ASSOLOMBARDA

ClubTi
Club per le Tecnologie dell'Informazione

**Al ClubTi si discute di sicurezza e protezione informatica.**

# Attacchi informatici e nuove misure di contrasto e prevenzione

di Marco Bozzetti e Emanuela Zanleone

*L'Osservatorio Attacchi Informatici(OAI)[1] ha di recente concluso il Rapporto annuale nel quale sono stati approfonditi i tipici attacchi e le vulnerabilità dei sistemi. Ma aspetto forse ancor più importante per le aziende sono le misure e sugli strumenti per proteggersi dagli attacchi e per circoscrivere e, dove possibile, eliminare le vulnerabilità.*

Il Rapporto dell'OAI per il 2009 comprende più di 100 risposte complete ed esaurienti[2], come ci racconta **Marco Bozzetti**. Il Rapporto ha evidenziato come l'84% degli attacchi sia rappresentato da Malware[3] ad ampio spettro rappresentati da Virus, Worm, Trojan horse, Spyware ed altri, seguiti dagli attacchi cosiddetti di Social Engineering (58%), e dal furto del laptop per la rivendita (50%). Gli attacchi di Social Engineering sono tecniche più o meno sofisticate che hanno lo scopo di sottrarre alla vittima codici personali, identità, ecc. sfruttando l'ingenuità a volte anche  Una delle tecniche più conosciute è il *phishing* del quale l'Italia è tristemente il quarto produttore mondiale. Dal 2007, infatti, per la criminalità organizzata l'attività informatica è diventata molto più conveniente rispetto addirittura alla vendita di stupefacenti. Questo non solo perché genera molti più profitti, comportando meno costi, ma anche perché questi reati sono, ad oggi, soggetti a una legge meno stringente e punitiva.

E' doveroso, inoltre, fare una considerazione sugli utenti aziendali e non: le password sono di norma molto deboli (dal classico *11111* all'*admin*), non vengono quasi mai cambiate nel corso e del tempo, vengono utilizzate da diverse persone (capoufficio e segretarie ad esempio) e trasmesse in modo totalmente non sicuro (scritte su foglietti, mandate via mail, ecc.). questo favorisce i criminali ad attuare attacchi che funzionano con lo stesso principio del "pizzo": *ti dimostro che posso entrare nei tuoi sistemi e sottrarti dati e informazioni, ma se mi paghi non lo faccio*. L'OAI ha messo in evidenza, altresì, che la modifica dei dati è l'attacco maggiormente tenuto dalle aziende.

Ma che caratteristiche hanno gli attacchi? Tre sono i fattori che rendono gli attacchi informatici sempre più pericolosi: vengono messi in atto in modo automatico, su vasta scala (multi attacco) e a grande velocità (grazie all'uso della banda larga). Non è quindi pensabile una risposta da parte dei singoli individui. La protezione deve essere automatizzata e funzionare alla stessa velocità dell'attacco. E ancora: la vulnerabilità dei sistemi *middleware* aziendali, a cominciare da quelle dei sistemi operativi, sono note. Inoltre le aziende sempre più spesso si dotano di meccanismi automatici e non di back up e *disaster recovery*, tuttavia quasi mai questi vengono realmente testati, causando danni, il più delle volte, al momento del recovery.

---

[1] L'OAI, Osservatorio Attacchi Informatici in Italia, è stato ideato da M. R. A. Bozzetti per conto di FidaInform ed il ClubTI di Milano, con il patrocinio di varie Associazioni (AIPSA, AIPSI, Assolombarda, FTI, Inforav cui si è aggiunta itSMF dal 2010) e la collaborazione della Polizia delle Comunicazioni. Obiettivo primario dell'Osservatorio è la pubblicazione annuale di un Rapporto che analizzi il fenomeno degli attacchi ai sistemi informativi di Aziende/Enti per fornire loro indicazioni e strumenti concreti per analizzare i rischi in Italia e poter attivare le idonee misure di prevenzione e protezione.

