l'azienda nel passaggio al nuovo Regolamento, che appare tortuoso e prevede nei due anni di transizione molteplici adempimenti.
- Iniziare con la valutazione d'impatto /analisi dei rischi. Nell'analisi dei rischi devono essere mappate le categorie di dati personali che l'azienda tratta identificando finalità e modalità, valutate la probabilità e i relativi impatti che potrebbero causare la perdita di riservatezza, calcolato il livello di rischio per i dati personali e definite le contromisure tecniche, organizzative e fisiche da implementare. A questo si aggiunge la necessità di disporre di un DPO, anche se non strettamente obbligatorio,

Quello che viene suggerito è poi che l'azienda mantenga costantemente nel tempo la compliance al Regolamento Generale anche perché Il Regolamento è

stato ideato proprio per spingere le aziende a considerare il processo relativo alla gestione dei dati personali come un aspetto fondamentale dell'azienda stessa e quindi da gestire, migliorare e modificare costantemente.
Il Nuovo Regolamento Generale, si evidenzia essere migliorativo rispetto al precedente, perché frutto dell'esperienza dell'applicazione dei singoli decreti legislativi in ambito Privacy in essere ormai da anni nei Paesi UE, anche se non è stato completamente raggiunto l'obiettivo di uniformare la norma e di renderla uguale per tutti i Paesi comunitari perché il Regolamento lascia ampi margini di modifica a ogni Stato Membro anche su aspetti fondamentali.
Cosa che rappresenterà di certo un problema per le aziende che operano in un contesto internazionale europeo, già alle prese con le differenze normative riguardo la riservatezza dei dati esistenti tra UE e USA, per non parlare di altre aree mondiali dove la riservatezza è ancor più aleatoria.

Sicurezza delle transazioni finanziarie: la rete SWIFT

Un poco in sordina rispetto alla normativa GDPR, modifiche normative sono avvenute anche per quanto riguarda strettamente il mondo finanziario e le transazioni economiche.
Il problema della sicurezza non poteva non interessare profondamente il settore finanziario, che ha definito significative modifiche alla normativa al fine di meglio garantire una maggior sicurezza per le transazioni finanziare.
SWIFT (acronimo di "Society of Worldwide Interbank Financial Telecommunication"), la società che fornisce all'ampia comunità di istituzioni finanziarie globali e aziende l'infrastruttura per le transazioni economiche, proprio per fronteggiare i rischi che corrono le entità finanziarie e gli scambi di denaro ha definito una più dettagliata normativa che ha l'obiettivo fondamentale di permettere lo scambio sicuro di informazioni sensibili inerenti le transazioni finanziarie che avvengono a livello internazionale e di contrastare efficacemente gli attacchi.

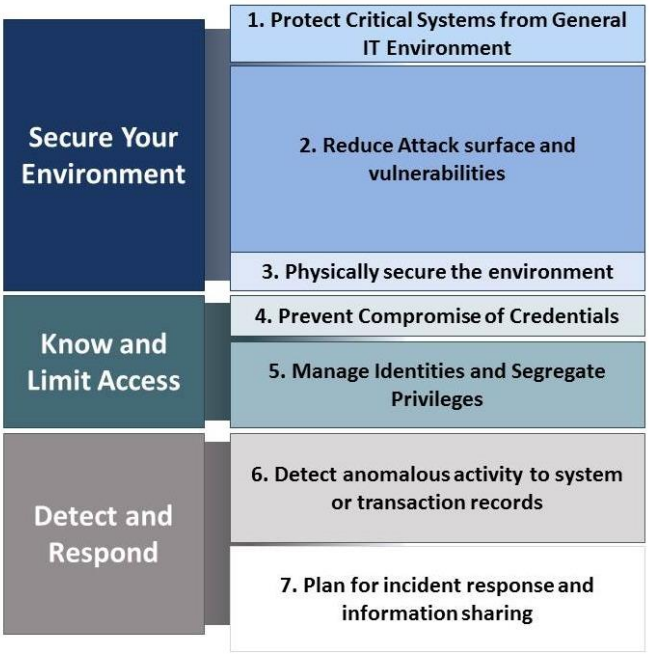


L'ampi insieme di utenti privilegiati della rete SWIFT

L'obiettivo degli attacchi è tipicamente quello di impossessarsi in modo fraudolento delle credenziali degli operatori SWIFT. Proteggere le credenziali e fare in modo che i cyber criminali non ne vengano in possesso è quindi uno dei passi essenziali per prevenire il realizzarsi di attacchi che possono tramutarsi in consistenti perdite economiche e di immagine.

Il Framework SWIFT

L'impegno di SWIFT si è tradotto in un frame-work che elenca 27 diversi tipi di controlli (suddivisi in Mandatory e Advisory) che nel complesso permettono di raggiungere tre obiettivi: Rendere sicuro l'ambiente; Conoscere e controllare gli accessi; Individuare e rispondere.



Gli obiettivi del frame-work SWIFT

Come dato di fatto, la complessità e la vastità dei controlli da intraprendere e le garanzie da fornire alla Community SWIFT sono tali, e da attuare in tempi brevi, da rendere molto difficile per un ente finanziario il procedere in modo autonomo per risultare compliant con quanto richiesto.

Non sorprende quindi che vi sia stato l'interesse per le società di sicurezza nello sviluppo di soluzioni atte a supportare le organizzazioni in un impegnativo percorso di adeguamento al frame-work tramite lo sviluppo di nuove soluzioni, che lo permettessero in toto o in parte, risultando difficile per la singola azienda far fronte a tutte contemporaneamente data la loro ampiezza e specificità.

Le soluzioni rese disponibili, ad esempio, forniscono competenze necessarie per essere compliant con le specifiche, come la possibilità di conoscere in ogni istante gli accessi alle applicazioni e ai sistemi informatici critici, nonché di rilevare e far fronte ad attività ad alto rischio implicite nelle sessioni di operatore quando hanno a che fare con la gestione di transazioni finanziarie.

I paragrafi seguenti illustrano in sintesi i tre obiettivi previsti dalla normativa, e come le soluzioni sul mercato permettano di far fronte ai requisiti in termini di sicurezza previsti e come aiutino le organizzazioni nel risultare compliant.

Rendere sicuro l'ambiente

Secure Your Environment e cioè rendere sicuro il contesto in cui si opera è il primo degli obiettivi previsti da SWIFT. Un attacco andato a buon fine, che sia dovuto ad una azione volontaria o involontaria, può causare vulnerabilità per quanto concerne le credenziali degli account.
Per disporre di un ambiente sicuro e a norma SWIFT, le soluzioni rese disponibili hanno come obiettivo primario quello di permettere di proteggere e controllare l'accesso a sistemi e infrastrutture critiche dell'ambiente SWIFT locale. Sono soluzioni con le quali le organizzazioni possono ad esempio rimuovere i diritti agli amministratori locali e utilizzare altre funzioni inerenti la gestione degli endpoint privilegiasti per fornire agli utenti la possibilità di realizzare interventi su base on-demand quando ciò è richiesto e previsto dalle policy di sicurezza aziendali.
In genere sono soluzioni che permettono altresì di disporre di una sicurezza multilivello che protegge le credenziali degli account privilegiati, incluso le password e le chiavi di sicurezza SSH che potrebbero essere usate per accedere a sistemi operativi Unix o Linux critici.

Conoscere e controllare gli accessi

Know and Limit Access è il secondo dei tre obiettivi fissati SWIFT. Una risposta a quanto previsto da questo obiettivo è fornito da soluzioni centrate sulla protezione delle credenziali e sulla gestione delle identità. Si tratta di applicazioni il cui scopo è di isolare, controllare e registrare le sessioni privilegiate dei sistemi critici, individuare comportamenti e attività sospette sin dal loro insorgere e terminare forzatamente da remoto sessioni dubbie.
Mettono anche a disposizione funzioni per l'analisi e la ricerca dei file di audit delle sessioni svolte, che possono essere memorizzate in vault a prova di

effrazione per prevenire che utenti che dispongono dei diritti necessari possano accedere ai file e rimuoversi dallo storico.

Individuare e rispondere

Detect and Respond, il terzo obiettivo, consiste precipuamente nell'individuare e contrastare qualsiasi tipo di attacco provenga dall'esterno volto a compromettere credenziali trusted all'interno della rete SWIFT. Per aiutare gli enti finanziari a fronteggiare questi rischi sono disponibili soluzione che comprendono la capacità di individuare abusi, l'uso non corretto dei privilegi e delle credenziali, e i tentativi di furto di credenziali privilegiate.
A questo si abbinano anche funzionalità per evidenziare rischi elevati e attività anomale in corso all'interno dell'ambiente SWIFT.

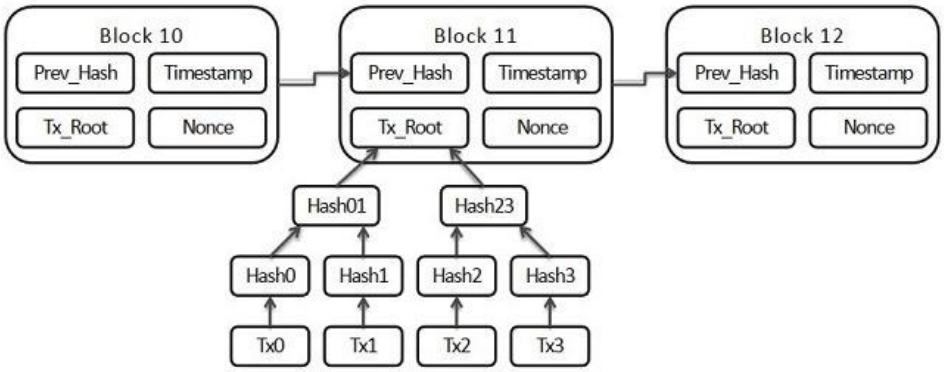
L'esigenza di un supporto valido

Come evidenziato e deducibile da quanto illustrato, si tratta di un corpus normativo molto ampio che tocca numerosi e vara spetti inerenti la sicurezza dell'ambiente It, della rete e delle procedure da eseguire. Per essere compliant disporre di soluzioni non basta. Per potere essere compliant, ed esserlo continuamente, servono anche altre attività.
Sono attività che vengono fornite da società specializzate nella sicurezza sia del sistema centrale e/o degli endpoint privilegiati, che hanno sviluppato modalità di affiancamento e di supporto all'ente finanziario quando questi si deve adeguare e quando necessita di risorse successive qualora non ne disponga per mantenere l'allineamento con le specifiche normative.
Il punto di partenza si evidenzia in ogni caso essere la conduzione iniziale di una approfondita analisi del livello di compliance dell'ente finanziario, essenziale per individuare il punto di partenza e le aree in cui intervenire.
Individuato dove l'ente non è aderente al frame-work SWIFT viene definito congiuntamente un piano per inserire nell'ambiente IT e procedurale in esame quei controlli di sicurezza attualmente non presenti ma che sono mandatory.

Dopo questa prima fase viene definita congiuntamente la road-map verso la compliance, quando e come introdurre nel sistema i controlli necessari e gli investimenti che devono essere sostenuti.
A seguito dell'assessment e del completamento del progetto di adeguamento al frame-work vi è la fase di implementazione della soluzione, a cui segue una fase di test dei componenti SWIFT che sono stati interessati dalle attività di messa a norma.
Come è deducibile si tratta di passi complessi, così come complesso è il frame-work ma, evidenziano specialisti e società di ricerca, indispensabili per ottemperare in pieno al frame-work e garantire al sistema finanziario e agli operatori, nonché ai clienti, che il sistema sia trusted.

Una sicurezza targata Blockchain

Un modo ideato per evitare attacchi e l'alterazione di informazioni, o meglio, permettere in modo certo di individuarlo in tempi rapidi, consiste nella tecnologia Blockchain, in italiano traducibile come catena di blocchi. Nella sua essenza consiste in è sequenza in costante crescita di record, chiamati blocchi collegati tra loro e resi sicuri mediante il ricorso alla crittografia.
Ogni blocco della catena contiene un puntatore hash che lo collega in modo biunivoco al blocco precedente, un timestamp e i dati della transazione da rendere sicura.
La sua sicurezza deriva dal fatto che è come se si avesse un registro aperto e distribuito che può registrare le transazioni tra due parti in modo sicuro, verificabile e permanente perché l'operazione è registrata in modo indelebile su un numero molto ampio di nodi della rete, nodi che formano una architettura database peer-to-peer abbinata ad un protocollo di convalida dei nuovi blocchi generati.



Catena di blocchi nell'architettura blockchain (fonte Wikipedia)

Una volta registrati, i dati in un blocco non possono essere retroattivamente alterati senza che vengano modificati tutti i blocchi successivi ad esso, il che necessiterebbe il consenso della maggioranza della rete, cosa che rende praticamente inefficace qualsiasi attacco fosse apportato.
Va anche osservato che la registrazione su più nodi ha anche l'effetto di evitare il rischio del tipico single point of failure.
Come accennato, la sicurezza si basa sulla cifratura a chiave pubblica, rappresentata da un indirizzo su blockchain. I token inviati nella rete vengono registrati come appartenenti a questo indirizzo. La chiave privata è invece una sorta e agisce come password per dare al proprietario la possibilità di accedere alle proprie risorse oppure di interagire con le funzionalità blockchain.

Interesse in crescita

Svariati i settori interessati alla tecnologia blockchain o già attivamente coinvolti in essa tramite reti trusted di operatori e provider specializzati. Tra questi:

- **Pubblica Amministrazione.** è possibile conservare e gestire i registri pubblici digitali in modo sicuro e decentralizzato: i protocolli algoritmici proteggono i dati da eventuali alterazioni volontarie o accidentali. È inoltre possibile gestire le identità digitali senza rischi per la privacy e amministrare in modo efficiente e sicuro sistemi di riscossione delle

imposte o di assegnazione e tracciatura di fondi. Reti trusted consentono anche di analizzare e incrociare grandi moli di dati nel rispetto della riservatezza dei cittadini, con importanti ricadute positive per la governance pubblica.

- **Settore Bancario e Finanziario**. In questi contesti, dove la Blockchain è già una realtà affermata, è possibile ricorrere a un network privato che garantisce sicurezza e affidabilità maggiori, a partire da gestione e conservazione dei dati. I protocolli algoritmici offrono benefici anche per il data sharing perchè permettono la condivisione dei dati anche tra operatori che non si conoscono, rendendo possibile lo sviluppo di nuovi modelli di business, fondati sulla collaborazione, senza che questo comprometta la confidenzialità delle informazioni o la competitività delle aziende coinvolte.
- **Settore Sanitario.** È possibile raccogliere e conservare dati clinici e gestire la verifica dell'identità dei pazienti in totale sicurezza. I dati possono inoltre essere utilizzati a supporto di attività di ricerca medica, per diagnosticare patologie o, in alcuni casi, persino per prevederne l'insorgenza. Il tutto nel pieno rispetto della privacy dei pazienti.
- **Settore Industriale.** In questo ambito, la blochchain rende possibile lo scambio di dati tra aziende, anche concorrenti, stimolando l'innovazione e creando nuove opportunità di business.

Da tempo si dice che la Blockchain sarà la prossima grande rivoluzione, che avrà un impatto impensabile sul nostro futuro. Ora questa rivoluzione è arrivata; non è più un futuro vago e fumoso, ma un'opportunità presente e concreta che ogni organizzazione, pubblica o privata che sia, può cogliere in totale sicurezza. Le potenzialità delle reti Blockchain private sono innumerevoli e stanno interessando settori sino ad ora impensati, come quello per la tracciabilità dell'agroalimentare.

Ad esempio una azienda nazionale ha realizzato una piattaforma basata sulla tecnologia blockchain per il tracciamento di materie prime e prodotti lungo tutta la filiera alimentare. In pratica la piattaforma crea un codice univoco, che può essere applicato sul supporto preferito (scegliendo tra QRcode, tag NFC o

Rfid), abbinato al prodotto che si intende tracciare e associato all'account del produttore.
Il codice riporta tutti i dati che l'azienda cliente intende rendere noti sotto diverse forme (video, immagini, certificazioni). Le informazioni diventano così fruibili in maniera trasparente, univoca, certa, inalterabile e indelebile a vita.
L'azienda produttrice può decidere quali informazioni immettere nel sistema e il grado di visibilità delle stesse. In particolare, è possibile rendere pubblici tutti i dati inseriti oppure riservare l'accesso a dati specifici solo a utenti identificati, con la libertà di poter cambiare disposizioni in ogni momento con una semplice operazione sull'applicativo.

Container e sicurezza

La diffusione dei container come strumento per semplificare la gestione di applicazioni e dati, processo riferito in letteratura anche con il termine anglosassone di "containerization", ha fatto emergere nuove problematiche concernenti la loro sicurezza.
I container rappresentano una componente di una architettura per i dati che permette di rendere le applicazioni più portatili tra ambienti di sviluppo, test e produzione e da questo deriva il loro successo e l'ampia accettazione.
In sostanza, aiutano a semplificare gli sviluppi del software e a risparmiare tempo, e di conseguenza costi di sviluppo.
Il problema segnalato da esperti del settore è però che un Container in quanto tale può agire, tramite il sottostante kernel del sistema operativo su cui gira, come punto critico per la diffusione di attacchi cibernetici.
Proprio per la loro portabilità, un altro fattore del loro successo, ed il fatto che contengano in un unico contenitore tutto quanto relativo a uno specifico progetto o attività business, ne risulta un aumento dei rischi connessi alla sicurezza.
Smarrire o aprire la strada verso l'interno di un container a un cyber criminale non è come perderne una limitata parte, quello che si mette a rischio è l'intero complesso, rischio che poi può essere aggravato dal suo porting in un altro contesto di suo utilizzo.

In proposito, un recente studio di Forrester commissionato ha rivelato che oltre il 50% dei decision-maker IT, pur fortemente interessati al concetto di container, ha identificato la sicurezza come principale freno all'adozione dei container.
Le aziende che intendono adottarli, se ne può dedurre, dovrebbero quindi guardare attentamente al modo in cui sia possibile garantire la sicurezza dei container, focalizzandosi in particolare su aspetti chiave quali:

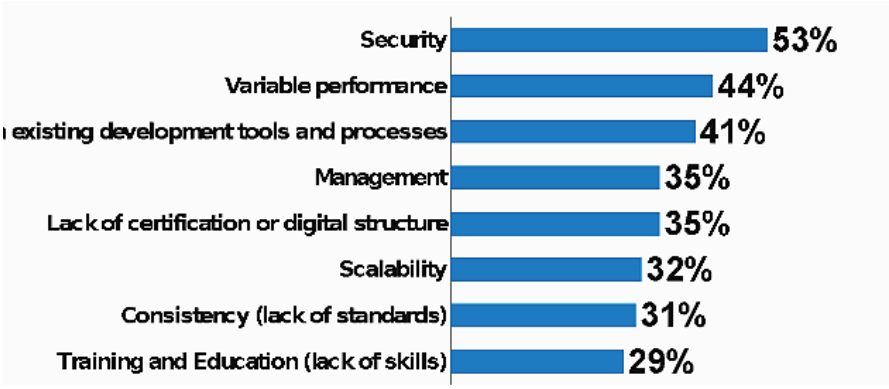
- La sua provenienza.
- Il suo contenuto.
- I modi di suo isolamento.
- La fiducia riposta nel suo utilizzo.

Certificare e ispezionare il container

La prudenza si impone. Oltre il 30% delle immagini ufficiali su Docker Hub, evidenziano manager di primarie società operanti nella sicurezza informatica, , contengono vulnerabilità importanti. In proposito, La certificazione con firme digitali permette per esempio di aggiungere un livello di sicurezza confermando chi ha creato il container e a quale scopo.
Per aumentare la sicurezza leader di mercato stanno lavorando per stabilire standard e practice per la certificazione dei container in modo da garantire aspetti chiave nel loro utilizzo sicuro e trusted quali:

- Che tutti i componenti provengono da fonti fidate.
- Che i container host non siano stati manomessi e siano aggiornati.
- Che l'immagine container non presenti vulnerabilità note nei componenti della piattaforma e nei sui livelli.
- Che i container siano compatibili e operino in ambienti ospitanti che risultino essere stati certificati

Verificare da dove viene un container è quindi importante, ma analizzare quello che c'è dentro l'immagine del container lo è ancora di più, mettono in guardia gli specialisti.
Un ruolo nel migliorare la sicurezza dei container lo può ad esempio avere la Deep Container Inspection (DCI).



I problemi incontrati dai manager con i container (fonte Forrester)

Come la deep packet inspection studia i pacchetti che viaggiano in rete alla ricerca di contenuti malevoli, così la Deep Container Inspection ha la funzione di esaminare il contenuto di un container. Avere visibilità sul codice all'interno del container è un punto fondamentale per mantenere la sicurezza durante e dopo lo sviluppo.

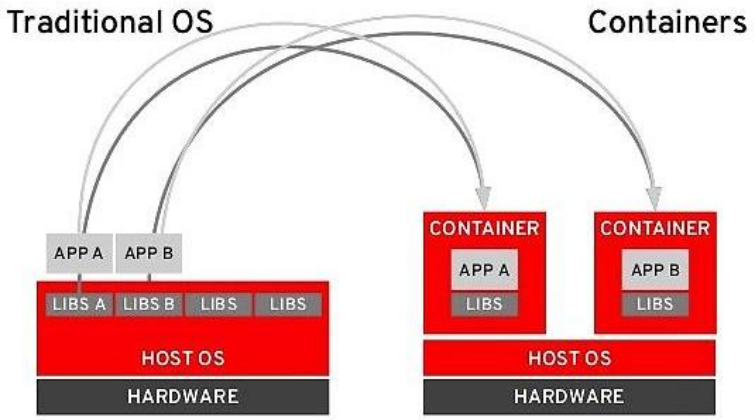
Isolare un container mette al sicuro il business

Una volta che le applicazioni container-based sono composte da container sicuri, il suggerimento degli specialisti è di assicurarsi che non vengano compromessi da altre immagini container sullo stesso host.
La realtà è che i container non contengono veramente delle applicazioni, è più corretto dire che i container pacchettizzano il codice di un'applicazione con quelle c he ne costituiscono le sue dipendenze. Se si pensa ai container come degli oggetto con delle pareti, si deve in sostanza essere consapevoli che si tratta di pareti estremamente sottili.
I contenuti malevoli in un container possono passare a un altro o al sistema operativo host che lo supporta. Ogni singolo processo che gira all'interno di un container parla infatti direttamente con il kernel dll'host, che lo è per tutti i container su quell'host.
Il kernel può in pratica fungere da single point of failure, compromesso quello ne risultano compromessi tutti i container che vi si appoggiano. Come dire che

una vulnerabilità all'interno del kernel Linux potrebbe permettere a coloro che accedono a un container di impossessarsi dell'host OS e di tutti gli altri container sull'host.
Per questo quello che viene ritenuto fondamentale è di affidarsi a un host OS che venga mantenuto da kernel engineer e che sia aggiornato frequentemente con i più recenti fix di sicurezza.
Come per una catena, la cui resistenza è quella del suo anello più debole, i containers basati su host deboli ereditano il modello di sicurezza compromesso di quell'host. Il kernel, è considerato il punto chiave, deve includere funzionalità che offrano livelli di isolamento e separazione appropriati come ad esempio SELinux, Seccomp, Namespaces, e altri.

Il fattore tempo

Un'altra variabile va considerata, quella temporale. Se nell'istante "t zero" l'applicazione basata su container- viene messa in produzione, cosa succede il giorno successivo? E quello successivo ancora?
Nuove vulnerabilità, come evidenziano con una certa dose di sadismo i frequenti report che vengono pubblicati dai ricercatori, vengono identificate quotidianamente e l'immagine container è sicura quanto il codice e le dipendenze che questi contiene. Red Hat per esempio ha segnalato di aver identificato e risolto 66 vulnerabilità di varia gravità nel JAVA Runtime Environment in 315 giorni, ma ne è sufficiente una per compromettere il container e, potenzialmente, l'intero stack dell'infrastruttura IT.
Quello che ne consegue è che anche i container e i loro host devono essere gestiti durante l'intero ciclo di vita e non solo nel momento della loro messa in esercizio. Un container sicuro oggi quasi certamente non lo è l'indomani.
Mantenerlo sicuro non è però una cosa che si può lasciare all'improvvisazione, soprattutto se in azienda il ricorso ai container è diffuso. Le aziende necessitano ai fini pratici e pragmatici di strumenti e di policy che automatizzino la gestione di versioni e upgrade, identità e accessi, sicurezza e prestazioni.



Architettura tradizionale vs Container

Come procedere per un container al sicuro

Anche se velocità e agilità rappresentano driver fondamentali per l'adozione dei container in azienda, suggeriscono i ricercatori, non devono essere integrati a spese della sicurezza.

Ecco perché una Deep Container Inspection eseguita a livello enterprise, associato a certificazioni, policy e fiducia è opportuno costituisca parte integrante dello sviluppo, della messa in produzione e della gestione dei container.

Per trarre il massimo vantaggio dai container pur garantendo la sicurezza di questi ultimi e dei loro contenuti, l'azienda deve trovare quindi modi più efficaci per determinarne la sicurezza operando principalmente in due direzioni

- **Provenienza**. Prima di spostare un container in rete, accertarsi di sapere cosa contiene e dove ha avuto origine. Analizzare la tecnologia di validazione e le certificazioni relative alle fonti. La Deep container inspection può guardare sotto questo punto di vista al di là dell'immagine per identificare e mitigare eventuali vulnerabilità.
- **Isolamento**. Considerare l'isolamento del percorso di esecuzione del container con strumenti quali SELinux (Security-Enhanced Linux). **SELinux** è un modulo di sicurezza del kernel Linux che fornisce un

insieme di strumenti per utilizzare e monitorare il controllo degli accessi incluso il Mandatory Access Control(MAC), tutto questo utilizzando i framework Linux Security Modules (LSM). In ambienti multi-tenant, è poi da valutare l'associazione di container con la virtualizzazione per uno strato di sicurezza aggiuntivo.

- **Ispezione periodica**. ispezionare regolarmente i contenuti dei container per ridurre eventuali rischi alla sicurezza per identificare ed eliminare le vulnerabilità.

2 - L'EVOLUZIONE DELLE MINACCE E LA SICUREZZA INTELLIGENTE

La prepotenza del ransomware, la potenza dei DDoS gonfiati dall'IoT, l'efficacia del phishing negli attacchi mirati, l'emergere del cyber warfare e dell'information warfare di propaganda. Lo scenario del rischio si trasforma con l'industrializzazione del cyber crime.

.

Dagli attacchi sofisticati a quelli di massa

Negli anni si è assistito a un costante aumento delle minacce, ma, cosa ancora più grave, a un continuo "miglioramento" delle stesse: in altre parole, sono sempre più sofisticate e difficili da rilevare. Soprattutto: sono più dannose e cattive. Meno poetiche anche: nel 2000 il worm "I Love You" era stato progettato per intasare i POP e riempire i server di file. In pratica, il suo unico scopo era quello di propagarsi il più rapidamente possibile. Fu stabilito un record da battere: effettuare il giro del mondo il più rapidamente possibile. Creò certamente danni e fermi del servizio Internet e di molte intranet interne alle aziende, ma i danni economici furono relativamente contenuti e indiretti.

Oggi gli strumenti di propagazione vengono impiegati per diffondere ransomware, dove ransom significa "riscatto" in inglese. È una vera e propria estorsione, che prevede il blocco del dispositivo e una richiesta appunto di riscatto per liberarlo. In altri casi, sono i trojan (cavalli di Troia) a essere propagati, i quali, una volta annidatisi "silenziosamente" sul dispositivo della vittima, aprono una porta sul retro (backdoor) per consentire al malintenzionato di prendere possesso del dispositivo stesso. L'obiettivo, però, è quello di non disturbare l'utente, anzi, ci sono anche casi in cui il sistema viene ottimizzato. Quando occorre, però verrà sfruttata la capacità elaborativa, collegandola a quella di migliaia di altri sistemi, per ottenere supercomputer che costituiscono una botnet, utile come piattaforma di attacco (per esempio per decodificare password o decifrare dati crittografati.

Una volta c'erano gli hacker e il loro spirito goliardico. Lo stesso termine "to hack", nato negli anni Cinquanta al MIT di Boston indicava un'innocua infrazione del regolamento interno: sfidare i divieti di accesso ad aree riservate per sfruttare i tunnel sotterranei come scorciatoie tra i padiglioni del campus universitario. Uno spirito goliardico testimoniato dalle firme nascoste nel codice e lasciate per acquisire "gloria" quantomeno negli ambienti underground.

Dall'iniziale obiettivo di mostrare il proprio valore penetrando in sistemi considerati inviolabili, il passaggio a un'attività criminale vera e propria non è stato breve, ma si è ormai compiuto. Non è più, dunque, il tempo dei virus di una volta, ma quello di più pericolosi malware e tecniche di attacco, quali

phishing, adware, spyware e botnet, che si combinano con codici maligni spesso scritti per specifici attacchi e con exploit kit specializzati.
Le minacce attuali vengono dalla combinazione di vecchi codici maligni e strumenti di attacco che sembravano dimenticati, come i worm, usati nel passato per diffondere rapidamente i virus e oggi adoperati per veicolare rapidamente altri codici.
Il rischio più alto lo generiamo da soli, non applicando le patch alle vulnerabilità note e che vengono sistematicamente sfruttate.
Il prossimo fronte della cyber war tra cattivi e buoni è sul terreno della artificial intelligence, con algoritmi che analizzeranno i big data della sicurezza a scopo preventivo, puntando a sistemi di protezione automatici, mentre i criminali si adopereranno per raffinare le tecniche di engineering atte a trovare i punti deboli e a raccogliere le informazioni per definire le strategie di attacco.

Le Advanced Persistent Threat (APT)

I ramsonware hanno inizialmente ridotto l'impatto dei cosiddetti attacchi mirati. Questi ultimi sono molto onerosi da condurre, ma la loro efficacia li rende molto utilizzati per ottenere informazioni da rivendere o per effettuare frodi economiche. La semplicità dei ricatti, che comprende anche la rapidità di monetizzazione senza i rischi delle frodi che richiedono di riciclare i proventi illeciti, grazie all'utilizzo dei BitCoin e di transazioni non tracciabili, hanno confinato gli APT a veri e propri attacchi mirati.
Questi sono comunque in aumento, ma con un tasso d'incremento crescente, sostenuto dal fenomeno dello spionaggio informatico e del cyber warfare, in preoccupante crescita.
Gli attacchi mirati, cioè condotti con un preciso fine, si accompagnano a quelli "silenti", cioè orientati a uno specifico obiettivo evitando di "far rumore". Sono quelli che vengono raccolti nella categoria Advanced Persistent Threat.
Gli APT sono sono utilizzati in tutti gli ambiti: nello spionaggio industriale o governativo, nelle azioni di sabotaggio, nei furti di proprietà intellettuale, nella sottrazione di dati e così via, anche se, come accennato, sempre meno per frodi monetarie.

Gli aggettivi "advanced" e "persistent" indicano le caratteristiche principali di questi attacchi: l'uso di tecniche sofisticate, la combinazione delle stesse in una strategia basata su più fasi e la tenacia con cui questa viene applicata con continuità fino all'ottenimento dell'obiettivo e oltre. Oltre, perché in casi come lo spionaggio, il malware è progettato per annidarsi e continuare a spiare anche per anni, finché non viene scoperto.
Recentemente, per esempio, sono stati trovati malware che "spiavano" enti governativi e aziende statunitensi, probabilmente di origine russa (un sospetto dovuto alla presenza di caratteri cirillici in alcune stringhe di testo incluse nel codice).
Le fasi di un attacco APT sono diverse: secondo alcune classificazioni 5, per altri 6 o 7. Di fatto, non c'è una reale uniformità, perché alcune di queste fasi possono mancare o, più spesso, essere accorpate in un'unica azione a seconda dei casi.

Le sette fasi di un attacco APT

La caratteristica principale è l'utilizzo di più tecniche organizzate secondo una sequenza abbastanza standard, perlopiù rappresentata in sette fasi. Queste sono:
1 - Ricognizione – Come detto, gli APT sono perlopiù attacchi mirati, che, come nella migliore strategia di guerra, sono preceduti da una fase di studio del

"nemico". In questo caso, il cybercriminale cerca dati sul bersaglio da colpire, partendo, tipicamente, dal sito Web e facendo sfoggio di capacità deduttive. Per esempio, un'offerta di lavoro in cui si ricerca personale specializzato in un determinato applicativo software permette di comprendere quali sistemi vengano utilizzati in un'azienda, identificando potenzialmente delle vulnerabilità. In generale, si vuole trovare dati personali tra i profili online, gli indirizzi e-mail, gli organigramma aziendali, gli hobby e interessi sui Social Network. Più informazioni si ottengono, maggiori sono le probabilità di affinare e rendere efficaci le successive fasi di attacco.

2 -- Adescamento – Questa fase è diventata più facile di quanto si possa immaginare con la diffusione dei sistemi mobile. La cultura sulla sicurezza informatica è scarsa ed è facile incuriosire, soprattutto se si conoscono (vedi fasi uno) i punti deboli della persona cui si spedisce un messaggio mirato. Inoltre, quando questi messaggi arrivano sullo smartphone, dove complice la "visibilità ridotta" e soprattutto l'abitudine a cliccare prima e pensare dopo, è alta la possibilità che il malcapitato caschi nella trappola. Quasi certamente non se ne accorgerà, perché il cybercriminale si guarderà bene dal creare disturbo, magari gli manderà un secondo messaggio di scuse perché il primo aveva avuto un comportamento strano, tranquillizzando gli eventuali dubbiosi.

I filtri antispam possono fermare attacchi di massa, ma nel caso di quelli mirati i messaggi puntano su comunicazioni normalmente attese dall'utente, che spesso questi filtri considerano attendibili. Secondo alcune ricerche fra i cinque argomenti più usati come esca via e-mail sono l'avviso riguardo un ordine, la conferma di un biglietto, l'annuncio di una consegna di un corriere espresso, un'e-mail di verifica e una notifica di informazioni sui rimborsi fiscali. Ma sono tattiche generiche usate da chi vuole sparare nel mucchio. Gli attacchi mirati usano anche messaggi apparentemente inviati dal proprio capo e sfruttano i dati raccolti, quindi la sicurezza aziendale, teoricamente, andrebbe estesa anche alla pagina Facebook dei dipendenti. Quantomeno, le informazioni sulle minacce raccolte dai sistemi di sicurezza aziendali dovrebbero correlare Web ed e-mail, anche considerando che il 92% dello spam via e-mail contiene un URL.

3 - Reindirizzamento – L'esca della fase due molto spesso reindirizza verso un sito Web dove è annidato un exploit kit. Anche in questo caso, c'è molta differenza tra gli attacchi APT di massa e quelli mirati. I primi cercano di

adescare il maggior numero di persone, ma per questo non possono essere troppo sofisticati nel messaggio e nel tipo di trappola. Per quelli mirati, ci si può anche prendere la briga di attaccare un sito insospettabile per installarvi sopra il kit di malware.

Fa specie che la tecnica tuttora più utilizzata per il redirect è basata sull'SQL injection, inventata prima della nascita di Internet. Insieme alla iFrame injection conducono gli utenti ignari verso servizi Web e contenuti non richiesti. Il cosiddetto "malvertising" (malware advertising) invece dirotta gli utenti inconsapevoli all'interno di siti conosciuti. I re-indirizzamenti di nuova generazione, infine, comprendono i post sulle bacheche dei social network, finti plug-in, certificati falsi e java script abilmente occultati. Tali reindirizzamenti sono spesso dinamici, cambiano cioè in continuazione, per cui i sistemi di Web Filtering avanzati devono poter verificare i link in tempo reale.

4- Exploit – La fase centrale è fondamentale per l'attacco vero e proprio, cioè per penetrare all'interno delle difese avversarie. Gli exploit sono sempre più sofisticati: per esempio i Blackhole utilizzano sistemi di cifratura difficili da identificare con soluzioni antivirus. Decisamente più efficaci possono essere i gateway di ultima generazione, come i Next Generation Firewall, ma non tutti arrivano a comprendere il reale funzionamento del malware, che, talvolta, rimane "inattivo" a lungo dopo l'installazione sulla rete del bersaglio. Rispetto al passato quando i kit erano numericamente di meno e basati su relativamente poche varianti, era possibile anche filtrare il traffico sulla base di signature, ma ormai questi sistemi possono essere paragonati ai cecchini invece che alle truppe d'assalto. Gli exploit kit, adesso colpiscono con un malware di tipo dropper (che si deposita direttamente nel sistema informatico attaccato), solo quando rileva una porta aperta sicuramente vulnerabile. In caso contrario devia l'utente verso una pagina web normale e rimane nascosto, aspettando la prossima occasione.

5 - Installazione – Siamo a quello che viene considerato l'attacco vero e proprio: il nemico avanza pronto a sfondare le barriere esterne. Non a caso, dunque, è qui che si concentrano i cosiddetti sistemi di protezione perimetrale, analizzando ogni file che penetra nella rete per rilevare eventuale malware. Come accennato, però, non è facile come prima rilevare i codici maligni di nuova

generazione attraverso signature e pattern, perché questi utilizzano pacchetti dinamici.

6 – Call Back – Una volta compiuta l'installazione del primo malware, il sistema informativo è presto in balia del cybercriminale. Il malware contatta un server e attiva il download di strumenti e altro codice maligno per raccogliere e inviare informazioni sul sistema violato, al fine di proseguire al suo interno fino all'obiettivo finale. Evidentemente, per la protezione in questa fase occorre un sistema che analizzi il traffico in uscita, ma sono ancora poco diffusi. Ne occorrono di abbastanza sofisticati, infatti, perché attraverso strumenti semplici, come un DNS dinamico i cybercriminali evitano il rilevamento delle operazioni di chiamata a casa verso indirizzi statici. Tuttavia è possibile inibire l'uscita di dati verso sistemi che non siano noti e quindi inibire l'uso di DNS che rimandano a server di "command and control". Del resto chi vuole nascondere la propria ubicazione geografica è in genere sospetto.

Una soluzione efficace viene applicata dalle soluzioni di Data Loss Prevention integrate con sistemi in grado di effettuare un'analisi contestuale dei dati: chi è l'utente, dove sono destinati i dati e altre variabili sono informazioni utili per i prodotti che devono evitare l'invio di informazioni riservate a Web mail personali, account di social network o mandate all'interno di app per la connessione a cloud storage privati.

7 – Azione – La fase finale è quello in cui l'attacco va tipicamente a buon fine se non si è riusciti a intervenire prima. Certamente, anche qui ci sono ancora margini per bloccare il furto dei dati obiettivo dei cybercriminali, ma occorre disporre di sistemi in grado, per esempio, d'identificare una password che sta uscendo dalla rete aziendale oppure di rilevare traffico criptato verso l'esterno con chiavi di cifratura illecite o estranee al proprio sistema di crittografia. Ci sono poi tecniche, chiamate drip (gocciolare), che trasferiscono file verso l'esterno in piccole quantità in tempi dilatati, per rendere più difficile il rilevamento.

Il Phishing

Lo spam è molto utilizzato per il phishing, termine con la medesima pronuncia, ma storpiato nell'ortografia, dell'inglese "fishing", pescare.

Si tratta di un sistema inizialmente indirizzato a carpire dati personali e, tipicamente, numeri di carta di credito, grazie alla collaborazione, in buona fede, delle vittime della frode. Il sistema è, concettualmente, molto semplice e perlopiù condotto via e-mail; il bersaglio si vede recapitato un e-mail da parte di un'organizzazione o di una banca nota, in cui lo si informa che, a causa di inconvenienti di vario tipo, si sono verificati problemi relativi al suo conto oppure che un acquisto da lui effettuato mediante la carta di credito non è potuto andare a buon fine. L'utente viene, quindi, invitato a collegarsi a un sito in cui inserire nuovamente i suoi dati, cliccando su un link contenuto all'interno del messaggio di posta elettronica che, apparentemente, corrisponde a quello del mittente del messaggio. Il sito è, ovviamente, fasullo, ma replica in modo perfetto quello originario, in modo da carpire le informazioni che è lo stesso utente a inserire.

L'e-mail, apparentemente, ha tutte le caratteristiche di un messaggio "ufficiale" riportando logo, informazioni di copyright, slogan e messaggi di marketing identici a quelli utilizzati tipicamente dalle presunte aziende o banche mittenti. Spesso sono contenuti dati personali carpiti magari attraverso siti di social networking, dando l'impressione che effettivamente ci si trovi davanti a un messaggio reale. I principali target di questo tipo di attacchi sono le banche e i siti finanziari e, tra le organizzazioni prese di mira, vi è anche la casa d'aste on line e-bay, che ha prontamente avvisato i propri utenti che l'invio di messaggi di questo tipo non rientra nelle proprie modalità operative.

Il contenuto delle mail può far riferimento alla necessità di inserire nuovamente i propri dati per una verifica del proprio conto, al fine di prevenire possibili frodi o di verificare che presunte violazioni che hanno interessato l'organizzazione finanziaria non abbiano arrecato danni allo specifico utente. Il tono può essere minimale, invitando a eseguire operazioni che vengono descritte come di routine, oppure più allarmista, sottolineando l'importanza e l'urgenza di collegarsi al sito e reinserire i dati; è anche possibile che inviti l'utente a scaricare e installare "security update" presenti in allegato al messaggio e contenenti codice maligno. Sebbene, apparentemente, possa sembrare un approccio ingenuo, il successo che ottiene questa tecnica è sorprendente.

Il phishing è in forte aumento e risulta tra le tipologie di attacchi più sviluppati negli ultimi anni con tecniche che si affinano molto. Le tecniche di social

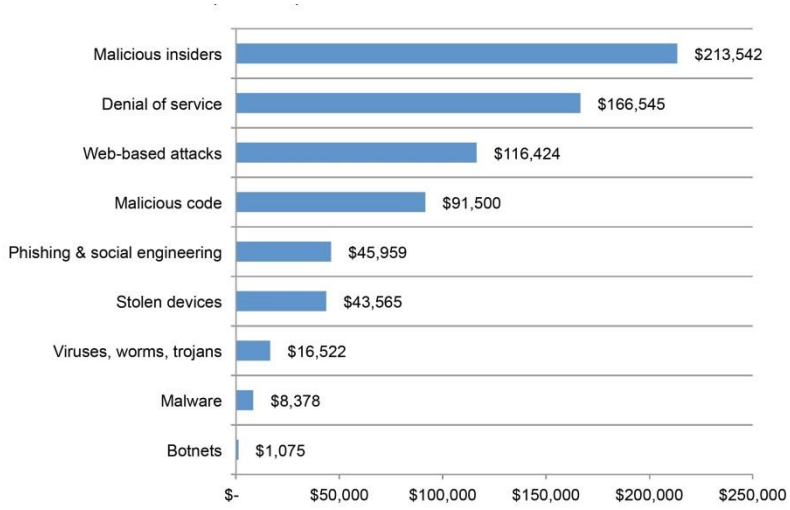
engineering, spesso adottate in abbinamento al phishing, hanno visto aumentare la loro efficacia con la diffusione del Web 2.0. Al successo di questo fenomeno si accompagna, secondo gli addetti ai lavori, un aumento delle problematiche di sicurezza, prima fra tutte il furto di identità: gli utenti si sentono fiduciosi e pubblicano in rete non solo i propri dati anagrafici, ma anche svariate informazioni sulla propria vita privata, tutti dati utili per truffe mirate.
Peraltro, oggi i tool necessari per attività di spamming e phishing sono pubblicamente disponibili su Internet e strumenti più sofisticati sono comunque in vendita online, mentre è possibile acquistare elenchi di indirizzi validi con milioni di nominativi per poche decine di euro. Il successo dello spamming è dovuto proprio ai grandi numeri: gli spammer vengono pagati pochi centesimi per ogni click registrato su un sito da loro indirizzato, ma pochi centesimi per decine di milioni di messaggi spediti fanno un sacco di soldi, pur considerando basse percentuali di messaggi andati a buon fine.
Esistono anche varianti del phishing, come il “pharming” (che fa riferimento alla manipolazione delle informazioni Domain Name Server per reindirizzare l’utente in modo inconsapevole su siti Web falsi), lo “spear phishing” (utilizzato per indicare attacchi indirizzati in modo molto mirato a specifici target), lo “smishing” (che fa riferimento ad attacchi portati sfruttando i servizi SMS disponibili sui telefoni cellulari) e il “vishing” o “voice phishing (che sfrutta la messaggistica vocale e, in particolare, il Voice over IP (VoIP), il cui vantaggio per gli attacker è che offre garanzie ai truffatori di non essere individuati poiché molti servizi telefonici via IP non prevedono un preciso punto di partenza della chiamata).

Lo spear phishing

La posta elettronica resta uno dei veicoli d'infezione preferiti o, quantomeno, uno degli strumenti utilizzati per le sofisticate tecniche di phishing o "spear phishing", quello, cioè, mirato. Lo spam tradizionale è infatti in calo, stando ad alcuni rilevamenti, ma sta crescendo quello collegato ai social network. Al contrario, sempre più efficaci si dimostrano gli attacchi mirati che partono con una mail di phishing appunto.
Quest'ultima tecnica si è evoluta, per cui bloccare tali email è molto più difficile che in passato, in quanto non si tratta di messaggi rivolti alla massa, quindi

standardizzati e facilmente riconoscibili. Lo spear phishing si basa su dati appositamente raccolti per colpire uno specifico target. Si tratta di email personalizzate, che non sono state osservate da altri sistemi precedentemente e che non sembrano "estranee" all'azienda.
Gli attacchi di phishing, in passato, erano tutti basati sulla stessa procedure: l'email inviata a centinaia di migliaia di indirizzi contava sulla legge dei grandi numeri. Statisticamente una piccola percentuale di destinatari reagiva alla mail finendo nella trappola dei cybercriminali e infettando il pc.
L'efficacia del sistema si basava sulla statistica e sull'ingenuità degli utilizzatori. Anche se di poco, però, la cultura di questi ultimi sulla sicurezza è andata aumentando negli anni e, parallelamente, è calata l'efficacia del phishing tradizionale. Ovviamente la maggior parte del merito va al miglioramento dei sistemi antispam e antiphishing, che adesso includono tecnologie come: la "reputation" del mittente, che classifica gli indirizzi di spedizione per bloccare quelli che notoriamente riversano spam; l'analisi lessicale sul contenuto delle email per individuare frasi e combinazioni di parole o schemi usati di solito per lo spam; l'integrazione con gli antivirus, che identificano i codici maligni noti abbinati alla posta elettronica.
L'efficacia della protezione, porta i cybercriminali professionisti a cercare nuove strade. Di fatto, la ricerca e sviluppo sul "lato oscuro" è avanti, preparando le tecniche innovative mentre ancora quelle tradizionali portano i loro frutti.
Il modello degli attacchi di phishing è quindi evoluto di conseguenza negli ultimi anni e, soprattutto, si è fatto ancora più mirato: indirizzandosi a piccole comunità, come possono essere i dipendenti o, più in dettaglio, i quadri di una specifica impresa. Si è anche semplificato, perché non contiene direttamente il malware, ma un link a un sito Web, non di rado legittimo, dove però è stato annidato il kit maligno. Inoltre, i server utilizzati non risentono di una cattiva reputazione, perché inviano pochi messaggi che non sono riconosciuti come spam.
Chiaramente questo presuppone qualche sforzo in più, per esempio per compromettere un sito legittimo senza che i suoi gestori se ne accorgano, anche solo per il tempo necessario a portare a termine l'attacco.
Il successo della tecnica resta ancorato alla ingenuità/diffidenza del dipendente, ma l'accuratezza di questi attacchi "ripaga" il malintenzionato. C'è da dire che

l'errore o il dolo del dipendente interno rappresenta sempre il rischio maggiore, come dimostrano costantemente tutte le ricerche del settore.
Rispetto allo spam, il phishing ha tassi di redemption più elevati, se poi è mirato l'efficacia è alta. Tali sforzi andranno ripagati, quindi il bottino sarà ricco: per esempio un numero elevato di dati, come i numeri di carte di credito o proprietà intellettuali (per esempio brevetti).
Anche l'analisi lessicale fallisce e lascia passare il phishing sofisticato, perché i contenuti, essendo mirati, sono compatibili con il contesto e non riconosciuti come spam. Gli antivirus non trovano malware da analizzare e bloccare.



Costo delle tipologie di attacco: il rischio interno è il più costoso (fonte Ponemon)

Occorrono soluzioni più sofisticate, che eventualmente siano in grado di seguire il link verso il codice maligno, riconoscerlo come tale e bloccare il download di dati compromessi. Meglio se possono operare in tempo reale.

Il social engineering

Può sembrare strano, ma uno degli strumenti più efficaci nella compromissione della sicurezza informatica è condotto senza l'utilizzo di strumenti informatici. Si tratta del cosiddetto "social engineering", una tipologia di attacco indirizzata a carpire informazioni sensibili attraverso l'uso del contatto umano, utilizzando

come complici inconsapevoli gli stessi obiettivi dell'attacco. Di fronte a sistemi evoluti progettati per analizzare traffico sulle porte, signature o anomalie di protocollo, il social engineering sfrutta una delle principali vulnerabilità nella sicurezza informatica di un'azienda: l'elemento umano.

Le motivazioni che inducono i cybercriminali all'utilizzo di tecniche di social engineering sono molteplici. Innanzitutto si tratta di un metodo più semplice rispetto alla violazione di un sistema e che non richiede costi elevati o tool sofisticati. Permette, inoltre, di aggirare sistemi di intrusion detection e non è influenzato dalla piattaforma operativa utilizzata all'interno dell'azienda target.

I bersagli tipici sono rappresentati dal personale di help desk, dagli addetti al customer service, da assistenti amministrativi, personale vendite, sistemisti o tecnici. Questo perché, da un punto di vista generale, i soggetti sono tanto più disponibili a fornire informazioni, quanto meno sono direttamente coinvolti o interessati dalla richiesta. Spesso, alle vittime di tali attacchi manca la consapevolezza del rischio o anche solo l'interesse a discutere o esaminare le motivazioni alla base di richieste che non sono direttamente pertinenti ai loro compiti specifici.

Un attacco giunto a buon fine può fornire numeri di dial-in o procedure di accesso remoto, permettere di creare un account o modificare privilegi o diritti di accesso fino a determinare l'esecuzione di programmi potenzialmente dannosi quali trojan horse. Questo tipo di attacco può anche essere indirizzato a carpire informazioni quali, per esempio, liste di clienti, dati finanziari, offerte associate a contratti o informazioni riservate sui processi produttivi. I metodi utilizzati per carpire informazioni sono vari e dipendono solo dalla fantasia dell'attaccante.

Una tecnica è quella di raccogliere preventivamente una serie di informazioni che possano fornire un pretesto credibile per la costruzione di un attacco e permettano di guadagnare la fiducia di chi subisce l'attacco. Tipicamente, infatti, il social engineering è una tecnica preparata e costruita in step successivi e basata su una precisa strategia, che preveda anche contro-argomenti in caso di possibili obiezioni e vie di uscita ragionevoli per non bruciarsi il "lavoro" svolto.

Va poi ricordato che, a differenza di un firewall, l'essere umano tendenzialmente è portato a fidarsi degli altri o ad avere illusione che certe cose a lui non possano capitare. Spesso accade anche che venga sottostimato il

valore dell'informazione o si abbia poca consapevolezza dalle conseguenze di azioni apparentemente innocue.
Altre tecniche sono indirizzate a costruire un rapporto di fiducia attraverso una serie di contatti ripetuti completamente innocui. Un metodo molto efficace è quello di raccogliere una serie di piccole informazioni che, singolarmente, non hanno utilizzo pratico ma che, se considerate nel loro complesso, possono rappresentare una fonte di informazione di valore elevato. Frammenti di informazione utili a tal fine possono essere facilmente recuperabili da un cybercriminale tramite i siti Web, l'organigramma aziendale, attraverso newsletter o anche documenti di marketing. Altre informazioni di carattere personale possono essere ricavate da siti Web che contengono nomi di parenti o di interessi specifici, a cui spesso un utente si ispira per elaborare le proprie password.
Inoltre, poiché l'uomo è naturalmente curioso, altri "trucchi" sono di lasciare supporti quali CD ROM o floppy contenenti codici maligni presso specifiche postazioni sperando che vengano aperti ed esaminati oppure inviare e-mail che invitano a visitare siti Web potenzialmente dannosi.
Un esempio di attacco di social engineering può partire dall'individuazione, da un documento di marketing, del nominativo di una persona che ricopre una specifica carica aziendale. Telefonando al centralino e chiedendo di essere messo in comunicazione con quella persona (citando nome e cognome) è facile che si venga passati al suo numero interno. Se la telefonata avviene in un giorno in cui questa persona non è sicuramente in ufficio, per esempio perché dal sito Web viene annunciata la sua partecipazione a un evento o a una conferenza, non è infrequente poter recuperare il numero dell'interno dal sistema di risposta automatica che invita a lasciare un messaggio. A questo punto si dispone già di un numero di informazioni utili a lanciare un attacco. Con un po' di astuzia è possibile, per esempio, ricavare informazioni riservate da un collega, ottenendo la sua fiducia adducendo motivazioni di urgenza, la stretta conoscenza del contatto "sfortunatamente" mancato e supportando le proprie affermazioni con i dati in proprio possesso. Spesso basta conoscere anche solo poche informazioni personali di un individuo per lasciare presupporre a qualcun altro una sua conoscenza approfondita.

Un'ulteriore fonte di informazioni è rappresentata dai rifiuti. Documenti, bozze, annotazioni o anche nomi di piani e di progetti, trovano spazio su documenti cartacei che vengono gettati nell'immondizia. Ancora più rischioso è gettare supporti di memorizzazione danneggiati quali hard disk o sistemi removibili da cui è sempre possibile ricavare informazioni parziali. Inoltre, l'appropriazione dei rifiuti altrui non è, di per se stessa, una pratica illegale.
Gli aspetti psicologici sono un elemento essenziale nel social engineering. In generale un attaccante che utilizza queste tecniche può essere individuato dal fatto che fa richieste fuori dall'ordinario o adotta comportamenti anomali, quali manifestare estrema urgenza in modo immotivato, utilizzare toni autoritari o intimidatori, offrire aiuto per risolvere un problema sconosciuto o citare il management come ente autorizzatore della richiesta. Particolari condizioni lavorative possono aumentare il rischio associato a tali attacchi. Per esempio, una forte pressione a svolgere i lavori in tempi rapidi, la presenza di uffici distribuiti in varie località o l'utilizzo di personale esterno all'azienda, sono tutti elementi che possono contribuire a facilitare le condizioni affinché un attacco di social engineering abbia successo. L'unico sistema per proteggersi efficacemente è quello di aumentare la cultura della sicurezza in azienda, in modo che questa non sia percepita come una perdita di tempo o un ostacolo all'attività lavorativa, predisponendo procedure apposite per la gestione delle informazioni e la loro classificazione e mettendo a punto policy per la "pulizia" della postazione di lavoro. La contromisura più efficace resta quella di attivare sessioni di addestramento indirizzate alla consapevolezza dell'importanza della sicurezza e dei possibili rischi associati a comportamenti superficiali.

Il furto di identità

La cronaca, a onor del vero, dà maggior risalto a fenomeni di massa, come i vari worm o pseudo tali che di tanto in tanto riescono a perforare le difese diffondendosi in tutto il mondo, ma le attività realmente criminali si concentrano su altri fronti: primo fra tutti il furto di identità.
Rubare l'identità di qualcun altro significa riuscire a raccogliere sufficienti informazioni al fine di spacciarsi per lo stesso, ad esempio, per commettere frodi, aprire conti correnti, navigare su siti pornografici, carpire dati aziendali

riservati o quant'altro. Alle volte lo scopo è indiretto, come nel caso dei database costituiti illegalmente tramite strumenti di spamming.
Un'identità può essere utilizzata per sferrare attacchi contro terzi o frodarli, con il rischio di dover anche affrontare spese legali per dimostrare la propria innocenza. Oltre al phishing, un metodo molto in voga per reperire/rubare informazioni è collegato all'utilizzo di programmi cosiddetti spyware, il cui scopo è quello di registrare il comportamento di navigazione, esplorare il disco rigido, esportare dati raccolti, intercettare posta elettronica o file, catturare dati immessi in sistemi Web (per esempio con i keylogger, che memorizzano i tasti premuti) e altro ancora. Con uno o più strumenti del genere è possibile "assemblare" sufficienti dati per mettere insieme l'identità di un individuo.

L'Internet of Things e le nuove botnet

Dopo il Web 2.0, si è cominciato a parlare di Web 3.0, una definizione che è stata presto abbandonata a vantaggio di due altre diciture: Machine to Machine (M2M) o Internet of Things (IoT). Di fatto, il Web è sempre stato concepito come l'interazione tra un individuo e una macchina (server), poi si è passati al 2.0, che prevede l'interazione tra gli individui, comunque mediata da una macchina. Il terzo passo è l'interazione diretta tra macchine.
Prima di lasciarsi andare a scenari apocalittici stile Matrix, si rifletta sul fatto che, al contrario dell'essere umano, le macchine non posseggono l'istinto della sopravvivenza né quello della perpetuazione della specie. Istinti poco programmabili.
Di fatto, sarà presto maggioritario il numero di dispositivi posti in rete per svolgere compiti diversi da quelli di mettere in comunicazione individui o fornire informazioni a questi stessi. Si tratta di, per esempio, sistemi di controllo di impianti industriali collegati a sensori che rilevano determinati parametri. Quando questi ultimi superano una soglia potrebbe partire un allarme e il sistema di controllo genera un'azione corrispondente. La possibilità di utilizzare la rete IP e Internet in particolare per attuare una soluzione del genere è già stata presa in considerazione. Ancora una volta, sono le problematiche di sicurezza che faranno la differenza. Quali saranno le sfide del futuro per le aziende che si occupano di sicurezza, una cosa è certa: non possono continuare a giocare a nascondino con i "ragazzi cattivi". Una rincorsa senza sosta da una

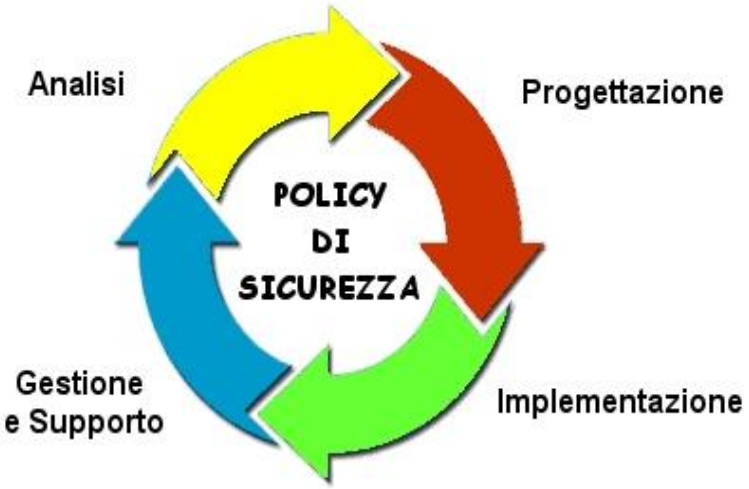
minaccia a un nuovo rimedio non ha senso. È necessario modificare le regole del gioco: cambiare approccio e anticipare le mosse dell'avversario, scendendo sul suo stesso terreno e partendo dagli obiettivi che si pone.
Le minacce rivolte all'IoT che, oggi, sono ipotizzabili, riguardano in primo luogo la disponibilità del servizio: un DDoS mette in seria difficoltà la trasmissione delle informazioni cui le macchine in rete sono preposte.
Ovviamente, gli attacchi a infrastrutture critiche rivolte a sistemi SCADA rappresentano un fronte di "guerra" e scenari da vera e propria Cyber War sono certamente realistici. In questi contesti è ipotizzabile che enti governativi possano stanziare i fondi necessari per sviluppare kit di attacco mirati, al fine di colpire un singolo obiettivo.
Già il costo per un sabotaggio è poco probabile sia sostenibile per colpire un concorrente, ma se si tratta di un "nemico" lo scenario cambia.
Il cybercrime, invece, si sta attrezzando per abbandonare le botnet così come oggi le conosciamo, cioè composte da pc e server, e sta sfruttando la maggiore superficie di attacco, grazie al fatto che un numero consistente di dispositivi M2M in Rete utilizzano sistemi noti come Linux.
Botnet complesse, composte da dispositivi di differente natura, sono già una realtà: è stato, infatti, registrato il primo caso di frigorifero utilizzato in una sorta di botnet per mandare spam. Il grosso rischio, in questo contesto, è che in molti di questi dispositivi vengano utilizzati vecchi pezzi di codice o, comunque, software open source che difficilmente saranno aggiornati: chi si occuperà dell'upgrade del firmware del forno a microndе o della lavatrice?
La probabilità che buona parte delle macchine in rete resti indifesa rende l'IoT una miniera d'oro per chi cerca una macchina da usare gratuitamente.
È, infine, ipotizzabile un futuro in cui avverrà il passaggio dalla minaccia informatica a quella fisica: già oggi alcuni modelli di automobile dispongono di componenti elettronici e computer di bordo raggiungibili da remoto via wireless, che potrebbero essere manomessi provocando un incidente.
A quel punto la sensibilizzazione verso l'importanza della cyber security sarà compiuta.

La Security Intelligence

Quando fu introdotto il concetto di UTM (Universal o Unified Threath Management), diversi anni or sono, cominciò a essere chiaro che non si poteva affidare la difesa da ogni singola minaccia a un dispositivo specifico. All'inizio si punto sull'efficienza dell'analisi del traffico, concentrandola in un unico passaggio, ma ben presto si comprese che questo non era sufficiente e che servisse poter valutare i dati raccolti da ciascuna tipologia d'analisi correlandoli tra loro. Questo perché le tecniche di attacco avevano cominciato a frammentare le attività maligne e diventava difficile intercettare una "firma" per bloccare l'intrusione o il traffico maligno.
Con le minacce che diventavano sempre più sofisticate e rapide, si è compreso che le tecniche per mantenere aggiornati i sistemi e per correlare le informazioni non solo dovevano accelerare fino al real time, ma dovevano anche contare su una maggiore intelligenza.
Si sono così sviluppati approcci nuovi che sfruttano il cloud, mettendo a fattore comune le informazioni provenienti da più fonti per creare motori di intelligence in grado di contare su sistemi a elevate prestazioni per realizzare le correlazioni o per testare il funzionamento di un codice in una sandbox (letteralmente scatola di sabbia è il quadrato in cui possono giocare al sicuro i bambini ai giardini pubblici) e poter così valutare la sua pericolosità o la sua attendibilità. Dopodiché l'informazione può essere condivisa con tutti i dispositivi collegati al sistema di intelligence.
Diversi vendo hanno sviluppato il proprio, ma ve ne sono diversi in "consorzio", perché il punto di forza di questi sistemi sta proprio nella condivisione delle informazioni, da cui tutti traggono beneficio. La differenziazione potranno farlo le capacità di tradurre l'informazione in un'azione protettiva più o meno rapida e/o efficace.
Inoltre, molti di questi sistemi possono integrarsi con il sistema interno di gestione degli eventi di sicurezza, che può utilizzare funzioni in più, per esempio una capacità d'analisi avanzata, in grado di esaminare grandi quanti di dati: i cosiddetti Big Data della sicurezza.

I SIEM "intelligenti"

La crescente complessità dei malware e la sempre maggiore sofisticatezza degli attacchi hanno reso rapidamente obsoleti quei sistemi di protezione che non prevedevano azioni automatiche.
In particolare, però, a dimostrare la propria inadeguatezza sono i SIEM (Security Information Event Manager) di prima generazione.
Inizialmente, la gestione della sicurezza era statica: si installava un firewall o poco più e, una volta definite le regole per governare il traffico, gli si lasciava seguire il proprio lavoro.
Man mano si sono aggiunti altri dispositivi e/o software per applicare alcuni controlli aggiuntivi, resi necessari dall'evoluzione delle minacce.
La definizione delle policy è un processo che richiede una certa dinamicità per essere efficace, perché le condizioni del traffico cambiano nel tempo. Anche la soluzione di sicurezza tecnologicamente più avanzata è, infatti, destinata a fallire se non è coadiuvata da regole implementate sulla base della specifica realtà e, quindi, tali da soddisfare gli obiettivi aziendali e i requisiti di applicabilità e idoneità.



Il ciclo di definizione e implementazione delle policy

Stabilire una politica di sicurezza significa prevedere tutte le possibili violazioni alla sicurezza e il modo per proteggersi da esse, formalizzandole anche in un documento. Documento che è importante, non solo per la compliance alle normative sulla sicurezza dei dati, ma perché riguarda la governance stessa dell'impresa. Le policy di sicurezza, infatti, riguardano questioni quali l'impostazione del livello di sicurezza relativo ai singoli apparati e alle soluzioni informatiche, la gestione del rischio di perdite finanziarie associato a intrusioni e le modalità comportamentali degli impiegati.

Il problema è che questo approccio ha dimostrato rapidamente la sua inefficacia sia per la rapidità con cui evolvono le minacce, ma soprattutto per la incredibile pressione che si deve sopportare: i log dei sistemi per la gestione di informazioni ed eventi di sicurezza arrivano a registrarne centinaia di migliaia al giorno. Chiaramente non è possibile analizzarli manualmente, ma neanche con i motori di correlazione di prima generazione, che riescono a incrociare alcuni dati, ma non hanno, in realtà, accesso a tutte le informazioni necessarie a rilevare attacchi ATP.

Questo scenario pone due problemi che sono stati affrontati aumentando "l'intelligenza" dei sistemi SIEM e, sotto un altro punto di vista, anche quella dei dispositivi per la protezione. In particolare, questi ultimi, come i firewall e gli IPS di nuova generazione sono stati raffinati per analizzare con maggiore dettaglio il traffico e i pacchetti che lo compongono. A tali capacità si aggiunge soprattutto una più semplice definizione delle policy, che non devono più essere impostate con parametri tecnici comprensibili solo agli esperti, ma sono espresse con formule "business", quindi più facilmente comprensibili anche all'interno di quel documento di programmazione, che viene così a far parte intrinseca del processo di gestione del rischio e governance aziendale.

Questo livello di semplificazione, dall'altro lato, comporta anche l'automazione delle regole poi effettivamente applicate e la possibilità di gestirle centralmente in maniera integrata. In pratica, se il SIEM è in grado di rilevare un innalzamento del livello di rischio generale, potrà automaticamente innalzare le soglie d'attenzione dei dispostivi. In parte, tale capacità può sfruttare le informazioni provenienti dai dispositivi sulla rete, combinando tecniche di Information Security utilizzate in diversi ambiti: per esempio quelle per la Web security e l'application security, con quelle di sicurezza fisica. Incrociando, per esempio, i

dati di autenticazione per l'accesso alle applicazioni con quelli per la registrazione delle presenze e/o con i controlli dei varchi d'ingresso nelle aree degli edifici e uffici, si potrà evidenziare l'anomalia di un utente che non risulta entrato in ufficio, ma il cui account sta accedendo dal suo desktop al sistema ERP o sta spedendo informazioni via mail.

Ma, per compiere un salto di qualità è necessario che il SIEM possa tener conto del livello di rischio su tutta la rete Internet e non solo su quanto sta accadendo al suo interno. Per questo, non bastano i semplici motori di correlazione interni. Questi ultimi, infatti, sono in grado di confrontare l'avvenire di eventi misurati sulla rete aziendale e quindi registrati nel log del SIEM. Con gli attacchi ATP, purtroppo, questo è necessario e può spezzare la sequenza di fasi di un attacco, ma non è detto che sia sufficiente, a causa della persistenza degli ATP.

Un attacco che comincia con una mail di spear phishing ha buone probabilità di arrivare indisturbato alla quarta fase e da qui alla quinta, senza che i sistemi di protezione se ne possano accorgere. A questo punto potrebbe essere troppo tardi. Peraltro, con un sistema SIEM in grado di ricevere e selezionare informazioni anche da fonti esterne alla rete aziendale, cioè di appoggiarsi a un sistema di "intelligence", l'attacco potrebbe essere bloccato alla fase 2 se non alla 1.

Per chiarire in cosa consiste un sistema di intelligence ripercorriamo appunto la sequenza di un attacco APT, dopo la ricognizione, partono le strategie di adescamento, nella maggior parte dei casi basate sull'invio di una mail di spear phishing. Un sistema antispam/antiphishing potrebbe bloccarla, ma è facile che gli sfugga, perché non è composta con lo stile classico dello spam o del phishing di massa. Soprattutto non fa parte di massicce campagne di spamming che vengono rilevate per gli elevati volumi. In genere contengono un link, ma un'analisi superficiale dei contenuti cui rimanda non è sufficiente a stabilirne la malevolenza. Peraltro, un'analisi accurata, per esempio con l'emulazione del comportamento attraverso tecniche di sandboxing, richiede del tempo e viene spesso effettuata offline. A meno che l'attacco non sia condotto a una singola impresa o, addirittura a uno specifico reparto di una singola impresa, è possibile che tali mail di spear phishing siano state già "sotto esame" su qualche sistema, magari dall'altra parte del mondo. Se quest'ultimo dovesse rivelare un elemento sospetto potrà "firmare" la mail (cioè trovare un elemento che la

contraddistingua e ne permetta l'identificazione) e di trasmettere immediatamente questa informazione in tutto il mondo.
Quest'ultima fase è quella che viene chiamata di threat intelligence, anche se le definizioni non sempre coincidono. In buona sostanza un sistema di threat intelligence è in grado di correlare informazioni di sicurezza registrate sulla propria rete e di confrontarle con quelle raccolte da un network, generalmente appoggiato su cloud. Quindi svolge una funzione di "intelligence", indagando sulla rete che gestisce. A sua volta, il sistema diffonderà le informazioni al network cui appartiene, secondo una logica di collaborazione e condivisione.
Queste soluzioni si stanno rivelando sempre più efficaci e utili, spingendo le imprese a sviluppare metodi di raccolta dati per l'intelligence. Partendo dal valutare quali risposte possono arrivare da soluzioni analitiche interne, vanno selezionate le fonti di informazioni che sono utili. Fino ad arrivare a un set ritenuto soddisfacente, eventualmente negoziando acquisizioni o scambi di dati con fornitori esterni. Quindi si potranno arricchire le analisi attraverso strumenti di threat intelligence esterni. Ottimizzando tali processi, inoltre, si può minimizzare l'aumento della capacità storage necessaria per supportare l'aumento dei log, che, come accennato, sta diventando critico.

Progettazione ed enforcement delle policy

Le istruzioni specificate dalle policy possono essere di tipo generale, cioè applicate indifferenziatamente a tutta l'impresa, oppure suddivise per tipologia di risorse aziendali o per aree di responsabilità. In ogni caso la progettazione di una policy deve recepire le indicazioni provenienti dall'analisi del rischio in merito alle risorse da considerare importanti e deve definire opportunamente gli step da seguire per la loro protezione. La messa a punto di una policy aziendale deve essere fatta in modo da favorire il suo effettivo utilizzo, evitando di trasformarsi in un documento formale per clienti o revisori, ma di nessuna utilità pratica. Spesso questo aspetto è legato alla presenza, in molte realtà aziendali, di criteri poco significativi, che restano troppo generici e non danno indicazioni precise sulle azioni da intraprendere.
L'intelligenza delle più recenti soluzioni per la sicurezza permette di superare quest'ultimo inconveniente, grazie alla definizione di regole tecniche basate su definizioni generali, ma occorre comunque che a livello strategico si adottino criteri che soddisfano requisiti di flessibilità, chiarezza negli obiettivi, applicabilità. Inoltre, i

criteri per la sicurezza dovrebbero essere introdotti in modo da evidenziare il sostegno incondizionato da parte della direzione dell'azienda e coinvolgere, per quanto possibile, i diretti interessati. Proprio per questo è stata semplificata la loro definizione.

Se male organizzato, paradossalmente, un criterio di sicurezza può determinare una riduzione del livello di protezione. Spesso policy troppo restrittive vengono ignorate, perché ostacolano l'attività lavorativa. Per esempio, l'utilizzo di password troppo lunghe o complesse e, pertanto, difficili da ricordare, potrebbe indurre gli impiegati a scriverle e lasciarle più facilmente in balia di possibili malintenzionati.

Per essere efficace un criterio di sicurezza deve essere diffuso e applicato: ci si deve assicurare che tutti gli impiegati conoscano le relative policy di sicurezza e che ne possano disporre prontamente e in qualunque momento e va garantita la pronta comunicazione di ogni loro eventuale cambiamento.

Per la diffusione efficace di ogni criterio è opportuno mettere a punto un insieme di regole scritte, che definiscono le responsabilità relativamente a chi progetta le policy, chi le garantisce, le implementa e la fa rispettare e le relative conseguenze a seguito di eventuali violazioni.

Infine, sarebbe buona pratica coinvolgere gli utenti influenzati dalle policy di sicurezza nel loro processo di sviluppo o almeno di revisione. Si tratta di un'opera di educazione e sensibilizzazione che, da sola, contribuisce a ridurre drasticamente il rischio: per esempio, rendendo difficile realizzare una mail di spear phishing.

Le vulnerabilità indotte dal comportamento dei dipendenti rappresentano il principale punto debole per tutte le imprese e coinvolgerli permette di ridurre il rischio da loro rappresentato. Per altro, è utopistico sperare di risolvere i problemi di sicurezza in questo modo, perché ci sarà sempre il nuovo assunto o l'ultimo dei "fannulloni" che non seguirà un comportamento corretto. Senza contare i casi di violazioni dolose.

Le tecnologie possono aiutare anche in questi casi, ma i risultati migliori si ottengono grazie agli automatismi che sono stati introdotti in molte delle soluzioni di ultima generazione, imponendo, di fatto l'enforcement delle policy di sicurezza, per esempio impedendo che un determinato file classificato come confidenziale, possa essere spedito via mail, magari anche solo per sbaglio,

senza che sia crittografato con un sistema che ne impedisce la decodifica se non attraverso un sistema aziendale.
Capacità di tal genere, peraltro, devono accompagnarsi a un SIEM di nuova generazione, che le potrà mettere a frutto configurando il sistema di sicurezza aziendale, in modo che sia pronto a fronteggiare le minacce "in arrivo", cioè quelle rilevate dai sistemi di threat intelligence e prontamente segnalate al SIEM. Anche tale configurazione dovrà avvenire il più automaticamente possibile (almeno in base alla flessibilità posseduta dal sistema di protezione stesso), perché il tempo è tutto nell'era della globalizzazione e nel mondo interconnesso del terzo millennio.

3 - LA MOBILE SECURITY

La diffusione dei dispositivi mobili rende questi ultimi l'obiettivo primario dei cybercriminali, aumentando il rischio per le imprese a causa di piani aziendali di BYOD non sempre supportati da un adeguato sistema di sicurezza. Soluzioni di Mobile Device Management di ultima generazione possono supportare strategie di Enterprise Mobility in grado di rinnovare i processi di business e aumentare produttività e competitività.

La centralità della sicurezza nella mobility aziendale

La mobilità, nell'odierno contesto lavorativo, non rappresenta una scelta ma un'esigenza dettata da mutate condizioni di gestione dei rapporti di un'azienda con i suoi partner, clienti e fornitori in un'ottica di massima apertura e in uno scenario di competizione estesa sempre più su scala globale. Un'esigenza che porta con sé molti benefici perché permette di incrementare la produttività personale, ottimizzare la gestione dei tempi e favorire una collaborazione più proficua e sinergica all'interno dell'azienda stessa. Ma che richiede, innanzitutto, la disponibilità di dispositivi personali abilitanti per un lavoro efficace in mobilità.

Con la diffusione dei telefoni cellulari è cominciato il cosiddetto lavoro in mobilità, grazie a una più facile reperibilità dei lavorato costretti a "uscire" dall'impresa. I laptop hanno contemporaneamente consentito di dotare tali lavoratori di una capacità computazionale che li rendeva operativamente più produttivi.

È qui inutile ripercorrere tutta la storia dei pc portatili che continuano a rappresentare uno strumento fondamentale per l'utilizzatore aziendale, al contrario di quanto sta accadendo sul fronte dell'utilizzatore consumer. Più precisamente, una ricerca condotta da Redshift Research ha rivelato che, secondo i CIO intervistati, i pc desktop sono destinati a rimanere il componente hardware dominante nelle aziende e si prevede che nel 2020 verranno ancora utilizzati quasi dalla metà dei dipendenti (46%). Analogamente, per i notebook è previsto un utilizzo del 29% nel 2020, pari a quello attuale.

Globalmente, comunque, è avvenuto il sorpasso da parte di smartphone e tablet nei confronti dei notebook, il che presenta particolari criticità dal punto di vista della sicurezza aziendale.

Il primo aspetto da considerare è l'abitudine all'utilizzo: come ormai da qualche anno ha insegnato la consumerization o quella che oggi è preferibile chiamare digital transformation, gli utilizzatori sono avvezzi a utilizzare strumenti semplici e si aspettano la stessa "user experience" in azienda. Come raccontato da un CISO (Chief Information Security Officer) di una nota casa del lusso, se prima

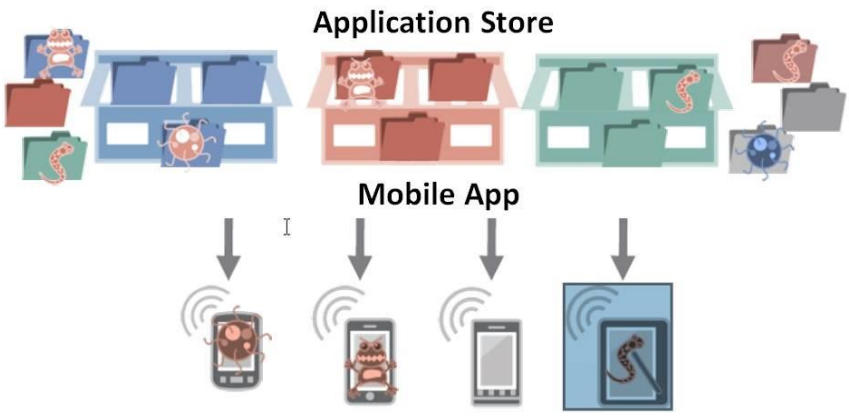
arrivavano all'IT richieste del tipo "ho bisogno di fare questa cosa", oggi il business manager chiede: "mi serve una app per fare questa cosa".
Il cambiamento è epocale e non c'è possibilità che si torni indietro. Questo implica ripensare i processi in chiave mobile e immaginare i futuri servizi sempre in quest'ottica. Alla base di questa rivisitazione deve esserci un'attenzione costante per la sicurezza, da porre al centro. Lo stesso Cisco di prima concludeva il racconto affermando che non vede altro modo di supportare queste esigenze integrando la sicurezza direttamente nell'applicazione mobile.
L'attenzione verso la sicurezza delle applicazioni non riguarda solo il mondo mobile, ma è centrale per tutta l'Information Security, poiché le applicazioni sono diventate un tramite per penetrare sulla rete aziendale sfruttandone le vulnerabilità e perché, sempre più, sono un obiettivo per arrivare ai dati. Ovviamente, essendo questi ultimi l'obiettivo finale, è anche direttamente sui dati che va impostato il sistema di sicurezza.
Come accennato, dispositivi come gli smartphone e i tablet ci hanno abituato a trovare online tutti i contatti e gli strumenti che servono per organizzare la nostra vita sociale e professionale, contribuendo in maniera sostanziosa al processo di "business transformation", che ridefinisce completamente i processi aziendali, aumentando la produttività, cambiando le relazioni di lavoro e sviluppando attività completamente nuove.
I nuovi modelli di lavoro in mobilità rappresentano la fase finale di quel processo di allargamento del perimetro aziendale cominciato con l'avvento di Internet di cui la mobilità ha rimosso gli ultimi limiti in termini di spazio e tempo, non solo per l'azienda ma anche per i suoi clienti e fornitori.
Le tematiche di sicurezza legate alla mobilità sono riconducibili a quelli che oggi le aziende si trovano a gestire nel loro complesso. Il primo problema è che la quasi totalità dei dispositivi mobili sono progettati e costruiti per il mondo consumer. Le prime generazioni di smartphone e tablet non consentivano di installare un antivirus, per esempio. Oggi che i device mobili intelligenti, cioè dotati di capacità computazionale, sono più diffusi di quelli "fissi", l'attenzione dei cybercriminali si è spostata e le minacce direttamente rivolte a tali dispositivi è aumentata. Questo, se aumenta il rischio generale, dall'altro lato ha portato le aziende produttrici a progettare con più attenzione i dispositivi e sta favorendo lo sviluppo di soluzioni specifiche per la sicurezza dei device mobili.

Ciò premesso, va sottolineato che le tecniche con cui nei dispositivi mobili si insidiano malware ed eventi di exploiting presentano la medesima complessità di quelli che attaccano i comuni pc e ne condividono i medesimi deleteri effetti. In alcuni casi possono causare un immediato danno economico, per esempio connettendo il dispositivo a servizi a pagamento, effettuando telefonate o spedendo SMS verso numeri Premium che applicano tariffazioni a consumo, o danni indiretti, magari esportando fraudolentemente dati.

Le criticità del BYOD

Un terzo fondamentale aspetto riguarda le modalità di utilizzo dei dispositivi mobili. È ormai entrata linguaggio comune la sigla BYOD (Bring You Own Device), che rappresenta una conseguenza del fenomeno più ampio della digital trasformation o consumerizzazione, portando con sé i rischi legati a un uso promiscuo, personale e aziendale, di dispositivi informatici.
Una soluzione parziale al problema è stata fornita dai principali produttori di software con soluzioni o appliance per la protezione degli endpoint, che si preoccupano di verificare che un dispositivo mobile che si vuole connettere alla rete aziendale soddisfi i requisiti di sicurezza e conformità necessari: per esempio che abbia installato l'ultima patch del sistema operativo o che non abbia disattivato funzioni di protezione.
Queste soluzioni forniscono una protezione efficace per evitare di portare all'interno della rete aziendale malware contratti all'esterno, ma non c'è tecnologia che tenga per proteggersi dalla superficialità e dalla noncuranza manifestata troppo spesso dagli utenti.
La possibilità di lasciare incustodito il proprio dispositivo mobile o di connettersi a una rete domestica che non dispone dei sistemi di protezione di quella aziendale, lascia aperta la possibilità di smarrire o di diffondere informazioni aziendali importanti e riservate, incluse password di accesso alla rete aziendale, dati sensibili o business critical.
Tuttora ogni persona dispone di più di un device personale, anche se è ipotizzabile un certo consolidamento nel tempo. Già oggi sono molti i sistemi "convertibili" che, per esempio, possono essere utilizzati come un pc portatile o come un tablet. D'altro canto, si stanno anche diffondendo i phablet, cioè smartphone dotati di un display maggiore di 5 pollici che consentono di navigare

su Internet con maggiore facilità che con gli smartphone e di telefonare anche senza un auricolare e certamente più agevolmente che con un tablet.
Quale che sia il dispositivo scelto, la tendenza è comunque di usarne uno solo sia per le attività personali sia per quelle attinenti alla sfera lavorativa. Da qui nasce il problema generato dall'ospitare sul quest'unico dispositivo mobile dati fondamentali per l'azienda: per esempio password di accesso alla rete che, di fatto, lasciano una porta aperta per entrare nell'intero network aziendale.
Altro ambito delicato è quello delle app. È facile che l'abitudine a utilizzare app e servizi per i propri dati personali venga "trasferita" anche ai dati aziendali. Per esempio, usando servizi come Dropbox per tutto o sincronizzando tutti i dati dell'iPhone su iCloud di Apple, senza preoccuparsi che i dati aziendali possano essere copiati, come è accaduto per le immagini private di alcune celebrità. Spesso manca la consapevolezza dei rischi.
L'utilizzo indiscriminato delle app porta altre implicazioni pericolose per le imprese. Per avere un'idea della portata del rischio si pensi che il numero di App potenzialmente nocive per Android è stato stimato abbia superato l'impressionante numero di due milioni.



Si stima in circa 2 milioni il numero di app contenenti malware sull'app store Android

Si tratta di un fenomeno che ricorda quello che ha caratterizzato altri sistemi operativi di grandissima diffusione, come Windows, con la differenza che lo sviluppo tecnologico sta rendendo tutto più rapido portando il numero di minacce a crescere costantemente sia in numero sia in pericolosità.

In sintesi, i rischi che si corrono nell'utilizzo di dispositivi mobili sono sintetizzabili nei seguenti:

- Malware (adware, ransomware, app malevole);
- Perdita o furto (con corredo di dati residenti sul dispositivo;
- Intercettazione di dati durante le comunicazioni;
- Exploit e uso inappropriato;
- Attacchi diretti (APT).

Una consapevolezza che cresce

La diffusione crescente di queste minacce sta portando anche nell'ambito mobile un po' di quella conoscenza che si era diffusa presso gli utilizzatori di pc.
In particolare, in base a uno studio condotto dall'istituto Redshift Research, le aziende stanno adottando una maggiore prudenza verso le iniziative BYOD perché hanno constatato che viene compromessa la sicurezza dell'organizzazione, almeno secondo la metà degli intervistati.
Tra i risultati di questo studio, emerge che il 20% delle aziende le quali hanno implementato un'iniziativa BYOD, ha subito almeno una violazione della sicurezza nell'ultimo anno. Inoltre, sempre negli ultimi dodici mesi, il 2% dei responsabili IT ha segnalato più di cinque violazioni correlate al BYOD. Tra i responsabili dei sistemi informativi, però, il 43% è certo che i dispositivi personali sono adeguatamente protetti per l'ambiente aziendale, mentre il 36% dichiara di essere preoccupato soprattutto per il trasferimento di malware e virus da tali dispositivi alla rete aziendale.
Oltre a esaminare l'atteggiamento attuale nei confronti del BYOD, la ricerca ha anche analizzato l'adozione dei dispositivi di mobilità aziendale, determinando che meno di un quarto dei responsabili dei sistemi informativi (24%) ritiene che la propria azienda sia adeguatamente attrezzata per il lavoro mobile.
Un ulteriore 8% pensa che la propria azienda non sia affatto equipaggiata. Il che corrobora le previsioni di un incremento consistente nella diffusione di dispositivi mobili entro il 2020. In particolare, secondo lo studio di Redshift Research, i tablet cresceranno del 17% e gli smartphone dell'11%.
Tra i fenomeni che recentemente hanno contribuito a creare sensibilità verso la sicurezza del mobile, vanno ricordati alcuni recenti attacchi con codici maligni noti come ransomware, che hanno provocato un certo panico tra gli utilizzatori

dei dispositivi mobili, i quali si sono trovati lo smartphone bloccato e una richiesta di riscatto per poterlo utilizzare di nuovo.
Nella maggior parte dei casi, purtroppo, non ci sono protezioni automatiche sufficientemente potenti da poter risolvere il problema. È invece molto più efficace seguire alcune regole comportamentali. Tre, in particolare, sono i suggerimenti che si possono seguire per evitare i ransomware o infezioni da malware:

- installare un antivirus, che, quantomeno, lancia un allarme quando si cerca di installare qualcosa di sospetto;
- installare le applicazioni solo se provenienti da fonti note e da sviluppatori affidabili o, in alternativa, indirettamente certificate dai commenti degli utenti, leggendoli con attenzione per valutarne la legittimità;
- attivare e impostare il codice di accesso sugli iPhone e iPad, in modo da imporre l'uso di tale codice di accesso per l'attivazione della funzionalità "Trova il mio iPhone", che viene sfruttata dai ransomware.

Queste e altre azioni preventive dovranno diventare un'abitudine, perché, come del resto è stato per i dispositivi fissi afflitti da virus, trojan, malware e via dicendo, si dovrà imparare a convivere con le minacce rivolte anche ai dispositivi mobili e a prendere le contromisure adatte a garantire la sicurezza di comunicazioni e dati. Fortunatamente, in parte, si potrà contare sul supporto dei fornitori di servizi, che si sono o si stanno attrezzando in tal senso.
Gli utilizzi più disparati sui si prestano soprattutto gli smartphone accresce l'interesse da parte dei malintenzionati: basti pensare alle applicazioni NFC (Near Field Communications) e, in particolare, all'uso del dispositivo come tramite per pagamenti elettronici. In sostanza, più i dispositivi mobili verranno usati per pagare o effettuare operazioni bancarie che richiedano l'immissione di password e dati sensibili maggiore sarà l'interesse per intercettarli e usare in modo fraudolento le informazioni bancarie inerenti il proprietario così ottenute. Di pari passo ci si attende che crescano SMS e MMS malevoli.
Considerando che la totale eliminazione del rischio è in ogni caso impossibile, si tratta di identificare il break-even tra l'ammontare degli investimenti economici in sistemi, software e applicazioni di sicurezza che si ritiene siano necessari, cui vanno aggiunti gli sforzi che si è disposti a sostenere dal punto di vista

procedurale, e la somma dei rischi (economici, amministrativi, legali e così via), che si può considerare accettabile aziendalmente.
A titolo esemplificativo e non esaustivo, si può prevedere di prendere una serie di provvedimenti:

- Sistemi anti-malware sul dispositivo per proteggerlo da applicazioni infette, spyware, schede SD corrotte e altri attacchi.
- Client SSL VPN per proteggere i dati sulla connessione logica e fisica e assicurare un'adeguata autenticazione dei dati e dei partecipanti a una sessione di comunicazione.
- Centralizzazione dell'amministrazione dei dispositivi mobili, attività di blocco del dispositivo (on site o da remoto), cancellazione dati, back up, ripristino dei dispositivi persi e/o rubati centralizzate.
- Rinforzare le policy di sicurezza.
- Utilizzare strumenti che aiutino nel monitorare l'attività del dispositivo in caso di perdita dei dati o di un suo uso inappropriato.

Le politiche di "enforcing" della sicurezza vengono attuate di solito o dal provider del servizio o a livello aziendale da parte dell'entità preposta, usualmente il reparto IT.
Nell'ambito aziendale è poi di rilevanza il coprire sia gli aspetti inerenti le modalità di accesso alle applicazioni business da parte di un dispositivo mobile che quanto concerne alla sua protezione da possibili e come si è visto molto probabili attacchi esterni.
Entrando nel dettaglio di una possibile policy aziendale per la sicurezza dei dispositivi mobili ci sono quindi diverse cose che si possono fare, in parte attinenti alla rete e ai sistemi informativi e in parte alla flotta di dispositivi, qualsiasi essi siano, perché oramai con le ultime generazioni di apparati, dal telefonino alla stampante, sono tutti dotati o dotabili di indirizzo IP e possono quindi essere oggetto di attacchi malevoli attuati allo scopo di prelevare informazioni e dati sensibili. Un forte controllo centrale, per esempio, può servire per impedire non solo l'accesso a certi dispositivi a determinate applicazioni (ottenibile definendo specifici profili di utente) ma anche per impedire che lo stesso sia usato per accedere a siti non sicuri, o per impedirgli di esportare informazioni sensibili tramite per esempio una semplice connessione diretta di tipo bluetooth.

Un esempio di gruppi funzionali di azioni e interventi preventivi da attuare al fine di incrementare il grado di sicurezza e la resistenza nei confronti di possibili attacchi può essere il seguente:

Antivirus

- Protezione in tempo reale da virus.
- Aggiornamento automatico del software antivirus e delle loro impronte.
- Scansione periodica dei file residenti sul dispositivo.
- Scansione costante delle connessioni.

Firewall:

- Filtraggio delle chiamate in ingresso e in uscita.
- Allarmi e logging delle attività a fini statistici e forensi.
- Personalizzazione funzionale e profilazione degli utenti.

Antispam:

- Blocco di sms e di connessioni in fonia non autorizzate.
- Filtraggio in base a blacklist.
- Diniego di chiamate o connessioni.

Protezione da perdita e furti:

- Blocco locale o remoto del dispositivo in caso di furto o di suo smarrimento.
- Backup e restore dei dati su un dispositivo alternative o sul medesimo quando ritrovato.
- Localizzazione del dispositivo via GPS per facilitarne il recupero.
- Notifica di variazioni della SIM.

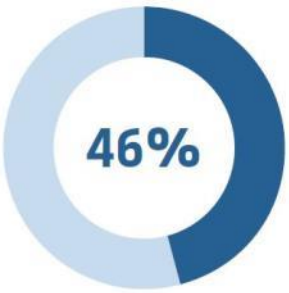
Controllo dei dispositivi:

- Inventario delle applicazioni.
- Monitoraggio dei contenuti.

La protezione degli account privilegiati

Un elemento che assume una crescente importanza in un'era sempre più mobile e dove cresce l'utilizzo di tablet e smartphone al di fuori dello stretto e controllato perimetro aziendale è la protezione degli account privilegiati. Non sempre e comprensibilmente le aziende e i loro manager sono propensi a parlare del loro status ma recenti survey sollevano in proposito e in parte il velo della riservatezza e fanno emergere non poche preoccupazioni.

Ad esempio secondo il survey CyberArk Global Advanced Threat Landscape Report 2018, quasi la metà, per l'esattezza il 46%, dei professionisti impegnati nella sicurezza cambia raramente in modo sostanziale la propria strategia, e questo persino dopo aver direttamente sperimentato e subito un significativo attacco cibernetico.



Il 46% delle aziende non cambia strategia anche dopo aver subito un attacco

E' anche questa inerzia nell'affrontare il problema della cyber security e nel non voler trarre insegnamento dagli insuccessi nel garantire la sicurezza che mette a rischio i dati sensibili, le infrastrutture e l'intero complesso degli asset IT aziendali.

Lo stato per quanto concerne gli endpoint, così come descritto dal survey realizzato da Vanson Bourne su 1.300 IT security decision maker, sviluppatori DevOps e App e LoB manager nei principali sette paesi mondiali fa emergere numerosi aspetti critici.

Cominciare col proteggere i Privileged Accounts

Il fatto che sia importante proteggere i privileged accounts è ampiamente riconosciuto. Una preponderante percentuale di professionisti IT nella sicurezza si dice convinta che la scurezza di un ambiente IT inizia proprio dalla protezione degli utenti privilegiati.
Quasi il 90% dei manager del settore ritiene infatti che sia l'infrastruttura IT che i dati sensibili non risultino adeguatamente protetti a meno che non lo siano anche gli utenti privilegiati, e che le loro credenziali e i privilegi di cui godono in funzione del ruolo aziendale siano messi al sicuro.
Se poi si scende nel particolare dl quale tipo di attacco ci si trova più di frequente a fronteggiare la situazione è la seguente:

- Phishing (56%)
- Threats interni (51%)
- Ransomware o malware (48%)
- Privileged accounts non sicuri (42%)
- Dati nel cloud non sicuri (41%)

La situazione diventa però ancor più critica per quanto concerne gli utenti privilegiati se si considera che secondo quanto riportato dai manager IT, il numero di utenti che dispongono di privilegi sul loro dispositivo endpoint è passato dal già elevato 62% nel 2016 a ben l'87% nel 2017, un incremento che richiede adeguate best practice e una maggiore sicurezza.