[2] Il campione considerato è significativo se confrontato anche con l'analoga iniziativa USA che comprende 500 questionari.

[3] Malware: un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi *malicious* e *software* e ha dunque il significato letterale di "programma malvagio"; in italiano è detto anche codice maligno *(Fonte: Wikipedia)*

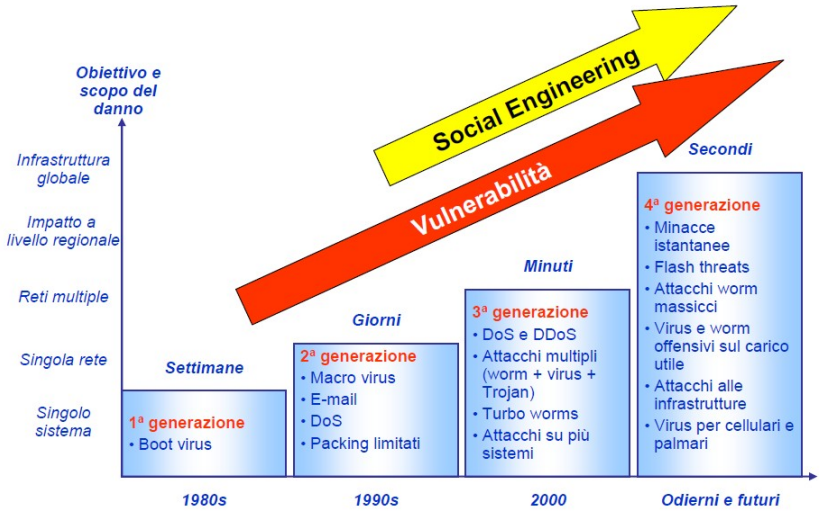


**Figura 1 - Passato, presente e futuro di minacce ICT (Fonte: "Sicurezza Digitale" di Marco Bozzetti)**

Da tutto questo si deduce una prima importante riflessione: la sicurezza è prima di tutto un problema organizzativo. I sistemi software vengono acquistati senza una verifica accurata delle loro caratteristiche di sicurezza, e soprattutto la conoscenza di questi fenomeni è frammentata in azienda. Di solito chi conosce bene i meccanismi di protezione della rete si preoccupa di quella così come fanno coloro che si occupano degli applicativi, senza una policy omogenea. La sicurezza assoluta non esiste, ma può essere maggiormente utile una protezione "media" che copra tutti gli ambiti aziendali, piuttosto che una protezione formidabile di un aspetto lasciandone altri totalmente scoperti. Alcuni esempi: di tutti i dati presenti in azienda quelli critici (ovvero dei dati su cui poggia il business) sono certamente quelli da proteggere in modo più deciso partendo dal presupposto che la formula del profumo o il disegno del brevetto sono *assets* vitali per l'azienda. E' necessario studiare una policy aziendale di sicurezza che permetta di proteggersi lungo tutta la catena del valore, ad esempio imponendo ai fornitori alcune norme. E' necessario mantenere aggiornati i sistemi (come ad esempio gli antivirus) e potenziare l'identificazione e l'autenticazione delle persone.

Ultimo, ma non per importanza, sensibilizzare le persone e far comprendere l'importanza di alcune buone prassi. E' in quest'ottica che la sicurezza può essere vista certamente come un costo, ma da confrontare con il costo della non sicurezza ricordando che una maggiore sicurezza garantisce maggior credito verso le banche, minori costi assicurativi, abbattimento delle sanzioni e così via.

In ambito sicurezza, un tema che certamente incontra l'interesse di molti è quello delle carte di credito. Lo affrontiamo partendo dalla descrizione generale di uno Standard emergente (PCI – DSS), dedicato alla sicurezza delle transazioni tramite carta di credito, che interessa issuers (es. banche), merchant (es. grande distribuzione o esercenti), service providers (es. outsourcers ICT).