L'89% ritiene le proprie infrastrutture non adeguatamente protette

Forte rischio di compromissione dei dati

Cosa è possibile dedurre dai risultati dello studio? I risultati evidenziano che l'inerzia in fatto di sicurezza sembra permeare numerose organizzazioni, con una conseguente incapacità nell'affrontare e nel contrastare i cyber attacchi, con tutti i rischi che ne possono conseguire. In particolare:

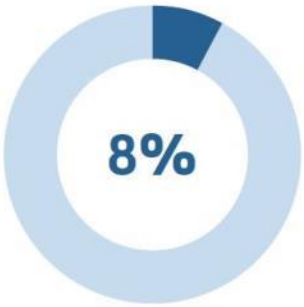
- Il 46% afferma che la propria organizzazione non è in grado di prevenire attacchi portati alla rete aziendale interna.
- Il 36% evidenzia che le credenziali amministrative sono conservate in documenti Word o Excel su Pc aziendali.
- Il 50% ammette che la privacy dei clienti può essere a rischio perché i loro dati non sono adeguatamente protetti oltre il minimo legale.

I rischi nel Cloud

Se si passa al Cloud la situazione non sembra migliore. L'automatizzazione dei processi inerenti Cloud e DevOps ha come conseguenza il fatto, mette in guardia Vanson Bourne, che privileged accounts, credenziali e informazioni riservate sono generate con un elevato tasso di prolificità.
Se queste informazioni vengono compromesse ciò può permettere ad un attaccante di fare il passo successivo e avere accesso a dati sensibili attraverso l'intera rete aziendale, ai dati, alle applicazioni, sino a poter fruire delle infrastrutture e delle risorse cloud per attività illecite, ad esempio di crypto mining.
Anche in questo caso si evidenzia una sostanziale differenza tra il dire e il fare. Le organizzazioni riconoscono sempre più la situazione di rischio e le sue possibili conseguenza, ma sembrano però mantenere un approccio rilassato nei confronti della sicurezza nel Cloud:

- Il 49% delle organizzazioni non ha approntato una strategia per la sicurezza nel cloud dei privileged accounts.
- Il 68% demanda la sicurezza al fornitore del servizio facendo conto sulla sicurezza native del provider.

- Il 38% afferma semplicemente che il cloud provider non fornisce la protezione adeguata .



Solo l'8% delle aziende conduce regolari test volti a individuare le vulnerabilità

Serve una cultura per la sicurezza

Per combattere l'inerzia nel campo della sicurezza cibernetica quello che serve, si evince dal survey, è il farla diventare un punto centrale nella strategia e nel comportamento di una organizzazione e non un qualcosa che sia dettato esclusivamente dalle esigenze commerciali e competitive. Anche in questo caso i dati del survey sono molto espliciti:

- L'86% dei professionisti per la IT security ritengono che la sicurezza dovrebbe essere uno dei punti regolarmente affrontati a livello di board.
- Il 44% afferma di riconoscere e premiare i dipendenti che aiutano nel prevenire falle nella sicurezza.
- Solo l'8% delle aziende conduce continuamente esercitazioni il cui obiettivo è individuare vulnerabilità critiche e le falle nella rete di sicurezza e ad identificare le contromisure più efficaci da mettere rapidamente in atto.

Quello che si legge tra le righe e analizzando i dati esposti è che mentre il cyber continua a far evolvere le proprie tattiche e ad utilizzare strumenti sempre più

sofisticati e potenti le aziende devono fronteggiare una persistente inerzia interna e mentale per quanto concerne la sicurezza, un comportamento che va a tutto favore degli attaccanti. Quello che si evidenzia necessario è una maggior urgenza nell'incrementare la resilienza in fatto di cyber security nel confronto dei moderni attacchi. Questo inizia dall'identificare appieno l'ampiezza in continua espansione della superficie di attacco alla sicurezza degli account e come questo ponga seriamente a rischio l'intera organizzazione.
Vincere l'inerzia richiede una forte leadership, misurabilità dei risultati, una strategia chiaramente definite e resa nota, nonché la capacità di adottare un approccio mentale del tutto simile a quello di un attaccante.

La disponibilità del servizio wireless

L'organizzazione aziendale risente delle nuove modalità operative, cambiando i modelli di conseguenza, ne è un esempio importante la crescita dei progetti di smart working che prevedono la realizzazione di spazi per il co-working in azienda. La rete deve necessariamente supportare queste nuove esigenze che si stanno posizionando alla base dell'innovazione nelle imprese. La connessione wireless diventa un imperativo.
Oggi sono sempre più le imprese che stanno implementando infrastrutture completamente wireless in azienda. Più precisamente, secondo lo studio Network Purchase Intention realizzato da ZK Research nel 2015, circa il 70% delle imprese interpellate avevano già implementato (15%) un'infrastruttura di rete "completamente" wireless o hanno espresso l'intenzione di implementarla entro il 2018, dove per completamente s'intende una rete wireless cui si collega più del 90% dei dispositivi client.
C'è poi un ulteriore tendenza in atto che pone il wireless sotto i riflettori: si tratta dell'IoT (Internet of Things). Siamo solo agli inizi di quella che si prospetta come una vera rivoluzione. Ci sono molte imprese che stanno sviluppato progetti e applicazioni IoT. La maggior parte sono grandi imprese che hanno fatto da apripista, ma delle medie sta crescendo e, presto, arriverà l'ondata delle piccole, cui gli operatori telco, in primis, forniranno soluzioni chiavi in mano, anche gestite.

Alle reti aziendali, dunque, saranno connessi anche numerosi dispositivi che nulla hanno a che vedere con pc, stampanti e altri dispositivi tipicamente informatici, appartenendo alla variegata categoria della operational tecnology. Sensori connessi alle catene di montaggio, telecamere di videosorveglianza, dispositivi per il monitoraggio sanitario, sonde tra le più disparate rappresentano e sempre più rappresenteranno un mondo interconnesso per la maggior parte attraverso reti wireless. Gli analisti di ZK Research prevedono che nel 2020 ci saranno oltre 50 miliardi di dispositivi connessi.
È una rivincita per le WLAN (Wireless Local Area Network), che hanno avuto una vita difficile in Italia, dove la loro installazione era sostanzialmente vietata o vincolata fin quasi alla fine degli anni Novanta. Le prestazioni erano penalizzate dal blocco di alcune frequenze e anche a livello internazionale lo sviluppo degli standard ha sempre viaggiato a rilento, ampiamente surclassato da quello relativo alle reti cablate. Oggi, però, non è più necessario scegliere fra i vantaggi del wireless e le prestazioni di Ethernet: LAN e WLAN sono ormai comparabili.
Questo non significa che tutte le reti wireless siano uguali e che non ci siano criticità da considerare nell'implementazione di un'infrastruttura, la quale deve evidentemente garantire affidabilità e sicurezza, senza aggravare i costi operativi. Non dimenticando, inoltre, che, a seconda dei casi, può essere richiesta un'elevata scalabilità.
Le prime implementazioni WiFi "appiattivano" le differenze, proponendo tipologie e topologie standardizzate, senza considerare che contesti di dimensioni e settori diversi non sono assimilabili: se già esistono differenze importanti da un negozio familiare e un grande magazzino, è facile figurarsi come lo stesso WiFi non possa funzionare in un campus universitario, in un grattacielo di uffici o in un ospedale. Sono quindi nate nuove architetture e topologie, che, normalmente, mantengono l'interoperabilità con dispositivi esistenti.
Secondo le esigenze e gli scenari di utilizzo, potranno risultare migliori reti impostate diversamente: in pratica sono quattro le "variabili" da considerare in modo da realizzare reti:

- con o senza controller;
- gestite on premise o in cloud;
- basate su canali multi-cella o a singola cella;

- con gestione e sicurezza delle applicazioni integrata o separata.

Tali variabili dovranno trovare posto in un'equazione che soddisfi le esigenze specifiche di ciascuna azienda, sempre considerando centrali i temi della gestibilità e della sicurezza. Oggi sono disponibili diverse soluzioni per realizzare reti wireless, alcune decisamente evolute rispetto le prime installazioni. Nel seguito si approfondiranno quelle proposte da Fortinet. Prima di esaminare l'evoluzione, soprattutto in chiave cloud, delle WLAN si evidenzieranno le problematiche legate alla sicurezza, che influenzano le scelte tecnologiche anche in termini di topologia di rete.

Va innanzitutto considerato che la trasmissione via etere e onde radio è intrinsecamente, per sua stessa natura, più esposta a intercettazioni di quella realizzata tramite reti fisse, perché non è nemmeno necessario collegarsi a un cavo (cosa poi particolarmente difficile nel caso di dorsali ottiche Wan o Lan), ma è sufficiente disporre di strumenti in grado di intercettare le frequenze Wi-Fi (Sniffing o MITM acronimo di Man in the Middle) e di decodificare i dati sui diversi canali trasmissivi. Sono attacchi molto difficili da evidenziare perché operano a un livello trasparente per il proprietario di un dispositivo. Lo sniffing si limita semplicemente a intercettare e decodificare le trasmissioni e se queste sono in chiaro (e cioè non cifrate mediante opportuni algoritmi) il gioco è fatto. Ancora più subdola è la metodologia di attacco MITM, che consiste sostanzialmente nel frapporsi tra due interlocutori.

È vero che esistono contromisure in proposito, ma spesso non vengono prese perché molti utilizzatori ritengono che il solo utilizzo di protocolli sicuri, quali HTTPS ed SSH, siano più che adeguati per proteggere i dati trasferiti nel corso della sessione. Va osservato che normalmente questo è vero, ma si tratta di protocolli che spesso sono implementati nei livelli alti della pila ISO/OSI (un modello definito negli anni settanta che rappresenta il riferimento generale per la realizzazione di sistemi informatici), e che possono però essere aperti ad attacchi portati ai livelli inferiori, quali appunto quelli di trasmissione radio delle informazioni.

In sostanza, tramite opportuni dispositivi, viene intercettato il segnale emesso dal dispositivo di origine e a quella che sarebbe la connessione diretta chiamante – chiamato si sostituisce un flusso che diventa "chiamante – sniffer – chiamato". Lo sniffer ha così la possibilità di intercettare i dati nelle due

direzioni e sostituirli a piacere, modificarli, registrarli, eccetera, il tutto senza che né il chiamante né il chiamato ne siano consci.
Una soluzione che supporti la Mobility aziendale deve comprendere tutti gli aspetti legati all'usufruibilità delle applicazioni e dei servizi. Quindi la garanzia non solo della disponibilità, ma anche di un livello minimo garantito di prestazioni. Soprattutto, però, questo significa poter utilizzare soluzioni che supportino appieno i processi aziendali.
Le suddette tematiche devono dunque essere affrontate con gli opportuni approcci tecnologici e, come già rimarcato, la strada per il futuro è certamente il cloud o IT as a Service, per la quale ciascuna azienda dovrà trovare la propria ideale combinazione tra private e public.
In questa chiave va dunque presa in considerazione l'organizzazione delle infrastrutture necessarie per fornire il servizio di mobility ai diversi utilizzatori in azienda. Ovviamente, la connettività esterna alle sedi aziendali non potrà che essere acquisita presso gli operatori, mentre internamente si potranno utilizzare le reti Wi-Fi. Per quanto concerne, invece, la soluzione dei requisiti prima enunciati, si potranno effettuare le scelte più opportune a seconda dei casi.
Quanto occorre è dunque una piattaforma MaaS (Mobility-as-a-Service), cioè una piattaforma di tipo "always on" di livello Enterprise, atta a erogare servizi di mobilità a un ampio numero di terminali di utente, dal comune telefono al più complesso terminale mobile. Il suo obiettivo primario è quello di abilitare la connessione di un utente e, tramite il dispositivo di cui è equipaggiato, permettergli di accedere alle proprie applicazioni e dati, il tutto con i processi di business che controllano il processo e cioè se l'utente è autorizzato a farlo, a che dati accede, che applicazioni richiede, quali dati generare così via.

Il Cloud Wi-Fi

Come prima accennato, una delle scelte da compiere, quando si vuole installare o rimodernare una rete WiFi è decidere se basarla su controller tradizionali o meno.
Oggi, infatti, sono ormai diffuse sul mercato soluzioni basate su servizi gestiti in cloud, che consentono di non installare i costosi e onerosi, in termini di gestione, controller.

In ambienti ad alta densità, con centinaia o migliaia di access point installati i controller sono probabilmente necessari, ma le imprese che hanno pochi punti di accesso wireless nonché quelle molto distribuite, che pure hanno pochi access point per sede, devono valutare i vantaggi offerti dalle soluzioni WiFi gestite nel cloud, che consentono ai clienti di acquistare solo gli access point, potendo fare a meno di controller o server di gestione.
Non è un caso, infatti che tali soluzioni siano nate soprattutto per sgravare le aziende molto distribuite dall'onere dei numerosi controller da installare.
I vantaggi non si fermano qui, anche considerando che queste soluzioni sono più recenti, quindi nate nell'epoca della user experience, con tutto ciò che ne consegue in termini di interfacce semplificate e maggiore gestibilità.
Un altro beneficio consiste nella flessibilità, tipica del cloud, che in questo caso, per un'azienda significa poter iniziare con un solo access point per poi crescere in base alle sopravvenute esigenze.
Tuttavia, il cloud può non essere un salto qualitativo completo, anche se riduce la complessità e i costi. La maggior parte delle soluzioni Cloud WiFi, però, deludono in termini di contenuti e sicurezza delle applicazioni. Esse, infatti, non spostano i paradigmi delle reti wireless basate su controller: semplicemente spostano questi ultimi fisicamente dall'azienda al data center del provider. Il che introduce anche problematiche, a cominciare da un potenziale point of failure dell'infrastruttura wireless, qualora la connessione con il cloud dovesse cadere. Inoltre, anche la sicurezza è fornita nel cloud, ma i punti di accesso restano ovviamente on premise, aprendo il fronte a nuove vulnerabilità.
Affinché una soluzione Cloud WiFi possa rispondere alle esigenze di un'impresa è necessario che risponda a una serie di attributi, soprattutto per realizzare una infrastruttura completamente wireless.

Sette requisiti per un Cloud WiFi a prova di business

Coerentemente con quanto finora esposto, la gestibilità va messa in primo piano: occorre un sistema di management completo per il provisioning di aggiornamenti e configurazioni degli access point. I controller, on premise o in cloud sono efficacissimi, ma l'evoluzione delle minacce informatiche, come prima illustrato, pongono l'esigenza di superare le forme di controllo basiche, a beneficio di una console unica la gestione di sicurezza e infrastruttura sull’intera rete. Un sistema di gestione in grado di scalare a piacere.

Il secondo requisito riguarda il provisioning, che, essendo in cloud, non deve prevedere interventi manuali. In pratica, ancora una volta a beneficio delle imprese molto distribuite, deve essere possibile distribuire nuovi access point da remoto, ovunque nel mondo, senza dover ricorrere al supporto tecnico locale. Per esempio, dovrebbe bastare collegare l'apparato, che, una volta online, viene registrato automaticamente nel cloud, scaricando le configurazioni predefinite per quella specifica azienda insieme al firmware più recente.
Terzo punto fondamentale è la visibilità granulare delle applicazioni. È fondamentale riconoscere il traffico che attraversa la rete e distinguere tra quello che è sensibile ai tempi di latenza o richiede larga banda. La molteplicità di servizi che oggi usano la rete rende ancora più necessario poter gestire al meglio la QoS (Quality of Service) sulle reti wireless.
Questo vale anche per svolgere gli adeguati e sempre più sofisticati controlli di sicurezza e, a tal riguardo, è fondamentale che le configurazioni eseguite nel cloud scaricano le relative policy negli access point in tempo reale.
L'autenticazione degli utenti su specifici SSID è il quarto requisito da soddisfare, affinché il personale IT possa creare profili di accesso separati per diversi gruppi all'interno dell'azienda: per esempio per definere policy diverse tra studenti, insegnanti e personale ATA in una scuola.
Un gruppo che viene tipicamente trattato a parte è quello dei "guest", per i quali occorre sia previsto (quinto punto) un captive portal apposito.
L'indagine Network Purchase Intention di ZK Research, cui si è già fatto riferimento, poneva l'accesso di utenti guest al secondo posto fra le applicazioni che le aziende intendevano implementare su WLAN.
La rete WiFi dovrebbe consentire la configurazione di SSID senza limiti quantitativi.
Il sesto attributo è nuovamente legato alla sicurezza, per la quale, come detto, non basta il controllo accessi, ma occorre poter analizzare lo stato e l'utilizzo delle applicazioni layer 7, in modo da consentire l'impostazione di un modello gestionale predittivo. È opportuno monitorare utilizzo e consumo di banda delle applicazioni e da parte di chi. Informazioni che servono per la sicurezza e per attività di manutenzione preventiva e programmazione.
Per ultimo, ma non ultimo, il settimo punto riguarda la capacità di supportare una sicurezza pensata per infrastrutture di rete completamente wireless.

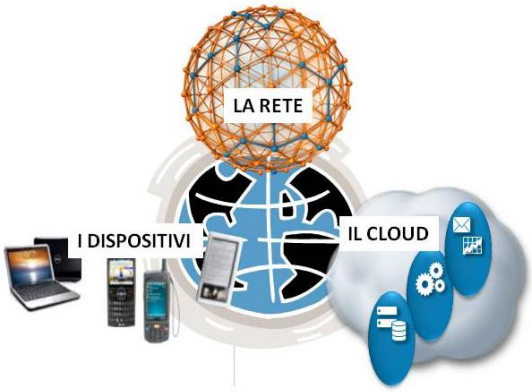
Si tratta di supportare le evoluzioni evidenziate in incipit. Secondo gli analisti di ZK Research la sicurezza rappresenta l'ostacolo principale nella diffusione dell'IoT.
Un sistema di sicurezza completo non può fermarsi all'autenticazione, come avviene per la maggioranza delle Cloud WiFi, e deve, invece, comprendere intrusion prevention e tutte le soluzioni che occorrono per mitigare la crescente ondata di minacce cyber.
La soluzione Cloud WiFi di Fortinet, che analizziamo in seguito, prevede funzioni di sicurezza avanzata integrate direttamente nell'hardware dell'access point, il che evita di dover installare in cloud le diverse soluzioni per la sicurezza che occorrerebbero.

Mobile Device Management

Il controllo è un prerequisito importante per la sicurezza mobile aziendale, in quanto esiste la possibilità di accedere alla rete tramite i dispositivi mobili e la quella che su tali apparati possano risiedere dati confidenziali.
La soluzione base per la gestione di smartphone e tablet è tipicamente denominata sistema di Mobile Device Management (MDM), che possiede alcune funzionalità di protezione e di sicurezza. Di livello più alto sono le soluzioni nominate sistemi di Enterprise Mobility Management (EMM), che all'MDM aggiungono almeno la capacità di gestire le app aziendali, spesso attraverso un vero e proprio app store privato.
I sistemi MDM ed EMM supportano le strategie aziendali relative alla mobility, qualunque queste siano. Tre sono i possibili modelli: il tradizionale COBO (Corporate Owned Business Only), l'affermato BYOD (Bring Your Own Device) e l'articolato COPE (Corporate Owned Personal Enabled).
La scelta deve soddisfare i tre fattori critici per il successo di una strategia di enterprise mobility:

- l'appagamento dell'utilizzatore finale;
- la sicurezza dei dati aziendali;
- la gestione dei dispositivi e delle applicazioni che su questi sono disponibili.

Tali obiettivi non sono indipendenti tra loro, anzi sono strettamente correlati e, per certi aspetti, contrapposti, in ogni caso sono frutto del prodotto dei tre abilitatori della mobility: la rete, i dispositivi e il cloud, che insieme contribuiscono a realizzare l'infrastruttura tecnologica su cui si appoggiano i processi, la sicurezza e, per ultima ma non ultima, la user experience.



I tre abilitatori della Mobility

Questi tre abilitatori, anche se in misura diversa, possono essere considerati le leve su cui si è innescato il profondo cambiamento in corso. Le aziende stanno affrontando la trasformazione della propria infrastruttura accentrando e al tempo stesso "allargando" il data center in chiave cloud, sia esso ibrido o totalmente basato su infrastrutture pubbliche.
La connettività è ormai data per acquisita, anche se rimangano differenze notevoli di servizio in alcune aree disagiate del Paese. Sul fronte dei dispositivi mobili, invece, l'evoluzione continua deve ancora esprimere ulteriori potenzialità di cambiamento. Le imprese, peraltro, sono oggi chiamate a scelte importanti, sotto la spinta anche delle richieste provenienti dal "basso", cioè dalla forza lavoro che con tali dispositivi ha ormai una confidenzialità quotidiana.
La user experience è fondamentale per ottenere l'appagamento dell'utilizzatore finale e dipende quasi completamente (ma non solo) dal dispositivo. È per questo motivo che nella realtà si sta affermando il BYOD. Intanto questa è una risposta implicita al COBO, che impone l'utilizzo di un dispositivo scelto

dall'impresa e utilizzabile solo per le attività di lavoro. Probabilmente la scelta più sicura, certamente quella che garantisce il maggior controllo da parte dell'azienda, ma anche quella che è stata scartata dal mercato sia perché l'utilizzatore non era soddisfatto sia perché quest'ultimo eludeva le policy aziendali e usava il proprio dispositivo anche per lavorare.
All'inizio molte imprese hanno visto l'opportunità di risparmio sull'acquisto dell'equipaggiamento e hanno incoraggiato questo fenomeno. Finché si trattava del giovane nuovo dipendente che preferiva usare il Mac al pc, poco male, ma quando si è trattato di configurare e gestire il tablet o lo smartphone di grido dell'amministratore delegato, si è verificato che i conti non sempre tornavano: a fronte di un risparmio sull'acquisto si aveva un considerevole aumento dei costi sull'help desk.
Peraltro,il BYOD si è affermato "in nome dell'experience", però, comporta due complicazioni: il suddetto aumento dei costi operativi per la gestione dei dispositivi e un incremento del rischio che possano avvenire violazioni alla sicurezza dei dati aziendali. In pratica, consentire ai dipendenti di utilizzare un proprio dispositivo per il lavoro permette di conseguire il primo requisito per il successo della mobility, quello sull'appagamento dell'utilizzatore finale, ma contemporaneamente ostacola il soddisfacimento degli altri due.
Un'alternativa può essere il COPE, che prevede l'utilizzo da parte del dipendente di un dispositivo messogli a disposizione dall'azienda. Una pratica logica, perché è effettivamente l'azienda a dover fornire al lavoratore gli strumenti per consentirgli di lavorare. È interesse dell'azienda permettere al lavoratore di produrre nel miglior modo possibile ed è sempre interesse dell'azienda che possa farlo senza mettere a rischio la sicurezza dei dati e dell'impresa stessa.
Secondo la logica del modello COPE, l'azienda, in pratica, torna a fornire il dispositivo al dipendente, ma gli permette di utilizzarlo anche per scopi personali. Questo cambia radicalmente la strategia attuabile, perché dà il permesso all'azienda di gestire l'apparecchio, di cui è proprietaria.
Per mantenere anche i vantaggi del BYOD, però, occorre un sistema di gestione che consenta di supportare qualsiasi tipo di dispositivo: solo così, infatti, l'azienda potrà comunque lasciare ai dipendenti una scelta ampia e non obbligare l'uso di un sistema operativo non gradito.

Altra caratteristica fondamentale per abilitare il COPE consiste nella capacità di "containerization", cioè la possibilità di tenere quanto più separati possibile i due diversi tipi di utilizzo. In altre parole, separare app e dati del lavoro da app e dati della sfera privata. Solo isolando e potendo intervenire sulla parte aziendale da remoto, salvaguardando la privacy del dipendente da incursioni dell'impresa e, al tempo stesso, evitando che un comportamento insicuro metta a rischio i dati aziendali, si possono prendere gli aspetti migliori del BYOD e quelli del modello COBO.

4 - SICUREZZA DEL DATO E BUSINESS CONTINUITY NELL'ERA DEL SOFTWARE DEFINED DATA CENTER

L'operatività aziendale dipende dalla disponibilità di informazioni e servizi a supporto del business. Ciò rende il data center un asset sempre più importante e costoso. Nuove tecnologie ne migliorano l'agilità nella gestione delle risorse informatiche, quali server e storage, ma ne rendono ancora più critici gli aspetti legati all'amministrazione dell'infrastruttura operativa, trasformando la sicurezza, l'affidabilità e l'ottimizzazione dei consumi in obiettivi di business

Il data center del futuro

Il data center come lo conoscevamo è negli ultimi anni profondamente mutato. I trend che l'hanno interessato e lo stanno tutt'ora interessando, sono numerosi. Vediamo di elencarli, anche se non in ordine temporale o di importanza e abbinando aspetti puramente architetturali con altri più operativi.

Nell'insieme danno però una idea dei problemi che un CIO e il suo staff si trovano giornalmente ad affrontare e quali decisioni si trovano a dover prendere. La virtualizzazione, il cloud, la ri-centralizzazione delle funzioni prima demandate ai server in un'architettura client-server che ha dominato le scene sino a ora, la virtualizzazione dei desktop, il BYOD e cosa ciò implica per la sicurezza dei dati e la gestione delle immagini e dei dati attinenti i dispositivi remoti, il cloud nelle sue diverse incarnazioni (public, private o hybrid) e, ultimo in ordine di tempo ma con un effetto dirompente, il Software Defined Data Center (SDDC).

Con quest'ultimo termine, in sostanza, si intende la capacità di organizzare un data center in modo che sia facilmente gestibile via software, con un disaccoppiamento tra hardware e la sua immagine virtuale così come viene proposta allo strato delle applicazioni e con la implicita possibilità di gestire in modo trasparente le diverse tipologie di risorse, che si tratti dei server, dello storage o della rete. È immediato capire come una tale evoluzione sia congruente con le esigenze di chi desidera adottare un cloud di tipo sia ibrido sia public.

La complicazione ovviamente non si ferma al contorno, perché se Software Defined deve essere un data center, software defined devono necessariamente essere tutte le sue componenti, come per esempio lo storage e il substrato di rete. Non a caso parallelamente all'interesse degli utilizzatori è fortemente cresciuto l'interesse e il coinvolgimento dei produttori per il Software Defined Storage (SDS) e il Software Defined Networking (SDN).

Quella dell'SDDC è un'evoluzione che era nell'aria e sembra essere la conseguenza diretta della virtualizzazione, oramai fortemente attuata dalle aziende, e dalla crescente diffusione del cloud, soprattutto di tipo ibrido, che appare sempre più essere la strada che imboccheranno le aziende nel passaggio

a un nuovo modo di concepire e fruire di un infrastruttura ICT il più possibile basato sul concetto di dinamicità nell'uso delle risorse, e del loro pagamento.
Esaminiamo due degli elementi fondanti di questa evoluzione, quella dello storage e quella della rete e le relative implicazioni. Prima però vediamo perché interessa sia gli operatori sia lo staff IT aziendale.
Dal lato degli utilizzatori e cioè dal punto di vista di chi gestisce un data center, software e servizi interessano la maggior parte delle risorse e assorbono buona parte degli investimenti. Fin qui nulla di particolarmente diverso rispetto al passato, ma cambiano radicalmente le modalità operative, abilitando un grado di libertà e una rapidità di intervento nettamente superiore a quella sperimentata finora.
Naturalmente quello che è chiaro e auspicato come punto di arrivo, cioè l'indipendenza teoricamente assoluta tra applicazioni e infrastruttura hardware, richiederà del tempo per essere raggiunta, ma è comunque un processo in itinere che appare oramai inarrestabile.
In sostanza, quello che ci si aspetta abiliti concettualmente un SDDC è di disaccoppiare del tutto le applicazioni dalla componente fisica sottostante, e tramite un strato software e un insieme di API (che permettano alle diverse componenti di interagire in modo standardizzato), far si che a una applicazione vengano automaticamente assegnate le risorse che le servono in funzione di parametri prestabiliti, come la potenza elaborativa necessaria, il volume di dati da trattare, il grado di sicurezza, il livello RAID, la dispersione geografica dei dati da accedere, eccetera.
Ciò vuol dire poter orchestrare automaticamente l'assegnazione delle risorse alle singole applicazioni e farlo non solo in modo fisso, ma anche in base alle esigenze del momento.
Per esempio, se un'applicazione di BI o ERP deve analizzare una certa mole di dati per estrarne informazioni decisionali utili, ma deve farlo in un tempo massimo prestabilito, si deve vedere assegnata in modo automatico la capacità di elaborazione e di storage necessaria, nonché la banda e le connessioni di rete conseguenti, senza che per farlo si debba procedere manualmente.
In pratica, ciò corrisponde a un affinamento dell'assegnazione delle risorse fatto in modo tale da ottimizzare al massimo le risorse stesse, con in più il vantaggio che, avvenendo l'interazione tra strato di orchestrazione e macchine fisiche in

accordo a protocolli e API standardizzate, quest'ultime possono essere sostituite (per manutenzione, upgrade o a causa di guasti) senza interrompere il funzionamento e in modo trasparente per l'applicazione. In pratica, ci si viene a trovare in presenza di un sistema che è in grado di scalare automaticamente sia verso l'alto sia orizzontalmente, garantendo (perlomeno teoricamente) l'assoluta continuità del servizio.

Altro corollario riguarda la possibilità di poter adottare hardware di terze parti senza essere vincolati a un unico fornitore. Questo perché l'orchestrazione delle risorse è gestita, tramite interfacce standard definite da enti o associazioni dedicate (si pensi per esempio a Open Stack e a Open Flow), da un livello software soprastante il piano fisico che disaccoppia applicazioni e infrastruttura.

Se un server non ha la capacità di memoria necessaria, o un dispositivo di storage non ha il tipo di RAID richiesto dalla applicazione, diventa impossibile adottarlo anche se costa di meno di un'altra macchina perché altrimenti avrei un degrado delle prestazioni complessive e l'impossibilità di soddisfare specifici SLA. Prevedibilmente, in un quadro di progressiva standardizzazione a livello di interfacce sarà su questi aspetti che i produttori si giocheranno la loro quota di mercato nello spazio che si apre per la realizzazione di questo nuovo concetto di data center.

Per quanto concerne la componete rete di un SDDC vale quanto esposto in generale, e cioè l'interesse nel poter impostare a software le caratteristiche che deve avere il substrato di trasporto in funzione delle esigenze applicative.

Ciò dal punto di vista architetturale e nel contesto della rete è ottenuto adottando un principio da tempo usato nei grandi sistemi di comunicazione pubblici e internazionali dove l'esigenza di poter far interagire reti costituite da apparati di fornitori diversi esiste da decenni.

In pratica, si è adottato il medesimo sistema di operare su due piani, un piano di alto livello software e un piano fisico di connettività costituito dai nodi di commutazione, in sostanza i router di backbone o periferici. È compito del piano di controllo (e cioè del software che risiede su una macchina specifica o è a sua volta distribuito) determinare quale risorsa, quale canale quale banda va assegnata alla applicazione, e che si preoccupa di orchestrare il tutto in modo da garantire ai dati di quell'applicazione un canale di comunicazione per il tempo necessario corrispondete alle esigenze, allo SLA e così via.

Come sempre, dato un accordo di massima tra gli operatori di mercato, il diavolo si nasconde nei dettagli ed esistono punti di vista diversi sotto il profilo terminologico. Per alcuni il punto centrale di un tale approccio, che effettivamente permette di creare una infrastruttura di rete molto flessibile e potenzialmente del tutto indipendente dal fornitore, è nella separazione tra piano di controllo e apparati di rete mentre altri puntano sulla trasformazione in accordo al concetto di openess delle interfacce di controllo sugli apparati quali i router.
In realtà lo scenario si presenta ben più complesso anche se entrambi i punti di vista ne possono far a ragione parte e il concetto di separazione tra piani è già noto e attuato da anni.
Un consistente passo avanti è quello che si è posto come obiettivo la definizione del protocollo Open-Flow, che dal campo accademico, una volta che è stato adottato dalla Open Networking Foundation (ONF), ha finito con il costituire un solido riferimento nel lavoro di standardizzazione in questo critico settore del data center.
Come tutti gli standard nella loro fase iniziale i problemi non sono mancati e alla sua definizione iniziale sono seguite attività di messa a punto favorite anche dal crescente interesse e coinvolgimento da parte dei produttori. Quale sia il punto di arrivo di una tale evoluzione è difficile da dire al momento, ma è prevedibile che sul carro del “software defined” in breve saltino anche i pochi che ancora non l’hanno fatto, fosse solo per opportunità di marketing. Una storia che si è già vista con il cloud computing.

Il data management

Un'infrastruttura basata sulla virtualizzazione e l'orchestrazione delle risorse virtualizzate in chiave software defined, rende evidentemente obsolete le infrastrutture di backup, restore e disaster recovery basate sulla copia dei dati, il vaulting fisico e tutte quelle procedure complesse e costose che, soprattutto, non sempre veniva condotte pienamente. In particolare, troppo frequentemente veniva saltata la fase di test con il rischio che, al momento del bisogno, non si riuscisse a effettuare il ripristino così come lo si era ipotizzato e, quindi, tornando allo stato ante disastro.

Peraltro, proprio la complessità di questi sistemi rende difficile abbandonarli in tempi rapidi, senza contare i vincoli legacy e quelli legali, che impongono di poter accedere a determinati contenuti e di rispettare alcune normative anche di settore.
Il risultato è che presso le aziende si è in una fase di transizione, passando ove possibile a nuove architetture incentrante sulla gestione dei dati, non più con le vecchie logiche di backup e restore, ma con nuove garanzie di availability del dato. Intere risorse e applicazioni possono essere memorizzate sostanzialmente in un file, i dati duplicati nel cloud e l'immagine del proprio sistema informatico, nel suo complesso ripristinata in tempi rapidi a piacere in qualsiasi parte del globo terrestre. Più facile a dirsi che a farsi, ma comunque possibile e, in futuro, sostanzialmente situazione standard.

Una sicurezza basata sulla business continuity e il disaster recovery

L'aspetto fondamentale di una strategia di business volta a salvaguardare i dati, le informazioni e i processi aziendali prevede un primo passaggio obbligatorio: la salvaguardia della continuità operativa del business. Può sembrare banale ma è inutile pensare e investire nella protezione di dati dai malintenzionati, ovunque questi si trovino, se per prima cosa non si garantisce che, quando necessario, questi dati possano essere fruiti e utilizzati per le esigenze applicative, il CRM, la business intelligence, le applicazioni amministrative, di magazzino e via dicendo senza dimenticare praticamente nessun ambito e processo aziendale, tanto l'Information e Communication Technology è integrata in un'impresa.
Il punto centrale e iniziale di una strategia volta ad assicurare la sicurezza e la disponibilità dei dati aziendali e del funzionamento delle applicazioni business o di produzione è, in sostanza, il data center, intendendo con questo quel luogo (o l'insieme dei siti decentralizzati) dove si trova il mainframe o i server e i dispositivi di storage e di rete che elaborano i dati e li trasformano in elementi fruibili dalle applicazioni tramite i dispositivi fissi e mobili di utente.
Da questo punto di vista, sicurezza e continuità vanno a braccetto e garantire, rendere sicure e ottimizzare le soluzioni per la business continuity, considerando

tutta l'infrastruttura del data center, non solo è indispensabile ma può sorprendentemente portare a importanti risparmi economici

La continuità del business è oramai un imperativo per qualsiasi azienda, indipendentemente dal settore in cui opera, ma il business dipende dalle applicazioni office o di produzione, e queste a loro volta dipendono dai dati e dalle capacità di elaborarli in tempi utili. In sostanza, tra quello che si desidera e quello che si ottiene si interpongono dei fattori che se non sono ben calcolati possono intervenire spiacevolmente e far si che un'applicazione non funzioni o che un'informazione non sia disponibile proprio quando serve e dove serve. Certe volte la continuità del business è però un concetto aleatorio di cui se ne scopre l'importanza quando è troppo tardi e ci si trova a un passo da eventi disastrosi o, peggio, il limite è stato superato.

Cionondimeno, le interruzioni dell'operatività aziendale possono essere improvvise, drammatiche e terribilmente estese e le stesse cause possono andare dai fenomeni naturali agli errori umani, dai guasti meccanici sino a eventi con carattere doloso.

A fronte di una crescente dipendenza delle applicazioni e dell'operatività quotidiana dai dati e dall'e-business, si delinea sempre più chiaramente l'importanza di elaborare, attuare e mantenere piani efficaci e aggiornati di business continuity e disaster recovery, anche sotto forma di semplici provvedimenti cautelativi.

Quello tra Business Continuity e Sicurezza rappresenta, in definitiva, un binomio inseparabile.

Ma dal punto di vista pratico? In pratica c'è da chiedersi se la propria azienda sia effettivamente pronta e sicura come dovrebbe e se sia in grado di progettare una riorganizzazione della propria infrastruttura in tempi rapidi. In ogni caso è meglio muoversi in fretta e valutare attentamente almeno due fattori: le competenze dei partner e i ritorni economici delle soluzioni proposte.

L'aspetto impiantistico

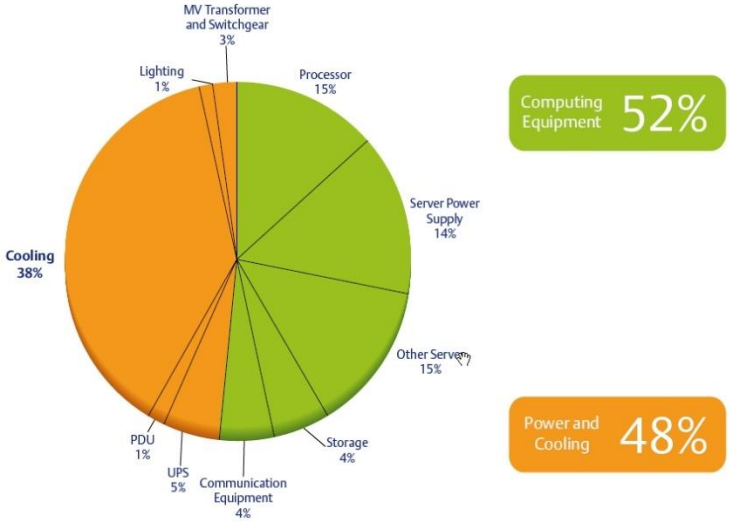
Per essere in grado di supportare applicazioni che, con la proiezione di un'azienda nel più ampio contesto Internet, devono essere attive 24 ore su 24, l'IT aziendale si è dovuto trasformare profondamente e l'insieme delle apparecchiature che lo costituisce sta necessariamente incorporando

caratteristiche di tipo enterprise class, ovvero in grado di assicurare un livello di funzionamento continuo del 99,999%.
Sottosistema storage, server, network e infrastruttura, compreso impianto di alimentazione e raffreddamento, è necessario e in ogni caso auspicabile, che adottino il medesimo approccio implementativo, scalabile, modulare, ridondato e con componenti sostituibili a caldo in caso di guasto.
Resta da valutare se le soluzioni pratiche per un tale approccio sono disponibili e realizzabili concretamente. La risposta a questo dubbio è positiva.
Soluzioni recentemente introdotte sul mercato stanno effettivamente aprendo la strada alla realizzazione di data center di nuova generazione, in cui i diversi sottosistemi operano con caratteristiche omogenee. L'architettura per la realizzazione delle infrastrutture che ne è risultata è basata su armadi standard che comprendono gli apparati attivi, le batterie di backup, le componenti elettriche, il cablaggio e così via.
In sostanza, si può realizzare un'infrastruttura distribuita e modulare che può arrivare a disporre, nelle configurazioni maggiori, di un livello di ridondanza basata su array (e cioè un insieme distribuito di moduli base) che può garantire una disponibilità statistica superiore al 99,9999%, pari a un fuori servizio di pochi secondi annui.
Dal punto di vista delle applicazioni il data center, va rimarcato, è l'elemento centrale nell'assicurare la continuità operativa e la salvaguardia delle informazioni, tramite un suo opportuno progetto e la predisposizione di procedure di backup e di recovery che rientrino in un piano periodicamente aggiornato di business continuity.
Il ricorso alle procedure di backup è solo il più eclatante degli accorgimenti che è necessario prendere per tutelarsi da problemi soprattutto relativi al disaster recovery.
Se la possibilità di poter recuperare dati è fondamentale, molto se non altrettanto importante appare anche la necessità di garantire ai propri utenti una continuità del servizio e una disponibilità dello stesso, oltre che dei dati.
Questo implica che non solo lo storage situato in un data center sia protetto con soluzioni di replicazione dei dati a distanza, ma anche che il resto delle infrastrutture sia, se non duplicato, quanto meno fornito delle caratteristiche

idonee ad assicurare il livello di servizio minimo per poter portare avanti le attività aziendali.

Nel far funzionare correttamente gli apparati di un data center un ruolo fondamentale lo gioca l'ambiente e l'infrastruttura di supporto e, in sostanza, quanto attinente al condizionamento ambientale e all'alimentazione energetica. La loro qualità è l'elemento indispensabile perché il sistema nel suo insieme funzioni correttamente e risulti sicuro. Sono svariati i problemi connessi all'infrastruttura e, in primis,quello energetico e quello ingegneristico.

I costi per il consumo energetico rappresentano una quota in costante e rapido aumento del Total Cost of Ownership delle sale CED (Centro Elaborazioni Dati) o data center. Il problema costituito dal contenimento dei consumi energetici interessa poi sia aspetti legati alle caratteristiche degli apparati IT sia all'infrastruttura fisica.



Distribuzione dei consumi energetici in un data center tradizionale

Un primo elemento riguarda il dimensionamento dell'infrastruttura. Le apparecchiature IT utilizzano, infatti, solo una parte dell'elettricità complessiva immessa nel CED. Di solito questa percentuale corrisponde a circa il 50% mentre il restante 50% dell'elettricità è utilizzato dai sistemi di raffreddamento, dagli

UPS, dai sistemi di condizionamento, dalle unità di distribuzione dell'alimentazione e da altri componenti vari.
Questo significa che un punto importante da cui partire per risparmiare energia (e quindi ridurre i costi operativi) coinvolge la parte infrastrutturale che, da sola, utilizza perlomeno la metà dell'alimentazione richiesta per il funzionamento di un data center e delle apparecchiature IT che contiene.
L'attenzione all'efficienza va riposta anche ai sistemi di continuità elettrica, il cui contributo può essere considerato trascurabile nel caso di ambienti con pochi sistemi, ma rappresenta un costo significativo nel caso di ambienti ad alta densità con carichi che possono superare gli 1 MW, dove un risparmio di qualche punto percentuale determina un consistente risparmio economico.
Anche utilizzare un'architettura e un sistema di condizionamento dell'aria più efficiente diventa essenziale all'interno del data center. Diverse sono le modalità per ottenere questo risultato.
Alcune opzioni possono consistere nell'utilizzare una serie di unità di raffreddamento anziché un sistema di raffreddamento unico per l'intera sala CED. Questo approccio può risultare particolarmente efficace negli ambienti ad alta densità. Peraltro, si sta rivelando molto utile anche la nuova generazione di soluzioni per il raffreddamento ad acqua, che permette di intervenire esattamente dove serve dissipare il calore prodotto senza essere costretti a condizionare costosamente un intero ambiente.
Va poi osservato che adottare soluzioni recenti permette anche di fruire delle migliori qualità progettuali e di una architettura modulare che permette di ridurre il rischio di guasto totale di un impianto e migliorare la sicurezza complessiva del sistema informativo dal punto di vista funzionale.

Alimentazione e condizionamento sempre più efficienti

Le tecnologie per la continuità dell'alimentazione sono in massima parte già giunte da tempo a buoni livelli di efficienza, tuttavia, quelle di ultima generazione arrivano a superare il limite del 90% di efficienza, anche di diversi punti percentuali.
Ma è anche sul fronte del raffreddamento che è possibile ottenere grandi incrementi. In passato, infatti, si è molto trascurata la progettazione di un data center efficiente, senza preoccuparsi di controllare l'eventuale formazione di

sacche di calore. Non esistevano, inoltre, le attuali tecnologie di precision cooling, che consentono di raffreddare solo dove occorre e con l'intensità strettamente necessaria. Altri accorgimenti, inoltre, permettono di sfruttare anche la fredda temperatura esterna nei mesi invernali o la vicinanza di corsi d'acqua a bassa temperatura, sia di fonte glaciale che di tipo sorgivo.

Ci sono, in altre parole, diverse soluzioni proposte dai principali protagonisti del settore che consentono di conseguire importanti risparmi sul costo dell'energia e di ridurre l'emissione di anidride carbonica (CO2), con un conseguente rispetto dell'ambiente che non guasta mai. Queste tecnologie, inoltre, non solo mantengono ma anzi aumentano l'affidabilità della protezione, incrementando il livello di disponibilità, per esempio, perché riducono gli interventi di manutenzione, consentendo anche un controllo e un monitoraggio da remoto.

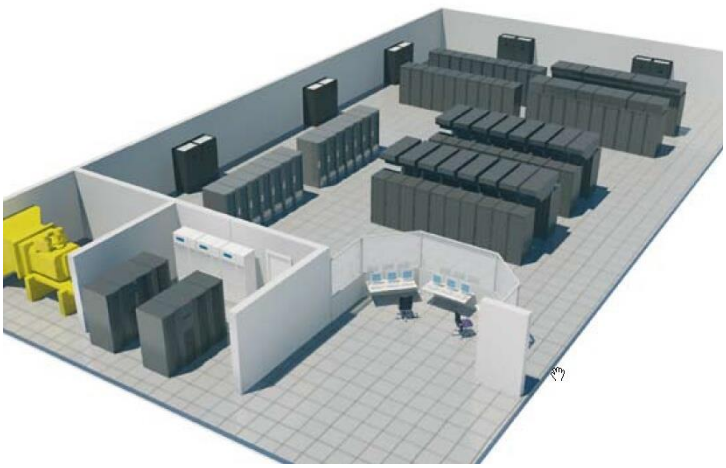
Si tratta, peraltro, di soluzioni che si basano, nella loro ultima incarnazione, su piattaforme ad alta efficienza, che permettono di aumentare la resa delle apparecchiature installate e ottenere un risparmio di fino al 50% dei costi energetici sinora sostenuti.

Anche se è difficile dire se a livello industriale l'ottimizzazione dei sistemi IT e dei consumi energetici derivi più da un amore reale per l'ambiente o da una maggior attenzione ai costi strutturali, una cosa è certa, il primo congresso mondiale sul cambiamento climatico si è svolto circa trent'anni fa e da allora è passato molto tempo.

Nel frattempo si è di molto sviluppata la consapevolezza di eco sostenibilità e di rispetto ambientale e i consumatori sono in modo crescente attivamente coinvolti nel tentativo di ridurre l'impatto sull'ambiente derivante dal costante sviluppo economico e dei consumi nonché dalla progressiva antropizzazione del territorio. La conseguenza è che, sia per ridurre i consumi che per mitigare l'impatto ambientale (riferito in letteratura, soprattutto anglosassone, come la carbon footprint) anche il mercato si sta sempre più orientando verso prodotti rispettosi dell'ambiente.

La necessità di soluzioni a basso consumo ed ecocompatibili deriva anche dalle normative in vigore, che interessano e coinvolgono nel processo di rinnovamento tecnologico anche quelle società che, per vari motivi, sono potenzialmente sono meno attente a questo trend evolutivo.

Uno degli ambienti che maggiormente possono essere interessati dalle normative, oltre che dall'interesse a ridurre i consumi anche per motivi di budget, è proprio quello dei data center.
Va osservato che minori consumi espongono anche a minori rischi per quanto concerne la mancanza di energia necessaria al funzionamento, implicano l'uso di macchine meno esigenti dal punto di vista dimensionale e in sostanza quello che ne deriva sono strutture che risultano meno critiche e più sicure
Non stupisce quindi che aziende del settore abbiano avviato la definizione di nuove architetture per quanto concerne i sistemi di supporto alle macchine IT (in particolare per l'alimentazione e la dissipazione del calore) che hanno l'obiettivo di ottimizzare il consumo globale, che inizia con i risparmi delle apparecchiature IT e si estende alle infrastrutture in modo da dare il via a un risparmio in cascata. Grazie alle nuove soluzioni l'impatto è significativo sia per quanto concerne data center di grossa dimensioni che, soprattutto, per quelli di medie e piccole dimensioni, che meglio corrispondono alla realtà del tessuto industriale italiano. Chi gestisce, e anche chi progetta Data Center, si trova continuamente alle prese con l'esigenza di far fronte a carichi più elevati e il disporre, ai costi attuali, di soluzioni che permettono di ripagare un investimento in server o altri apparati IT con il risparmio energetico ottenibile nel loro ciclo medio di vita è di certo attraente.



Struttura e disposizione tipica di un data center

In sostanza, con le soluzioni ora disponibili sul mercato è possibile ridurre i costi energetici fino al 50% senza per questo impattare su affidabilità e performance.
In genere, ridurre i consumi e ridurre la produzione di calore ha invece un impatto positivo sulla durata delle macchine e quindi sulla sicurezza di poter continuare a godere delle applicazioni IT.

Come aumentare la sicurezza e ridurre i consumi

Se non il massimo dei benefici che i produttori comprensibilmente evidenziano ed enfatizzano, perlomeno una parte significativa di questi è possibile ottenerla e un insieme di regole comportamentale può essere in questo di aiuto. Per esempio:

- Utilizzare Processori di ultima generazione a basso consumo energetico.
- Adottare alimentatori per i server e altri apparati IT ad alta efficienza.
- Avere una gestione attiva delle alimentazioni.
- Realizzare ambienti server e storage virtualizzati.
- Adottare Blade Server, che possono essere singolarmente disattivati quando non utilizzati e che aumentano la sicurezza complessiva perché nativamente ad alta ridondanza.
- Ottimizzare le unità per il condizionamento (per esempio adottando condizionatori a resa variabile).
- Optare, quando possibile, per soluzioni ad alta densità.
- Monitorare in modo attivo i sistemi di condizionamento.

L'importanza per la sicurezza e per l'ambiente che deriva da una elevata efficienza di un data center ha fatto si che associazioni di settore, consulenti e venditori abbiano promosso delle best practice a cui si può fare riferimento per migliorare l'efficienza energetica di un data center.
Si tratta di regole che prendono in considerazione diversi aspetti quali, per esempio, il tipo di illuminazione o il sistema di raffreddamento e che offrono alle aziende, qualora adottati, la possibilità di invertire o perlomeno rallentare il gradiente di incremento del consumo energetico del proprio data center.
Se l'efficienza energetica ha assunto un ruolo di linea guida nello sviluppo di un data center e dell'IT in generale, è però opportuno distinguere tra una

tecnologia green e una che sia sostenibile dal punto ambientale e che al contempo aumenti la sicurezza dell'ambiente IT.
In particolare, mentre un apparato green rappresenta un intervento una tantum, quest'ultima si basa invece su una pianificazione a lungo termine e richiede investimenti in infrastrutture flessibili, anche di tipo strutturale.
A fronte di investimenti iniziali più elevati è però l'approccio che permette di ottenere nel tempo i maggiori risparmi in risorse.
Ad esempio, pensare in prospettiva vuol dire non solo ottimizzare la struttura fisica di un edificio, ma anche adottare strategie di provisioning delle apparecchiature IT nel quadro di una architettura virtuale che permette di ridurre il numero di macchine, utilizzarle invece del 20% sino all'80% o oltre delle loro capacità o sviluppare una strategia di thin provisioning delle risorse IT, una strategia cioè che permetta di approvvigionarsi degli apparati solo quando strettamente necessario.
Peraltro, è una strada facilmente percorribile adottando le soluzioni più recenti che sono state sviluppate proprio per permettere la realizzazione di ambienti server e storage virtuali.
Esempi sul campo hanno ampiamente dimostrato come sia possibile ridurre di un ordine di grandezza e anche oltre le macchine server e storage necessarie al funzionamento delle applicazioni, ottenendo contemporaneamente una base elaborativa per le applicazioni business estremamente sicura e performante, che maschera all'utilizzatore l'improvviso fuori servizio di un server perché l'applicazione può essere trasferita in modo trasparente per il fruitore su un'altra macchina simile, il tutto in modo automatico.
Un medesimo discorso vale per lo storage o per le soluzioni di business continuity che prevedano data center distribuiti sul territorio anche a grandi distanze geografiche.
In pratica, quindi, la virtualizzazione di server e storage e le tecnologie che la rendono possibile, a partire dai processori di base, associate con il concetto di thin provisioning, permettono alle aziende di consolidare i propri sistemi e accrescerne le possibilità d'utilizzo, riducendo in modo significativo l'ammontare dell'energia richiesta per il loro funzionamento e, come conseguenza diretta, per la climatizzazione.

Se si considera che l'ammontare di energia richiesta per far funzionare gli apparati (compreso quelli che l'energia la generano) corrisponde grosso modo a quella richiesta per il condizionamento il risparmio che se ne ottiene è quindi doppio.

Ottimizzare la climatizzazione e ridurre i costi e i fuori servizio

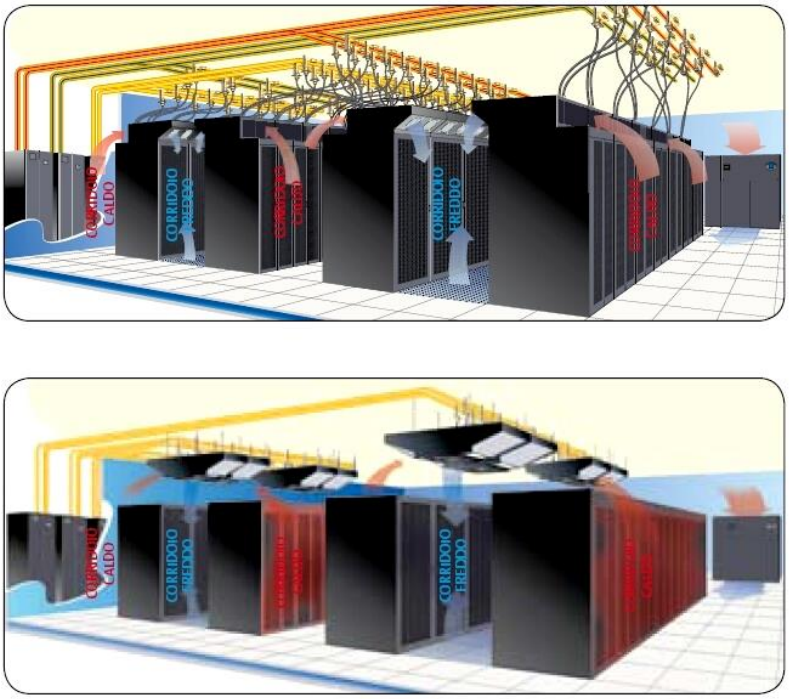
Il problema della ottimizzazione della climatizzazione non è sorto di recente. È sempre esistito. Solo che sinora la tecnologia a disposizione e i metodi di controllo non permettevano di procedere in modo puntuale e analitico come è invece ora possibile.
In molti data center best practice per la climatizzazione sono già state poste in pratica o sono in via di attuazione, tra queste la disposizione dei rack e degli armadi a corridoi alternati caldo/freddo.
Esistono però altre possibilità di intervento, per esempio prevedendo l'installazione di pannelli di chiusura degli spazi liberi fra i diversi armadi in modo da evitare che vi sia la miscelazione fra l'aria calda e quella fredda. L'ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers) ha pubblicato in proposito numerosi articoli relativi a tali pratiche.
Applicando questi suggerimenti in fase di costruzione del proprio data center è possibile incrementa quasi del 5% la sua efficienza energetica, con una riduzione che è stimata nell'ordine dell'1% nei costi dei sistemi ausiliari, e questo senza che sia richiesto alcun investimento in nuove tecnologie.
Un secondo punto riguarda poi il problema della resa dell'impianto.
I sistemi di climatizzazione dei data center sono dimensionati, come avveniva per i server prima della virtualizzazione e dello sviluppo di sofisticati sistemi di gestione automatica) per far fronte ai picchi di carico, eventualità questa che si presenta raramente ma che non si può ignorare, anche se il sistema di climatizzazione ambientale normalmente non funziona a pieno carico.
I fattori sono diversi. per esempio, le condizioni ambientali esterne variano sia nel corso della giornata che delle stagioni, il carico termico di server e storage è funzione del loro grado di fruizione, oppure può cambiare il grado di umidità per cui le unità di climatizzazione sono state dimensionate.

L'insieme di questi motivi porta a un sovradimensionamento rispetto alle esigenze reali che si traduce in macchine più grosse e potenzialmente più critiche. Lo sviluppo di nuove soluzioni tecnologiche affronta proprio questi problemi e consente, per esempio, di disporre di alte efficienze anche con carichi parziali, il tutto anche tramite un controllo più preciso e accurato della temperatura ambientale.
Ad esempio, la compressione di tipo Digital Scroll rispetto a quella tradizionale permette di spostare dal tipico 20% a un 50% il coefficiente di rendimento della potenza erogata. Recenti tecnologie hanno permesso di spostare ulteriormente verso l'alto il grado di rendimento, per esempio riducendo il numero di avviamenti del compressore, un fattore che contribuisce a incrementare l'efficienza energetica e a prolungare significativamente la vita del sistema.

Il problema dei blade e dell'alta densità

La diffusione dei blade ha aperto la strada alla virtualizzazione delle risorse e al forte incremento della sicurezza per quanto concerne la continuità operativa.
Esiste però l'altra faccia della medaglia. La necessità energetica e il corrispondente carico termico che in passato si trovava in un intero Data Center viene ora a trovarsi concentrato in un solo armadio. Una spinta in tale direzione è stata data dalla disponibilità di tecnologie server a blade, ovverossia delle schede che possono essere inserite in un rack con una elevata densità e che possono alloggiare un numero elevato di processori multicore. La capacità di calcolo concentrata in una sola scheda è enorme, ma altrettanto lo diventa l'esigenza di energia per funzionare e il calore prodotto nonostante l'adozione di processori a basso consumo di ultimissima generazione.
Quello che ne deriva è che si creano delle zone ad alta densità di calore che necessitano non solo di sistemi di alimentazione più potenti ma soprattutto di un tipo di condizionamento specifico, perché quelli usuali richiederebbero uno spazio di molti metri quadrati.
In sostanza, ci si deve spostare da sistemi di tipo tradizionale (a 3kW per rack) ad ambienti che possano supportare densità molto più alte di fino a 30 kW o oltre. Ciò ha richiesto ai produttori un approccio nuovo, per esempio con unità centrali e supplementari che possano essere installate direttamente sopra o a

fianco degli armadi che alloggiano gli apparati che costituiscono la sorgente del carico termico.

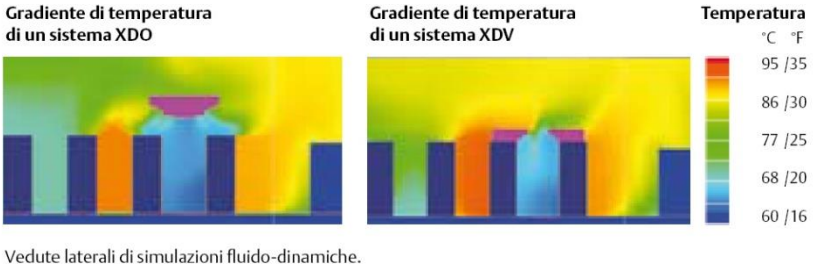


Posizionamento del condizionamento e flussi d'aria

Secondo dati dei costruttori, queste unità supplementari, confrontate con i sistemi tradizionali, permettono di ottenere una riduzione anche del 30% dei costi per la climatizzazione.

In sintesi, il risparmio deriva dal fatto che erogando la potenza termica dove è necessaria è possibile ridurre la potenza elettrica dei ventilatori che movimentano la portata d'aria in gioco.

La mossa dei produttori è consistita quindi nello sviluppo di unità di nuova generazione molto compatte che possono essere anche montate a soffitto e riprendono l'aria dai corridoi caldi e mandano aria fredda nei corridoi freddi dove sono installate. Si tratta di soluzioni che abilitano un forte risparmio energetico e non occupano spazio utile per l'installazione di altri armadi di apparati server o storage.



Vedute laterali di simulazioni flusso dinamiche che evidenziano l'importanza di interventi di condizionamento puntuale

Altre soluzioni prevedono invece l'utilizzo di moduli che possono essere posti in linea con gli armadi. In questi casi l'aria che proviene da un corridoio caldo entra nella parte posteriore dell'unità, viene trattata e mandata nel corridoio freddo.

Monitorare e controllare l'ambiente per un IT sicuro

Anche se le più recenti architetture IT si basano su dispositivi storage, server e di rete con fattore di forma a blade, esiste comunque una certa disomogeneità tra quello che ancora è installato e allocato nei diversi armadi di un data center.
La diversità di apparati, con volumi, fattori di forma e caratteristiche fisiche ed elettriche diverse, è una delle cause di una parte dell'aumento dei carichi termici che l'armadio o il rack sopporta.
Questo perché è la non uniformità stessa che impedisce una circolazione ottimale dei flussi di raffreddamento e di estrazione anch'essa ottimale dei flussi caldi. Peraltro, a secondo del grado di utilizzo e senza interventi di ottimizzazione, ciò può causare pericolosi sovra riscaldamenti e portare a un cattivo funzionamento degli apparati e dei processori che li equipaggiano, sino a giungere, nel peggiore dei casi, al loro fuori servizio.
È per questo che soluzioni recenti di monitoraggio e controllo prevedono la distribuzione di sensori nei diversi punti di un data center e all'interno degli armadi stessi, sensori che si affiancano anche ai sensori che sono presenti in processori di ultima generazione o negli apparati, siano essi a blade o di tipo più convenzionale.
La funzione di questi moderni sistemi di controllo del raffreddamento è di monitorare in tempo reale le condizioni termiche dei data center, coordinare le

attività delle varie unità che forniscono il condizionamento, evitando conflitti e abilitando una raccolta di informazioni centralizzate che possono essere fruite integrandole con quelle inerenti lo stato di funzionamento (o di malfunzionamento) di server e storage.
In pratica, è possibile correlare il degrado delle prestazioni di un server e dei suoi processori con la condizione termica dell'armadio in cui questo server è allocato e avviare rapidamente, manualmente o automaticamente, gli interventi necessari a risolvere il problema. per esempio aumentando esclusivamente in quell'armadio il flusso di raffreddamento o diminuendo la velocità di funzionamento dei processori che lo equipaggiano.

Architetture tradizionali per il disaster recovery

Il problema della sicurezza di funzionamento, e cioè la continuità operativa e la disponibilità dei dati, oltre che su un impianto infrastrutturale adeguato si basa anche su una architettura informatica che permetta di salvare in modo sicuro i dati e ripristinarli quando necessario e, a causa di un disastro naturale o di un semplice errore, siano andati persi.
Correlato alla continuità di funzionamento vi è quindi il problema di come far fronte a disastri che minino in parte o in toto la disponibilità dei dati aziendali e la continuità di un'elaborazione degli stessi.
Una tale considerazione porta, immediatamente, a cercare di stabilire cosa rientra nella definizione di disastro che infici la sicurezza della continuità operativa e, soprattutto, in quali condizioni si verrà a trovare l'azienda al suo verificarsi, ammesso che sia in grado di sopravvivere allo stesso.
Non che definire cosa si intende per disastro sia facile. Si può però essere fondamentalmente d'accordo nel considerare in questa categoria eventi come lo Tsunami in Thailandia, l'uragano Katrina a New Orleans o il tragico attentato alle Torri Gemelle di New York.
Se l'elemento più appariscente che costituisce il denominatore comune è l'impatto che hanno avuto sulla vita umana, perché immediato, non va tuttavia trascurato l'effetto a lungo termine costituito dalla minaccia alla continuazione dell'attività delle aziende coinvolte, che possono anche non sopravvivere. L'alluvione di Genova, il terremoto in Emilia Romagna o il blocco dell'autostrada per la protesta degli autotrasportatori, anche se, fortunatamente, non hanno

presentato un conto salato in vite umane, hanno comunque avuto un impatto sul business.

In effetti, la sicurezza di un'azienda non sempre viene messa a così dura prova e la maggior parte delle minacce si manifesta su una scala di gravità minore. Per esempio, sotto forma di guasti hardware, di errori nelle applicazioni o di errori operativi da parte degli addetti che causano il crash dei sistemi e la conseguente indisponibilità delle informazioni.

Poiché questi eventi non possono essere del tutto evitati, la capacità di un'azienda di contenere queste minacce dipende essenzialmente dal suo stato di preparazione, in quanto buona parte dei potenziali malfunzionamenti derivanti da un evento catastrofico possono essere evitati con un'adeguata pianificazione, implementazione e sperimentazione di un adeguato piano di emergenza.

Un piano accurato del tipo "what if" può assicurare la continuità operativa (Business Continuity Plan, in sigla BCP). In sostanza, un BCP consiste in un'analisi sull'impatto sulle proprie attività (in inglese BIA, acronimo di Business Impact Analysis) e nella elaborazione di adeguati piani di disaster recovery. Un tale approccio permette a una azienda di incrementare la garanzia della continuità operativa al verificarsi di eventi critici, che possano porre in forse servizi o intere infrastrutture.

A prescindere dalle sue dimensioni, un'azienda che abbia predisposto degli interventi significativi per assicurare la continuità operativa è pronta ad affrontare eventuali eventi calamitosi, grandi o piccoli che siano.

Va però osservato che, anche se sono le catastrofi maggiori che attirano l'attenzione dei media, tra gli eventi potenzialmente rischiosi vanno annoverati sia i guasti minori dell'hardware quanto gli errori umani dalle conseguenze gravi. Peraltro, eventi qualificabili come vere e proprie catastrofi sono usualmente l'eccezione mentre generalmente i motivi di un fermo di sistemi e applicazioni sono, nell'ordine:

- errori operativi (40%);
- errori hardware (40%);
- malfunzionamenti applicativi (12 %);
- disastri (5 %);
- altre cause ambientali (3 %).

L'esperienza sul campo indica in circa un ottanta per cento i fermi macchina provocati da malfunzionamenti dell'hardware o da interruzioni operative dovute a errori umani, anche se non ne deriva che il relativo impatto sull'azienda sia meno devastante.

Malfunzionamenti e disastri

La sicurezza di un'applicazione copre sia aspetti temporali, connessi alla sua erogazione, che topologici, connessi all'area in cui la stessa viene erogata (si tralasciano, qui, gli aspetti correlati alla sicurezza logica e le relative misure, quali crittografia, antivirus, firewalling e così via).
In entrambi gli aspetti, presi in considerazione, emerge che la prima dimensione da considerare per un malfunzionamento è la sua sfera d'interesse. Gli effetti di un malfunzionamento possono avere, infatti, portata ed estensione variabili e finire con il coinvolgere e avere un impatto su una specifica applicazione oppure su un'intera area geografica della rete aziendale.
Gli aspetti e le problematiche attinenti alla sicurezza dei dati e al ripristino di applicazioni e sistemi di ambito locale sono usualmente note e generalmente sono risolte tramite strategie di backup e recovery atte a evitare la potenziale alterazione dei dati tramite la creazione di copie di sicurezza dei dati e delle applicazioni da conservare in un'altra sede aziendale o in apposite strutture di outsourcing. Ciò che invece spesso è difficile controllare sono le minacce alla sicurezza attinenti a un edificio o all'area geografica circostante la sede aziendale, comprendendo in questo sabotaggi, incendi, inondazioni, uragani, terremoti e mancanza di alimentazione elettrica, eventi che non a caso di solito vengono riferiti in contratti di assistenza e di garanzia come "acts of God", al fine di giustificarne l'esclusione dalla usuale responsabilità connessa alla fornitura o erogazione di un servizio.
Appare comunque evidente che un adeguato livello di sicurezza inserito in un piano riguardante un fuori servizio provocato da un disastro di portata locale o regionale deve prevedere la disponibilità di una sede alternativa, posizionata a una congrua distanza dall'area potenzialmente soggetta a un disastro.
Un secondo aspetto connesso a un guasto informatico è rappresentato dal costo dei fermi di sistema e delle relative applicazioni. Anche se i dati si riferiscono a

realtà di dimensioni medie superiori a quelle usuali europee (e italiane in particolare), un rapporto pubblicato da Contingency Planning Research in merito alle conseguenze finanziarie dell'indisponibilità delle applicazioni evidenzia come il costo dei fuori servizio possa variare in misura notevole a seconda del settore e dell'applicazione, ma che in ogni caso le interruzioni operative finiscono con l'avere un impatto significativo sulle revenue aziendali.

Impatto economico del fermo di un'applicazione

I costi riportati in tabella relativi ai fermi applicativi danno un'indicazione concreta dell'importanza di un'applicazione ai fini della sopravvivenza di un'impresa investita da un disastro e quindi dell'importanza connessa alla sicurezza nell'erogazione di un'applicazione.
Un esame più analitico permette poi di distinguere due componenti, il software infrastrutturale e i dati correnti. In linea di massima, può non essere difficile rimpiazzare
il software applicativo anche se non va sottovalutato l'insieme delle attività tecnico sistemistiche necessarie per l'eventuale personalizzazione dello stesso, prima che possa diventare eseguibile.
Discorso analogo vale poi anche per quanto riguarda i sistemi operativi e il software che gira sui server.

APPLICAZIONE	SETTORE	COSTO/ORA (in $)
Intermediazioni mobiliari	Finanziario	6.45 milioni
Autorizzazioni vendite con carte di credito	Finanziario	2.6 milioni
Pay-per-view	Media	150.000
Home Shopping (TV)	Retail	113.000
Vendite per corrispondenza	Retail	90.000
Prenotazioni di biglietti aerei	Trasporti	89.500
Vendite di biglietti *on-line*	Media	69.000
Spedizione di colli	Trasporti	28.000
Commissioni Bancomat	Finanziario	14.500

I costi di un fermo del sistema informativo per settore industriale
(Fonte: Contingency Planning Research)

Se si prescinde dalla vita umana, che ovviamente non ha prezzo, sono i dati il patrimonio più prezioso di un'azienda e, a seconda del livello di criticità di un'applicazione, cresce parimenti l'importanza di disporre di dati che siano aggiornati, vecchi anche di alcuni giorni in alcuni casi (piuttosto che non disporne affatto!) o, per applicazioni fortemente critiche, aggiornati in tempo reale.

La pianificazione alla base della sicurezza operativa

Un elemento fondamentale per la sicurezza operativa è rappresentato dalla pianificazione.
Spesso però i termini stessi del problema sono confusi e, per esempio, non sono pochi coloro che utilizzano i termini di Business Continuity Plan (BCP), Business Impact Analysis (BIA) e Disaster Recovery come dei sinonimi, quando invece tra essi le differenze sono fondamentali.
Il Business Continuity Plan, riferito a volte anche come Contingency Plan, interessa l'intero spettro di attività a partire dall'individuazione e dalla valutazione dei rischi per l'impresa, fino alla pianificazione degli interventi risolutivi o assicurativi individuati come necessari.
Interessati sono anche i meccanismi che consentano all'azienda di essere operativa (in pratica di continuare a esistere in quanto tale) sia nella fase di recovery sia durante il ripristino dell'operatività vera e propria conseguente al verificarsi di un disastro.
È nel piano di continuità che un'azienda valuta tanto la probabilità dei diversi scenari, quanto il livello di tolleranza nei confronti dei costi relativi agli interventi pianificati.
La Business Impact Analysis è invece un elemento chiave all'interno del Business Continuity Plan che prende in considerazione le diverse tipologie di eventi distruttivi, in modo da quantificare e qualificare quello che si ritiene necessario fare per evitarli.
Il Disaster Recovery è un ulteriore elemento in gioco al fine di assicurare l'operatività aziendale e consiste in un piano operativo quanto più dettagliato possibile che illustra come reagire in presenza di un disastro e come procedere nel ripristino dei sistemi critici, privilegiando aspetti quali la rapidità, l'efficienza e l'economicità.

Il Business Continuity Plan

La realizzazione del Business Continuity Plan (BCP) è una attività che può essere gestita internamente in azienda oppure affidata a consulenti esterni che siano esperti nella pianificazione. In entrambi i casi coinvolge in modo esteso hardware, software, dati, infrastrutture, personale e applicazioni.
Il punto di partenza consiste nell'analisi dettagliata dell'asset aziendale al fine di individuare i processi critici per l'operatività aziendale stessa e cioè, in sostanza, i processi da ripristinare prioritariamente entro un intervallo di tempo molto breve, per esempio le quattro ore. La selezione ha l'obiettivo di consentire la classificazione di applicazioni e processi sotto il profilo della loro priorità a seconda dell'urgenza con cui devono essere ripristinati nonché di contenere i costi stessi del ripristino. Un ripristino immediato, ovviamente costoso, riguarda in genere le applicazioni contenenti dati che servono a erogare servizi ai clienti esterni, come per esempio avviene in ambienti bancari per quanto riguarda operazioni di sportello o applicazioni connesse al pagamento mediante carte di credito e terminali Eft-Pos e ATM. Il BCP deve considerare anche quanto connesso ai sistemi trasmissivi, alle strutture alternative, per arrivare sino alla sicurezza dei dipendenti. Definire un piano ottimale è però solo il primo passo, necessario ma non sufficiente. La garanzia (ragionevole) di una sua riuscita richiede che lo stesso sia noto e accettato da tutto il personale coinvolto.
Gli elementi che ne determinano il successo possono essere riassunti nei seguenti punti:

- Presa visione e accettazione da parte del Management
- Analisi e riduzione dei rischi
- Valutazione di minacce, risorse e alternative potenziali
- Business Impact Analysis con la quantificazione degli impatti operativi, finanziari, legali e normativi
- Strategie di ripristino (dispiegamento delle risorse atte a garantire la continuazione delle funzioni aziendali in caso di disastro; elaborazione e documentazione di un piano; identificazione della sfera di influenza; individuazione della linea di comando; istituzione delle procedure).
- Opera di sensibilizzazione, addestramento, implementazione e aggiornamento periodico

La Business Impact Analysis

La Business Impact Analysis è il primo step nella definizione di un piano di continuità e consiste in un processo che consente all'azienda di definire, quantificare e classificare le proprie esigenze in base all'importanza che rivestono per la strategia di business continuity.

L'analisi che viene realizzata consiste, in essenza, nel porre delle domande e trovare delle risposte. Nel caso dell'IT, l'analisi ha l'obiettivo di valutare i rischi relativi ad apparecchiature, applicazioni e dati e di rispondere a domande quali:

- Quali sono le funzioni aziendali veramente critiche?
- Quale è il costo di ogni ora in cui viene meno una determinata funzione aziendale?
- Quant'è il peso dell'e-commerce per l'impresa?
- Qual è il suo attuale stato di preparazione?
- Con quale rapidità e in quale ordine devono essere ripristinati i vari sistemi?

L'elenco, non esaustivo, serve a stabilire quali sono le attività critiche, quelle importanti e quelle che possono essere procrastinate senza pregiudicare l'operatività aziendale. In pratica ciò vuol dire identificare le aree dove concentrare, inizialmente, le risorse umane e finanziarie.

Una tale attività, proprio per il tipo di risorse che coinvolge, nel momento in cui sono definite le priorità, richiede il coinvolgimento del top management e questo non solo per gli aspetti connessi ai budget da allocare da parte delle diverse divisioni, ma anche per assicurare il sostegno di tutta l'azienda a tutti i livelli, che è opportuno non dare per scontato.

Scegliere la gerarchia di sicurezza e di ripristino: RTO e RPO

Nel ripristino di sistemi e applicazioni è di estrema importanza definire una gerarchia ben precisa. Una tale gerarchia può essere costruita analizzando la quantità, il tipo e il valore del software e dei dati presenti in impresa, classificando ogni componente in ordine d'importanza e tenendo conto del potenziale impatto finanziario che la indisponibilità di un elemento o di un insieme di elementi (dati, apparati, eccetera) finirebbe con l'avere sull'organizzazione. In questa costruzione gerarchica e in presenza di una realtà operativa permeata da Internet, alcune

applicazioni e dati devono essere costantemente disponibili, cosa che implica maggiori complessità, un maggior dispiego di risorse e, di conseguenza, maggiori costi. In generale, più pressante è l'urgenza più elevato è il costo di un ripristino. Uno schema di classificazione di applicazioni, dati, funzioni e processi in ordine di priorità può per esempio basarsi su un'esigenza di disponibilità temporale. Per esempio, con insiemi di processi per cui si richiede una disponibilità:

- immediata,
- entro le 4 ore
- in giornata o entro le 8 ore
- entro le 24 ore
- entro le 72 ore
- oltre le 72 ore

In pratica, si tratta di definire un parametro noto come Recovery Time Objective (RTO), cioè entro quanto tempo un determinato servizio di business deve essere ripristinato. Non si può effettuare un calcolo approssimativo, perché anche solo un millesimo o un centesimo percentuale di disponibilità corrisponde a una differenza dell'ordine di centinaia di migliaia di euro.

Modalità di protezione dei dati

Una classificazione può poi essere fatta anche raggruppando i dati per categoria d'appartenenza suddividendoli in insiemi comprendenti:

- Dati critici: funzioni appartenenti al livello più costoso che comprendono sistemi, applicazioni e dati cruciali per l'operatività aziendale, utilizzati nei processi strategici chiave oppure obbligatori per legge.
- Dati vitali: è meno oneroso rispetto ai dati critici ed è un gruppo che include dati e/o applicazioni senza i quali l'azienda è in grado di operare per brevi periodi di tempo. In questa categoria rientrano i dati utilizzati nei processi aziendali standard o che rappresentano un investimento significativo e sono difficili da ricostruire.
- Dati nevralgici: sono considerati nevralgici i dati utilizzati nelle operazioni quotidiane per i quali esistono, tuttavia, delle fonti alternative, così come quelli ricostruibili con una certa facilità.

- *Dati non critici*: sono dati ricostruibili a un costo molto basso e includono gli elementi già duplicati che hanno bassi requisiti di sicurezza.

Un'analisi efficace permette di identificare le risorse necessarie a gestire le funzioni critiche sia nel breve che nel lungo periodo, individuando le risorse necessarie per far passare l'azienda dalla fase di ripristino a quella di normale attività.

Si tratta di definire un parametro normalmente indicato come RPO (Recovery Point Objective): identificare, in sintesi, quali punti del sistema informativo sono più critici, quali servizi più importanti per il business.

Determinata la portata della propria vulnerabilità, un'azienda può decidere di adottare dei provvedimenti atti a farvi fronte. Approcci tattici di tal genere ne sono stati sviluppati diversi e sono alla base degli interventi da parte di società specializzate nei sistemi operativi o in settori pesantemente coinvolti nella sicurezza aziendale dei dati, come quello dello storage, dove alcune società hanno già maturato una consistente esperienza in proposito.

Il piano deve contemplare la conservazione di copie multiple dei dati in diverse località geografiche a una certa distanza di sicurezza dalla sede principale, da stabilire in base alle probabilità di un sinistro; per esempio, le misure da adottare in previsione di un incendio non richiederanno la stessa distribuzione geografica necessaria per un sisma o un uragano.

Altrettanto critica è la sostituzione dell'infrastruttura informatica primaria. Le copie dei dati critici sono di ben poco valore, se poi non esistono apparecchiature su cui utilizzarle: server, storage, reti e configurazioni devono essere disponibili entro un lasso di tempo ragionevole.

Una volta disponibile l'infrastruttura IT, si devono ripristinare i processi critici del business per consentire la ripresa del servizio alla clientela.

Ma quali sono gli elementi di un recovery? Applicazioni ad alta criticità, come i database, possono richiedere un hot site dotato di energia elettrica, apparecchiature e funzionalità di comunicazione.

A questo scopo alcune aziende preferiscono utilizzare delle strutture secondarie predisposte in maniera pressoché identica al CED principale, con i dati che vengono trasferiti elettronicamente dal centro primario a quello ridondante con metodi diversi.

In alcuni casi i locali secondari ospitano delle applicazioni attive in un'ottica di load sharing dove i dati, come quelli transazionali, vengono spostati dinamicamente dal centro primario a quello ridondante. Sotto questo aspetto, la sicurezza dei dati ha visto di recente affermarsi due meccanismi per proteggere i dati in un sottosistema a dischi: lo shadowing e il mirroring.
Lo shadowing è un processo di natura asincrona che mantiene una replica dei database e dei file system (che definiscono il metodo per archiviare e recuperare i dati) rilevando in continuo eventuali modifiche che verranno successivamente applicate alla copia presente nel centro di recovery. I tempi del ripristino si riducono notevolmente, tipicamente fino a uno/otto ore, a seconda del tempo richiesto per l'applicazione dei file di log.
Il mirroring mantiene, invece, una replica dei database e dei file system applicando eventuali modifiche al centro di backup in modo sincrono rispetto a quelle apportate presso il centro principale. In questo caso, un'operazione di I/O si considera completata non appena viene aggiornata la copia primaria, mentre la copia secondaria può anche essere aggiornata in un secondo tempo.
Ne risulta una riduzione dei tempi di recovery compresa tra 20 minuti e alcune ore, mentre il ripristino dai file di log si limita alla sola perdita delle transazioni non portate a termine. Il mirroring richiede una banda trasmissiva significativamente più ampia rispetto allo shadowing; se l'ampiezza di banda è troppo esigua o le latenze troppo elevate, la performance dei sistemi di produzione risulta degradata. Questo è il motivo per cui in genere non si utilizza il mirroring per ambienti caratterizzati da alti volumi di transazioni.
Il "trucco" sta nel sapere qual è il meccanismo più adatto in ogni situazione. Se la ripresa dei processi elaborativi può essere rimandata di un giorno o due, è probabilmente sufficiente un cold site in cui installare e configurare le apparecchiature solo dopo la messa in opera del piano di ripristino. Pur essendo decisamente meno costoso da manutenere rispetto a un hot site, un cold site può richiedere accordi sulla consegna delle apparecchiature con i principali fornitori dove il fattore tempo svolge un ruolo fondamentale.

Clustering e Disaster Recovery

Come evidenziato, in un numero sempre maggiore di aziende anche un piccolo downtime dei sistemi, sia imprevisto che pianificato, rappresenta un evento in

grado di avere impatto sul business in termini di fatturato o di immagine. Per queste ragioni, alta disponibilità e disaster recovery rappresentano ormai due concetti di importanza fondamentale e che si fondono l'uno nell'altro.
La scelta dell'architettura più adatta per implementare una soluzione di disaster recovery va valutata in base alla tipologia di business e di servizio erogato e cercando di conciliare le esigenze di protezione dei dati con quelle dei costi di implementazione e dell'infrastruttura disponibile
La continuità delle operazioni e il ripristino dei dati in una situazione di disaster recovery possono essere garantiti attraverso architetture di clustering implementate a livello locale, metropolitano o geografico. I differenti approcci architetturali di clustering per il disaster recovery, restano caratterizzati da specifici vantaggi e svantaggi, in relazione alla capacità infrastrutturale preesistente, ai fondi disponibili, alla quantità di dati che è ammissibile perdere e alle pianificazioni future.

Il ripristino su scala locale, metropolitana e geografica

Il primo e più semplice modo di utilizzare un cluster è a livello locale, per garantire l'alta disponibilità e il recovery dei dati in caso di failover di server, applicazioni o database.
In questa configurazione tutte le componenti del cluster risiedono all'interno di un singolo data center e tutti i nodi condividono tra loro le risorse di storage disponibili in rete.
Questa architettura permette di ripristinare le applicazioni e il database in tempi estremamente rapidi senza alcuna perdita dei dati, utilizzando le informazioni presenti sulle risorse di storage condivise.
Si tratta di un sistema adatto a fronteggiare situazioni di failover locale, legato a singoli server, ma che non è in grado di fornire protezione nel caso di incidenti che coinvolgano l'intero edificio in cui si trova il data center. In altre parole, il data center rappresenta un "single point of failure".
Per garantire una maggiore protezione delle applicazioni e ripristinare un servizio che è venuto a mancare a seguito di un disastro che ha coinvolto l'intero data center è necessario prevedere la presenza di un secondo sito, che possa entrare in funzione e sostituire le funzioni del primo. Quando si considera un

sito preposto alla funzione di disaster recovery, si tende di solito a pensarlo situato a una grandissima distanza dal primo (anche migliaia di Km).
Tuttavia la maggior parte di cause in grado di mettere fuori uso un data center sono spesso confinate su distanze molto più contenute. Si può pensare, per esempio, a blackout prolungati, incendi, allagamenti o crolli.
Per garantire funzioni di disaster recovery su distanze che rientrano, per esempio, nei confini di una stessa città, è possibile utilizzare un'architettura clustering a livello metropolitano. Si tratta di una soluzione che prevede, in un certo senso, di estendere al di fuori dell'edificio il concetto di cluster locale, realizzando una connessione in fibra ottica che collega due o più cluster.
Poiché, topologicamente, si tratta ancora di una stessa sottorete, esiste un limite sulla massima distanza che separa i due siti determinato dalla tecnologia Fibre Channel (FC). Questo tipo di architettura si adatta a casi in cui esiste già una infrastruttura SAN FC e permette di scalare facilmente verso una soluzione più completa di disaster recovery.
Prevede il mirroring remoto dei dati in modalità sincrona tra i due siti, evitando la possibile perdita di dati: se sussistono problemi sul sito principale, viene attivato quello secondario su cui sono già presenti i dati aggiornati.
Un'alternativa possibile, nei casi in cui un'azienda non preveda di installare un'infrastruttura SAN su FC, è quella di prevedere un clustering metropolitano in cui i dati vengono replicati sui nodi presenti sul secondo sito, utilizzando il protocollo IP su una connessione Ethernet.
A fronte di un risparmio nei costi questa architettura resta limitata a due siti e fornisce prestazioni di ripristino inferiori (la replicazione è meno efficiente del mirroring). Inoltre, la replica dei dati per un recovery automatico deve essere necessariamente effettuata in modo sincrono e questo può penalizzare le prestazioni delle applicazioni.
Il caso che offre la massima protezione è rappresentato da un clustering a livello geografico (Wide Area). In tal caso i due siti sono due data center distintiti, appartenenti a due sottoreti separate. I dati vengono replicati in modo sincrono o asincrono da un sito all'altro mediante una connessione IP. Nei casi in cui la replica venga fatta in modalità asincrona esiste la possibilità di perdita di parte dei dati.

Una tale architettura ha il vantaggio di offrire massima protezione anche da disastri che avvengono su scala metropolitana (per esempio terremoti di grandi proporzioni, zone di guerra); la scelta del sito secondario dovrebbe, pertanto, essere scelta in modo accorto, evitando per esempio, di collocarsi sulla stessa dorsale di alimentazione elettrica, piuttosto che vicino ad aeroporti o zone critiche. Questo tipo di architettura è molto costosa e viene di solito implementata da società che sono obbligate a farlo per soddisfare requisiti legali o governativi.
L'esigenza di fornire soluzioni di protezioni di questo livello e, nel contempo, di contenere i costi, può indurre a considerare la possibilità di utilizzare sedi distaccate all'estero per realizzare un'architettura di clustering di tipo geografico.

L'aspetto economico di una soluzione tradizionale

Fondamentale, in quanto connesso alla sicurezza operativa, è l'aspetto economico. Oggigiorno, la maggior parte delle attività informatiche necessita di una soluzione equilibrata che supporti una molteplicità di applicazioni mission-critical e ausiliarie. Per soddisfare nel modo ottimale i fabbisogni finanziari e i requisiti di trasferimento e riduzione dei rischi è quindi indispensabile prendere in considerazione un insieme di alternative che vanno dai servizi di outsourcing a quelli di gestione remota .
Le applicazioni mission-critical a impatto elevato e i database che richiedono installazioni hot site ricavano un consistente beneficio da funzioni di mirroring elettronico in tempo reale. Le soluzioni di virtualizzazione storage che si sono diffuse sul mercato negli ultimi tempi e che utilizzano il meccanismo PPRC (Peer-to-Peer Remote Copy) sono, per esempio, in grado di soddisfare i requisiti di piani di ripristino mission-critical in hot site, soprattutto per la loro capacità di eseguire il mirroring dei dati compressi e ridurre gli overhead quali i dati sullo spazio libero occorrente.
Le soluzioni costituite da nastroteche automatizzate sono un altro metodo molto conveniente per archiviare grandi quantitativi di dati nel raggio di una vasta area geografica. Rimovibili e trasportabili, le soluzioni basate su nastri sono disponibili sul mercato per ogni livello di esigenza, a partire dalla fascia bassa fino a nastroteche dal mirroring completo con capacità pressoché

illimitata. Le nastroteche possono anche avvalersi di soluzioni di virtual storage management usate per creare unità a nastri virtuali, cosa che permette di risparmiare sui costi, ridurre i tempi e semplificare la gestione.
Nel caso di applicazioni con minore impatto sul business si può poi optare per soluzioni quali gli Automated Cartridge System, che assicurano la ridondanza dei dati a prezzi molto convenienti. In caso di interruzione, le copie su nastro sono subito disponibili presso il centro di recovery, cosa che elimina la necessità di farsi inviare le copie da un centro gestito da terze parti.
Funzioni ora disponibili, quali la migrazione automatica dei dati dai dischi ai nastri, consentono anche di eseguire in modo economico il backup articolandolo su diverse generazioni. Va infatti considerato, quando si parla di dati, che nel caso dei dischi gli errori o i problemi di corruzione dei dati primari vengono automaticamente riprodotti nelle copie remote, per cui gli utenti possono essere costretti a risalire di diverse generazioni, prima di trovare una copia integra dei dati. Con i nastri, invece, le copie multigenerazionali sono poco costose e si recuperano rapidamente.

Software di gestione

In caso di un evento catastrofico che porti alla perdita di dati, il software svolge un ruolo sempre più chiave nel trasferimento rapido dei file, perché consente di ripristinare anche file di grandi dimensioni nel giro di pochi minuti. Recenti rilasci sfruttano in modo intensivo gli sviluppi che si sono avuti nella virtualizzazione dello storage per automatizzare la gestione e il recupero dei dati all'interno della gerarchia di storage. Il tutto si basa su apposite policy definite dagli utenti per scaricare i dati dalla cache su disco ai nastri in modo da creare copie multiple per il centro primario, il "caveau" e l'archiviazione in remoto.

Data Center remoti e backup in outsourcing

La tendenza ad affidarsi a servizi esterni per quanto riguarda applicazioni anche critiche, come il backup, discende dalla complessità di gestione e, soprattutto, dalla maggiore efficacia che una soluzione appoggiata al data center di un provider remoto può garantire.
La crescente dipendenza dai sistemi informativi delle imprese, del resto, rende fondamentale l'efficienza della protezione: backup e restore non possono

essere trascurati, come troppo spesso si faceva in passato, né, per molte realtà, risultano accettabili tempi lunghi.
Fino a non molti anni fa, le finestre notturne erano sufficienti a coprire le esigenze di backup della maggior parte se non totalità delle imprese. Oggi, la crescita smodata dei dati in azienda ha finito con il rendere obsolete molte architetture e strumenti per il salvataggio dei dati. Dall'altro lato, tempi di ripristino lunghi, anche se non portano necessariamente al fallimento di un'impresa, certamente ne condizionano la produttività e rappresentano un importante spreco di risorse.
Se a questo si abbina l'opportunità d'integrare il backup con politiche di disaster recovery, che sono del resto imposte anche da precise normative di legge, ecco che si comprende il successo di un mercato emergente quale quello dei servizi di backup e disaster recovery appunto.

L'importanza del partner

Naturalmente, le imprese possono scegliere di ricorrere a un partner esterno anche solo per l'hosting di propri apparati e soluzioni, ma in ogni caso, il fornitore prescelto dovrà rispondere a precisi requisiti.
A parte il gioco di parole, è evidente che per garantire l'affidabilità di soluzioni e servizi dovrà essere affidabile, ma, nel caso si richiedano anche servizi di system integration, è necessario valutare attentamente anche l'esperienza maturata nell'implementazione di soluzioni dedicate alla gestione e al salvataggio dei dati in ambienti eterogenei. Una tale esperienza è comunque opportuna, anche solo considerando che, come per il resto del l'IT, è fondamentale gestire consolidamento, pianificazione e ottimizzazione degli ambienti di backup. Per questo, peraltro, è importante che il provider abbia una precisa esperienza nel monitoraggio e controllo del backup: dalla pianificazione (capacity planning) alla gestione della robotica e dei dispositivi (Device Management). In funzione del livello di disponibilità che ci si vuole garantire, potrà essere opportuno, oltre al valore tecnico e all'esperienza, cercare in un partner la capacità di fornire risorse e servizi dedicati, organizzazione locale, supporto 24 ore su 24 per 7 giorni la settimana e 365 giorni l'anno.
Va considerato che le soluzioni di backup e restore devono comprendere tutte le estensioni della rete, le piattaforme, i sistemi operativi e i database, oltre che

i sistemi di storage e le funzionalità software in esse integrate, garantendo in tal modo il salvataggio di tutti i dati presenti in azienda.
La protezione deve essere dettata da una politica unificata, schedulazioni automatiche e policy di protezione dinamiche. È determinante quindi il pieno supporto per i più diffusi database e applicativi presenti in commercio: tra cui, Oracle, Informix, Sybase, IBM DB2, Microsoft SQL Server, SAP R/3, Lotus Notes, Microsoft Exchange Server. Oltre che dei file system più importanti quali: Windows, Linux, NetWare, MacOS, Irix, OpenVMS, Solaris, AIX, HPUX. Per la gestione, è poi opportuno che la programmazione del backup sia gestita da un'interfaccia grafica intuitiva e flessibile.
Considerata anche la dinamicità del mercato, proprio per non dover cambiare architettura di backup alla rincorsa delle ultime tecnologie, è opportuno ricercare l'efficienza già nella scelta di un sistema di backup in grado di garantire flessibilità e affidabilità nel tempo.
In questo senso la soluzione scelta è opportuno che sia sufficientemente diffusa sul mercato perché garantisca una certa longevità e, al tempo stesso, una relativamente facile reperibilità di partner e tecnici esperti nella sua operatività.
Inoltre, è opportuno che sia indipendente, in grado cioè di garantire anche il supporto di dispositivi e applicazioni terze e la piena compatibilità con un ampio numero di piattaforme e sistemi operativi. Indipendente, ma ovviamente abilitata a utilizzare prodotti certificati e supportati dalle più importanti società del settore. Infine, è importante che la soluzione sia basata su standard e sufficientemente aperta per consentire di sfruttare sistemi e programmi sviluppati da terze parti di riferimento per il mercato del mass storage e archiviazione dati, quali applicazioni dedicate all'ottimizzazione dei processi di backup (specie in ambienti complessi) e di gestione e controllo delle attività e dell'impatto economico che l'ambiente di backup ha nel contesto complessivo aziendale.
La grande maggioranza delle soluzioni di backup o, quantomeno, tutte quelle dei principali fornitori utilizzano il modello client/server per il salvataggio dei dati e, in generale, supportano più sistemi operativi, piattaforme hardware, database e applicativi, garantendo così la massima apertura e scalabilità. Grazie a questo modello, infatti, i client e il server di backup costituiscono due ambienti

che sono funzionalmente cooperanti, condividono la stessa interfaccia grafica, si integrano a tutti i livelli e sono progettati per lavorare insieme.
L'implementazione dell'architettura, peraltro, non è così banale. È intanto opportuno che il software di backup possa essere installato su di un server collegato direttamente a tutti i nodi della rete o, laddove non sia possibile, al meno che possa raggiungerli in qualche modo. Le tecniche di virtualizzazione moderne aiutano in tal senso, ma solo nel nascondere la complessità sottostante. Il concetto è quello di realizzare una gestione integrata, che fornisce uno strumento di controllo centralizzato del backup e consente l'attuazione di procedure volte a garantire la massima sicurezza nella conservazione dei dati.
Un ulteriore vantaggio è dato dalla capacità di effettuare contemporaneamente le operazioni di salvataggio dei dati su più dispositivi di memorizzazione: sistemi RAID, NAS, DAS, CAS, soluzioni nastro, dispositivi ottici riducendo e ottimizzando la durata delle operazioni. Le esigenze prestazionali nella fase di resto re costringono a un recupero dei file salvati quanto più semplice e veloce. Per questo, è opportuno che i file memorizzati con le precedenti operazioni di backup risiedano in uno speciale database online, tramite cui è possibile rintracciare un file in pochi secondi, semplicemente specificando il nome del file o della directory. Infine, l'impiego di logiche multilivello sarà di supporto alle eventuali politiche di Information Lifecycle Management impostate in azienda.