**Massimo Cotrozzi**, Partner Sernet Spa, membro ONPS (Osservatorio Nazionale Permanente sulla Sicurezza) e Responsabile del Dipartimento di sicurezza dell'Osservatorio Internazionale Card, sullo standard PCI (Payment Card Industry) DSS (Data Security Standard) per la sicurezza delle carte di credito ci racconta in cosa consiste e come funziona.

Lo standard è stato creato dal Payment Card Industry (PCI) Security Standards Council, fondato da 5 brand[4], per incrementare le misure di sicurezza su tutta la filiera e proteggere, dunque, i clienti dalle frodi. È stato, inoltre, sviluppato per favorire e migliorare la protezione dei dati di titolari di carta e semplificare l'implementazione di misure di sicurezza dei dati coerenti a livello globale.

Il PCI – DSS si basa su 12 requisiti di sicurezza e li abbina alle corrispondenti procedure di test in uno strumento formale e rigoroso di valutazione della sicurezza. Ogni requisito prevede, poi, una serie di statement (ben 227) che identificano anche il livello di sicurezza cui la singola azienda o ente deve sottostare[5]. Una volta individuato il livello e rispettati i requisiti richiesti è possibile avere la certificazione[6].

Per potere accedere alla certificazione è anche necessario stabilire il perimetro all'interno del quale si spostano i dati delle carte in una logica restrittiva. Ovvero è necessario ridurre al minimo all'interno del Sistema Informativo l'utilizzo delle Carte di Credito ed esclusivamente per motivi di business. Questo significa che non è possibile spostare dati solo per motivi tecnologici. Laddove le carte sono presenti, devono potere accedere solo utenti autorizzati. Queste regole si basano su un principio estremamente semplice, ma altrettanto efficace: tanto più viene ristretto l'ambito di circolazione delle carte, tanto più sarà semplice proteggerle sia sul fronte della vulnerabilità (quanto il sistema di per sé è debole) sia su quello della violabilità (come si entra nel sistema e quanto costa per farlo).

| | |
|---|---|
| **Sviluppo e gestione di una rete sicura** | |
| Requisito 1: | Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta |
| Requisito 2: | Non utilizzare valori predefiniti del fornitore per le password di sistema e altri param |
| **Protezione dei dati di titolari di carta** | |
| Requisito 3: | Proteggere i dati di titolari di carta memorizzati |
| Requisito 4: | Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche |
| **Utilizzare un programma per la gestione delle vulnerabilità** | |
| Requisito 5: | Utilizzare e aggiornare regolarmente il software antivirus |
| Requisito 6: | Sviluppare e gestire sistemi e applicazioni protette |
| **Implementazione di rigide misure di controllo dell'accesso** | |
| Requisito 7: | Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario |
| Requisito 8: | Assegnare un ID univoco a chiunque abbia accesso a un computer |
| Requisito 9: | Limitare l'accesso fisico ai dati di titolari di carta |
| **Monitoraggio e test delle reti regolari** | |
| Requisito 10: | Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta |
| Requisito 11: | Eseguire regolarmente test dei sistemi e processi di protezione |
| **Gestire una politica di sicurezza delle informazioni** | |
| Requisito 12: | Gestire una politica che garantisca la sicurezza delle informazioni |

**Figura 2 - PCI - DSS: 6 Obiettivi, 12 Requisiti**

[4] American Express, Discover Financial Services, JCB International, MasterCard Worldwide e Visa, Inc.

[5] Il Livello 1, ad esempio, è riservato a *merchant* che trattano più di 6 milioni di transazioni all'anno, mentre il livello 4 a coloro che ne gestiscono fino a 20.000.

[6] grazie all'intervento di un certificatore PCI o anche con autocertificazione

Con **Mario Pitassi**, Ceo di Technology Estate Srl, abbiamo, infine, affrontato il tema della firma dei documenti, tema altrettanto scottante. Tutti noi conosciamo la firma digitale, la scansione della retina, dell'impronta digitale o del viso, ma questi sistemi di firma sono da un lato legati nativamente ad una firma cartacea e dall'altro ad un sistema di autenticazione "fisico" in alcuni casi replicabile (l'impronta digitale si duplica in 10 minuti).