5 - LA NETWORK SECURITY AUTOMATION

Una volta le chiamavano "autostrade dell'informazione" ed è evidente che le reti restano l'elemento abilitante per la realizzazione di qualsiasi servizio IT a supporto del business aziendale. Questo significa che devono essere intrinsecamente sicure e un elemento attivo nella protezione degli asset informativi aziendali. Pur restando il punto di accesso all'infrastruttura, però, non ne costituiscono più il perimetro. Per questo s'integrano in un contesto più ampio di machine learning per realizzare le Intent Based Network.

La sicurezza delle reti

Il problema di come impostare una strategia per l'infrastruttura di rete aziendale si abbina, in una buona parte delle realizzazioni, al modo di predisporre la migrazione e la sostituzione partendo dalla situazione preesistente e trovando il modo più adatto per perseguire una trasformazione che determini il minor impatto possibile.

Da questa esigenza specifica, ma basilare nel contesto di un'operatività aziendale che non può subire interruzioni, non possono prescindere i fornitori di piattaforme, che si trovano a dover predisporre modelli architetturali in grado di adattarsi da subito a nuove esigenze e requisiti di business, integrando l'esistente, elevando le prestazioni e mantenendosi aperti per un'evoluzione scalabile.

I requisiti sono sempre più legati ai temi di sicurezza, convergenza, gestione unificata fisso-mobile, virtualizzazione. Tutto ciò contribuisce a delineare un'evoluzione tecnologica e una strategia di trasformazione delle reti in una direzione ben identificata in grado di dare agli utilizzatori (aziende e operatori) una risposta alle loro necessità.

Il legame tra requisiti applicativi caratteristiche dell'infrastruttura di rete e un progressivo orientamento verso un modello orientato ai servizi ha portato l'approccio al networking sempre più vicino a quello dell'IT. Per questa ragione perseguire un approccio che punti semplicemente alle prestazioni può rappresentare, ora più che mai, una scelta miope. Per esempio l'aspetto della semplicità e dell'unificazione gestionale diventa sempre più importante. Per le aziende semplificare le reti significa poter ridurre sostanzialmente i costi di manutenzione, incrementare i servizi esistenti offrendone altri multimediali e integrati, incrementare l'affidabilità e il controllo. Ciò che a volte si sottovaluta è quanto questi aspetti (si pensi per esempio alla semplificazione) contribuiscano anche in modo significativo ad aumentare la capacità di controllo del rischio e favorire un maggiore livello di sicurezza.

A livello di sicurezza, la crescente sofisticazione degli attacchi e il fatto che questi avvengano tramite una rete trasmissiva obbligano il manager dei sistemi informativi a considerare quali possono essere le soluzioni al problema in termini progettuali, le strategie da attuare e la localizzazione più adatta degli

strumenti e delle applicazioni che a questi attacchi si devono opporre. In pratica, sia che si tratti della rete di un carrier, di una rete virtuale privata (VPN) o di una rete aziendale, il problema consiste nell'abbinare le funzioni di sicurezza con quelle di trasporto della rete in modo che le stesse risultino sinergiche ed efficaci, idealmente massimizzando i livelli sia di protezione sia di servizio.
Un ulteriore elemento in grado di caratterizzare il modello architetturale e condizionare l'efficacia di una rete a supportare innovativi modelli di business è la capacità di implementare un livello di intelligenza e di distribuirlo in base agli specifici requisiti di business. Per queste ragioni, sempre più spesso, le funzioni di sicurezza sono affidate a dispositivi posti sulla rete e integrati con quelli preposti a realizzare le funzioni di switching e routing, mentre cresce la diffusione di appliance dedicate, pronte a integrare all'interno di quelli che in passato erano semplici switch (anche periferici) una serie di funzionalità in costante evoluzione. Tutto ciò si va sempre più combinando con modelli as a service e "cloud based".

L'evoluzione della network security

A monte di qualsiasi progetto per la sicurezza è necessario effettuare un'operazione culturale. Errare humanum est e appunto sfruttando l'ingenuità, l'ignoranza o comportamenti irresponsabili dei dipendenti, gli "attacker" penetrano nei sistemi e reti aziendali.
Negli anni sono aumentati gli attacchi perpetrati attraverso il social engineering. È facile credere a una mail che arriva apparentemente da un dirigente aziendale con un tono minaccioso e quindi cascare in trappole tese da un malintenzionato che era riuscito a impossessarsi di un paio di informazioni, magari raccolte su un sito di social networking, dove in molti si confessano liberamente. Il phishing, in particolare, è nato proprio con il concetto di sfruttare l'ingenuità delle persone e, utilizzando tecniche di spamming, colpisce sempre più facilmente nel segno. Statisticamente, inviando centinaia di migliaia di e-mail, c'è certamente qualcuno che crede a messaggi sempre più plausibili e clicca sul link-esca.
Le logiche dei grandi numeri fanno il resto: se "abbocca" l'1% dei destinatari (è una percentuale stimata da diversi security advisor), significa migliaia di identità elettroniche, numeri di carta di credito, password o altre informazioni rubate.

Anche percentuali inferiori portano a risultati interessanti, che spesso rappresentano solo la base di partenza per ulteriori crimini.
Conoscenza e consapevolezza riducono il rischio, ma, soprattutto nelle grandi imprese, non è facile diffondere una cultura sulla sicurezza a tutti i dipendenti. Senza contare che combattere la pigrizia e la debolezza della natura umana è una battaglia persa in partenza.
Allora la guerra va combattuta e vinta su altri terreni e, vista la sofisticazione e la crescente rapidità degli attacchi, l'unica strategia possibile consiste nell'applicare strumenti automatici.
Un esempio può aiutare a comprendere le dimensioni del problema. A partire dalla seconda metà del 2007, si è assistito all'affermazione di una tecnica preoccupante: "l'infezione" di siti insospettabili.
Su home page e pagine interne di Web facenti capo a enti governativi, università, aziende anche note sono stati inseriti link che attivano il download di codici maligni. È evidente che qui non c'entra la cultura e solo un software di protezione può impedire all'utente ignavo di scaricare malware. Peraltro, il sistema di sicurezza deve essere sofisticato e aggiornato in tempo reale: in altre parole, automatico. Altrimenti non può essere efficace. Basta infatti considerare che viene pubblicata una pagina infetta ogni 5 secondi e una percentuale sempre più alta di tali pagine appartiene a siti "innocenti".
Siti che non ricevono alcun danno e, quindi, difficilmente possono percepire che c'è qualcosa di sbagliato, almeno non in tempi rapidi. Il punto è che queste azioni sono rapidissime: viene pubblicata la pagina infetta, contestualmente vengono mandate centomila e-mail utilizzando pc "puliti" all'insaputa del proprietario (questo sì colpevole di scarsa protezione). Nel giro di pochi minuti, se non secondi, circa mille malcapitati (l'1% dei destinatari) avranno cliccato sul link trappola.
Oggi, esistono soluzioni che proteggono da tecniche come queste, ma non tutti ne dispongono. I primi passi in questa direzione sono stati compiuti con le soluzioni NAC (Network Access Control) che consentono di verificare il livello di sicurezza dei client prima di concedergli l'accesso alla rete aziendale. Ma in realtà il problema da affrontare è quello accelerare l'aggiornamento dei sistemi aziendali per diffondere la protezione a ogni sistema contemporaneamente.

Nell'ultimo periodo soprattutto tra gli ambiti emersi come i più critici nell'ambito della network security possiamo ricordare: l'esigenza di protezione degli endpoint in uno scenario di mobilità crescente, gli attacchi DDoS (Distributed Denial of Service), le minacce APT e la lotta alle intrusioni che ha portato allo sviluppo di Firewall e IPS (Intrusion prevention system) di "prossima generazione".

Controllare chi o cosa vuole entrare nella rete: i rischi degli endpoint

Il punto di partenza è che non solo qualunque utente, ma anche qualsiasi sistema dovesse chiedere accesso alla rete potrebbe portare traffico nocivo.
Abbandonando il concetto di perimetro, gli endpoint sono da sempre un pregiato oggetto di attacco. Oggi più che in passato, perché molte delle tecniche emergenti, oltre a tentare di sfruttare l'ignoranza o la disattenzione dell'utilizzatore, sono state sviluppate proprio per agganciare un "endpoint" e usarlo come chiave d'accesso al sistema aziendale. Il tutto all'oscuro del proprietario del mezzo, cui si cerca di dare meno fastidio possibile.
Per questo, l'approccio al controllo degli accessi è profondamente cambiato nel giro di pochi anni e, se in passato appariva sufficiente controllare l'identità di chi chiedeva l'accesso, oggi risulta sempre più importante verificare anche le condizioni del sistema utilizzato per il collegamento. In altre parole è opportuno capire se il computer con cui un utente si vuole connettere è dotato di quei requisiti di sicurezza che si ritengono necessari.
Questo controllo è importante tanto per il pc dell'utente occasionale (il partner, il fornitore, il cliente) quanto, anzi di più, per quello del dipendente. Non è più pensabile affidarsi alle policy aziendali, che vengono sistematicamente disattese (troppi utenti, per esempio, disattivano l'antivirus o la suite di sicurezza perché rallenta troppo le applicazioni, ancora oggi che le soluzioni sono decisamente più performanti di un tempo). Non è un caso che, negli anni, si è assistito a un proliferare delle caratteristiche di "enforcement" all'interno delle soluzioni per la protezione del pc: queste sono necessarie per obbligare l'utente a mantenere adeguato il livello di sicurezza della propria macchina. La probabilità dell'attacco e la rapidità dello stesso, infatti, non consentono di avere un pc "scoperto".

L'errore dell'utente, dolente o nolente, è statisticamente tra le principali cause di problemi per la sicurezza ed è ovvio che i malintenzionati cercheranno sempre di approfittarne. Per questi motivo, l'adozione di sistemi automatizzati per la protezione degli endpoint è diventata ancor più cruciale con la diffusione di minacce nascoste, che si annidano sul terminale per poi trasferirsi all'interno del sistema aziendale una volta che il pc si connette alla rete. Anche senza dolo, l'utilizzatore potrebbe essere il punto debole attraverso il quale viene sferrato un attacco.
Il problema ha assunto un ulteriore carattere d'urgenza, con il proliferare di sistemi portatili, spesso impiegati anche per attività personali e frequentemente collegati a reti e sistemi di terze parti, sulla cui sicurezza l'azienda fatica ad esercitare un controllo. Ma anche perché è sempre più necessario e frequente far entrare anche utenti occasionali, come partner e fornitori.

Le vulnerabilità dei sistemi SCADA

Un tema collegato alla Cyber War e al cyber terrorismo e che riguarda la network security è quello delle infrastrutture critiche che erogano servizi essenziali ai cittadini.
In particolare, il tema riguarda gli Industrial Control Systems (ICS) che sono dispositivi, sistemi, reti e controlli utilizzati per operare e/o automatizzare i processi industriali, presenti in quasi ogni settore, dalla produzione di veicoli al trasporto, dall'energia al trattamento delle acque. Gli ICS comunicano con i sistemi e le reti SCADA (Supervisory Control And Data Acquisition) che forniscono agli operatori i dati per le attività di supervisione e la capacità di controllo per la gestione dei processi.
La sicurezza di sistemi ICS/SCADA resta un tema importante perché sono comunemente utilizzati per il funzionamento di industrie di grande rilevanza e per il monitoraggio e controllo della maggiore parte dei servizi essenziali ai cittadini, come la fornitura di acqua, elettricità, gas e anche i mezzi di trasporto.
In ambito industriale i sistemi ICS/ SCADA sono utilizzati da tempo e, mano a mano che l'automazione continua a evolversi e diventa più importante a livello mondiale, la loro diffusione e importanza cresce. Una crescita a cui, purtroppo, fa eco una mancanza di protezione ben documentata e ampiamente conosciuta. È noto, per esempio, che attraverso Internet si possono effettuare ricerche che

restituiscono facilmente l'accesso ai pannelli di controllo di sistemi SCADA, l'identificazione delle macchine e delle loro funzioni. Altri siti vengono sempre più spesso utilizzati per la diffusione di informazioni legate ai dispositivi ICS/SCADA come, per esempio, i loro indirizzi IP.

Tutto ciò ha favorito e continua a favorire le azioni del cyber crimine che, negli ultimi anni, ha segnato importanti punti a proprio favore con minacce quali Stuxnet considerato uno dei codici malware più sofisticati che sia mai stato scritto.

Va rimarcato che i sistemi ICS/SCADA, sebbene simili nelle funzioni ai sistemi di ICT Security, differiscono notevolmente da questi ultimi nel modo di interpretare l'esigenza di sicurezza. La prima priorità dei sistemi IT di sicurezza è tipicamente la protezione dei dati mentre nei dispositivi ICS/SCADA si tende a privilegiare l'affidabilità e l'accessibilità dei dati per non compromettere la produttività.

Ogni sistema SCADA presenta poi caratteristiche specifiche in termini di requisiti di disponibilità, architettura, obiettivi e requisiti prestazionali e questo richiede che vengano trattati in modo unico. Solitamente i sistemi SCADA non prevedono di default la presenza di soluzioni anti malware. Questo è legato sia alla loro natura intrinsecamente legacy sia perché si tratta di macchine deputate al controllo di altri strumenti per cui una qualsiasi forma di ritardo nel calcolo computazionale introdotta da un sistema di controllo potrebbe causare inconvenienti. Per questa ragione solitamente il controllo dei sistemi SCADA viene effettuato a livello di singola macchina in modalità batch e, in molti casi, non è neppure possibile effettuare controlli in rete.

Un altro problema di cui le aziende solitamente non si preoccupano è che le macchine SCADA sono gestite e manutenute da terze parti. Pertanto, se non si ha la possibilità di esercitare un'azione di controllo sui processi di queste operatori o se non si mette a loro disposizione un sistema per effettuare un controllo in linea della macchina, il rischio di introdurre malware su uno di questi dispositivi diventa elevato.

In base a queste considerazione, l'approccio più efficace che emerge per la protezione di questi sistemi (analogo a quello utile per fronteggiare le APT) è di predisporre un modello di security intelligence in grado di fornire un

monitoraggio affidabile e continuo del comportamento di reti e sistemi per segnalare prontamente eventuali anomalie sospette.

La Intent Based Network Security

L'instradamento e il controllo della rete costituiscono attività critiche da sempre e da diversi anni si è cercato di automatizzarle. Inizialmente l'intenzione era soprattutto ottimizzare le prestazioni, ma ben presto, in parallelo, è cresciuta anche l'esigenza di protezione.

Concentrandoci su questo aspetto è facile comprendere le difficoltà iniziali nella gestione di log infiniti. L'intrusion detection e la successiva intrusion prevention si sono basate su motori di correlazione che fornivano e, in molte installazioni, tuttora forniscono una sintesi dello stato infrastrutturale, utile a prendere decisioni.

Questi strumenti sono diventati sempre più sofisticati, con SIEM (Security Information Event Manager) che integrano sistemi di analytics per gestire big data e aumentare il grado di accuratezza.

Uno dei primi problemi che le aziende si sono poste con l'apertura verso il Web è stato il controllo degli accessi alla rete aziendale, per il quale sono stati sviluppati opportuni protocolli di autenticazione.

È stato però subito evidente che dalla Rete potevano arrivare sul sistema e sul Web aziendale dei malintenzionati. Inizialmente, si temeva più che creassero danni per gioco, mentre oggi si sa che vogliono colpire in maniera mirata per sottrarre informazioni di business da rivendere o sfruttare ai propri fini.

Sono nati i firewall, che si preoccupavano di "chiudere" alcune porte della rete, permettendo il passaggio solo di "traffico giusto". Nel corso del tempo, tuttavia, i firewall di tipo tradizionale si sono dimostrati inadatti a filtrare in modo efficace il traffico di rete per bloccare le minacce avanzate che sono diventate anche capaci di eludere, con piccole modifiche al codice, il sistema di rilevazione degli IPS tradizionali, basato sulla corrispondenza tra "signature" di sicurezza ed exploit.

L'evoluzione del firewall

I firewall sono nati nei primi anni '90 con lo scopo di controllare il traffico in ingresso e lasciar passare solo quello "lecito", in linea generale verificando la correttezza dei protocolli. Da un'azione sostanzialmente di monitoring si è rapidamente passati ad attuare dei controlli via via più accurati. Sono così arrivati diversi tipi di firewall.

Firewall packet filtering
Nei primi anni ’90 è stata commercializzata una delle prime tecnologie firewall (filtraggio dei pacchetti), che veniva integrata principalmente nei router e negli switch per filtrare determinati protocolli e indirizzi IP. Quindi è stata sviluppata una versione migliorata del filtraggio dei pacchetti, detta stateful inspection.

Firewall Stateful Inspection
A differenza del semplice filtraggio dei pacchetti, il firewall stateful inspection era in grado di mantenere informazioni sullo stato, che gli permettevano una maggiore sicurezza nella metodologia di ispezione. Anche se la tecnologia stateful inspection eseguiva controlli efficaci sui livelli inferiori dello stack OSI, non era altrettanto affidabile quando si trattava di capire e proteggere i dati al livello applicativo.

Application Firewall, IPS e Web Filtering
Alcuni anni dopo sono stati realizzati i firewall applicativi, in grado di capire determinati protocolli e applicazioni comuni negli ambienti aziendali. Anche se i firewall applicativi sono in grado di capire e decifrare il traffico di tipo HTTP (web) o SMTP (email), possono incidere pesantemente sulle prestazioni di rete e richiedono molti interventi di ottimizzazione e aggiornamento per funzionare correttamente. La necessità di comprendere il contesto applicativo ha inoltre portato allo sviluppo di soluzioni di sicurezza specializzate, come i sistemi di intrusion prevention (IPS) e i prodotti di web filtering, che sono infine diventati prodotti di sicurezza con una propria area specifica di applicazione.
Spesso i responsabili della sicurezza nelle aziende distribuivano sia firewall stateful inspection che applicativi per la difesa del perimetro principale. Ciò portava a una complessità elevata e a sfide collegate alla gestione e configurazione delle svariate tecnologie di sicurezza di rete.

Firewall Unified Threat Management

Intorno agli anni 2000 entrò sulla scena la tecnologia Unified Threat Management (UTM), che consentiva di combinare, elaborare e gestire i controlli stateful e applicativi da una singola piattaforma. Il firewall UTM (coniato da IDC) si riferiva a un prodotto di sicurezza all-inclusive che combinava firewall di rete e altre tecnologie di ispezione a livello applicativo, come IPS, web filtering, antispam e antivirus, in un unico fattore di forma. Dal momento che i firewall UTM all-inclusive richiedevano risorse di elaborazione massicce, vennero adottati nelle piccole e medie imprese, dove i requisiti di larghezza di banda erano minori. A causa di considerazioni economiche e di esigenze consolidamento di diverse tecnologie di sicurezza a livello di applicazione, le imprese IT all'interno di questi mercati vincolati dal budget adottarono questa soluzione su larga scala.

Dal momento che i firewall UTM mancavano della granularità e del controllo necessari per alcune delle funzioni di sicurezza più avanzate (ad esempio IPS, web filtering, antispam), le imprese più grandi continuarono con il modello di difesa tradizionale, che prevedeva sia un firewall stateful che diverse forme di tecnologie di sicurezza a livello applicativo distribuiti lungo il perimetro aziendale esteso. La separazione e la scarsa comunicazione tra i diversi controlli di sicurezza non contribuivano a risolvere il problema della complessità di gestione e manutenzione di soluzioni di più fornitori.

Next Generation Firewall

La terminologia NGFW (firewall di nuova generazione), è stata coniata da Gartner, che nel suo "Magic Quadrant for Enterprise Network Firewalls" del 2009 individua come requisiti caratterizzanti per questo tipo di soluzioni l'integrazione delle seguenti funzioni:

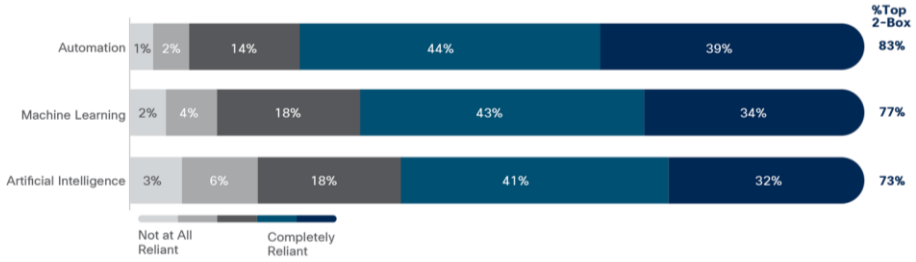
- analisi approfondita dei pacchetti (Deep Packet Inspection),
- Intrusion Detection,
- capacità di riconoscere le applicazioni,
- capacità di controllo granulare.

Inoltre i Next Generation Firewall differiscono dai firewall tradizionali nella loro efficacia quando operano anche come sistemi di Intrusion Prevention (IPS).

Una rete automatica

Lo sviluppo delle software defined network ha aperto nuove frontiere nella gestione delle reti, alimentando un "desiderio" nella mente del network manager: definire lo stato operativo ideale della propria rete per gli scopi che vuole realizzare e disporre di un software di orchestrazione automatizzato che implementa le policy necessarie. Sono le fondamenta per le cosiddette Intent based network, dove "intent" è l'intento che ci si prefigge, meglio traducibile come "scopo". Su tali basi è possibile, secondo Andrew Lerner, un ricercatore senior di Gartner, arrivare a realizzare la Intent Based Network Security (IBNS).
Lerner sostiene che una IBNS deve possedere quattro caratteristiche. La prima è la capacità di traduzione e validazione, cioè la capacità di tradurre i comandi degli amministratori di rete in azioni realizzate dal software. In altre parole, i network manager definiscono delle policy di alto livello, in un linguaggio semplice che si potrebbe definire "business": il software deve poter verificare se le suddette policy siano eseguibili.
Seconda caratteristica che una rete basata sullo scopo deve possedere è l'implementazione automatica: una volta che l'amministratore ha definito lo stato di rete desiderato, il software che realizza la IBNS deve poter agire sulle risorse di rete in modo da raggiungere tale stato, garantendo l'enforcement delle policy.
Terzo elemento fondamentale è l'awareness, sostiene Lerner, intendendo una capacità profonda di monitoraggio, che implica la capacità di raccogliere tutti i dati necessari per controllare la persistenza dello stato di rete preferito.
Infine, una IBNS deve possedere il trinomio di capacità: assurance, dynamic optimization e remediation. In sostanza la capacità di assicurare costantemente lo stato desiderato.
Grazie ad algoritmi di machine learning e alle suddette capacità la rete intent based è in grado di mantenere lo stato richiesto attuando le azioni correttive che di volta in volta si ritengono necessarie.
In pratica gli interventi per conservare lo stato ideale della rete sono realizzati automaticamente dal software creato ad hoc per gestire la rete.
Secondo Lerner ci vorranno ancora un paio d'anni prima che le reti IBN maturino. Almeno fino a quando potranno integrare tutti i controlli e gli

strumenti necessari per alimentare i sistemi di intelligenza artificiali e consentire loro di prevenire e rilevare gli attacchi eventuali. Non basta, infatti, notare che un determinato parametro esca dai limiti stabiliti, deve essere possibile capire se si tratta, per esempio, di un picco di traffico lecito che ha bisogno di un aumento temporaneo della banda disponibile oppure di un'azione diversiva, che maschera un un assesement per cercare vulnerabilità con un workload pesante. Come pure si deve riuscire a osservare del codice maligno, magari spedito in tranche separate, all'interno di un attacco DDoS, su cui si concentra l'attenzione. La crescita dei flussi di dati criptati, per sacrosante ragioni di sicurezza, rende ulteriormente difficili le analisi del traffico.
Ma il mondo degli addetti ai lavori ha grandi aspettative.



La fiducia nella network automation

Ci sono diversi produttori attivi su più fronti di ricerca, da chi è partito ponendosi come principale obiettivo la gestione automatica della rete, per poi integrare uno strato per la cyber security e chi si è concentrato sull'infrastruttura di sicurezza, che si somma alla rete.
Un ruolo importante lo gioca la virtualizzazione, su cui ovviamente si appoggiano alcuni vendor, che semplifica ed estende le capacità di gestione via software. In particolare, vanno considerati gli sforzi di VmWare, con sua la soluzione per la sicurezza delle reti software defined VmWare NSX, e di Citrix, che ha progettato un modello architetturale di sicurezza per realizzare il Secure Digital Perimeter.
Tra le prime aziende che hanno cominciato a lavorare in questo ambito c'è Juniper Networks, che ha da subito cercato di unire prestazioni e sicurezza nell'automazione della rete.

Anche Fortinet può considerarsi tra i pionieri concentrati sul fronte della security. Visto il settore non può mancare Cisco, che è certamente avanti nell'automazione per l'ottimizzazione della rete e sta facendo rapidi passi nell'integrazione della sicurezza, promuovendo, inoltre, la definizione di standard e chiamando a raccolta gli altri attori.

6 - LA SICUREZZA DELLE APPLICAZIONI

Cresce costantemente la pressione degli attacchi che mirano al livello applicativo per sfruttarne le vulnerabilità. Questo incremento di rischio pone l'enfasi sulla necessità di rafforzare il controllo di sicurezza nei processi di sviluppo del codice e di predisporre accurate azioni di test, per approdare alla realizzazione di nuove tipologie di applicazioni in grado di resistere agli attacchi con sistemi di autoprotezione.

Una protezione multilivello

Il 24% degli attacchi informatici che si sono verificati nel 2013 e nel primo semestre del 2014 hanno sfruttato vulnerabilità note. Almeno stando al Rapporto Clusit 2014, che ha analizzato solo gli attacchi resi pubblici. Peraltro, altre ricerche dimostrano che non solo le vulnerabilità sono ancora al primo posto tra le "falle" preferite, ma che addirittura l'80% degli attacchi sono rivolti al layer applicativo.

La maggior parte delle soluzioni di sicurezza sono concentrate, storicamente, sul "perimetro" aziendale. Un concetto che sta perdendo vieppiù di significato. Anche per le applicazioni i fornitori di Information Security hanno seguito questo approccio, per esempio con i Web Application Firewall e altre soluzioni un po' più sofisticate, progettate per identificare anomalie.

L'evoluzione delle minacce, però, ha reso poco efficaci le classiche tecniche per l'analisi del traffico, richiedendo controlli "contestualizzati", al fine di comprendere la natura di determinate azioni, apparentemente maligne ma, in realtà lecitamente previste dall'applicativo.

La sicurezza perimetrale resta fondamentale per monitorare il traffico e bloccare una gran numero di attacchi. Anche se il perimetro aziendale è sempre più "liquido", sul mercato si trovano soluzioni che sono in grado di adattarsi alle nuove architetture "aperte".

Esistono, però, diversi aspetti da considerare quando si guarda alle applicazioni. il primo è quella delle vulnerabilità: cioè dell'utilizzo improprio di quelle soluzioni applicative o di altre componenti software, un cui difetto di programmazione permette di superare i controlli di sicurezza. Il secondo aspetto riguarda il traffico applicativo, che è in forte aumento e ancor più lo sarà, tanto per il successo della mobility, quanto e soprattutto per quello del cloud. Infine, un terzo aspetto riguarda l'utilizzo delle applicazioni, che va monitorato soprattutto per verificare che un utilizzatore non abusi dei propri privilegi, accedendo, magari, a informazioni riservate (per esempio, l'ammontare dello stipendio dei colleghi), ma anche per evitare che ci si distragga troppo, magari su Facebook, o addirittura mettendo a rischio l'impresa (accedendo a contenuti illegali, come quelli pedopornografici).

In particolare, per quanto riguarda la mobility, bisogna distinguere tra quello che è l'accesso alle applicazioni aziendali attraverso dispositivi mobili, da quello che è invece il traffico generato verso Internet per l'utilizzo di app non direttamente aziendali.
Le app aziendali sviluppate sui diversi sistemi operativi per dispositivi mobili, che, di fatto sono iOS di Apple, BlackBerry 10 di BlackBerry, Windows 8 e le molteplici versioni di Android, rispondono alle stesse logiche di qualsiasi pezzo di software sviluppato internamente.
Diverso è il caso delle app scaricate dagli store disponibili commercialmente. Queste, infatti, non sono sotto il diretto controllo dell'azienda e presentano diverse criticità: innanzitutto ne esistono molte che contengono direttamente malware o reindirizzano a esso. Altre potrebbero contenere vulnerabilità che consentono di penetrare sul dispositivo e qui carpire informazioni aziendali. Questo ultimo caso, in genere, viene affrontato dalle soluzioni di mobile security, in particolare, con quelle recenti di "containerization", che isolano i dati aziendali dal resto dispositivo, impedendone l'accesso se non attraverso le app aziendali.

Design sicuro e vulnerability patching

Una strategia di sicurezza accurata è basata sulla gestione del rischio, il cui processo è basato su tre fasi: identificazione delle minacce cui sono soggette le risorse (insieme e singolarmente); identificazione delle vulnerabilità (o vulnerability assessment); valutazione del rischio. Nel vulnerability assessment, che identifica tutte le aree di esposizione alle minacce, dall'errore involontario del dipendente al dolo, al disastro naturale, è compresa anche l'analisi delle vulnerabilità applicative o di sistema.
Tali vulnerabilità sono, in generale, dovute a errori o trascuratezze di gestione: una configurazione superficiale, un bug del software, una versione non aggiornata dell’antivirus e così via. Tali errori sono molto diffusi e si possono identificare con accurate analisi sia del software stesso, attraverso specifici strumenti, sia delle minacce note, perché la vulnerabilità potrebbe sorgere grazie a una combinazione di elementi.
Un difetto di un programma, però, non è necessariamente una vulnerabilità, se non consente di sfruttare l'errore per penetrare nella rete aziendale. In altre

parole, una vulnerabilità diventa una minaccia quando viene anche realizzato un exploit.
Quando viene rilevata da uno dei tanti ricercatori assoldati perlopiù dai vendor di soluzioni informatiche, la vulnerabilità viene comunicata all'editore del software che presenta il bug, consentendogli di mettersi subito al lavoro per "riparare" il buco. Passato del tempo il problema viene reso noto. Questo normalmente avviene quando è disponibile una patch (toppa in inglese), cioè un aggiornamento del software che elimina la vulnerabilità correggendo il difetto. Il giorno in cui viene disvelata la vulnerabilità è detto "0 day". Un tempo, occorreva qualche giorno prima che venissero inventati gli exploit, ma ben presto si è cominciato a parlare di "0 day threat": in realtà, oggi, sono molte le vulnerabilità che vengono scoperte e denunciate, dopo che un malintenzionato le abbia sfruttate.
Sono diversi gli exploit sviluppati dagli attacker e hanno un ciclo di vita variabile, ma spesso inopinatamente lungo. Si potrebbe pensare che la disponibilità di una patch ponga fine a tale ciclo vitale, ma sono molte le imprese che non riescono a stare dietro ai processi di path management e questo permette di usare una vecchia vulnerabilità anche ad anni di distanza, come nel caso della SQL Injection.
Per risolvere queste problematiche, sono stati realizzati negli anni dei sistemi che consentono di realizzare una sorta di pathing virtuale. Sono tecnologie che consentono di proteggere l'infrastruttura aziendale, come se fosse stato corretto il difetto, anche se, permanendo il difetto, un eventuale secondo exploit potrebbe non essere coperto.
Queste difficoltà hanno portato alcuni editori di software tra i più diffusi a impostare regole ferree nella fase di sviluppo del software: in altre parole, l'idea è quella di eliminare il problema alla base, producendo software che non contenga errori.
Ovviamente questa è una soluzione preventiva efficace che permette di mitigare il rischio derivante dagli attacchi evidenziati nel rapporto Clusit e non solo. Tale azione può essere effettuata con l'application security testing. Quest'ultimo permette di verificare passo il funzionamento del software e di controllare che non si possano utilizzare le sue caratteristiche in maniera malevola. In altre parole impedisce di mettere in esercizio applicazioni che

contengono vulnerabilità note e previene il rischio che si lascino altre falle nei nuovi sistemi sviluppati.
Certamente sono stati compiuti giganteschi passi avanti rispetto al passato, quando alcuni software vendor trovavano "naturale" e forse divertente demandare ai clienti la bug discovery. Oggi i processi sono stati notevolmente migliorati e le applicazioni sono molto più sicure sin dalla nascita, ma le esigenze di time to market, le conoscenze non sempre approfondite sulla sicurezza e, soprattutto, le maggiori risorse di sviluppo sul fronte dei cyber criminali, rendono impossibile disporre di un'applicazione sicura al 100%. Questo non significa che non si debbano seguire processi di testing accurati per progettare le applicazioni il più sicure possibili.

L'analisi del traffico applicativo

Secondo il rapporto Clusit 2014, gli attacchi dovuti ad azioni di Cybercrime (furti o frodi, perlopiù) sono circa un quarto del totale. Il resto sono attacchi dei cosiddetti hactivist (sempre meno numerosi e sempre meno dannosi, perché crescono le protezioni contro il Distributed Denial of Service), azioni di sabotaggio e spionaggio.
Diversi sono i percorsi di attacco, ma molti di questi hanno un elemento in comune: le applicazioni, che sono poi il motivo per cui ci si collega a Internet e al Web o, se si preferisce, il motivo per cui si utilizzano dispositivi mobili e non. In ogni caso, il dato è comunque l'obiettivo finale nella stragrande maggioranza dei casi.
Senza considerare, per ovvie ragioni, gli enormi volumi di traffico generati dagli attacchi DDoS, peraltro sempre più destinati a essere bloccati direttamente dal provider di connettività, il traffico applicativo risulta fortemente cresciuto e si prevede che continuerà a crescere, per la diffusione e il successo delle soluzioni in cloud: dai Web Service al Software as a Service. A questo si aggiunge la crescente tendenza a consentire il telelavoro, che prevede l'accesso da remoto alla rete e alle applicazioni che risiedono nel data center aziendale.
Si consideri che, tra globalizzazione, internazionalizzazione, mobility e, non ultima, una rivoluzione nell'ambito delle procedure di backup, di fatto il sistema informativo non viene più spento (almeno nella stragrande maggioranza delle

imprese), come avveniva fino a qualche anno fa. Dunque questo flusso continuo di traffico deve trovare canali di comunicazione aperti che, pertanto, possono diventare una comoda porta d'accesso all'infrastruttura IT aziendale.
Per questo motivo le nuove tecniche per la prevenzione delle minacce informatiche si basano su analisi approfondite del codice in ingresso sulla rete aziendale. Non è una questione banale, perché queste grandi quantità di traffico non possono essere rallentate a piacere. In generale, ne risente la produttività dei lavoratori, che avvertono anche la frustrazione di una user experience non ottimale. In particolare, inoltre, ci sono applicazioni che sono altamente sensibili alla latenza della rete: basti pensare alla videoconferenza, che è una soluzione di comunicazione sempre più apprezzata da quando nuovi standard di compressione ne permettono l'utilizzo attraverso Internet direttamente dal proprio pc, senza tutte le complessità delle grandi sale riunioni con i sistemi complessi di una volta.
Da qui il successo e il crescente interesse verso i firewall e gli Intrusion Prevention System (IPS) di ultima generazione, che implementano soluzioni per l'analisi delle anomalie e per la simulazione del "comportamento" applicativo.
Perlopiù si tratta di soluzioni cosiddette di "sandboxing". Come nelle "scatole di sabbia" in cui giocano al sicuro i bambini nei parchi giochi, in queste sandbox è possibile depositare il codice e "giocarci" con tranquillità per verificarne le azioni e la sua pericolosità. Aspetto fondamentale dei sistemi di sandboxing è classificare il malware che viene riconosciuto come tale, in modo da poterlo facilmente identificare una seconda volta.
La logica, inoltre, è creare una "signature" o qualcosa che permetta comunque ad altri sistemi di riconoscere l'impronta di questo malware. Tali analisi possono essere accelerate da servizi in cloud, che aggiornano prontamente tutti i dispositivi non appena una nuova minaccia viene identificata e, in qualche modo, resa immediatamente riconoscibile da tutti i sistemi.

Applicazioni e RASP

L'aspetto della rapidità non è indifferente, considerando che non si può pensare di bloccare tutto il traffico solo sulla base di un sospetto. Per questo i Web Application Firewall, che originariamente nascono per controllare i contenuti e l'utilizzo delle applicazioni per impedirne abusi, non possono agire in tempo

reale, ma devono aspettare i risultati delle analisi, e quando li ricevono potrebbe essere troppo tardi.
Un altro problema è rappresentato dalle più recenti tecniche impiegate dai cyber criminali nelle minacce APT (Advanced Persistent Threat) utilizzate per attacchi mirati. In questi casi, il codice non viene prodotto per colpire un gran numero di computer, ma bersagli precisi, con più fasi. Una delle quali può essere l'annidamento di un codice nocivo non identificabile con l'analisi del comportamento. Questi malware, infatti, se vengono lanciati in esecuzione non compiono alcuna azione maligna. Ma, dopo un programmato lasso di tempo che può essere anche piuttosto lungo, attivano nuove funzioni che ne cambiano l'azione.
Non tutte le soluzioni sono in grado di rilevare queste minacce. Così come tecniche dette "evasive" possono confondere firewall e IPS. A questo si aggiunga il sempre attuale tema delle vulnerabilità e relative patch e si arriva a comprendere quanto complesso possa essere il fronte applicativo nella lotta al cybercrime.
È dunque a ragion veduta che gli analisti del Gartner, già nel 2012, avevano evidenziato l'importanza delle soluzioni per il collaudo delle applicazioni. Non solo un test statico, utile soprattutto prima del rilascio del software, ma anche un testing dinamico e, addirittura interattivo. Queste funzionalità si uniscono a quelle dei Web Application Firewall per costituire una nuova classe di soluzioni, chiamate RASP (Runtime Application Self Protection), che si stanno rivelando fondamentali per una protezione in tempo reale delle applicazioni.
Di fatto, le applicazioni devono essere intrinsecamente sicure, a partire dal progetto e dalla fase di sviluppo. Questo non basta, però, perché solo in runtime è possibile verificare il funzionamento. Ricordiamo che l'applicazione è sviluppata per svolgere determinate funzioni e non è possibile immaginare tutti i possibili "abusi" di tali funzioni. Solo analisi durante la fase d'elaborazione, con i dati e le query reali, possono intercettare situazioni anomale. Proprio questo è l'ambito in cui operano le soluzioni RASP.

Le soluzioni Runtime Application Self Protection

Le soluzioni "Runtime Application Self Protection" (RASP) non nascono per sostituire questi primi due livelli di protezione, ma per aumentarne l'efficacia. I

Web Application Firewall, infatti, sarebbero in grado di eseguire le azioni protettive necessarie, se solo avessero le informazioni giuste e le avessero in tempo, ma in ogni caso forniscono tecnologie dedicate alla protezione delle applicazioni.

La protezione RASP è appunto capace di analizzare il codice in tempo reale e di attuare contromisure sulla base dei risultati. Punto fondamentale: l'analisi deve avvenire nel contesto reale, direttamente nell'ambiente di produzione.

Questo perché solo il reale funzionamento, con l'utilizzo dei dati effettivi permette di portare a termine l'analisi: per capire il comportamento di una query SQL, per esempio, è necessario guardare la query completa, che si costruisce, di fatto, all'interno dell'applicazione.

Le soluzioni RASP, definite da Gartner un "must to have" per la prima volta nel 2012, dunque, costituiscono una protezione essenziale per le applicazioni in produzione.

Come accennato, il funzionamento di un'applicazione varia anche in base alla tipologia di dati che essa deve elaborare. Per verificarne il comportamento è dunque necessario osservare lo stesso nell'ambiente d'elaborazione, durante l'elaborazione stessa.

Attualmente, le soluzioni sul mercato effettuano questo tipo di controlli con dispositivi "esterni" all'ambiente di runtime, come firewall e IPS. Si tratta di soluzioni certamente valide ma la cui efficacia potrebbe essere ridotta dall'impossibilità d'entrare nella logica dell'applicazione, della sua configurazione e delle sue relazioni con i flussi dei dati e degli eventi. Non a caso sono spesso "relegati" a una funzione di alerting, non potendo garantire l'accuratezza necessaria a evitare tassi di falsi positivi accettabili.

Secondo gli analisti di Gartner, le imprese cosiddette "pioniere" della tecnologia hanno già adottato tecnologie RASP o lo stanno facendo, mentre le altre dovrebbero comunque implementarle entro i prossimi tre anni. Un lasso di tempo durante il quale le tecnologie oggi sul mercato arriveranno a una piena maturità. Già adesso, peraltro, sono in essere soluzioni che, appoggiandosi al cloud, permettono alle imprese di utilizzare lo stato dell'arte in ambito RASP, seguendone "naturalmente" l'evoluzione e, non per ultimo, di incontrare minori difficoltà nell'implementazione, installazione e gestione delle soluzioni.

Peraltro, sempre secondo Gartner, entro il 2017 il 25% degli ambienti di elaborazione avranno capacità di autoprotezione integrate (rispetto a meno dell'1% nel 2012).
Questa "urgenza" deriva dalla crescente pressione delle minacce sul layer applicativo. È fondamentale che le applicazioni siano in grado di "autoproteggersi": cioè disporre di funzioni che le proteggano durante l'elaborazione. Queste devono idealmente poter osservare qualsiasi dato entri o esca dall'applicazione, tutti gli eventi che la riguardano, ogni istruzione eseguita e tutti gli accessi al database.
Una soluzione RASP possiede tutti questi requisiti e così permette all'ambiente d'elaborazione di rilevare gli attacchi e proteggere l'applicazione più a fondo.

Web Application Firewall e Interactive Application Security Testing

In buona sostanza, le soluzioni RASP combinano le tecnologie dei Web Application Firewall (WAF) e dell'Interactive Security Testing (IAST), mettendo insieme funzionalità di scansione, monitoraggio in real time, detection, protezione, analisi dell'esecuzione e analisi del traffico. In pratica, si tratta di una nuova tecnologia resa possibile solo grazie all'interazione di altre tecnologie. La componente IAST, di recente introduzione, è fondamentale, perché è questa che "arma" l'ambiente di runtime. Tali soluzioni di testing s'integrano per esempio in una Java Virtual Machine (JVM) o nel .NET Common Language Runtime (.NET CLR) diventando parte.
Essendo all'interno della JVM o del .NET CLR, il sistema di test riesce a "vedere" i flussi indotti da un attacco. Meglio ancora, li può simulare per prevederli.
Le soluzioni RASP prendono a prestito tale capacità dalle tecniche IAST e, contemporaneamente, utilizzano la capacità di reazione in tempo reale dei Web Application Firewall per terminare una sessione "maligna" o per lanciare un alert in caso di esecuzioni sospette rilevate dall'Interactive Application Testing.
È quindi la combinazione delle due tecnologie che rende possibile la Runtime Application Self Protection. Di fatto, la massima efficienza si ottiene combinando tutte le tipologie di application protection disponibili, dal testing statico a quello dinamico fino a quello interattivo. Non solo, perché le analisi delle vulnerabilità e quelle degli attacchi condotte da queste tecnologie sono

alla base delle soluzioni RASP. Proprio la loro combinazione realizza la self protection, permettendo di superare i principali limiti. Se l'analisi statica permette di sospettare una vulnerabilità in una linea di codice, solo l'analisi in runtime consente di verificare la consistenza di un exploit che sfrutta la vulnerabilità ipotizzata. Potrebbe dunque accorgersene il test dinamico dell'applicazione. Nessun sistema di test, peraltro, è in grado di fermare un attacco. Può invece farlo il RASP, prendendo la decisione in base alle informazioni fornite dal testing applicativo e utilizzando le capacità d'azione real time del WAF.

In effetti, può avvenire anche il contrario: la componente Web Application Firewall può rilevare traffico sospetto e "richiede" alla componente IAST di effettuare un supplemento di analisi testando il flusso d'elaborazione e di dati durante l'esecuzione.

In ogni caso, la soluzione RASP sfrutta la combinazione delle tecnologie, ma non le sostituisce. Il Web Application Firewall, infatti, ha ragione di sussistere anche a sé stante per bloccare un'azione potenzialmente dannosa, come il collegamento a un sito Web elencato in una blacklist.

Le soluzioni RASP rappresentano una prima pietra miliare di un percorso verso il cosiddetto "Application Shielding", che potremmo tradurre come la "blindatura delle applicazioni". Blindare un'applicazione per renderla resistente agli attacchi, permettendole di difendersi direttamente da sola.

Ancora una volta, sottolineiamo che non si tratta di sostituire un precedente livello di protezione, né, in realtà di aggiungerne uno nuovo, ma più semplicemente di allargare l'orizzonte di protezione, per rispondere all'espansione del fronte di attacco.

È ancora presto per capire fino in fondo come si svilupperà l'Application Shielding o quanto rapidamente si affermeranno le tecnologie RASP. Anche perché ci sono diversi fattori che intervengono nel disegnare tale scenario. Per esempio, l'adozione di soluzioni per la Runtime Application Self Protection sarebbe probabilmente accelerata dalle alleanze che i produttori di applicazioni e/o quelli del middleware per gli ambienti d'elaborazione potrebbero siglare con i vendor che sviluppano e vendono soluzioni RASP. In pratica, si potrebbero realizzare ambienti di runtime blindati alla nascita.

Questo avrebbe anche il benefico effetto di rendere meno invasiva l'analisi di sicurezza e testing, riducendo il rischio di impatti sulle capacità di elaborazione.
Un contributo ad accelerare la blindatura delle applicazioni potrebbe arrivare anche dal cloud, come precedentemente accennato. L'ambiente di runtime è pressoché totalmente controllato dal cloud provider. Per costoro è quindi logico installare soluzioni RASP che garantiscano la sicurezza dell'elaborazione. Con tale garanzia possono girare la responsabilità di eventuali attacchi alla connessione di rete utilizzata dal loro cliente.
Lasciare la gestione della soluzione RASP al provider è un vantaggio anche per il cliente, che non si dovrà più preoccupare di installare e manutenere tali soluzioni.
In un circuito virtuoso queste soluzioni contribuiscono a sciogliere i dubbi sulla sicurezza del cloud che rimane uno dei principali ostacoli alla sua adozione.

7 – LA SICUREZZA LOGICA INCONTRA QUELLA FISICA

L'utilizzo delle tecnologie informatiche diventa sempre più funzionale a garantire la sicurezza aziendale non solo all'interno dei processi di tipo logico come l'autenticazione informatica, ma anche nei controlli di accesso fisico. Le tecniche di rilevazione biometriche e la videosorveglianza rappresentano i componenti più evidenti di questo trend in atto, che si prepara a raggiungere nuovi livelli con l'avvento dell'Internet of Things

La convergenza tra sicurezza logica e sicurezza fisica

L'Information Security è stata storicamente separata dalla sicurezza fisica, intesa come impianti antincendio, sistemi antifurto, barriere all'ingresso.
Di fatto si tratta di una distinzione che non ha più senso. Innanzitutto i due mondi sono sempre meno disgiunti, considerando la pervasività dell'IT. In secondo luogo ci sono sempre più contatti, tanto che si parla ormai apertamente della convergenza tra sicurezza fisica e sicurezza logica. Se ne parla soprattutto in termini di protezione più efficace e contributo a valore, derivante dall'integrazione delle soluzioni.
Ci sono poi aspetti legali che dovrebbero spingere in questa direzione. In particolare, basti pensare che la legge sulla Privacy è oggi considerata la legge principale in materia di sicurezza IT.
Eppure il responsabile della privacy in azienda è normalmente una figura dirigenziale che si occupa di tutt'altro che informatica: tipicamente il direttore del personale. La maggior parte dei dati sensibili in azienda, infatti, sono quelli relativi ai dipendenti. Purtroppo, risorse umane e IT raramente seggono allo stesso tavolo per discutere di progetti collegati alla sicurezza.
Ci sono poi ambiti tecnologici in cui la convergenza è forte, per esempio, quello del controllo degli accessi o delle presenze in azienda, oggi sempre più attuato con badge elettronici direttamente connessi con i sistemi ERP aziendali, oppure mediante lettura di dati biometrici digitalizzati.
Altro ambito in forte sviluppo è quello della videosorveglianza integrata su IT, dove si aprono interessanti scenari sul fronte della digitalizzazione di immagini e video.
Tutte queste soluzioni hanno una componente informatica e sono relative alla protezione degli asset aziendali.
È pertanto evidente che la correlazione tra gli eventi che vengono registrati dall'una e dall'altra parte porta benefici in termini di efficacia della protezione.

La biometria

L'utilizzo di dispositivi e tecnologie per la raccolta e il trattamento di dati biometrici è in costante incremento per rispondere a esigenze sempre più stringenti di controllo e verifica dell'identità.
Sistemi basati sull'analisi di parametri biometrici possono essere adottati per il controllo fisico ed elettronico degli accessi, per abilitare l'accesso fisico a locali e aree specifiche, l'attivazione di macchinari oppure per un controllo degli accessi di tipo logico (autenticazione informatica). In alcuni casi le tecniche biometriche possono essere utilizzate anche a scopo facilitativo, per esempio per l'accesso a biblioteche o l'apertura di cassette di sicurezza.
Un caso a parte è quello dei sistemi di firma grafometrica, finalizzati alla sottoscrizione di documenti informatici senza che necessariamente sia effettuato un riconoscimento biometrico.
Con la firma grafometrica vengono, infatti, incorporate all'interno del documento informatico una serie di informazioni strettamente connesse al soggetto firmatario che possono consentire lo svolgimento di analisi grafologiche da parte di un perito calligrafo (velocità di tracciamento, accelerazione, pressione, inclinazione, salti in volo e così via) analogamente a quanto avviene con le firme apposte sui documenti cartacei.

Metodi di confronto

Il metodo alla base della sicurezza biometricie è quello di impiegare delle caratteristiche personali quali le impronte digitali, i lineamenti del volto, l'immagine della retina, l'iride, il timbro vocale, la calligrafia, la struttura venosa delle dita, la geometria della mano per autenticare un individuo tramite comparazione. La comparazione può essere condotta in due modi, che implicano tipicamente diversi utilizzi del sistema biometrico: la verifica o l'identificazione.
Il processo implica due fasi. La prima consiste nella registrazione del tratto biometrico, che viene catturato, estrapolato e convertito in un codice binario per generare un modello biometrico che sarà memorizzato in modo persistente e invariabile nel tempo all'interno di un database. Questo modello costituirà la base per una comparazione basata su metodi statistici e metriche tipici del

sistema biometrico prescelto. Per rendere più veloce il sistema o per applicazioni particolari, il modello originale può essere memorizzato anche direttamente su una smart card, ovviamente con tecniche cosiddette di tampering, che ne impediscono la manomissione. Per esempio, questo può essere utile per applicazioni di servizio pubblico: l'utente porta con sé un certificato digitale che contiene il template biometrico che può impiegare per autenticarsi presso determinati sportelli o enti. Si evita, così, il collegamento a un server remoto con un significativo aumento del livello delle prestazioni.
La seconda fase è quella di "matching". Quando l'utente richiede l'accesso (per esempio, quando si presenta alla porta d'ingresso di un laboratorio riservato, oppure quando semplicemente dal proprio PC vuole accedere a dati riservati) è chiamato a sottomettere il tratto caratteristico precedentemente registrato all'apposito lettore biometrico, in modo che venga rilevato e comparato con il modello presente nel database.

Esempio di architettura di un sistema di autenticazione con dati biometrici

Nelle applicazioni di verifica biometrica l'immagine acquisita viene sovrapposta al modello per verificare l'identità dichiarata della persona (è il caso utilizzato per le tecniche di autenticazione). Il metodo della verifica, impiegato in un sistema di autenticazione, può essere poi abbinato ad altri elementi di

identificazione, come user ID, password, token, smart card e così via, per incrementare ulteriormente il livello complessivo di sicurezza.
Nel processo di identificazione biometrica, invece, il sistema confronta il modello rilevato con tutti i modelli biometrici disponibili all'interno di una banca dati per individuare l'identità del soggetto (confronto uno a molti). Si tratta della modalità tipica da investigazioni utilizzata dalla Polizia.

I rischi della biometria

L'elevato grado di unicità nella popolazione di molte caratteristiche biometriche espone al rischio che soggetti privati e istituzioni possano acquisire informazioni sui singoli individui per finalità differenti da quelle per cui tali dati biometrici sono stati in origine raccolti, incrociando e collegando dati provenienti da più banche dati.
Peraltro, alcune caratteristiche biometriche possono essere acquisite senza la consapevolezza o la partecipazione di un individuo.
Un altro elementi di rischio specifico è la possibilità di furto di identità biometrica che può causare effetti lesivi rilevanti e duraturi poiché, diversamente dai sistemi di autenticazione tradizionali, diventa impossibile fornire alla vittima del furto una nuova identità biometrica che utilizzi la stessa tipologia di dato biometrico,.
Inoltre, va ricordato che Il riconoscimento biometrico avviene generalmente su base statistica e non deterministica e, pertanto, non è esente da possibili errori. In particolare, un sistema di autenticazione biometrica può commettere due tipi di errore: può portare erroneamente ad accettare il confronto con una persona che è in realtà un impostore (falso positivo) oppure negare l'accesso a un utente autorizzato (falso negativo). In generale, i sistemi in commercio dichiarano il tasso di errore dei due tipi e sarà l'impresa utilizzatrice a dover scegliere quale dei due rischi è il meno grave. Nel primo caso, si può prevedere di inserire, come accennato, ulteriori meccanismi di controllo, migliorando l'accuratezza originale del sistema.
Non va neppure esclusa, in teoria, la possibilità di falsificazione biometrica . È stato, per esempio, dimostrato nel caso delle impronte digitali che è possibile ricostruire un campione biometrico corrispondente a un modello biometrico di partenza. Si pensi, per esempio, alla possibilità di realizzare una sorta di "dito

artificiale" che riproduca le sembianze anatomiche del polpastrello, magari utilizzando tecniche di stampa tridimensionale a basso costo.
La diffusione di sistemi mobili e di modelli BYOD, da una parte diffonde l'utilizzo di sistemi di autenticazione biometrica (predisposti magari dall'azienda sul Tablet di un dipendente con il suo consenso) e dall'altro espone a rischi maggiori rispetto allo svolgersi del trattamento all'interno del perimetro di sicurezza aziendale. Infatti, l'uso promiscuo dei dispositivi solitamente mal si concilia con la sicurezza dei dati e sull'adozione puntuale e continua di meccanismi di controllo degli accessi anche di tipo basilare e di modalità di connessione sicura con protocolli avanzati per proteggere i dati in mobilità.

Caratteristiche e tipologie dei sistemi biometrici

Le tecniche biometriche possono essere classificate in diversi modi. Possono essere interattive ovvero richiedere la consapevole partecipazione dell'interessato durante l'acquisizione del dato biometrico (per esempio scansione della retina o firma autografa) oppure passive come quando si effettua la registrazione dell'immagine di un volto o una voce senza che l'interessato ne sia reso partecipe. Possono essere basate su caratteristiche biologiche, fisiche o comportamentali (per esempio nel caso di apposizione della firma). In ogni caso devono possedere caratteristiche di univocità per ogni persona e di presenza in ogni individuo.
I diversi parametri biometrici sono differenti anche in merito alla stabilità temporale e alla tipologia di decadimento per cause naturali o accidentali e questo può avere un effetto sul confronto con il modello di riferimento.
Le principali tipologie di parametri biometrici vengono descritte brevemente di seguito.

Impronte digitali
Il trattamento biometrico delle impronte digitali è quello più diffuso e utilizzato da maggior tempo. Il modello biometrico viene solitamente realizzato su una rappresentazione sintetica numerica dell'impronta di partenza. A differenza di quanto si crede l'univocità del modello all'interno di un database biometrico non è garantita e, soprattutto in grandi archivi dattiloscopici, a più di una impronta può corrispondere un medesimo modello. Questo inconveniente non

sottrae nulla all'efficacia del suo utilizzo come indice per la ricerca di corrispondenze all'interno di un database, come viene fatto abitualmente dai sistemi di riconoscimento automatico delle impronte digitali utilizzati da forze di Polizia e da agenzie investigative.

Modalità di apposizione della firma autografa

La firma autografa è contraddistinta da caratteristiche dinamiche che si possono far rientrare tra le caratteristiche biometriche comportamentali.

Attualmente l'acquisizione avviene non solo tramite tavolette grafometriche ma anche tramite Tablet generici dotati di specifici programmi software che consentono di rilevare, oltre al tratto grafico, anche i parametri dinamici associati alla firma.

L'acquisizione delle caratteristiche dinamiche di firma può essere funzionale a procedure di riconoscimento biometrico, anche se presenta tassi elevati di falsi negativi.

Riconoscimento vocale

Con crescente frequenza i sistemi di riconoscimento stanno prendendo il posto delle password nelle conversazioni telefoniche.

Le caratteristiche dell'emissione della voce sono parametri biometrici perche sono legate all'anatomia del tratto vocale, alla sua lunghezza, alle risonanze e anche alla morfologia della bocca e delle cavità nasali. In molti casi il riconoscimento non si limita all'analisi dei segnali vocali, ma prevede anche procedure in cui l'interessato viene invitato a ripetere delle frasi, nomi o numeri e vi è anche la possibilità di richiedere all'utente un'informazione aggiuntiva nella sua disponibilità cognitiva (PIN, codice identificativo, codice utente e così via). La rilevazione segnale vocale è un tipico parametro biometrico che può essere acquisito senza la partecipazione attiva dell'interessato e senza l'uso di sensori specializzati, essendo sufficiente un normale microfono (anche telefonico).

Struttura venosa delle dita o della mano

Uno dei sistemi più avanzati e di recente presenza sul mercato per la verifica biometrica è quello basato sulle caratteristiche della rete venosa delle dita e della mano di un individuo: caratteristiche che si sviluppano addirittura antecedentemente alla nascita. L'acquisizione di questi tratti biometrici avviene

tramite sensori che rilevano la forma e la disposizione delle vene delle dita, del dorso o del palmo della mano utilizzando una sorgente luminosa a lunghezza d'onda prossima all'infrarosso. Questo sistema ha il vantaggio di essere percepito come poco invasivo poiché non richiede il contatto del corpo con la superficie del sensore. Fornisce un'accuratezza elevata, in genere superiore a quelli basati sulle impronte digitali e non lascia tracce nel processo di acquisizione (a differenza, per esempio, delle impronte digitali); non fornisce indicazioni su dati sensibili e mantiene un'elevata stabilità nel tempo. La sua rilevazione deve essere effettuata con la partecipazione attiva dell'interessato.

Rilevamento della struttura vascolare della retina

Questa tecnica biometrica prevede l'uso di un fascio di luce a infrarosso a bassa intensità che illumini la parte posteriore dell'occhio. Si tratta di un sistema attualmente utilizzato in ambiti che richiedono un livello di sicurezza particolarmente elevato poiché non sono, a oggi, noti meccanismi efficaci per replicare la struttura vascolare della retina. Inoltre non è possibile utilizzare tessuti di persone morte (come si vede qualche volta nei film di azione) poiché il sensore rileva la circolazione sanguigna.

Tale caratteristica biologica non lascia traccia, è altamente distintiva dell'individuo e ha elevata stabilità nel tempo. Tuttavia può determinare malfunzionamenti nel caso siano presenti patologie oculari.

Lettura della forma dell'iride

Si tratta di una tecnica che prevede la rilevazione della forma della pupilla e della parte anteriore dell'occhio mediante immagini ad alta risoluzione: una caratteristica altamente distintiva dell'individuo. È un procedimento di elevata accuratezza e velocità di comparazione, caratterizzato da un basso livello di falsi positivi ed elevata stabilità nel tempo. La sua rilevazione può essere effettuata senza la partecipazione attiva dell'interessato.

Topografia della mano

È una tecnica basata sulla rilevazione delle proprietà geometriche dell'arto acquisite in modalità bidimensionale o tridimensionale mediante un apposito sistema di scansione che rileva caratteristiche quali la forma, la larghezza e lunghezza delle dita, la posizione e la forma delle nocche o del palmo della mano. Va osservato che quelli acquisiti sono tratti distintivi non caratterizzanti

in modo unico un individuo e che sono soggetti ad alterazione nel tempo. Di conseguenza, questa tecnica è poco adatta per applicazioni di identificazione biometrica tra un numero ampio di persone ma trova uso efficace ai fini della verifica biometrica.
L'ingombro del sistema di rilevamento ne impedisce l'integrazione all'interno di dispositivi mobili.

Riconoscimento del volto
Il riconoscimento automatico di un individuo tramite l'analisi delle sue sembianze facciali è un procedimento complesso, che risente della difficoltà di eliminare variabili legate a caratteristiche anche transitorie quali barba, capelli, occhiali e così via. Anche la luce può essere un problema e, infatti, le stesse tecniche basate su riprese a infrarosso sono più efficaci. L'utilizzo in combinazione con tecniche di grafica computerizzata (per esempio per gestire le ombre) ne garantisce comunque l'elevata l'accuratezza e ne favorisce l'elevata stabilità nel tempo.
Il riconoscimento facciale può arrivare a essere molto accurato e le sembianze facciali possono lasciare tracce, potendo essere acquisite automaticamente tramite sistemi di videosorveglianza anche senza la partecipazione attiva dell'interessato.

Ciclo di vita e conservazione dei dati biometrici

I sistemi per l'identificazione biometrica richiedono la costituzione di banche dati centralizzate di modelli biometrici di riferimento per effettuare confronti con il modello biometrico ricavato dalla caratteristica presentata.
Per le operazioni di verifica biometrica è invece possibile adottare sia una conservazione centralizzata all'interno di in un'unica banca dati sia una conservazione decentralizzata, in cui i riferimenti biometrici sono conservati direttamente sui dispositivi di rilevazione su cui avviene il confronto o su dispositivi sicuri affidati alla custodia dell'interessato.
Per esempio, per l'accesso a un sistema bancario si può usare un sistema basato sul rilevamento dell'impronta digitale in cui come prima cosa il dito dell'utente viene sottoposto a scansione e, se l'impronta corrisponde, viene sbloccata una smart card cifrata che invia i codici di autorizzazione alla banca. In questo modo

è l'utente che detiene il proprio codice biometrico e non la banca, che riceve soltanto il messaggio inviato dalla SIM.
I dati biometrici dovrebbero essere conservati solo per il tempo necessario al perseguimento degli scopi per cui sono stati raccolti (salvo specifici obblighi di legge) ed essere cancellati o resi anonimi quando non sono più necessari rispetto alle finalità per cui erano stati acquisiti.
Peraltro, nei casi eventuali di conservazione centralizzata dei dati biometrici in un server, si dovrebbe avere sempre l'accortezza di conservare i dati identificativi degli utenti separatamente dai relativi dati biometrici e di utilizzare soluzioni di cifratura con lunghezza delle chiavi adeguate alla dimensione e alla criticità della banca dati. Inoltre, è opportuna l'adozione di sistemi di registrazione degli accessi da parte dei soggetti abilitati a svolgere mansioni tecniche di manutenzione e gestione del server.

L'intervento del Garante della Privacy

I dati biometrici sono direttamente e univocamente collegati all'individuo e il loro utilizzo rientra tra i trattamenti che presentano rischi specifici e che può essere svolto previa richiesta di verifica preliminare al Garante della Privacy.
Alla luce della crescente diffusione di dispositivi biometrici, anche incorporati in prodotti di largo consumo, a fine del 2014 il Garante Privacy è intervenuto sul tema della biometria per fornire un quadro di riferimento unitario, fornendo Linee Guida e introducendo altresì la terminologia essenziale per la descrizione degli aspetti tecnologici. Data la particolare delicatezza del tema, prima del varo definitivo del provvedimento e delle linee guida, l'Autorità ha anche deciso di sottoporre i testi a una consultazione pubblica.
In questo intervento sono state individuate alcune tipologie di trattamento che, per le specifiche finalità perseguite, presentano un livello ridotto di rischio e che pertanto possono essere considerate esenti da una verifica preliminare da parte dell'Autorità per l'adozione di tecnologie biometriche (definendo però un preciso quadro di regole a tutela delle libertà personali).
In particolare vengono indicati come esenti da verifica:

- le caratteristiche biometriche dell'impronta digitale o dell'emissione vocale come credenziali di autenticazione per l'accesso a banche dati e sistemi informatici;

- le caratteristiche dell'impronta digitale o della topografia della mano per il controllo di accesso fisico ad aree "sensibili" e utilizzo di apparati e macchinari pericolosi;
- l'apposizione a mano libera di una firma autografa per la sottoscrizione di documenti informatici;
- l'impronta digitale e la topografia della mano per scopi facilitativi, purché con il consenso degli interessati.

Il Garante ha ribadito che ogni sistema di rilevazione dovrà essere configurato in modo tale da raccogliere un numero limitato di informazioni (principio di minimizzazione), escludendo l'acquisizione di dati ulteriori rispetto a quelli necessari per il conseguimento della finalità perseguita. Tra le numerose misure di sicurezza individuate dal Garante vi è quella che obbliga a cifrare il riferimento biometrico con tecniche crittografiche, con una lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.

8 - SOLUZIONI PER LA PROTEZIONE DEI DATI

L'obiettivo degli attacchi è, nella gran maggioranza dei casi il dato, pertanto è su questo che la protezione deve concentrarsi, a prescindere che esso risieda nel data center aziendale, nel cloud o sui dispositivi utilizzati dagli impiegati, magari in mobilità all'esterno dell'impresa. Oltre a controllare l'identità di chi richiede l'accesso al dato, va aggiunto un ulteriore livello di sicurezza: direttamente collegato al dato stesso. In particolare, nuove generazioni di tecniche per la cifratura e la decodifica dei dati prevedono approcci innovativi.

L'approccio gestionale alla sicurezza dei dati

Il riconosciuto valore dell'informazione per un'azienda, accompagnato dalla crescita indiscriminata del numero delle stesse, ha portato nel tempo verso la definizione di regole di tipo standard per l'organizzazione della sicurezza che non si limiti agli aspetti tecnologici, ma che prenda in considerazione anche aspetti di tipo operativo, logico, materiale e legislativo focalizzandosi sugli aspetti di tipo gestionale.

Le esigenze aziendali che inducono a considerare l'adozione di un approccio gestionale verso la sicurezza delle informazioni sono molteplici. Da un lato la risposta a esigenze interne relative a conseguire un miglioramento dell'efficienza e a ottimizzare l'organizzazione dei processi di business, dall'altro il desiderio di ridurre i costi e aumentare il ritorno dagli investimenti effettuati.

A queste si aggiungono una serie di "pressioni" provenienti dall'esterno e legate, per esempio, alla necessità di adeguarsi progressivamente a direttive comunitarie unificate, di controbattere le crescenti minacce provenienti da Internet o, ancora, di rispondere a specifici requisiti legali relativi alla manutenzione e protezione dei dati e alla tutela della privacy.

Un Sistema di gestione per la sicurezza delle informazioni (SGSI) prevede che l'azienda implementi una politica di sicurezza allo scopo di gestire le aree a rischio. I principi fondamentali alla base di un SGSI sono di definire una gamma di policy per la sicurezza delle informazioni, prevedendo l'assegnazione specifica di responsabilità e l'implementazione di metodologie che considerino la gestione della business continuity, il report degli incidenti e una serie di controlli periodici per assicurare il raggiungimento degli obiettivi previsti nell'ambito della security. Tutto ciò all'interno di un processo di educazione, sensibilizzazione e training verso le tematiche della sicurezza.

Il passo successivo è quello di adottare un sistema per verificare il proprio SGSI, attraverso una certificazione, in conformità ad alcuni standard specifici. Tutte le organizzazioni possono trarre beneficio da questo tipo di certificazione ma soprattutto quelle che devono proporre all'esterno un'immagine di sicurezza

come aziende operanti in ambito finanziario, delle telecomunicazioni, dell'erogazione di servizi IT o la Pubblica Amministrazione.

Le 3A della sicurezza

Il tema centrale attorno al quale costruire queste politiche di sicurezza ruota attorno alle cosiddette "3A" ovvero all'insieme delle tecniche di autenticazione, autorizzazione e "accounting" che, insieme, svolgono un ruolo coordinato e sinergico all'interno del processo di protezione dei dati e dei servizi aziendali.
Questi concetti riassumono le procedure e le funzioni necessarie per lo svolgimento di molti dei processi di sicurezza che avvengono sul Web. In un contesto di accesso geograficamente distribuito alle risorse informatiche è indispensabile, infatti, trovare dei metodi e delle regole in grado di garantire e proteggere il corretto svolgimento delle operazioni tra le parti che scambiano informazioni.
Le 3A sovrintendono proprio a questo tipo di funzioni. In particolare l'autenticazione è il processo per garantire in modo univoco l'identità di chi si appresta ad accedere alle risorse, l'autorizzazione definisce i privilegi di cui dispone questo utente, mentre l'accounting si riferisce all'analisi e alla registrazione sistematica delle transazioni associate a un'attività di business sul Web. La sicurezza di questi processi viene assicurata da una serie di tecnologie e procedure che si appoggiano su protocolli e standard.

Implementare un sistema di autenticazione

I trend che alimentano il mercato delle tecnologie di autenticazione sono molteplici. Innanzitutto va considerata la continua espansione dell'accessibilità alle informazioni, legata alle nuove categorie di lavoratori mobili e da remoto nonché alla progressiva apertura del network delle grandi aziende verso partner e clienti. Inoltre cresce il numero di informazioni critiche e, conseguentemente, delle misure necessarie per controllare il loro accesso. A questi va aggiunta quella che si potrebbe definire come la "crisi delle password" ormai definitivamente abbandonate da tutti i principali fornitori di tecnologie in cerca di soluzioni più affidabili e meglio gestibili.
A controbilanciare questi argomenti concorrono aspetti quali i lunghi tempi di implementazione (trattandosi spesso di soluzioni che coinvolgono un

grandissimo numero di utenti), i costi associati alla realizzazione di infrastrutture dedicate, ma anche la giustificazione dell'investimento rispetto ad altri ambiti tecnologici e di business, in un momento in cui i budget scarseggiano.

Resta in ogni caso il dilemma della scelta del sistema e della tecnologia da adottare tra le molteplici opzioni disponibili sul mercato. La risposta a quest'esigenza risiede nella valutazione di una serie di motivazioni che devono tenere in considerazione gli aspetti specifici di ogni azienda e dei suoi processi di business. Come sempre non esistono ricette uniche ma, di seguito, cercheremo di fornire alcuni spunti metodologici per orientarsi meglio in questo processo decisionale.

Il primo e fondamentale punto è quello di riconoscere che l'individuazione di una soluzione di autenticazione rappresenta un compromesso tra costi, sicurezza e praticità d'uso e che, pertanto, ogni decisione in merito dovrebbe essere presa come risultato di un'analisi di questi tre aspetti. La cosa è complicata dal fatto che si tratta di parametri generalmente antagonisti fra loro: incrementare il livello di sicurezza determina costi proporzionalmente crescenti e una riduzione della flessibilità e semplicità d'uso perché richiede l'adozione di strumenti, procedure e tecnologie.

Un approccio metodologico dovrebbe partire da una metricizzazione di tali aspetti, inizialmente da un punto di vista qualitativo delle implicazioni e, se possibile, successivamente anche di tipo quantitativo. Per esempio è possibile individuare tutti gli aspetti significativi e correlarli attribuendo loro un indice numerico.

Anche se a qualcuno potrebbe sembrare un esercizio un po' accademico, l'adozione di una metodologia di questo tipo permette di chiarirsi le idee su domande di difficile risposta quali: di quanta sicurezza ho effettivamente bisogno?

Non da ultimo, permette di facilitare la comprensione di determinate scelte tecnologiche anche da parte di chi mastica più il linguaggio del budget che quello tecnologico.

Affrontare l'aspetto dei costi significa, ovviamente, considerare il Total Cost of Ownership della soluzione, che comprende non solo i costi di acquisizione, ma anche e soprattutto quelli di deployment e operativi, che vanno associati alle tecnologie, al personale, ai processi e alla struttura.

Eseguire un'analisi degli aspetti di sicurezza e praticità è, invece, il risultato di una valutazione strategica difficilmente ingabbiabile in regole. Tuttavia è possibile almeno separare gli aspetti legati al valore di una soluzione di autenticazione rispetto agli utenti e all'azienda.
La praticità e la semplicità d'uso, per esempio, dipendono, in generale, dalla tipologia di utenti che si stanno considerando e cambiano a secondo che si tratti di partner, dipendenti o clienti. Accanto alla complessità di apprendimento va considerata anche la praticità di utilizzo, che può inibire il suo impiego.
Anche gli aspetti legati alla trasportabilità della soluzione di autenticazione (indice importante della sua flessibilità) possono essere sensibilmente differenti in funzione della tipologia di utente e sono spesso legati a doppio filo con i costi. Per esempio, l'adozione di soluzioni che richiedono la presenza di un software sul lato client possono limitare l'accessibilità da aree esterne quali le filiali aziendali.
Un altro esempio può essere quello di soluzioni di autenticazione che sfruttano dispositivi mobili e che possono essere condizionate dall'area di copertura del servizio.
Un ulteriore valore per l'utente può essere la versatilità. A volte il sistema di autenticazione può essere costituito da un dispositivo specifico, ma in altri casi può combinare in un unico dispositivo una pluralità di funzioni: sistema di autenticazione, documento di identità dotato di foto, strumento di memorizzazione di dati e così via.
Dal punto di vista della valenza strategica per l'azienda l'elemento primario da considerare è la sicurezza relativa, che deve tenere conto del livello di protezione offerto dal sistema di autenticazione, della sicurezza della sua implementazione, dall'adeguatezza a proteggere la tipologia di informazioni per cui lo si vuole utilizzare e anche della garanzia di compatibilità con la normativa.
A ciò va aggiunta la possibilità di integrazione all'interno dell'infrastruttura esistente e l'interoperabilità con i sistemi di back-end.
In una valutazione non va, infine, trascurata la possibilità di lasciarsi aperte opzioni per le future evoluzioni tecnologiche.

L'identity management

La diffusione attraverso il Web o le reti aziendali di dati ad alto valore, collegata a transazioni, all'accesso ad applicazioni e a processi di business che prevedono il trasferimento di informazioni sensibili, ha accresciuto l'importanza di possedere un'identità digitale sicura.

Determinare un sistema per poter dimostrare ad altri di essere un individuo con determinate caratteristiche, rappresenta un modo per interagire con le regole che caratterizzano le attività che svolgiamo. Disporre di un'identità digitale significa possedere credenziali che consentono lo svolgimento di determinati compiti, abilitano l'accesso a informazioni e servizi e permettono l'utilizzo di determinate applicazioni.

Il parallelo tra l'identità all'interno di un concetto di rete enterprise virtuale e il mondo reale è fin troppo ovvio. Appare quindi immediatamente chiaro che una specifica identità digitale deve essere associata a un unico utente; è inoltre auspicabile che uno specifico utente possa disporre di un unico set di credenziali per accedere a ogni tipo di servizio ed è altrettanto importante che un utente possa disporre delle credenziali ogni volta che gli vengano richieste. In questi processi la sicurezza rappresenta un requisito fondamentale.

Resta però il fatto che, in un mondo digitale caratterizzato dalla distribuzione delle informazioni, dalla loro accessibilità virtualmente da qualsiasi terminale connesso in rete, in uno scenario di sistemi informativi eterogenei per tecnologia, protocolli e regole, gestire un'identità digitale in modo da realizzare i requisiti di sicurezza, unicità e affidabilità appena espressi, rappresenta un compito tutt'altro che banale.

La prima osservazione che si può fare è che la gestione di un grande numero di persone, sistemi, policy e privilegi differenti introduce possibili cause di inefficienza, errori o compromissione della sicurezza.

Si deve poi considerare il fatto che soluzioni quali, per esempio, CRM, ERP o la posta elettronica si sono spesso diffuse all'interno delle aziende in relazione a specifiche esigenze e, dunque, in modo separato le une dalle altre per quanto riguarda la gestione del loro accesso. Pertanto le informazioni relative all'identità sono spesso frammentate e distribuite attraverso molteplici sistemi.

Infine ci si deve confrontare con l'esigenza, da parte di diverse funzioni aziendali (quali l'IT, la gestione delle risorse umane e la sicurezza), di mantenere un certo grado di controllo e visibilità rispetto ad alcune informazioni relative all'identità di un utente, quali il tipo di attività svolta, i privilegi di accesso o l'indirizzo di posta elettronica.
La difficoltà nell'affrontare in modo unificato e automatizzato queste difficoltà induce spesso ad adottare un sistema di controllo dell'accesso basto su procedure impostate in modo manuale che, tuttavia, introducono una serie di rischi per la sicurezza e di ritardi non accettabili in relazione, per esempio, all'attribuzione o alla revoca di privilegi.
L'affermazione del concetto di Identity Management e delle tecnologie a suo supporto nascono proprio da questa esigenza di gestione efficace dell'accesso e di autenticazione mediante un'identità digitale univoca.
L'interesse per questa tematica è alimentato (e alimenta a sua volta) dalla presenza in formato digitale di informazioni critiche per il successo di un'azienda e dalla progressiva affermazione delle modalità di erogazione di servizi on-demand.
Si capisce dunque che occuparsi di identity management non significa parlare di un prodotto, ma di una serie di modalità, regole, processi che si appoggiano su tecnologie e architetture specifiche e su un'infrastruttura di supporto per la creazione, il mantenimento e l'utilizzo di identità digitali. Pertanto, un unico tool o una singola suite di strumenti non è in grado di risolvere tutti i problemi di gestione dell'identità e dell'accesso ma serve un approccio di protezione più strutturato e integrato.
Nella relazione che intercorre tra utente e fornitore di servizio all'interno di un processo di Identity Management, l'utente deve essere garantito in termini di sicurezza, affidabilità e tutela della privacy. Da parte sua, il fornitore dei servizi deve predisporre un sistema di autenticazione che consenta di potersi fidare dell'identità dell'utente, deve esercitare un controllo costante attraverso sistemi di gestione dell'accesso basati su regole ed effettuare un'attività continua di verifica per assicurarsi che le regole vengano applicate in modo corretto.
Va detto che nella sua accezione più completa, una soluzione di identity management si adatta in modo particolare alle esigenze di una grande azienda, in cui i vantaggi forniti possono essere valorizzati e bilanciare i costi di

implementazione. In aziende con un grande numero di addetti, una soluzione di questo tipo permette, per esempio, di mettere immediatamente a disposizione di un nuovo impiegato tutte le risorse a cui ha necessità di accedere per il suo lavoro in modo rapido e attraverso una gestione centralizzata nonché di aggiornare o rimuovere immediatamente i criteri e i privilegi di un utente che fuoriesce dalla azienda o che cambia mansioni.
Il primo passo verso la realizzazione di una soluzione di Identity Management è rappresentato dalla disponibilità di Single Sign-On (SSO) che realizza la possibilità di accedere, con un unico set di credenziali, a tutte le applicazioni e i servizi a cui si ha diritto all'interno di un dominio, nel pieno mantenimento dei criteri di sicurezza e, per quanto possibile, in modo trasparente, delegando al sistema la gestione di tutto il sistema di protezione.
L'idea di base è di spostare la complessità dell'architettura di sicurezza verso il servizio di SSO, liberando così altre parti del sistema da determinati obblighi di sicurezza. Quindi un utente deve autenticarsi soltanto una volta, anche se interagisce con una molteplicità di elementi sicuri presenti all'interno dello stesso dominio. Il server SSO può essere anche rappresentato da un servizio cloud che, in un certo senso, "avvolge" l'infrastruttura di sicurezza che sovrintende alla funzione di autenticazione e autorizzazione.

La Data Loss Prevention

Quando si parla di ICT security si fa generalmente riferimento ai pericoli che sono al di fuori del perimetro aziendale, ovvero agli attacchi dei cyber criminali, ai virus, alle intrusioni nei sistemi. Gli investimenti delle aziende, che mirano a contenere al più basso livello possibile i rischi per il business, si concentrano su tecnologie quali i firewall, gli intrusion prevention o i software anti-malware, che hanno appunto il compito di elevare una sorta di muraglia difensiva che non fa entrare nella rete aziendale nessun utente e nessuna porzione di codice considerati pericolosi.
Non ci si preoccupa quasi mai, invece, di quello che i dipendenti, o comunque persone autorizzate, possono portare via dall'azienda, ovvero del pericolo che deriva dalla fuoriuscita, intenzionale o meno, di dati sensibili e informazioni

strategiche: anagrafiche clienti, listini, numeri di telefono, offerte, contratti, documenti con rilevanza legale e via discorrendo.
In assenza di policy specifiche, di un'adeguata cultura della prevenzione e di tecnologie ad hoc, è troppo facile, per chiunque abbia accesso a un pc collegato alla rete aziendale, entrare in possesso di tali documenti e divulgarli: con una chiavetta USB, con un tablet, spedendole via mail, stampandole, faxandole o banalmente salvandole nel pc portatile che poi viene rubato al bar sotto l'ufficio mentre il dipendente sta prendendo l'aperitivo. O, ancora, usando sistemi di e-mail via Web, che spesso sfuggono ai sistemi di controllo della posta aziendale, o attraverso l'instant messaging, anch'esso raramente posto sotto osservazione, o semplicemente su fogli di carta, che quasi mai vengono distrutti prima di essere gettati nei cestini.
Recenti indagini confermano che il fenomeno ha una portata significativa.
L'insieme di soluzioni tecnologiche che mirano ad arginare il problema sono definite con locuzione anglosassone di Data Loss Prevention (DLP) e vengono spesso associate a quelle di monitoraggio e filtro dei contenuti, che presentano funzionalità analoghe.
Tali soluzioni stanno attirando sempre più interesse, anche perché costituiscono una protezione di secondo livello per le intrusioni dall'esterno. Se un cyber criminale riesce a entrare nella rete aziendale, infatti, si troverà poi a dover affrontare il sistema DLP che gli impedisce di portare fuori le informazioni sensibili, per esempio con un filtro che non riconosce come valido l'indirizzo IP a cui il malintenzionato tenta di inviare i dati o con l'impossibilità di aprire il file protetto. Inoltre, potrebbe essere autorizzato ad aprire un determinato documento, per esempio un pdf, solo chi è in possesso di una specifica chiave hardware.
I vantaggi ci sono e alcuni studi lo hanno dimostrato. L'aumento dei furti di proprietà intellettuale e dati rende pressoché ineluttabile l'adozione della DLP.
Le soluzioni DLP possono agire a livello di rete o di singolo host, individuando i comportamenti non conformi alle policy che l'azienda si è data. A questo punto possono intervenire bloccando l'azione oppure mettendola in quarantena fino a che qualcuno, in possesso di opportuna autorizzazione, verifichi se esisto o no una reale violazione.

La notifica del pericolo può essere indirizzata al responsabile di settore, a quello delle risorse umane o al manager di area, ma comunque a qualcuno che sia in grado di valutare il valore dell'informazione da un punto di vista del business. Anche all'utente è opportuno segnalare il problema, poiché la maggior parte della fuoriuscita di dati non è da imputare a cattive intenzioni, ma solo a imperizia o ignoranza.
Per implementare in modo efficace questo tipo di soluzioni diventa indispensabile comprendere quali sono i dati da proteggere e qual'è il rischio che questi vengano resi noti all'esterno dell'organizzazione.
In altre parole è necessaria un'attività di risk assessment mirata a classificare i dati: un'operazione tutt'altro che banale e che, se non viene fatta con attenzione, rischia di vanificare anche la tecnologia più sofisticata.
Il rischio di falsi positivi e l'ampia zona grigia che emerge quando si cerca di dividere le informazioni da proteggere da quelle poco sensibili rendono lo scenario complesso e spostano il peso dell'investimento più sulla parte di servizi di consulenza che su quello della tecnologia in sé.

Rivedere i processi e coinvolgere i dipendenti

Definire e classificare le informazioni da proteggere è un problema complesso, ma a volte risulta ancora più complicato individuare tutte le diverse modalità con le quali i dipendenti riescono a portare le informazioni al di fuori dell'organizzazione. Ecco perché implementare una soluzione DLP può avere come risultato sia quello di rilevare le "fughe" di dati sia di identificare processi di business poco efficaci e renderli più sicuri, implementando controlli più rigorosi. In altre parole, è un'occasione per monitorare a fondo le attività e scoprire i punti deboli, verificando "chi" può accedere a "cosa".
Si pone, ancora una volta, il problema di bilanciare le esigenze di security con quelle di business, ovvero di proteggere l'azienda senza, però, porre vincoli operativi troppo stringenti che portano a inevitabili perdite di tempo e, non ultimo, a malcontento.
Questo tipo di attività richiede il massimo coinvolgimento dei dipendenti, che devono essere informati dei rischi e devono uniformarsi alle policy di sicurezza nel trattamento dei dati sensibili che ogni azienda dovrebbe avere. Tuttavia, nella pratica, ciò avviene molto raramente.

La sicurezza nell'era dell'as-a-service e del cloud

L'evoluzione verso il cloud computing rappresenta il punto finale di un lungo processo di apertura delle aziende verso l'esterno. Le reti aziendali, una volta roccaforti gelosamente celate a qualsiasi utente esterno, si sono progressivamente aperte prima ai fornitori, poi verso i clienti fino ad approdare ai social media.

Con l'avvento del cloud questa apertura è stata estesa non solo all'accesso delle informazioni, che in precedenza restavano comunque custodite all'interno di un perimetro di rete ben definito, ma alle informazioni stesse che, potenzialmente, sono libere di spostarsi ovunque e anche di allontanarsi molto dall'azienda.

Le soluzioni di protezione hanno quindi dovuto rinnovarsi ed espandere il livello di protezione perimetrale per "agganciarsi" ai dati e seguirli nei loro spostamenti.

Ecco allora che nel cloud la protezione diventa sempre più focalizzata sul dato pur mantenendo le tradizionali difese di tipo perimetrale, perché gli attacchi di tipo tradizionale continuano e, anzi, sono costantemente in crescita per numero e sofisticazione.

Il cloud stesso viene poi utilizzato per rafforzare il livello di protezione: l'analisi delle minacce si avvale, infatti, sempre più spesso di meccanismi di diffusione collettiva della conoscenza che, non appena vengono identificate nuove minacce, permettono di esercitare istantaneamente la protezione su tutti i client connessi per ridurre al minimo i rischi e i possibili contagi.

Sicurezza negli ambienti private e public cloud

Il tema della sicurezza negli ambienti private cloud è in buona parte, riconducibile a quello della protezione in ambienti virtualizzati, che ha alcuni requisiti specifici.

Tra i temi tecnologici da affrontare vi è per esempio quello di determinare dove collocare il livello di protezione in relazione all'hypervisor.

Un altro problema che emerge in modo preponderante negli ambienti virtualizzati (più che in quelli fisici) è quello della business continuity che sta

diventando anch'essa sempre più un'offerta di servizi. Per rendersene conto basta riflettere sull'impatto che può derivare dal guasto di un singolo sistema fisico su cui sono ospitate le immagini anche di migliaia di macchine virtuali.

Il cloud porta con sé anche nuove opportunità per la protezione dei sistemi informativi, con servizi di backup as a service e disaster recovery as a service, mentre si affacciano anche nel nostro Paese le prime offerte di servizi per il backup dei dati sul cloud e per il disaster recovery delle virtual machine presenti nel cloud, effettuati direttamente sul cloud anziché (o in aggiunta) sui sistemi interni all'azienda.

In molti ritengono che le opportunità più significative aperte dal cloud computing vadano ricercate nel public cloud. È infatti in questo caso che la flessibilità diventa massima ed è possibile per le aziende aggiungere risorse IT a piacere, in modalità on-demand e pagandole solo per il tempo effettivo di utilizzo, avendo la possibilità di scavalcare gli alti costi di investimento necessari per innovare e modernizzare l'infrastruttura informatica, senza doverci rinunciare.

Il public cloud, però, porta i dati fuori dall'azienda, anche se non sempre fuori dal controllo dell'azienda. Non è comunque infrequente che il proprietario delle informazioni, che è anche il soggetto che risponde di fronte alla legge di eventuali irregolarità, non sappia dove fisicamente siano collocati i propri dati o che non disponga degli strumenti per poter controllare che tutti i processi che coinvolgono i suoi dati siano conformi alle normative del proprio Paese o perlomeno alle policy interne aziendali in merito alla sicurezza.

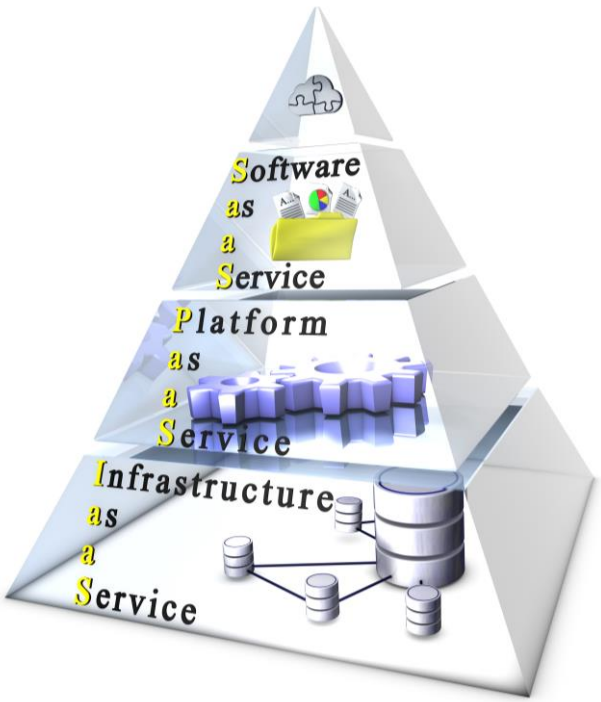
Va rimarcato che l'esternalizzazione di servizi da parte di aziende o Pubbliche Amministrazioni che adottano soluzioni di cloud computing non le esime dalle loro responsabilità legali in merito, per esempio, al trattamento o alla diffusione di dati sensibili personali. La responsabilità di assicurarsi che il fornitore di servizi cloud tratti i dati nel rispetto della Legge e delle finalità del trattamento resta, infatti, a carico dell'azienda che possiede i dati e, nel caso di trattamento illecito o diffusione incauta, sarà quella che ne risponderà direttamente.

Per garantire il livello di protezione necessario per gli ambienti public cloud sono state messe a punto sofisticate soluzioni di cifratura e gestione delle chiavi, tool per garantire la conformità, sistemi di gestione dell'accesso sicuri e operanti all'interno di strutture federate sicure.
Diventa in ogni caso essenziale scegliere in modo oculato il cloud service provider a cui affidarsi considerando che il trasferimento della gestione della sicurezza a un fornitore di servizi esterni trasforma, di fatto, le pratiche di gestione del rischio in Service Level Agreement (SLA) contrattuali valutati sulla base di parametri di riferimento specifici e oggettivi.
Ma dopo aver concordato e definito gli SLA con il security service provider, l'azienda deve anche avere a disposizione gli strumenti per monitorarli attraverso strumenti di reportistica e indicatori che possono preferibilmente anche essere personalizzati in base alle esigenze specifiche del business. La perdita del controllo diretto sulla gestione del patrimonio informativo resta, peraltro, uno dei nodi centrali che attualmente rallentano l'utilizzo dei servizi public cloud.

La sicurezza delle applicazioni eseguite nel cloud

Il software applicativo che viene sviluppato oppure eseguito all'interno degli ambienti di cloud computing si trova sottoposto a una serie di requisiti legati alla sicurezza che dipendono dalla tipologia di modello di distribuzione cloud a cui è indirizzato.
Per valutare il livello di sicurezza delle applicazioni in un ambiente cloud, i security manager aziendali si trovano, pertanto, non solo a dover decidere se sia opportuno sviluppare o eseguire un'applicazione su una piattaforma di cloud computing ma, nel caso in cui decidano di farlo, anche di scegliere accuratamente la modalità più appropriata per farlo.
Per garantire la sicurezza delle applicazioni in un ambiente cloud almeno due aspetti vanno considerati.
Il primo è di determinare i controlli di sicurezza che un'applicazione deve fornire in aggiunta al livello di controllo intrinseco alla piattaforma cloud. Un secondo punto chiave riguarda le modalità che legano il ciclo di vita di sviluppo a livello enterprise con quello degli ambienti cloud.

Questi due aspetti vanno esaminati in relazione alle differenti tipologie di piattaforma cloud ovvero IaaS, PaaS e SaaS.
All'interno di un'infrastruttura erogata sotto forma di servizio (IaaS), il fornitore mette a disposizione dell'utente diversi componenti virtuali e un primo aspetto da considerare per garantire la sicurezza applicativa è che l'immagine virtuale fornita dal provider IaaS sia sottoposta allo stesso livello di controllo di sicurezza e di conformità a cui sono soggetti gli host presenti all'interno della rete enterprise.



Le tre opzioni d'offerta di servizi cloud

Va poi evidenziato che la maggior parte delle applicazioni interne all'azienda enterprise non si preoccupa eccessivamente di garantire la sicurezza della comunicazione tra gli host di un'applicazione distribuita, poiché il traffico transita solo attraverso una rete sicura. In un ambiente cloud gli host operano, invece, all'interno di un'infrastruttura condivisa con altre aziende e, pertanto, un'applicazione "cloud based" deve farsi carico anche di garantire la

comunicazione tra host per evitare che, durante l'elaborazione, possa verificarsi una diffusione non autorizzata di dati sensibili. Tutte le precauzioni adottate all'interno dell'ambiente enterprise a protezione dei dati sensibili dovrebbero perciò essere applicate anche alle applicazioni ospitate all'interno di un ambiente IaaS.
Nel valutare l'impatto del PaaS sull'architettura di sicurezza delle applicazioni si deve tenere conto che questo tipo di piattaforme fornisce anche l'ambiente di programmazione per accedere e utilizzare i componenti applicativi aggiuntivi, il quale ha un impatto non trascurabile sull'architettura dell'applicazione.
In un ambiente Software as a Service (SaaS) vanno affrontate le medesime cautele di sicurezza degli ambienti PaaS e IaaS. Come le piattaforme PaaS, anche il SaaS rappresenta, di fatto, un nuovo ambiente di programmazione che richiede la messa a punto di specifici schemi di codifica e di progettazione sicura.
Un'azienda che decide di adottare questo tipo di servizi dovrebbe anche poter disporre di un modo per stabilire che il ciclo di vita di sviluppo del proprio fornitore di servizi software sia sicuro quanto il proprio e dovrebbe, preferibilmente, richiedere SLA contrattuali e verificabili.

Scegliere il cloud security service provider

Ma quali sono gli elementi ideali che dovrebbero caratterizzare un fornitore di servizi di sicurezza per l'ambito cloud enterprise?
Perlomeno tre sono gli aspetti che si evidenziano come particolarmente critici e che, in fase di identificazione, è opportuno considerare attentamente.
Il primo riguarda l'esistenza di un framework di riferimento che permetta di traslare le policy e le procedure in servizi reali applicabili alle attività di business e che fornisca informazioni inerenti il livello di sicurezza esistente nonché una visione sul grado di efficacia delle specifiche regole e procedure attivate.
Inoltre, è importante che un fornitore di servizi di sicurezza nel cloud metta a disposizione delle aziende anche le capacità umane necessarie per supportarle nello sviluppo di servizi aziendali, guidandole nella valutazione del livello di sicurezza esistente e della sua efficacia.

Ultimo aspetto, ma non per importanza, è che l'offerta comprenda adeguati servizi di Security service management che permettano di fondere, in un unico insieme, le attività di business e di sicurezza, favorendo lo sviluppo di un modello di governance e della valutazione dei risultati dello specifico ambiente business.
Intervenendo in queste aree fondamentali è possibile personalizzare il sistema di sicurezza in modo che risponda alle specifiche necessità di un'azienda e del suo modo di condurre il business e fare in modo che l'approccio basato sul cloud diventi un'efficace leva competitiva.
Il tema della scelta di un fornitore di servizi cloud (e quindi anche di servizi di cloud security) è stato affrontato anche dal Garante della Privacy che ha messo in evidenza l'importanza di effettuare delle verifiche sulle certificazioni possedute oltre che sui servizi offerti e sulla qualità della sua infrastruttura, sull'idoneità della piattaforma tecnologica, sulle competenze del personale e sulle misure di sicurezza che garantisce in caso si verifichino situazioni di criticità.
Se il fornitore non fa parte dell'Unione Europea è meglio verificare che sia possibile effettuare il trasferimento dei dati personali verso il Paese in questione (consentito nei casi previsti dal D.lgs. 196/2003) e che ci sia una legislazione che garantisca un adeguato livello di protezione della privacy. Altrimenti è opportuno sottoscrivere dei modelli di contratto che siano stati approvati dalla Commissione Europea e dal Garante della Privacy.
Se, invece, il fornitore svolge un ruolo da intermediario appoggiandosi a un terzo soggetto, è opportuno non perdere di vista l'allocazione fisica dei server. L'azienda deve sapere con certezza sotto quale giurisdizione risiedono i dati per conoscere la legge applicabile nel caso di controversie tra l'utente e il fornitore del servizio o in cui l'autorità giudiziaria debba eseguire ordini di perquisizioni, sequestro e così via.
Nel caso in cui l'azienda decide di trasferire il servizio a un nuovo fornitore, bisogna accertarsi anche dei tempi che intercorrono dalla scadenza del contratto alla cancellazione definitiva dei dati da parte del fornitore che li ha avuti in gestione, il quale deve garantire di non conservare i dati oltre i termini stabiliti per contratto.

Sempre nell'ottica di un passaggio ad altro fornitore è utile privilegiare i servizi che garantiscono la portabilità dei dati, quindi basati su formati e standard aperti, che facilitino la transizione da un sistema cloud a un altro, anche se gestiti da fornitori diversi.

La protezione crittografica dei dati

La crittografia è una scienza antica, nata per proteggere le comunicazioni militari ai tempi di Giulio Cesare. Il concetto è semplice: inventare una regola che modifica il significato del dato scritto, cosicché non possa essere compreso da chi non conosce tale regola.
I sistemi più antichi si basavano sulla trasposizione delle lettere dell'alfabeto. Il metodo Cesareo, per esempio, sostituiva ogni lettera con quella successiva: in questo modo ROMA diventava SPNB. Una versione più evoluta di questi sistemi prevedeva anche una regola di sostituzione.
La crittografia moderna si basa ancora sui sistemi di sostituzione e trasposizione, ma la sicurezza non è più affidata alla segretezza dell'algoritmo di cifratura (i sistemi di crittografia moderni sono, infatti, rilasciati con i codici sorgenti), ma a quella di una chiave esterna. Le tecniche di crittografia delle informazioni si basano, infatti, su sofisticati algoritmi di tipo matematico che utilizzano una chiave per modificare il dato. Quanto più bit sono utilizzati, quanto più è lunga la chiave, tanto più, tanta più potenza di calcolo sarà necessaria per "crackare" il sistema e ottenere la chiave.
Il limite di un modello di crittografia statica è di non essere in grado di modificare il tipo di protezione offerta in funzione dell'esperienza acquisita. In altre parole, una volta superata la protezione cifrata, il successivo tentativo di intrusione non incontrerà più ostacoli.
Considerando che la disponibilità di potenza di calcolo è in continua crescita, si intuisce quanto rapidamente possa aumentare l'obsolescenza di un sistema per la cifratura, che dipende dalle prestazioni dei computer disponibili e dagli sviluppi delle tecniche di criptoanalisi. Anche grazie alla dinamicità offerta dalla virtualizzazione e dal cloud, si stanno sviluppando nuove tecniche di crittografia che prevedono una cifratura "interna" al dato stesso, in particolare per applicazioni in ambito cloud storage.

Su altri fronti, si lavora per migliorare la criptazione dei canali per la comunicazione.
In ogni caso, le soluzioni di sicurezza crittografiche vanno riviste periodicamente nel tempo, per garantire che il livello di protezione si mantenga costante e adeguato.
Da un punto di vista del business, le funzioni di sicurezza garantite dalla crittografia contribuiscono in modo significativo a estendere il livello di protezione nel processo di gestione degli accessi, intervenendo nei seguenti ambiti:

- Autenticazione, che assicura che il mittente e il destinatario di un messaggio siano quelli che affermano di essere;
- Confidenzialità, che fa in modo che le informazioni siano accessibili solo da chi è preposto a farlo;
- Integrità, garantendo la non alterazione delle informazioni da parte di persone non autorizzate;
- Non ripudiabilità, impedendo a utenti di negare la paternità delle informazioni trasmesse;
- Identità, verificando l'associazione tra uno specifico individuo e una risorsa o un'informazione;
- Autorizzazione, che definisce i privilegi e le azioni permesse rispetto a una specifica risorsa.

Le tecniche di crittografia delle informazioni utilizzano sofisticati algoritmi di tipo matematico per rendere incomprensibili i dati a un utente non autorizzato e fornire nel contempo, a chi è autorizzato a farlo, la possibilità di ricostruire le informazioni in un formato comprensibile riconvertendo il testo cifrato in testo in chiaro.
Lo strumento alla base del processo di cifratura/decifrazione delle informazioni è quello della gestione delle chiavi.
I modelli di base da cui discendono le diverse evoluzioni dei sistemi di gestione delle chiavi sono quelli a chiave condivisa e chiave pubblica, che vengono brevemente ricordati di seguito.

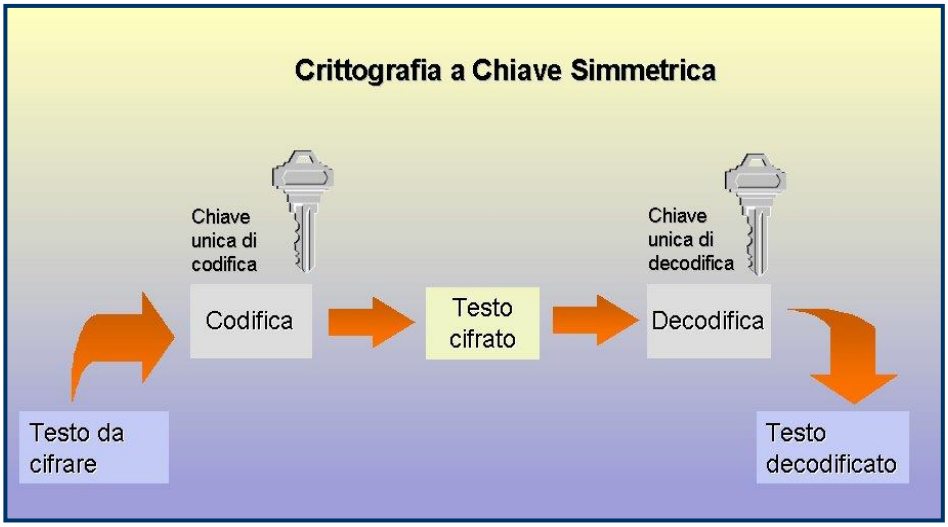
Il sistema di crittografia simmetrico o a chiave condivisa

Un sistema di crittografia simmetrica (detto anche a chiave condivisa) prevede che venga utilizzata un'unica chiave per effettuare le operazioni di cifratura e decifrazione del testo.

Si tratta di un sistema che si basa sulla reciproca fiducia delle due parti e in cui i detentori della chiave, che in questo contesto viene anche detta "privata" (per distinguerla da quella "pubblica"), confidano sulla protezione che ognuno, reciprocamente, garantirà alla chiave in suo possesso. Questo sistema richiede una fase di scambio della chiave tra le due parti che deve essere effettuata in condizioni di sicurezza.

Si tratta di un metodo che consente di cifrare grandi quantità di dati in modo rapido e veloce, soprattutto se eseguito in modalità hardware.

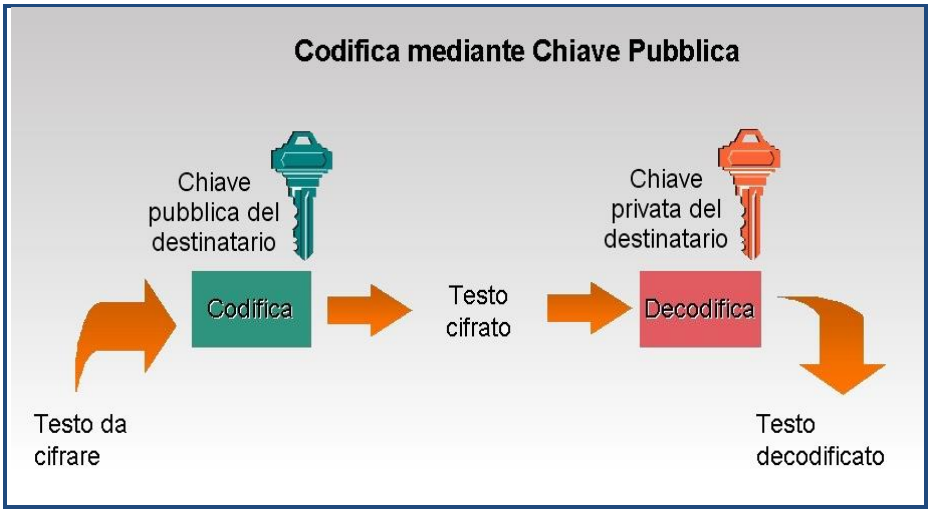
La garanzia di sicurezza in questo sistema è determinata dalla dimensione della chiave: quanto più è lunga la chiave, tanto più numerosi sono i tentativi che devono essere effettuati per individuarla.



Schema di un sistema di crittografia simmetrico basato sull'uso di chiavi private

Il sistema di crittografia asimmetrico o a chiave pubblica

La crittografia di tipo asimmetrico prevede l'utilizzo di due chiavi distinte che interoperano tra loro per realizzare le procedure di cifratura e decifrazione dei dati. Le due chiavi, una pubblica e una privata, hanno funzionalità reciproca, in modo che i dati cifrati con una chiave possono essere decifrati solo con l'altra.
Ogni utente dispone di due chiavi: una chiave privata specifica e univoca conosciuta solo dal suo possessore e una chiave, detta pubblica, inserita in un archivio liberamente consultabile e mantenuto a cura di un ente certificatore (Certification Authority).
Un utente che voglia inviare un messaggio protetto, provvede a cifrarlo mediante la chiave pubblica del destinatario, il quale potrà risalire al messaggio originale decifrandolo per mezzo della propria chiave privata.
Questo sistema si basa sul principio che la conoscenza della chiave di cifratura non permette di ricostruire alcuna informazione su quella di decifrazione, poiché le due chiavi non hanno alcun elemento in comune.



Schema di un sistema di crittografia asimmetrico basato sull'uso di una coppia di chiavi distinte (pubblica e privata)

I sistemi crittografici di tipo asimmetrico garantiscono un elevato livello di sicurezza, ma richiedono una notevole potenza di calcolo e sono più lenti di

quelli simmetrici. Richiedono, inoltre, massima attenzione nella conservazione della chiave privata poiché, in caso di sua perdita, l'unico modo per recuperare i dati è quello di ricorrere ad agenti autorizzati.

Protezione nel cloud con una crittografia embedded

L'esigenza di una crescente sicurezza nell'accesso alle informazioni è fortemente aumentata con la diffusione di Internet e con lo sviluppo di modelli di interazione tra aziende che hanno portato a un concetto di azienda estesa, dove la relazione tra le entità coinvolte si basa sulla certezza dell'interlocutore (sia esso una persona fisica o un programma) e sulla inalterabilità dei dati e delle informazioni (per esempio ordini, fatture, bolle di spedizione, documenti amministrativi e legali, bollette) che sono scambiate nel corso delle usuali attività di business.
I nuovi modelli cloud e l'affermazione della mobilità hanno ulteriormente contribuito a complicare lo scenario della gestione del rischio. Per esempio, la componente di cloud pubblica rende difficoltoso sia conoscere la collocazione fisica dei dati di business affidati al proprio cloud provider sia riuscire a seguirli nei loro spostamenti.
Indipendentemente dall'approccio di sicurezza seguito, il dato rappresenta, in ultima analisi, l'elemento da proteggere.
Proteggere i dati significa molte cose: garantirne la disponibilità, l'accessibilità, la conservazione ma, dal punto di vista del business, una delle esigenze primarie è quella di impedirne la diffusione non autorizzata e la riservatezza.
In molti casi mantenere i dati privati e sicuri costituisce anche un requisito di conformità, per esempio alle norme Sarbanes-Oxley (SOX), al Payment Card Industry Data Security Standard (PCI DSS) o alle direttive sulla protezione dei dati dell'Unione Europea che richiedono che le organizzazioni proteggano i loro dati a riposo e garantiscano efficaci difese contro le minacce.
L'adozione di tecnologie di crittografa consente di predisporre un livello di sicurezza intrinseco al dato stesso, che viene esercitato al momento stesso della sua creazione e che è in grado di spostarsi insieme all'informazione.
Questo livello di protezione è alla base dell'offerta di soluzioni che si appoggiano a servizi "on demand" per proteggere i dati inattivi, attivi e in

uso nel corso del loro intero ciclo di vita, all'interno di ambienti cloud, on-premises e mobili. Si tratta di soluzioni di ultima generazione, in massima parte ancora in fase di start up e che, in estrema sintesi applicano la cifratura nel momento in cui si chiede l'accesso al dato. La chiave, in taluni casi, può cambiare per ogni dato.
Molte di queste tecnologie nascono per la protezione in ambito mobile, per cui la protezione viene attivata nel cloud e non dal dispositivo. Una precauzione importante per le applicazioni di pagamento tramite device mobili.

Crittografia e cloud

Diverse sono i benefici che le aziende possono ottenere spostando applicazioni e dati nel cloud: dalla scalabilità, all'agilità, alla riduzione dei costi. Tuttavia, ai potenziali vantaggi sono associati anche nuovi rischi.
Peraltro, va ricordato che i cloud provider che offrono servizi di Infrastructure as a Service (IaaS) e Platform as a Service (PaaS) propongono solitamente un modello di "responsabilità condivisa" per le applicazioni e i dati dei loro clienti e, di conseguenza, la responsabilità della sicurezza dei dati nel cloud è un problema la cui soluzione spetta alle aziende proprietarie dei dati.
La crittografia dei dati è uno dei metodi più efficaci per proteggere i dati a riposo nel cloud, ma non tutte le tecnologie sono identiche. Al fine di selezionare la soluzione più efficace per le proprie specifiche esigenze aziendali, è importante analizzare alcuni aspetti fondamentali legati alla gestione del processo di crittografia e al modo in cui viene esercitata la protezione dei dati in uso o a riposo attraverso ogni fase del loro ciclo di vita e a come viene affrontata la gestione e la sicurezza delle chiavi di crittografia.
Una delle preoccupazioni primarie per chi sceglie modelli cloud di tipo ibrido o pubblico è proprio quella di garantire la massima segretezza delle chiavi di cifratura riuscendo, nel contempo, a mantenerne la proprietà e il controllo: due obiettivi spesso tra loro antagonisti.
Infatti, tutti i sistemi di crittografia dei dati, sia nel cloud o in un data center fisico, condividono una vulnerabilità comune: hanno bisogno di utilizzare le

chiavi di crittografia e, quando queste sono in uso, è possibile, ipoteticamente, rubarle.
Nell'analizzare una soluzione di crittografia è anche opportune valutarne il livello di versatilità e la sua capacità di supportare i diversi possibili casi d'uso: crittografia del disco, del database, del file system e dello storage distribuito.

STRATEGIE E SOLUZIONI PER LA SICUREZZA E LA PROTEZIONE DEL DATO

CyberArk

Proteggere le credenziali è il punto chiave per la sicurezza degli utenti privilegiati

Per garantire la sicurezza degli account privilegiati CyberArk, società specializzata nella protezione di questo tipo di utenti business critici per le aziende a causa dei dati riservati di cui sono sovente in possesso, sia quando operano dal loro ufficio che quando si trovano in mobility e accedono alle applicazioni e ai dati mediante dispositivi mobili, ha inglobato nel suo portfolio numerosi sviluppi che permettono di accelerare l'adozione di soluzioni di sicurezza che si posizionano tra quelle più avanzate disponibili sul mercato.
Le funzionalità hanno l'obiettivo primario di rendere più semplici le modalità necessarie per rafforzare la sicurezza, migliorare l'automazione dei processi di security e ridurre il rischio complessivo in cui possono incorrere gli utenti privilegiati. Nel loro insieme, evidenzia CyberArk, fanno di CyberArk Privileged Account Security Solution V10 (CyberArk V10) una piattaforma di sicurezza che può facilmente scalare in funzionalità al fine di proteggere da exploit critici gli account privilegiati ovunque si trovino, sia quando utilizzano infrastrutture ICT on-premise che quando accedono ad applicazioni e dati tramite ambienti cloud ibrido o attraverso workflow DevOps.

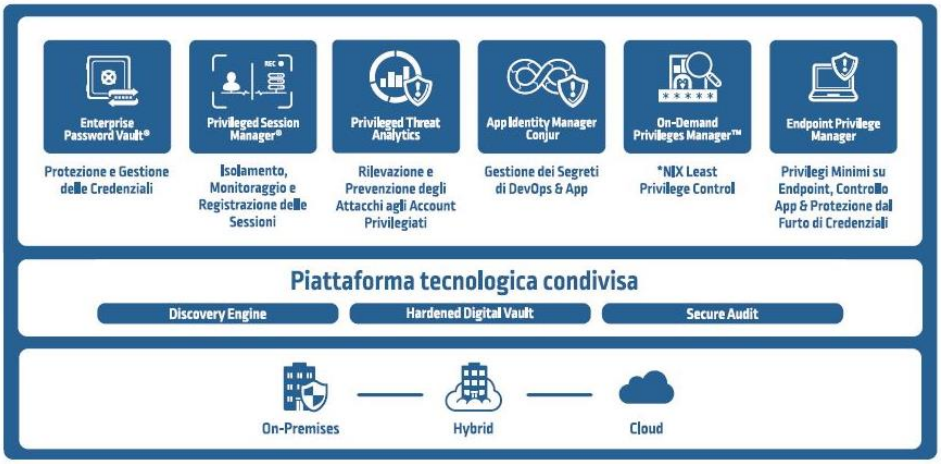
Accelerazione dei processi di sicurezza

Un punto chiave di CyberArk v10 è di accelerare fortemente il deployment di una soluzione di sicurezza e semplificare i processi di protezione degli account privilegiati. L'obiettivo è perseguito tramite:

7. Biometria e videosorveglianza: la sicurezza logica incontra quella fisica

- **User experience semplice e snella:** gli aggiornamenti apportati con la V10 hanno perseguito l'obiettivo di ridurre di un ordine di grandezza il tempo che deve essere dedicato per garantire la protezione dei privileged account e allo stesso tempo ridurre di un fattore 5 l'impegno che deve essere dedicato dagli auditor IT nell'analisi delle registrazioni delle sessioni. La nuova user interface semplifica anche i workflow, visualizza i rischi, monitorizza le attività privilegiate ed è compliant con quanto prescritto da policy e Audit.

- **Strategia Customer-Driven basata su API**: Si basa su API funzionalmente estese che permettono di accelerare l'integrazione della soluzione CyberArk Privileged Account Security all'interno dell'architettura di sicurezza esistente, delle Operation e degli strumenti DevOps. Ad esempio, nuove REST API danno la possibilità ai responsabili IT di ridurre di sino al 90% il tempo necessario per inserire nel sistema di sicurezza gli account, un aspetto questo molto critico in aziende di ampie dimensioni che devono distribuire e fornire la sicurezza a migliaia di utenti contemporaneamente.



Le funzioni di CyberArk Privileged Account Security Solution

Machine learning per una protezione ubiqua delle credenziali

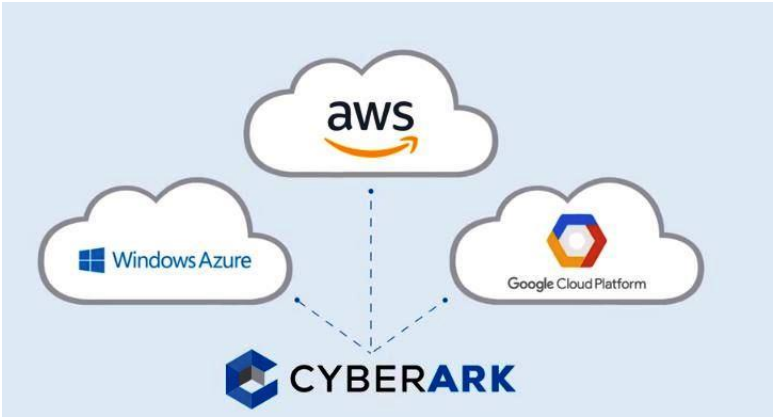
La crescente mobilità di personale e manager che costituiscono account privilegiati e l'utilizzo di reti mobili e cloud per accedere ai dati e collaborare pone il problema di come proteggere adeguatamente le credenziali in contesti ad alto rischio, sia per le carenze nei criteri di security che possono essere native delle reti o del cloud pubblico utilizzato, che dell'ambiente pubblico in cui l'account privilegiato fisicamente si muove. Credenziali non adeguatamente protette costituiscono un target molto attraente per gli attaccanti esterni o per malintenzionati interni all'azienda stessa.
Si tratta di rischi che sono amplificati per quelle aziende che hanno fatto del cloud la loro strategia di digital transformation e hanno allo stesso tempo accelerato l'adozione di DevOps.
Indipendentemente dalle dimensioni dell'azienda, le nuove funzionalità presenti nella versione V10 di CyberArk Privileged Account Security Solution sono volte a permettere di :

- Prevenire l'attacco ad account privilegiati sugli Endpoint: Gli end-point costituiscono uno dei punti maggiormente critici per la sicurezza, soprattutto per la crescente mobility degli utenti privilegiati. Per eliminare il rischio connesso alla perdita di dati o credenziali, CyberArk ha sviluppato CyberArk Endpoint Privilege Manager, una soluzione che ha il compito di bloccare e contenere attacchi dannosi proteggendo l'end-point da exploit che mirano alle credenziali privilegiate. In pratica, tramite le funzionalità contenute in CyberArk Application Risk Analysis Service si ha la possibilità, mediante funzioni di machine learning e analitiche basate su cloud, di aiutare a bloccare gli attaccanti e impedire, rilevando le applicazioni potenzialmente dannose e in grado di accedere a dati e informazioni sensibili, che questi possano posizionarsi in un end-point.

- **Accelerare la sicurezza nel Cloud:** V10 estende il supporto per Amazon Web Services (AWS), automatizza il caricamento delle credenziali tramite l'integrazione con CloudWatch e Auto Scaling. In pratica, viene

ridotto significativamente il rischio di credenziali non gestite in ambienti di elastic computing e il team dedito alla sicurezza ha la possibilità di ridurre sensibilmente il tempo che vi deve dedicare in modo da potersi meglio focalizzare sulla mitigazione dei potenziali rischi. CyberArk garantisce anche la sicurezza delle credenziali attraverso piattaforme cloud pubbliche quali AWS, Microsoft Azure e Google Cloud Platform (GCP) ed ha validato la sua capacità di attivare la sicurezza per account privilegiati su AWS in un massimo di 15 minuti.

Per quanto concerne il cloud e le funzionalità di CyberArk Privileged Account Security Solution v10 relativamente alla Google Cloud Platform (GCP), la tipica configurazione GCP comprende l'esecuzione delle vault primarie e di disaster recovery, nonché il monitoraggio della sessione in modo da rendere sicuro il workload che gira in un ambiente nativo GCP.



Con CyberArk utenti privilegiati e credenziali sono protette on-premise e nel cloud

L'organizzazione aziendale può, in alternativa, estendere la propria installazione di CyberArk (ad esempio che gira su piattaforma on-premise, AWS o Azure) in modo che possa aiutare nel rendere sicuro anche l'accesso alla console GCP e a renderne sicuri i relativi workload.

Citrix

La ricetta per proteggere il business e la reputazione delle aziende nell'era del cloud ibrido

Nuove e sempre più sofisticate minacce, un perimetro aziendale che per effetto della trasformazione digitale assume confini meno definiti e quindi più difficili da proteggere, una graduale migrazione dei workload dalla rete locale al cloud, regolamenti comunitari (come il GDPR) che richiedono l'adozione di misure di sicurezza ben oltre l'ambito prettamente tecnologico: sono questi solo alcuni dei principali problemi delle aziende italiane, a cavallo tra l'esigenza di crescere nel competitivo scenario internazionale e il rischio costante di vedere messa a repentaglio la propria immagine e la sicurezza dei dati critici per il proprio business e per quello dei clienti.

Per contrastare queste e altre minacce in costante evoluzione senza rinunciare ai benefici della trasformazione digitale, le imprese devono adottare nuovi paradigmi di cybersecurity basati su sistemi, architetture e modelli che tengano in considerazione l'evoluzione del mondo IT. In base a una recente survey, l'83% dei CIO, CISO e IT Executive ritiene che la complessità delle infrastrutture IT tradizionali non rappresenti soltanto un problema per il business, ma introduca anche un considerevole rischio di sicurezza.

«*Sebbene tuttora in atto, la Digital Transformation ha già modificato in maniera significativa i connotati delle imprese. Ciò che un tempo era un'eccezione, ovvero la presenza di lavoratori mobili, l'utilizzo di device personali per l'accesso a dati aziendali, la fruizione di servizi cloud e così via, è diventato ormai una regola e la Security non può che adeguarsi al nuovo scenario*", evidenzia David Cenciotti, Sales Engineer e Security Evangelist di Citrix.

Con l'avvento del cloud, dello smart working e l'imminente proliferazione dei device IoT (Internet of Things) è dunque necessario cambiare approccio: occorre definire un nuovo perimetro digitale di sicurezza e gestire il cyber risk in un ambiente ibrido, in cui l'utente accede in mobilità, da qualsiasi rete e con qualsiasi device ad applicazioni e dati che possono essere situati ovunque, all'interno di un data center o nella "nuvola". In tale scenario, il posto di lavoro non è più un luogo ben preciso, ma una configurazione che assume caratteristiche differenti a seconda del "contesto".

David Cenciotti, Sales Engineer e Security Evangelist di Citrix Systems

Facciamo un esempio molto semplice: si consideri un utente che deve accedere a un'applicazione aziendale.
Se l'utente si collega da un hotspot pubblico all'interno di un aeroporto, ovvero da un ambiente non presidiato dove il rischio di sicurezza è più elevato, dovrà superare uno o più step di autenticazione supplementari e avrà l'accesso limitato a un sottoinsieme di applicazioni rispetto al dipendente che accede dalla sede aziendale e che lo potrà fare autenticandosi una sola volta.
Parliamo quindi di "Secure Digital Workspace", ovvero di uno spazio di lavoro virtuale, che segue l'utente e adatta le misure di sicurezza al contesto di accesso. È un modo per garantire la sicurezza rendendo la security "sostenibile", cioè senza inficiare la fruibilità dell'applicazione».

In questo modo, un "perimetro digitale sicuro" consente di applicare un approccio centralizzato basato sull'identità, ma anche di cambiare molto rapidamente e dinamicamente le policy aziendali.
Si possono scegliere impostazioni diverse per chi si collega al cloud, dall'ufficio o da un'altra postazione ritenuta sicura e per chi invece si connette da un hot spot pubblico in un aeroporto o da un albergo.
Location, dispositivo usato (e caratteristiche specifiche dello stesso), applicazione richiesta e comportamento dell'utente sono tutti elementi utilizzabili per variare le condizioni di accesso e uso delle applicazioni e dei servizi aziendali. Sono dati, infatti, che permettono di definire una "postura" di sicurezza attorno alla quale applicare le regole aziendali.
Ma non solo. Uno degli aspetti più importanti del nuovo paradigma di sicurezza Citrix è rappresentato dall'utilizzo di strumenti di analisi predittiva che consentono la rilevazione degli attacchi e l'adozione di contromisure in maniera automatizzata.
Per contrastare in maniera efficace le minacce più evolute è infatti necessario acquisire quella che gli esperti Citrix definiscono "Information Superiority", ovvero una superiorità informativa basata sulla conoscenza di quanto accade all'interno e all'esterno del Secure Digital Perimeter e tradurla, grazie a logiche di Machine Learning, in capacità di scoperta di attacchi che si nascondono nel "rumore di fondo" della normale operatività o che si sviluppano in intervalli temporali molto ampi.

Gli elementi Secure Digital Perimeter

Il Secure Digital Perimeter è un modello che semplifica l'erogazione di applicazioni su qualsiasi device, garantendo una security a 360 gradi, attiva, reattiva e predittiva attraverso strumenti di analytics che permettono di estendere il controllo anche nel cloud.
I mattoni di questo modello, spiega Cenciotti, sono:

- La Virtualizzazione delle sessioni, ovvero l'esecuzione centralizzata delle applicazioni, indifferentemente da luogo, rete e dispositivo, grazie a un app store dal quale viene lanciata l'applicazione.

- L'Application Delivery Controller, vero front-end dell'applicazione virtualizzata, che implementa le policy di autenticazione, security e ottimizzazione e che pubblica l'app store, disaccoppiando l'utente dalla risorsa acceduta
- L'SD-WAN è la tecnologia usata per ottimizzare le prestazioni per gli utenti remoti, potendo realizzare anche un'infrastruttura hybrid cloud, interfacciandosi con i provider.
- Il Mobile Store che controlla le applicazioni installate sui sistemi mobile in uno scenario BYOD (Bring Your Own Device)
- L'Analytics Service, cioè la componente essenziale per la gestione dell'architettura, basata su algoritmi di machine learning e Big Data analysis, per fornire la massima visibilità agli IT manager sull'intero ambiente con tracciamento delle irregolarità nel comportamento degli utenti.
- Management Plane, ovvero lo strato di management, per effettuare le configurazioni di tutta l'architettura.

La cosa interessante è che ognuno di questi componenti è disponibile sia on-premise (ovvero localmente) che direttamente sul Cloud di Citrix.

F-Secure

Endpoint al sicuro con l'intelligenza artificiale e il blocco compartimentale che migliorano la difesa dal cyber crime

F-Secure, società che sviluppa soluzioni per la cyber security, ha annunciato il potenziamento della sua suite per la sicurezza degli endpoint, Protection Service for Business, una soluzione di sicurezza basata su cloud.
La nuova versione è stata sviluppata per migliorare la propria tecnologia di protezione degli endpoint aggiungendovi capacità di blocco comportamentale per Windows e Mac in modo da proteggere contro le minacce usate dagli attaccanti.
Protection Service for Business comprende la tecnologia XFENCE, che l'azienda ha annunciato lo scorso Aprile, e ora ne ha integrato le capacità in Computer Protection for Macs.
F-Secure XFENCE evita che processi e applicazioni abbiano accesso ai file, ai dati, e anche a microfoni, tastiere, e webcam senza il permesso dell'utente.
Fondamentalmente agisce come un firewall per file evitando, per esempio, che il ransomware crittografi file sui dispositivi infettati. La nuova release include numerosi aggiornamenti, tra cui:

- Un motore di rilevazione su base comportamentale per Windows, DeepGuard di F-Secure che include un uso estensivo dell'intelligenza artificiale per prendere decisioni su file e processi malevoli senza chiedere nulla agli utenti.
- Un firewall aggiornato con una maggior compatibilità con applicazioni e appliance di terze parti, nonché un set di regole per contrastare le minacce

come ad esempio quelle ransomware auto-propaganti e a movimento laterale.

- Una gestione dei profili che facilita la schedulazione delle scansioni, il profile grouping, il product filtering.
- Una funzionalità di Device Control che impedisce l'uso di hardware non autorizzato come chiavette USB, hard disk esterni e webcam.

Protection Service for Business, la soluzione F-Secure basata su Cloud

Un portfolio per la security riconosciuto da Gartner

L'offerta attuale di protezione per gli endpoint cloud-based Protection Service for Business si affianca a Business Suite, una soluzione per la sicurezza on-premise anch'essa erogante capacità di protezione basate sul comportamento.
Entrambe le soluzioni, tramite numerosi miglioramenti funzionali apportati nell'ultimo anno, permettono di affrontare i punti deboli delle organizzazioni in fatto di cyber security e assicurano la protezione dalle minacce più recenti.
A Protection Service for Business, per esempio, è stato aggiunto DataGuard, una funzione che fornisce un livello ulteriore di protezione contro minacce come il

ransomware; una nuova funzione di protezione delle password che rende semplice usare password forti e univoche per le organizzazioni; e un'architettura software migliorata che permette a F-Secure di sviluppare e implementare rapidamente aggiornamenti o nuove funzionalità.
A questo si aggiunge nel portfolio F-Secure anche una soluzione di rilevazione e risposta (detection and response) chiamata Rapid Detection Service.
L'approccio alla cyber security adottato da F-Secure e centrato sull'analisi comportamentale e sull'intelligenza artificiale è stato riconosciuto da Gartner, che l'ha posizionata come Visionaria nel report Magic Quadrant 2018 per le Piattaforme di Protezione Endpoint.

Protezione degli end-point e IoT

La sicurezza degli end-point vede F-Secure impegnata anche nel segmento in forte evoluzione dell'IoT.
L'Internet of Things (IoT) così come la si conosce, osserva F-Secure, apre forti opportunità per quanto concerne la digital transformation e l'evoluzione verso una smart economy ma, di fatto, rappresenta una minaccia considerevole per i consumatori a causa di regolamenti inadeguati sulla sicurezza e sulla privacy.
Questo è quanto evidenziano e su cui mettono in guardia gli esperti intervistati nella realizzazione del report "*Internet of Things: Pinning down the IoT"* sponsorizzato da F-Secure.
Milioni di dispositivi end-point e connessi in rete o via Cloud, evidenzia F-Secure, sono già stati compromessi per essere usati come parte della botnet Mirai.
E non sono pochi i produttori che immettono prodotti velocemente sul mercato senza prendere in considerazione i requisiti e le impostazioni minime di sicurezza. Anche se milioni di nuovi dispositivi si connettono online ogni giorno, gli utenti non sono poi ancora generalmente consapevoli che i loro nuovi apparati "intelligenti" andranno online.
«*Col tempo quasi tutti i dispositivi domestici saranno online e non sembreranno dispositivi intelligenti all'utente finale. Sembreranno dispositivi stupidi, ma saranno in realtà intelligenti pur non offrendo alcuna funzionalità al consumatore finale, perché il vero motivo per cui andranno online sarà per*

*riferire e riportare dati al produttore che li ha costruit*i», mette in guardia nel report Mikko Hypponen, Chief Research Officer di F-Secure.
La prova dell'assunto di Hypponen è semplice: già oggi è difficile trovare un modello di un qualsiasi dispositivo, ad esempio un televisore, che non supporti la connessione a Internet.

Mikko Hypponen, Chief Research Officer di F-Secure

La realtà, evidenzia F-Secure, è che in breve tempo miliardi di dispositivi saranno potenziali punti di attacco alla sicurezza e le aziende sembrano ignorare il problema, e sino a che gli utenti non inizieranno a chiedere che questi dispositivi siano anche sicuri i produttori difficilmente considereranno la sicurezza come una priorità.
F-Secure è attivamente impegnata nel garantire la sicurezza degli end-point ma la loro parte devono farla anche i governi, che devono preoccuparsi della qualità della tecnologia che viene messa nelle mani e nelle case degli utenti, si osserva nel report.

Forcepoint

L’analisi predittiva e comportamentale in ambiente cloud rende sicuri dati e applicazioni

Il diffondersi del concetto di Smart IT e l’impatto che su di esso ha la sicurezza, ha come corollario negativo l’intensificarsi dell’intelligenza degli attacchi cibernetici. Il problema che si pone è che, secondo Gartner, il tempo medio per rilevare una violazione è di oltre tre mesi, cosa che lascia a malware e ad altri tipi di attacchi il tempo di infiltrarsi e localizzarsi.
Un modo per ridurre questo intervallo consiste nello sfruttare dati ed analitiche. La società di ricerca prevede in proposito che entro il 2018 l'80 per cento delle piattaforme di protezione degli endpoint includerà il monitoraggio delle attività e le capacità forensi e stima che almeno un quarto delle violazioni verrà evidenziato attraverso l’analisi del comportamento degli utenti e degli asset.

La criticità del cloud e degli ambienti ibridi

Il problema dei tempi intercorrenti tra il rilevamento di un nuovo tipo di attacco e il momento in cui le patch sono disponibili risulta enfatizzato quando da un ambiente esclusivamente privato si passa ad un ambiente migrato sul cloud pubblico o a uno scenario cloud di tipo ibrido o multi cloud.
La combinazione di ambienti IT caratterizzati da una forte presenza di dispositivi mobili che si collegano alle applicazioni business tramite infrastrutture cloud ibride e multi-cloud apre la strada a problematiche connesse allo stato di aggiornamento delle infrastrutture di terzi che si interpongono tra il dispositivo end user e il data center o i data center dove risiedono dati e applicazioni.

Non che i service provider non siano più che intenzionati ad apportare rapidamente le necessarie correzioni ma la realtà è caratterizzata dal fatto che non pochi degli operatori hanno sviluppato le loro infrastrutture quando gli attacchi apportati da cyber hacker non erano così sofisticati come lo sono ora, con la capacità che hanno di far leva su attacchi distribuiti, complessi e strutturati, attacchi che richiedono per essere rilevati da analisi approfondite non solo del traffico, ma anche di come questo si scosta per il singolo cliente da quello che è l'usuale comportamento delle applicazioni business fruite.
In sostanza, può avvenire che per mettersi al passo con la sofisticatezza degli attacchi e delle capacità elaborative e di analisi richieste si renda necessario apportare modifiche significative alla infrastruttura che data la scala di intervento richiesta ad un provider possono finire con il ritardare l'entrata in funzione delle contromisure di sicurezza atte a contrastarli.
Per rimuovere questo potenziale vulnus, Forcepoint, bypassando e compensando le eventuali carenze dell'infrastruttura cloud dei provider, ha spiegato Luca Mairani, Senior Sales Engineer di Forcepoint in Italia, ha puntato sull'analisi comportamentale estesa a livello di end-point.

Luca Mariani – Sales Engineer di Forcepoint

La società, che è un'azienda che sviluppa software di sicurezza operante a livello mondiale e con un solido background in due dei temi più all'attenzione dei manager, la cyber security e il cloud, ha con questo obiettivo di recente aggiunto al proprio peraltro già ampio portfolio di soluzioni per la sicurezza in cloud, nuove funzionalità che abilitano ulteriori controlli comportamentali previsionali che semplificano la protezione dei dipendenti, dei dati aziendali critici e della proprietà intellettuale.

Sicurezza più Smart con l'analisi comportamentale

La vision strategica è consistita nel rendere disponibili funzionalità basate sull'analisi del comportamento e sull'analisi predittiva, volte a rafforzare le policy di sicurezza per quanto concerne lo scambio dei dati tra ambiente informatico legacy da e verso il cloud esterno (CASB: Cloud Access Security Broker), come ad esempio nel caso delle banche i cui dipendenti utilizzano Microsoft Office 365, la sicurezza su Web e quella della posta elettronica.
Approcciare la security attraverso un filtro human-centric, osserva Forcepoint, aiuta le organizzazioni a comprendere meglio gli indicatori del normale comportamento informatico e identificare rapidamente attività e operazioni, quali la shadow IT, che rappresentano i maggiori rischi.
Il rafforzamento delle policy di sicurezza è stato perseguito con lo sviluppo di funzionalità che permettono di valutare il rischio di condivisione di file e di altre applicazioni cloud e proteggono dalla perdita di dati sensibili non archiviati nella rete aziendale, analizzando parametri quali il comportamento dell'utente e le caratteristiche dell'applicazione, ad esempio i dati, il dispositivo e la posizione da cui si accede.

Microsoft 365 e Azure sicure con Forcepoint CASB

L'obiettivo di rafforzare e rendere sicure le attività in Cloud e in ambienti quali Microsoft 365 e Azure si è concretizzato, come in precedenza evidenziato, con il recente rilascio di ulteriori controlli di analisi comportamentale che permettono

di semplificare la protezione di dipendenti, dati aziendali critici e proprietà intellettuale.
Le funzionalità, disponibili per Forcepoint CASB, Forcepoint Web Security e Forcepoint Email Security, hanno l'obiettivo primario di fruire del cloud come motore per lo sviluppo del proprio business in modo sicuro e affidabile. L'obiettivo, per le specifiche soluzioni, è stato perseguito apportando aggiornamenti che comprendono rispettivamente:

- **Forcepoint Web Security**: funzionalità che consentono un controllo più granulare delle applicazioni cloud e bloccano eventuali attività di shadow IT.
- **Forcepoint Web Security**: strumenti di migrazione in cloud che consentono agli utilizzatori di Forcepoint Web Security con installazioni locali di migrare in ambiente Cloud in qualsiasi momento.
- **Advanced Malware Detection (AMD) Powered by Lastline:** disponibile per le piattaforme on-premise e in Cloud Forcepoint Web Security e Forcepoint email security. L'integrazione della tecnologia AMD sandbox consente poi di proteggere in tempo reale gli utenti ovunque si trovino.

In pratica, la analisi comportamentali di Forcepoint CASB analizzano il comportamento dell'utente e le caratteristiche dell'applicazione, ad esempio i dati, il dispositivo e la posizione da dove si accede. A questo Forcepoint ha aggiunto una rinnovata User Risk Dashboard single-view che evidenzia sia le attività dei dipendenti che il potenziale impatto sul business basato sulle autorizzazioni che l'utente detiene all'interno dell'organizzazione.

Fortinet

L’automazione è il modo più immediato per ridurre i rischi aziendali

Secondo una recente ricerca commissionata da Fortinet, specialista della network security, quasi la metà dei decision maker appartenenti al dipartimento IT in aziende di tutto il mondo, con oltre 250 dipendenti, ritiene ancora che il management non veda nella cyber security una priorità assoluta, né un’area d'interesse, nonostante continuino a verificarsi attacchi informatici di alto profilo.

Le minacce, peraltro, continuano ad aumentare d'intensità, forse anche a causa di questo atteggiamento, infatti Filippo Monticelli, regional director Italy in Fortinet, riporta: «Il nostro Global Threat Landscape Report mette in evidenza come una scarsa attenzione alle pratiche di sicurezza informatica e l'utilizzo di applicazioni rischiose consentano ad attacchi distruttivi worm-like di sfruttare gli exploit a velocità record. I criminali impiegano meno tempo a sviluppare nuove modalità d'intrusione, concentrandosi invece sull'uso di strumenti automatici e intent-based per insinuarsi con un maggiore impatto sulla continuità del business». Il manager italiano, aggiunge, però: «Negli anni abbiamo visto come la cyber security sia diventata un investimento fondamentale per le aziende, dove un numero crescente di manager di alto profillo la considerano parte integrante della propria strategia IT».

Oggi siamo quindi in una fase per certi versi transitoria, con il 44% dei decision maker IT italiani, il quale ritiene che la sicurezza informatica non rappresenti ancora una priorità assoluta per il consiglio di amministrazione. Ma ciò non sembra avere un impatto sui budget, dato che il 53% delle aziende dichiara di aver investito addirittura oltre il 10% del proprio budget IT in sicurezza, in aumento dallo scorso anno per il 72% degli intervistati.

Inoltre i manager, per il 79%, sono convinti che la cyber security diverrà una priorità assoluta. Una tendenza guidata, secondo i rispondenti italiani, da tre fattori chiave:

- Aumento di security breach e attacchi informatici a livello globale, che ha influenzato il 48%delle aziende, soprattutto dopo attacchi globali come WannaCry.
- Maggiore pressione dai regolamenti, soprattutto per il rischio delle pesanti sanzioni previste dal GDPR.
- Migrazione verso il cloud nell'ambito del proprio percorso di trasformazione digitale, che spinge a investire in sicurezza il 77% delle imprese, con 83% degli intervistati che indica in come priorità assoluta la cloud security nei prossimi 12 mesi.

Filippo Monticelli, regional director Italy in Fortinet

La sicurezza automatica con il Security Fabric

Fortinet ha investito da tempo nello sviluppo di sistemi in grado di correlare tutti i dati raccolti dagli strumenti presenti sulla rete aziendale, affinché questi possano intervenire automaticamente quando rilevano attività che

potenzialmente nascondono una minaccia. Oggi il Fortinet Security Fabric è un elemento chiave di una strategia di Intent-Based Network Security caratterizzata da funzionalità avanzate di automazione quali self-provisioning, self-operating e self-correcting.
Le reti "Intent-Based" sono nate nell'intento, appunto, di svolgere al meglio i servizi che s'intendono realizzare, in pratica per supportare la digital transformation e aumentare l'agilità della rete, incrementando al contempo affidabilità e disponibilità.
La crescente complessità delle reti, da un lato, la carenza delle competenze (progettazione, implementazione e operatività) dall'altro e la necessità di gestire processi sempre più in tempo reale, praticamente obbligano a un'automazione sempre più spinta.
A complemento delle tecnologie di rete specifiche, la vision di Fortinet è di fornire alle reti Intent-Based una sicurezza che permetterà al Security Fabric di tradurre automaticamente le necessità di business in azioni per la sicurezza di rete sincronizzate senza intervento umano.
A detta dei responsabili di Fortinet, ciò consentirà di progettare architetture di sicurezza avanzate, ma più semplici da gestire riducendo gli oneri operativi, fino a fornire infrastrutture tecnologiche in gran parte autosufficienti, capaci di mantenere una posizione di sicurezza ottimale su tutta la superficie di attacco.
L'automazione del Security Fabric è anche la chiave per un futuro sicuro per l'IoT, affermano sempre in Fortinet, evidenziando l'onerosità di analisi in un tale contesto, impossibile da gestire senza automazione.
Il Security Fabric è anche la risposta alle preoccupazioni, espresse in recente studio di ESG Research da un 62% di professionisti della cyber security, circa la difficoltà a ottenere lo stesso livello di visibilità sui workload che si trovano nel cloud, rispetto a quelli nel reti fisiche. Così come fornisce una soluzione al 56% dello stesso campione che non ha livelli appropriati per l'automazione e orchestrazione necessari per il cloud.

Il Global Threat Landscape Report di Fortinet

La ricerca, effettuata dagli esperti del FortiGuard Labs di Fortinet su base trimestrale, evidenzia come una scarsa attenzione alle pratiche di sicurezza

informatica e l'utilizzo di applicazioni rischiose facilitano lo sviluppo di nuove modalità d'intrusione.
Di seguito alcuni elementi di riflessione.
Attacchi disastrosi, come WannaCry e NotPetya, resi noti dalle cronache e appartenenti alla categoria dei worm-like, non sarebbero stati neanche realizzati se le imprese avessero una buona gestione della sicurezza, mantenendo aggiornati i sistemi e applicando le patch, spiegano gli esperti dei FortiGuard Labs. A parte le modalità di diffusione, il ramsonware che approfitta delle vulnerabilità è comunque in crescita: il. 90% delle organizzazioni ha registrato exploit su vulnerabilità vecchie di tre o più anni. Anche dopo dieci o più anni dalla scoperta di una falla, il 60% delle imprese registra ancora attacchi correlati.
Le minacce automatizzate non si riposano mai: quasi il 44% di tutti i tentativi di attacco si sono verificati il sabato o la domenica. Il volume medio giornaliero nei fine settimana è stato il doppio dei giorni feriali.
I cybercriminali sono pronti a sfruttare debolezze o opportunità legate a nuove tecnologie o servizi. In particolare, l'uso di software di estrazione non aziendale e la vulnerabilità dei dispositivi IoT su reti iperconnesse rappresentano un rischio potenziale se non gestiti correttamente.
La crittografia del traffico Web, in forte crescita, anche se è un bene per la privacy e la sicurezza su Internet, crea problemi a molti strumenti di difesa, che hanno scarsa visibilità su comunicazioni crittografate.
Le applicazioni non sicure, come il peer-to-peer, creano vettori di rischio: le aziende che le consentono registrano botnet e malware sette volte più numerosi rispetto a quelle che non le consentono. Analogamente, le aziende che consentono applicazioni proxy denunciano una presenza di botnet e malware quasi nove volte superiore rispetto a quelle che non le consentono.
Quasi un’organizzazione su cinque ha registrato un malware destinato ai dispositivi mobili, mentre quelli IoT sono una sfida perché non hanno il livello di controllo, visibilità e protezione dei sistemi tradizionali.

G DATA

Risk management e trasferimento del rischio a un'assicurazione è l'approccio di G DATA alla sicurezza

La sicurezza IT è un argomento che non si dovrebbe sottovalutare in nessuna circostanza, tuttavia ad essa non sempre viene tributata la dovuta attenzione, specie nelle piccole aziende che non dispongono di personale interno specializzato. L'entrata in vigore del GDPR obbliga però a confrontarsi con molteplici proposte non di rado poco chiare.
In questo frangente, l'offerta "GDPR-ready" di G DATA, diretta in Italia dal suo country manager Giulio Vada, proprio ai fini della chiarezza contempla strumenti con cui si è proposta di consentire alle PMI di avventurarsi nel percorso verso la compliance con tranquillità, esternalizzare la gestione della sicurezza della propria infrastruttura e trasferire il rischio economico residuo a terzi.

Controllo e tutela dell'IT su misura e a consumo

Le recenti sfide informatiche hanno reso improcrastinabile un radicale cambiamento di paradigma per le politiche di sicurezza IT. La sicurezza, intesa come best practice e tutela integrata degli asset aziendali, va considerata quale parte integrante del risk management e quindi deve permeare i processi produttivi di qualsiasi organizzazione.
Ciò non solo per adeguarsi al GDPR ma soprattutto per proteggersi efficacemente contro le perdite economiche conseguenti ad un incidente

informatico, contro l'impatto economico delle sanzioni previste e l'impatto reputazionale in presenza di un furto di dati.
Quello della sicurezza è però un impegno a largo spettro. Una risposta olistica che la vede come un processo e non un mero prodotto è stata ideata da G DATA con lo sviluppo di soluzioni che consentono di implementare una buona strategia di sicurezza, con la garanzia di avvalersi di strumenti conformi ai dettami del nuovo regolamento e in grado di proteggere in modo proattivo l'infrastruttura IT dalle eventuali minacce.

Giulio Vada, country manager di G Data Italia

La sicurezza IT si coniuga con il risk management

Ai fini operativi, tramite la suite G DATA Total Control Business l'azienda ha voluto mettere a disposizione delle aziende una soluzione che fosse affidabile contro minacce esterne e interne e restituire all'IT manager la supervisione costante della propria infrastruttura.

Per farlo, la suite monitora la rete verificando lo stato operativo dei sistemi e notifica in tempo reale eventuali disservizi o comportamenti anomali delle macchine.
A questo abbina una piattaforma di patch management che semplifica la manutenzione di periferiche e client e velocizza la chiusura di vulnerabilità come quelle sfruttate da WannaCry e Petya.
La soluzione fa inoltre leva sulla nuova tecnologia anti-ransomware integrata in tutte le suite per la sicurezza del suo portfolio e consente di gestire policy e filtri centralmente, anche per i dispositivi mobili, che vengono gestiti come qualsiasi altro client di rete. In pratica, evidenzia G DATA, implementare la suite permette di ancorare saldamente la sicurezza IT al risk management.
Per le aziende che hanno l'esigenza di ottimizzare Capex e Opex, le soluzioni sono fruibili anche in modalità MES (G DATA Managed Endpoint Security), una formula a consumo che si fa carico delle esigenze di flessibilità delle aziende che desiderano esternalizzare i servizi di sicurezza IT affidandoli a professionisti, di abbattere gli investimenti e diluire i costi operativi in canoni mensili.
A ciò aggiunge la possibilità di attivare o disattivare tempestivamente licenze in base alle esigenze, con un controllo trasparente dei costi e delle installazioni attraverso una piattaforma professionale per la gestione remota quotidiana del parco installato.

Conoscere le vulnerabilità dell'infrastruttura a priori

Implementare qualsiasi misura protettiva senza aver condotto un'analisi delle vulnerabilità dell'infrastruttura equivale ad affidarsi al caso, una condizione già intrinsecamente rischiosa. Dato che il mero malfunzionamento di un sistema critico ha ripercussioni economiche che, in base a gravità ed estensione, potrebbero minare l'esistenza dell'azienda, è quanto meno opportuno identificare tutti i fattori di rischio presenti nella rete.
Per aiutare le aziende a valutare le vulnerabilità delle infrastrutture, G DATA ha sviluppato il servizio G DATA Advanced Analytics, che sarà disponibile progressivamente a partire dal secondo trimestre 2018.
Con l'introduzione del GDPR, osserva G DATA, è necessario adottare le migliori armi di difesa presenti sul mercato per mettere in sicurezza la rete aziendale e

i dati trattati, ma questo non senza un'attenta analisi preliminare dell'infrastruttura.

Trasferire il rischio residuo a un'assicurazione cyber

Con l'introduzione del GDPR le aziende devono preoccuparsi più che in precedenza del rischio di furto di dati sensibili e della vulnerabilità dell'infrastruttura di operatori a cui hanno commissionato servizi che richiedono la condivisione dei propri dati riservati.
Ai rischi legati alla propria sicurezza concorre anche l'intrinseca debolezza dei processi legati al trattamento dei dati rispetto alle esigenze normative.
Dalla collaborazione tra G DATA, Reale Mutua e il broker Margas, è così derivata la soluzione Insurtech, denominata Privacy & Cyber Risk, che integra le tecnologie di sicurezza G DATA con una polizza assicurativa per la Responsabilità Civile dedicata alle PMI, in modo che queste possano intraprendere più tranquillamente il percorso verso la compliance normativa.
La polizza non sostituisce una corretta Data Governance, avvisa G DATA, ma sostiene finanziariamente i fruitori delle proprie soluzioni in caso di leakage, trasmissione di ransomware e pubblicazione di informazioni lesive della reputazione e della privacy di terzi, come conseguenza di un incidente informatico.

Veeam

Business always-on e dati critici al sicuro su Microsoft Azure eliminano i costi del ripristino

Il business delle aziende dipende ormai fortemente dall'information technology, a cui si richiedono piani precisi atti a mantenere l'operatività qualora si verifichino interruzioni di servizio.
La realtà però è che, nonostante il rischio di danni economici e di immagine consistenti, per molte aziende le strategie per il backup e il ripristino volte a mettere in sicurezza la continuità del business non sono sostenibili, o si avviano a non esserlo: da un lato il costo di un sito di ripristino remoto per un sistema replicato, con hardware e software duplicati, è proibitivo a causa dell'elevata spesa in conto capitale; dall'altro il backup e il ripristino richiedono elevati investimenti in termini di tempo e risorse.
Una risposta all'esigenza di coniugare sicurezza e economicità l'ha ideata Veeam Software, specializzata nelle soluzioni per l'Availability for the Always-On Enterprise, con l'annuncio di Veeam Recovery to Microsoft Azure with Veeam PN (Powered Network).
E' una soluzione on-demand, già disponibile, che ha l'obiettivo di assicurare una rapida continuità operativa e che include anche il nuovo prodotto gratuito Veeam PN, una soluzione software defined networking (SDN che elimina la necessità di creare VPN e semplifica la configurazione di rete quando si vuole creare un sito di ripristino su Microsoft Azure.

Dati al sicuro su Azure

Veeam Recovery to Microsoft Azure fornisce in pratica, ha evidenziato Veeam, un mezzo semplice e sicuro per il recupero dei carichi di lavoro on-premises su cloud pubblico.

I responsabili IT possono avviare automaticamente un'istanza cloud Azure ed erogare in modo sicuro servizi a clienti, partner e dipendenti raggiungibili ovunque essi siano, il tutto senza dover sopportare gli investimenti necessari per realizzare in azienda un sistema ridondante di standby.
A livello funzionale la nuova soluzione, che viene fornita già pronta all'uso, abilita il ripristino cloud per i backup Veeam ed è arricchita come accennato da Veeam PN, una soluzione SDN per definire un sito di ripristino in Microsoft Azure.
Veeam Recovery to Microsoft Azure con Veeam PN fornisce un recupero dati basato su cloud e permette di evitare le spese connesse alla costruzione e manutenzione di un sito remoto di ripristino di proprietà.
«*Con Veeam Recovery to Microsoft Azure, i dirigenti e gli imprenditori possono dormire sonni tranquilli, sapendo che, in caso di disastro, l'azienda continuerà ad operare nel cloud pubblico - senza spendere una fortuna od occupare tutto il tempo del personale IT*», ha osservato Danny Allan, Vice President Product Strategy di Veeam.
Veeam Recovery to Microsoft Azure con Veeam PN è stato espressamente progettato per semplificare e automatizzare la configurazione di un sito di ripristino in Microsoft Azure riducendo la complessità delle implementazioni di VPN, indipendentemente dalle dimensioni delle aziende o dei service provider, e fornire un collegamento di rete sicuro tra le risorse IT locali e quelle in Azure mediante una connettività da sito a sito.

Veeam assicura la business continuity

Una conferma del livello di sicurezza e di business continuity garantite dalle soluzioni Veeam arriva dalla decisione di KPNQwest di adottarne le soluzioni per garantire la continuità operativa ai propri clienti.
KPNQwest Italia, società nazionale che offre servizi di telecomunicazioni su tutto il territorio italiano, ha scelto Veeam Backup Replication Enterprise Plus per supportare l'efficienza, la visibilità e la scalabilità su diversi ambienti IT, oltre a supportare i propri clienti nel percorso di Digital Transformation caratterizzato dalla disponibilità dei dati "Always On" e dalla rapidità di ripristino.

KPNQwest Italia fornisce a migliaia di aziende italiane servizi di connettività in fibra ottica, data center e cloud computing ad altissima affidabilità e performance. Tali servizi sono erogati a partire da quattro data center di proprietà, ubicati presso il "Fiber Hub" italiano di via Caldera a Milano, ed attraverso una rete di accesso in larga banda nazionale.

«*Ciò che ci contraddistingue nel settore dei Cloud Service Provider è l'alta specializzazione dell'infrastruttura. L'offerta KPNQwest Italia unisce l'affidabilità, la sicurezza, le prestazioni e la resilienza della propria infrastruttura di data center alle migliori tecnologie hardware e software per il cloud computing disponibili, per creare il servizio di Virtual Data Center tra i migliori presenti sul mercato*», ha osservato Matteo Flavi, product manager di KPNQwest Italia.

Tra le soluzioni per l'always-on sul mercato, ha evidenziato l'azienda, la soluzione Veeam è stata quella che si è rivelata più matura ed idonea per il mondo degli Internet Service Provider rispetto a soluzioni più complesse ma carenti di funzionalità fondamentali, come ad esempio il restore agentless su qualunque sistema operativo ed ancora di più per le ampie funzionalità di multi-cloud.

Albert Zammar, SEMEA Vice President di Veeam Software

«*Siamo orgogliosi di essere stati scelti da KPNQwest Italia per tante ragioni diverse. Ci hanno scelto per la nostra indiscussa superiorità tecnologica e perché moltissimi dei loro clienti, che utilizzavano già la soluzione Veeam, ne hanno promosso presso KPNQwest la semplicità, la scalabilità e la perfetta integrazione con gli ambienti multi- cloud. Questo per noi è un apprezzamento molto importante e ci lusinga molto*», ha commentato Albert Zammar, SEMEA Vice President di Veeam Software.

StormShield

Per un'Industria 4.0 sicura servono soluzioni specializzate e standard severi

Il susseguirsi di cyber attacchi nell'ultimo anno ha portato all'attenzione del mondo industriale e dei servizi ad esso rivolti il fatto che un semplice incidente informatico può avere conseguenze catastrofiche, dall'interruzione della produzione alla chiusura di interi siti produttivi, dalla perdita di dati aziendali critici al danneggiamento della reputazione di un brand.
Il mondo produttivo si trova quotidianamente a confrontarsi con attacchi sempre più sofisticati, che evidenziano la difficoltà di aziende private come degli enti della PA di rispondere efficacemente a minacce di nuova generazione, come se i rischi informatici tangessero esclusivamente terzi.
E' però assolutamente illusorio, mette in guardia Alberto Brera, Country Manager di Stormshield Italia, pensare che i cyber attacchi possano essere fermati del tutto. Le aziende devono però rinunciare al ruolo di spettatore passivo che si sono ascritte e prendere provvedimenti.
Proteggere l'azienda con soluzioni adeguate ha di certo un costo, non nasconde il manager, ma tale investimento è necessario tanto quanto siglare una polizza assicurativa: la sicurezza IT va inquadrata come colonna portante di una strategia di governance aziendale contemplando tutti gli aspetti di natura tecnologica e organizzativa.

Una protezione certificata UE, dal posto di lavoro alla rete

Per affiancarsi e supportare il mondo industriale nell'affrontare in modo sicuro il processo della digital transformation e le problematiche poste dalla crescente interazione tra OT (tecnologia operativa tradizionale) e l'IT (infrastruttura informatica), Stormshield ha sviluppato un portafoglio di soluzioni che affronta

la cyber security su più livelli e ambiti aziendali. Esso comprende soluzioni di sicurezza punto-punto per la protezione delle reti (Stormshield Network Security), delle postazioni di lavoro (Stormshield Endpoint Security) e dei dati (Stormshield Data Security).
Come osserva l'azienda, si tratta di soluzioni di nuova generazione certificate dai severi enti europei preposti (EU RESTRICTED, e ANSSI EAL4+) e dalla NATO, atte a garantire la protezione delle informazioni strategiche, dei processi produttivi e di business in modo affidabile.
Implementabili in qualsiasi tipologia di azienda, istituzione ed organizzazione, si rivelano ideali per la flessibilità con cui si adattano ad ogni esigenza e sono commercializzate attraverso una rete di distributori, integratori di sistema e operatori certificati in grado di erogare un qualificato servizio pre e post vendita.

Alberto Brera, Country Manager di Stormshield Italia

Partnership per un'Industry 4.0 sicura

Il problema della sicurezza permea profondamente il settore industriale. Nonostante il crescente interesse per un'Industry 4.0, in Italia il settore manifatturiero sembra focalizzarsi primariamente su esigenze business quali la remotizzazione delle operazioni e del monitoraggio di sistemi esistenti, più che

trasformarsi in industria di nuova generazione, e mettere in secondo piano valutazioni concernenti i rischi connessi a questa innovazione strategica.
Ne è la riprova, evidenzia Stormshield, un test condotto nel 2016 che ha rivelato oltre 13.000 sistemi SCADA esposti su internet senza alcun controllo.
A fronte del tipico ciclo di vita di un impianto, è un dato che nel 2017 non avrà subito grandi variazioni. Il problema è che i firewall tradizionalmente specializzati nella prevenzione di incidenti informatici in una rete aziendale non sono in grado di interpretare i protocolli SCADA, né di individuare un eventuale traffico malevolo o non autorizzato su tali protocolli, dando luogo ad un quadro allarmante come quello evidenziato, ma evitabile con soluzioni di sicurezza adeguate.
Dello stesso parere di Brera è anche Gruppo SIGLA, partner di Stormshield, che operando da anni nel settore dell'automazione industriale presso principali aziende sia nazionali che multinazionali, osserva come queste reagiscano all'esigenza di aprirsi sempre più verso utenti ed applicazioni esterne, introducendo apparati che possano integrarsi a quelli esistenti, facendo quindi evolvere l'infrastruttura attualmente in uso per evitare di rinnovarla completamente.

Sni40, firewall industriale per la sicurezza dei sistemi IT e OT

Un punto chiave della partnership tra il produttore e Gruppo Sigla è l'attenzione dedicata da Stormshield alla messa in sicurezza dei sistemi di produzione con una proposta di sistemi UTM/IPS sviluppati attorno al mondo SCADA, in grado di reagire proattivamente contro le minacce che nascono al crocevia tra l'automazione industriale e la rete informatica, con l'obiettivo primario di supportare concretamente le aziende manifatturiere a trasformarsi in Industry 4.0 in accordo al principio della sicurezza 'by design'.

Strategica per Stormshield al fine di abilitare un'Industry 4.0 a prova di cyber crime è anche la partnership con Schneider Electric, azienda specializzata nella gestione dell'energia e nell'automazione.

La complementarità delle rispettive aree di competenza – quella di Stormshield nella protezione di reti, server e workstation, e quella di Schneider Electric in ambito OT – ha portato allo sviluppo di un prodotto di sicurezza flessibile, lo Stormshield Sni40, un firewall industriale "hardenizzato", specificamente progettato per far fronte alle esigenze di sicurezza dei sistemi IT e OT e quindi adatto ai diversi ambienti industriali, in cui Sni40 riconosce e fornisce protezione proattiva anche per il traffico dati SCADA.

Radware

Applicazioni al sicuro con i cloud service per l'analisi comportamentale e la gestione automatica delle policy

Approntare soluzioni in grado di bloccare attacchi sempre più sofisticati è un compito complesso. Richiede una profonda esperienza nel settore e una pari conoscenza delle dinamiche aziendali e delle specifiche esigenze, in primis quelle normative.
Un approccio pragmatico al problema è stato adottato da Radware, società pubblica worldwide con oltre 1000 dipendenti, che per individuare le specifiche necessità ha realizzato un rapporto centrato sulle applicazioni globali e sulla sicurezza delle reti in modo da individuare le dinamiche derivabili da attacchi e casi reali di clienti e identificare cosa serve ai manager preposti della sicurezza.
Il rapporto ha evidenziato punti specifici che sono stati alla base delle risposte date da Radware tramite i suoi canali commerciali , tra questi Arrow, tra i maggiori attori italiani nella distribuzione di soluzioni di sicurezza, alle esigenze emerse. In particolare:

- Lo scenario di chi attacca, cosa attacca e perché attacca
- I l potenziale impatto sulle aziende in termini di costi associati ai vari cyber-attacchi
- Le esperienze di organizzazioni dei vari settori
- Le minacce emergenti e come proteggersi

I paragrafi seguenti esaminano come Radware ha risposto alle esigenze espresse dai responsabili della sicurezza tramite servizi fruibili in cloud, che permettono di esternalizzare la complessità insita nell'assicurare una protezione aggiornata, dinamica e aderente alle normative.

Al sicuro con l'analisi comportamentale

La sfida che si pone quando si migrano applicazioni su cloud, evidenzia Nicola Cavallina, Channel Manager per Italia di Radware, è quella del controllo, della governance e della visibilità. Per contrastare attacchi DDoS che possono bloccare le applicazioni, Radware ha sviluppato il servizio *Cloud DDoS Protection Service*, basato su un robusto motore di analisi comportamentale. Il servizio protegge da attacchi DDoS sia la rete aziendale che le applicazioni, crea firme dinamiche in tempo reale per proteggere contro attacchi zero-day e dispone di una protezione SSL DDoS adattabile a specifiche esigenze. La soluzione è completata da una dashboard che dà una profonda visibilità sia sulla rete interna che nel cloud.
Come gli altri sviluppati da RADware, ha evidenziato Cavallina, permette di esternalizzare il compito della sicurezza e di disporre di una sicurezza sempre aggiornata e garantita da SLA.

Nicola Cavallina, Channel Manager Italia, Grecia, Cipro e Malta di Radware

Cloud WAF Service per la protezione in Web

Un secondo aspetto critico, osserva Cavallina, è la complessità nello sviluppo di applicazioni web e la vulnerabilità a cui sono soggette. Per contrastare le minacce Radware ha sviluppato il servizio *Cloud WAF*, basato su un modello di machine learning che fornisce una esaustiva protezione contro le vulnerabilità evidenziate da OWASP, la comunità aperta che abilita le organizzazioni a sviluppare applicazioni sicure. Il servizio mappa in real-time le applicazioni, individua i cambiamenti e attiva dinamicamente le policy che ottimizzano la sicurezza. Tra i compiti del servizio vi sono policy di sicurezza che individuano ed eliminano i falsi positivi, realizzano una protezione DDoS built-in, integrano la protezione da attacchi Bot net e aiutano nel proteggere i dati in aderenza al GDPR.
Numerose le certificazioni, che includono PCI e HIPAA e standard di sicurezza in cloud quali le ISO 27001, ISO 27017, ISO 27018 e ISO 27032.

Cloud Malware Protection Service

Un ulteriore punto critico per le aziende è costituito dai malware zero-day, circa il 50% degli attacchi malware, e che non sono identificabili dai sistemi basati sulla firma sino a che non è disponibile.
Il servizio, che protegge oltre 2 milioni di utenti, complementa le soluzioni dei clienti e difende da malware zero-day analizzando i log file anonimizzati delle comunicazioni su Internet. I dati sono analizzati da oltre 70 algoritimi concorrenti di machine learning, analisi comportamentale e tecniche di sandboxing che isolano in fase di test i potenziali malware e reti di bot Command& Control.
Per verificare le difese analizza il comportamento posturale relativo ai malware e alle policy di sicurezza, valuta la resilienza delle infrastrutture verso comportamenti non corretti nella comunicazione verso l'esterno e compara lo stato di protezione dei gateway verso internet in riferimento a benchmark globali.

Partnership al servizio delle aziende

“Radware è per Arrow una componente fondamentale della nostra offerta in tema Sicurezza, Cloud e IoT”, ha dichiarato Roberto Branz, Division Director Security e IoT Arrow ECS Italia, “Con Radware i partner di Arrow hanno a disposizione gli strumenti ideali per proteggere il business a valore dei loro clienti. La protezione garantita dai servizi Cloud permette quella continuità di business necessaria alle aziende innovative che cavalcano progetti IoT, cloud computing e intelligenza artificiale”.

Roberto Branz, Division Director Security e IoT Arrow ECS Italia

Proprio in ambito IoT, Arrow ha avviato il programma “Sensor to Sunset” in EMEA, una iniziativa per sviluppare l’ecosistema IoT e facilitare il percorso dei partner di canale nel loro mercato. E’ una strategia che ha fatto di Arrow un distributore globale in grado di offrire soluzioni IoT affidabili e sicure, per soddisfare ogni aspetto tecnologico. Con il programma IoT, basato su un’ampia gamma di soluzioni e servizi professionali gestiti, in cui si inserisce anche il portfolio Radware, fornisce al canale anche nuove opportunità di vendita.

Selta

Mettere al sicuro le infrastrutture e le public utilities richiede soluzioni ad hoc e una profonda conoscenza tecnologica

Il diffondersi della trasformazione digitale, l'evoluzione verso l'Industry 4.0 e la realizzazione di infrastrutture e servizi pubblici a forte automazione, sta ponendo all'attenzione di manager e autorità pubbliche il problema di come proteggere adeguatamente infrastrutture, fabbriche e servizi, che per loro natura devono essere sempre operativi e a prova di attacchi cibernetici.
Se realizzare soluzioni di protezione per l'end user, il suo pc, lo smartphone o il tablet, è relativamente semplice e le soluzioni sul mercato non mancano, ben diverso si presenta il problema quando si tratta di garantire la sicurezza di impianti e servizi pubblici primari perché, evidenzia Selta, azienda italiana specializzata nello sviluppo di soluzioni per infrastrutture critiche, questo richiede una forte esperienza impiantistica nel settore e nei relativi standard, dallo SCADA all'IoT, nonché dei dispositivi connessi.
«*Selta è nata 45 anni fa nel settore dell'automazione delle reti energetiche, poi si è espansa alle Tlc tradizionali. Tutto quello che è il mondo dell'IoT e dell'automazione è quindi un ambito che percorre da decenni. Da molti anni SELTA si occupa di cyber security, prima ancora che si chiamasse così, e quindi per noi unire le diverse anime che ci rappresentano è stato piuttosto semplice. Oggi Selta è proiettata nel mercato della creazione di soluzioni e fornitura di servizi per le infrastrutture critiche nazionali, con un occhio particolare alla sicurezza. Si tratta di soluzioni innovative e soprattutto progettate in Italia nei nostri due centri di R&D perché, nonostante farlo sia complicato e costoso, riteniamo che la progettazione di infrastrutture critiche nel Paese e anche all'estero, fatta e certificata in Italia, sia intrinsecamente più sicura*», ha evidenziato Gianluca Attura, AD di Selta.

Gianluca Attura , Amministratore Delegato di Selta

Infrastrutture critiche, SCADA e IoT al sicuro con la tecnologia italiana

I settori di interesse e in cui Selta opera sono tipicamente quelli infrastrutturali. Le soluzioni che sviluppa trovano applicazione nella sicurezza ed efficienza di impianti critici per l'economia nazionale e il benessere dei cittadini. Tra queste: embedded cyber security per settori quali i trasporti e i servizi di telecomunicazioni; l'accesso sicuro a reti ultrabroadband di service provider; la sicurezza di soluzioni UCC/IoT in ambienti cloud e on-premise pubblici e privati; la sicurezza di ambienti governativi e della difesa.

Uno dei settori su cui si sono concentrati gli sviluppi della società è quello dell'IoT e delle soluzioni SCADA, alla base dell'Industry 4.0. La interconnessione in rete di apparati e impianti industriali e la diffusione di dispositivi IoT, se migliora produzione e time to market, apre però la strada ad attacchi potenzialmente disastrosi.

Basandosi sull'esperienza acquisita negli anni nel settore industriale, Selta ha sviluppato soluzioni e servizi specifici per la protezione ad alto livello di ambienti

SCADA, in modo da garantirne non solo la protezione ma anche la business continuity e il disaster recovery.

«Per quanto concerne l'offerta di Selta, a partire dai sistemi di automazione energetica, sviluppiamo soluzioni che mettono in sicurezza le infrastrutture critiche, consentono l'applicazione di protocolli di sicurezza internazionali, sistemi di telecomunicazione cifrati, eccetera. Siamo però molto attenti e preoccupati per l'estensione del mondo dell'IoT, perché si è sviluppato in maniera disorganica e insicura. Basti pensare che esistono nove famiglie di protocolli principali, più una infinità di sotto protocolli; uno scenario che apre enormi falle nella sicurezza. Così come siamo preoccupati per i sistemi SCADA e siccome SCADA è alla base di grandi infrastrutture critiche, il compito che ci siamo assunti è di operare al fine di creare attorno al mondo SCADA una bolla di sicurezza che permetta di filtrare eventuali attacchi. In un mondo dove la tecnologia ha preso il sopravvento dobbiamo fare il possibile affinché la sua diffusione sia messa sotto controllo», ha osservato Attura.

La cyber security inizia dall'uomo

L'approccio alla Cyber Security si articola, nella strategia di Selta, in due direzioni complementari: lo sviluppo di soluzioni e la fornitura di servizi di sicurezza.

Il portfolio di prodotti comprende soluzioni per la protezione dell'ambiente di lavoro, la gestione di dati classificati o non classificati, sistemi anti

intercettamento (protezione da intercettazioni realizzate tramite emissioni elettromagnetiche del computer).

Ampio è parimenti il portfolio dei servizi. Comprende servizi di consulenza professionale nella progettazione di reti sicure, l'analisi delle vulnerabilità, assessment, cybersecurity e crittografia, la gestione a più livelli di dati classificati, soluzioni di disaster recovery.

Per chi desidera esternalizzare del tutto la complessità della Cyber Security Selta fornisce soluzioni per l'erogazione di servizi di gestione dal centro. Ma in definitiva, mette in guardia Attura, il problema è nell'essere umano.

«Il problema della Cyber Security è principalmente un problema umano , non di infrastrutture tecnologiche. Gli attacchi avvengono perché all'interno delle aziende ci sono uomini. Quindi si deve partire da una grande campagna di informazione e sensibilizzazione, oltre che dalla definizione di architetture segmentabili in modo che l'attacco possa essere individuato prima che si diffonda; resta fondamentale comunque partire dalla strategia e dalla formazione delle persone, dopo e solo dopo intervengono le macchine e l'infrastruttura tecnologica. Selta, con la sua esperienza e la sua offerta, può supportare efficacemente le aziende in tutto questo», mette in guardia Attura.

Trend Micro

Le analisi sulla cyber security preannunciano il dilagare degli attacchi informatici

Il 2018 appena iniziato vedrà crescere ancora la pressione del cybercrime, con vecchie e nuove minacce, oltre quelle "reingegnerizzate". Gli oltre duemila ricercatori di Trend Micro hanno stilato le previsioni sulla sicurezza, che vede sempre più strumenti automatici sofisticati utilizzare tecnologie all'avanguardia, come il machine learning e la blockchain, per eludere i controlli e sfruttare ogni vulnerabilità.

Queste ultime sono i "buchi" del software che andrebbero "rattoppati" con le operazioni dette di patch management, sulle quali punta il dito Gastone Nencini, country manager di Trend Micro Italia: «Molti attacchi, che sono stati devastanti nel 2017, hanno sfruttato vulnerabilità conosciute e le loro conseguenze si sarebbero potute evitare se i sistemi fossero stati aggiornati preventivamente. Per questo patch management e formazione dei dipendenti devono diventare una priorità».

Per questo ma non solo, aggiunge il manager, spiegando: «Abilità e risorse sono i due elementi che costituiscono l'arsenale di un aggressore che, tuttavia, non è in grado di violare la sicurezza o addirittura eseguire attacchi sofisticati senza aver prima individuato i punti deboli di un sistema. Attacchi malware massivi, furti tramite email, dispositivi compromessi e servizi interrotti richiedono tutti una vulnerabilità nella rete, sotto forma di tecnologia o persona, per poter essere attivati.

Il GDPR (General Data Protection Regulation) sarà certamente un'occasione per spingere le imprese a investire nella sicurezza, ma per assurdo, teme Nencini, rappresenta un'opportunità per i cyber criminali, che potrebbero fissare il costo

del riscatto, nel caso dei ramsonware, basandosi sulle sanzioni previste dal regolamento europeo cui bisogna essere conformi dal 25 maggio prossimo.
Gli importi dei riscatti saranno sempre più ingenti, perché cresceranno gli attacchi di questo tipo mirati ad alcune imprese e preceduti da una fase di analisi e raccolta dati per "tarare" le richieste.
La superfice di attacco, inoltre, cresce, rimarca ancora il manager italiano, perché alle tecnologie informatiche si sommano le tecnologie operative, cioè quelle tipiche di ciascun settore, finora ritenute sicure in quanto isolate nelle fabbriche o in varie strutture, ma oggi sempre più connesse e quindi a rischio. In generale una connettività sempre maggiore porterà nuove opportunità ai cybercriminali per penetrare nelle reti aziendali.
Ci sono già stati attacchi di Denial of Service (cioè servizi Internet bloccati) che hanno sfruttato infrastrutture preposte ad altro, come le videocamere per la sorveglianza usate per trasmettere dati in massa, saturando la rete e causando danni da centinaia di milioni di dollari alle imprese dell'ecommerce.

Gastone Nencini, country manager di Trend Micro Italia

9 miliardi di dollari sfumati per le Business email compromise

Attenzione particolare, Nencini la dedica agli attacchi " BEC (Business Email Compromise), che purtroppo hanno ottenuto molti successi. Si tratta delle false

email, confezionate con cura e spesso precedute da un'accurata fase di raccolta dati per colpire al momento giusto. Tipico è il caso della falsa email spedita dal Ceo al Cfo con una richiesta di effettuare un bonifico urgente. Qui la sicurezza è una questione di processi e di cultura aziendale.
Esistono anche attacchi Business Process Compromise, che cercano di sfruttare appunto i processi, in genere del reparto finanziario, modificandoli, possibilmente tramite le vulnerabilità della supply chain (la catena di fornitura). Sono stati devastanti per Target nel 2014, ma richiedono una pianificazione a lungo termine e maggiore lavoro e in Trend Micro ritengono meno probabile che questi attacchi emergeranno nel 2018, mentre valutano che le perdite globali generate dalle truffe Business Email Compromise supereranno i 9 miliardi di dollari, dopo aver raggiunto nel 2017 i 5 miliardi.

La cyber propaganda e le fake news

In Italia si vota il 4 marzo, ma nel 2018 ci sono elezioni in diverse nazioni, compresi gli Stati uniti: un'opportunità di mercato per i "servizi" di cyber propaganda, le cui campagne saranno perfezionate utilizzando tecniche già sperimentate con successo in precedenza. In effetti, sembra che nel dark bleu siano disponibili pacchetti di cyber propaganda as a service.
Il triangolo delle fake news consiste in motivazioni su cui si basa la propaganda, i social network che servono come piattaforma per il messaggio e gli strumenti e servizi che sono impiegati per spedire il messaggio stesso.
«Nel 2018 – spiega Nencini – ci aspettiamo che la cyberpropaganda si veicoli attraverso tecniche familiari, come quelle utilizzate nel passato per diffondere lo spam tramite e-mail e il Web».
Il manager aggiunge:« Kit software fai da te, per esempio, possono eseguire spam automatizzato sui social media. Anche l'ottimizzazione del motore di ricerca Black Hat è stato adattato per l'ottimizzazione dei social media, con una base utenti di centinaia di migliaia, in grado di fornire traffico e numeri a diverse piattaforme. Dalle e-mail spear phishing inviate ai ministeri degli Esteri all'uso plateale di documenti per screditare le autorità, al contenuto dubbio che può diffondersi liberamente e scatenare opinioni violente o addirittura proteste reali».

Azioni per la sicurezza

Dato lo scenario, gli esperti di Trend Micro suggeriscono di adottare soluzioni di cyber security per una protezione multilivello, in modo da ridurre al minimo i rischi di compromettere ogni ambito aziendale. Occorre, per questo, una visibilità su tutti i livelli, con strumenti che possano fornire rilevamento real time e protezione contro vulnerabilità e attacchi.

«Qualsiasi potenziale intrusione e compromissione degli asset verrà evitata grazie a una strategia di protezione dinamica che utilizza tecniche transgenerazionali adeguate alle varie minacce», afferma Nencini, che conclude: «È fondamentale seguire pratiche di comportamento adeguato alla sicurezza, come modificare le password predefinite, utilizzandone di complesse e uniche per i dispositivi smart, specialmente per i router; implementare la crittografia in modo da prevenire il monitoraggio e l'utilizzo dei dati non autorizzati; applicare puntualmente le patch, aggiornare il firmware alla sua versione più recente; evitare il social engeneering prestando attenzione alle email ricevute e ai siti visitati in quanto potrebbero essere usati per spam, phishing, malware e attacchi mirati».

Western Digital

La data protection richiede supporti di storage capaci e sempre disponibili

Si fa un gran parlare di sicurezza, anche perché siamo in campagna elettorale, ma il dibattito è spesso superficiale, mentre in ambito tecnologico occorre andare in profondità per cogliere la differenza tra una soluzione supportata da un prodotto adeguato e quella che si basa su sistemi all'avanguardia, progettati per elevata affidabilità e alte prestazioni.

Un sistema per il controllo video di un'azienda, un ufficio o una casa deve garantire la qualità delle riprese e la registrazione continua. Gli hard disk per la videosorveglianza di Western Digital sono stati progettati per un utilizzo a tutti i livelli.

Le unità WD Purple, in particolare, sono state progettate e costruite, ci spiegano presso WD, per sistemi di sicurezza ad alta definizione, destinati a funzionare ininterrottamente (24 ore al giorno per 7 giorni la settimana). Non a caso sono in grado di supportare fino a 64 telecamere e sostenere un tasso di workload (cioè la quantità di dati trasferiti da un hard disk a un altro), che arriva fino a 180 TB all'anno. Cioè, precisano gli esperti WD, un tasso tre volte superiore a quello tipico di un'unità desktop.

Si tratta di sistemi che sono stati ingegnerizzati appositamente per la videosorveglianza, dotati, infatti, di un software di storage specifico per questa applicazione e potenziato da una tecnologia esclusiva di WD, pronta per supportare l'Ultra-HD, chiamata AllFrame 4K.

Quest'ultima migliora lo streaming ATA per limitare la perdita di fotogrammi, ottimizzare in generale la riproduzione del video e aumentare il numero di alloggiamenti di hard disk supportati all'interno di un NVR (Network Video Recorder).

Davide Vento, Business Manager Italia e Grecia Storage Device Dept di Western Digital

Scalabilità, affidabilità e durata

Sono caratteristiche che consentono di creare e installare un sistema di sicurezza affidabile su misura per le proprie esigenze di business e destinato a durare nel tempo.

A tal proposito, evidenziano presso WD, le unità WD Purple sono realizzate con componenti anti-ossidazione, al fine di garantire l'attività anche in ambienti difficili. Inoltre, il già ricordato supporto fino a 64 telecamere consente di espandere il sistema, qualora si dovesse allargare il perimetro da sorvegliare.

La capacità, per questo, non è un problema, grazie alle unità WD Purple da 8 e 10 TB, pensati per i carichi dei video in 4K. Più in generale, le unità sono realizzate con la tecnologia HelioSeal, giunta alla quarta generazione e collaudata sul campo (di 15 milioni di unità fornite fino allo scorso aprile).

L'affidabilità è testimoniata, peraltro, dai numerosi test d'integrità funzionale cui WD sottopone i propri prodotti prima di commercializzarli. A questo si aggiunge l'ampia knowledge base maturata negli anni.

Inoltre gli hard disk WD Purple sono stati progettati per la compatibilità, proprio per consentire di aggiungere capacità al sistema di sorveglianza rapidamente e

senza interruzioni. Grazie all'ampia serie di case e chipset supportati è più semplice configurare la soluzione NVR o DVR (Digital Video Recorder) più adatta alle proprie esigenze.

La data protection con gli hard disk WD Gold

Le soluzioni per la salvaguardia dei dati variano secondo le esigenze specifiche di ciascuna applicazione e necessità aziendale. WD fornisce ogni tipo di supporto e tecnologia storage (hard disk, SSD, NAS e altri sistemi per data center di ogni dimensione), per aiutare imprese e persone a usare e proteggere i dati.
Gli hard drive WD Gold presentano caratteristiche avanzate con una capacità di supportare workload a elevate prestazioni: fino a 10 volte il tasso gestito dall'hard disk di un desktop, sostengono presso la casa madre.
Si tratta, infatti di una soluzione "enterprise class", che presenta caratteristiche di efficienza energetica e prestazioni elevate. Una soluzione progettata per un utilizzo tipicamente destinato a server aziendali, ambienti di data center, sistemi di storage aziendali, data warehousing e datamining, NAS aziendale.
Ampia la scalabilità offerta da questa famiglia di hard disk da 3,5 pollici, che presenta unità da 1 TB fino a 12 TB, con la capacità di gestire workload fino a 550 TB all'anno, secondo quanto comunicato dalla casa madre.
Come abbiamo premesso l'affidabilità è una delle caratteristiche che fa la differenza, specialmente quando si parla di salvaguardia dei dati: gli hard disk WD Gold forniscono livelli di durabilità e affidabilità elevati: fino a 2,5 milioni di ore di MTBF (Mean Time Between Failure- tempo medio tra un guasto e un altro), realizzato pensando alla necessità di gestire operazioni 24x7 in ambienti esigenti.
Per questo gli hard disk WD Gold sfruttano soluzioni all'avanguardia. Di quella HelioSeal si è già accennato, ma la gamma WD Gold impiega anche le tecnologie RAFF e Dynamic fly-height. La prima include un'elettronica sofisticata che controlla l'unità e corregge le vibrazioni lineari e rotazionali in tempo reale. In questo modo si ottiene un significativo miglioramento delle prestazioni in quegli ambienti, per esempio ad alta densità, che comportano vibrazioni più elevate di quelle che percepiamo nei pc.

La tecnologiaDynamic fly height, invece, si preoccupa costantemente di regolare l'altezza della testina per ogni azione di lettura e scrittura, in modo da assicurare sempre le massime prestazioni, ridurre gli errori e massimizzare l'affidabilità.
Inoltre, un sistema con due attuatori per il posizionamento della testina, migliora l'individuazione delle tracce dati. Più precisamente, l'attuatore primario provvede al posizionamento generale, affidandosi ai principi elettromagnetici degli attuatori tradizionali. L'attuatore secondario utilizza un movimento piezoelettrico per posizionare le testine con la massima accuratezza.
Infine, i WD Gold dispongono di un sistema per il ripristino degli errori limitati nel tempo (TLER) specifico per RAID. Questo permette di ridurre i lunghi blocchi della macchina, dovuti ai processi di ripristino da errori dell'hard disk tipici delle unità desktop.

Azioni per la sicurezza

Dato lo scenario, gli esperti di Trend Micro suggeriscono di adottare soluzioni di cyber security per una protezione multilivello, in modo da ridurre al minimo i rischi di compromettere ogni ambito aziendale. Occorre, per questo, una visibilità su tutti i livelli, con strumenti che possano fornire rilevamento real time e protezione contro vulnerabilità e attacchi.
«Qualsiasi potenziale intrusione e compromissione degli asset verrà evitata grazie a una strategia di protezione dinamica che utilizza tecniche transgenerazionali adeguate alle varie minacce», afferma Nencini, che conclude: «È fondamentale seguire pratiche di comportamento adeguato alla sicurezza, come modificare le password predefinite, utilizzandone di complesse e uniche per i dispositivi smart, specialmente per i router; implementare la crittografia in modo da prevenire il monitoraggio e l'utilizzo dei dati non autorizzati; applicare puntualmente le patch, aggiornare il firmware alla sua versione più recente; evitare il social engeneering prestando attenzione alle email ricevute e ai siti visitati in quanto potrebbero essere usati per spam, phishing, malware e attacchi mirati».

INFORMATION SECURITY & DATA PROTECTION

Cyber security, object Storage, biometria, difesa globale e intelligence per un business always-on

I dati e le informazioni sono un asset sempre più centrale nella dinamica di business aziendale. Una violazione alla loro sicurezza, in termini di riservatezza, integrità e disponibilità, provoca danni economici potenzialmente devastanti. Proteggere i dati e, al contempo, mitigare il rischio d'impresa sono obiettivi basilari per un imprenditore o un consiglio d'amministrazione. Conseguire tali obiettivi implica valutare quanto investire in sicurezza, confrontando l'investimento con il risparmio atteso dall'impedire un incidente di sicurezza.

L'evoluzione delle minacce, la disposizione di tecnologie innovative, l'offerta di servizi ad hoc, nonché la trasformazione dell'IT aziendale verso un concetto più allargato di "digital technology", sono tutti elementi da considerare per definire una strategia aziendale per la protezione dei dati e dell'impresa stessa

Se, del resto, implementare misure per la protezione del dato è previsto dalle normative italiane e internazionali, risulta altresì un elemento imprescindibile in uno scenario globale dove la rincorsa di una maggiore competitività, include la capacità di sfruttare le opportunità di Internet e delle nuove tecnologie, dalla mobility al cloud, dai big data al machine to machine. Ancor di più oggi, nel nuovo mondo "digital" dove non si vendono più prodotti ma esperienze.

***Giuseppe Saccardi** è autore e coautore di numerosi libri, rapporti, studi e survey nel settore dell'ICT. Ha lavorato in società di primo piano nel campo dell'informatica e delle telecomunicazioni nazionali e internazionali, maturando una trentennale esperienza nel settore. È laureato in Fisica ed è iscritto all'ordine dei giornalisti della Lombardia. È cofondatore e President di Reportec.*

***Gaetano Di Blasio** ha lavorato presso alcune delle principali riviste specializzate nell'ICT. Giornalista professionista, è iscritto all'ordine dei giornalisti della Lombardia ed è coautore di rapporti, studi e survey nel settore dell'ICT. Laureato in Ingegneria, è cofondatore e Vice President di Reportec.*

***Riccardo Florio** ha collaborato con le principali case editrici specializzate nell'ICT. È coautore di rapporti, studi e Survey nel settore dell'ICT. È laureato in Fisica ed è iscritto all'ordine dei giornalisti della Lombardia. È cofondatore e Vice President di Reportec*

Reportec S.r.l.
Via Marco Aurelio, 8 - 20127 Milano
www.reportec.it
Reportec