Il concetto di firma biometrica nasce in Israele e permette il riconoscimento delle firme apposte da un individuo in base a 5 parametri: ritmo, velocità, pressione, accelerazione e movimento oltre alla possibilità di tracciare i cosiddetti movimenti volanti, ovvero quei movimenti in cui si stacca la penna dal foglio e ci si sposta in un altro punto per apporre un puntino sulla i o una stanghetta alla t.

La firma biometrica presenta una caratteristica essenziale per ridurre i costi di sicurezza: nasce digitale. Per capire meglio questo aspetto Mario Pitassi ci ha illustrato i costi medi per una banca, ad esempio, obbligata per legge a conservare le ricevute di versamento dei clienti, che contengono la firma originale de cliente, che ammontano a circa 72 milioni di euro all'anno. Stesso discorso vale per le telco, che per conservare in modo sicuro i documenti di attivazione di una SIM, spendono circa 7€ a pratica moltiplicata per milioni di clienti. Se ci spostiamo sui finanziamenti parliamo di 13/18€ a pratica per circa 1,2 milioni di pratiche all'anno il cui valore è esattamente pari al finanziamento erogato.

La firma biometrica viene conservata crittografata, direttamente digitale e, dunque, elimina completamente questi costi.

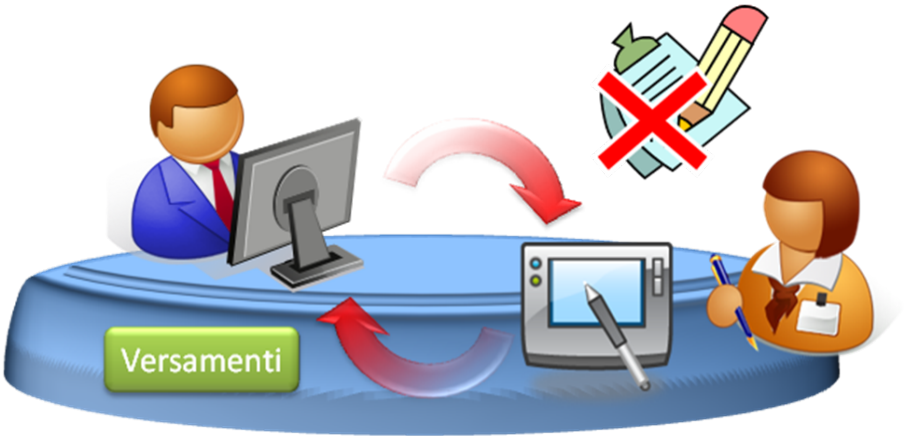


**Figura 3 – Esempio di processo di Firma Biometrica in banca**

La firma biometrica permette, inoltre, il confronto tra firma biometrica e biometrica, tra biometrica e statica (nel caso in cui un cliente apponga una firma in modo tradizionale), e tra statica e biometrica permettendo il passaggio dall'una all'altra. Riguardo il confronto biometrica/ biometrica si sottolinea come il sistema sia in grado di auto apprendere le modifiche che, inevitabilmente, nel tempo si verificano sulla firma di ciascun individuo e sia, dunque, in grado di riconoscere la firma anche se modificata.

Ad ogni firma viene anche associato un rating, ovvero un indice che valuti la corrispondenza, che può essere impostato in base all'importanza dell'operazione svolta (ad esempio più basso in caso di versamento, più alto per il prelievo in banca).

Perché non si può copiare? Perché la firma biometrica è protetta in due modi diversi: la firma viene confrontata, come detto, con le precedenti non solo per verificare la conformità, ma anche per evitare che possa essere usata una firma 2 volte. È infatti impossibile che una firma sia assolutamente identica ad una precedente. Inoltre la firma viene marcata con data e ora ed è altrettanto non ammessa una firma con identica data e ora, il che esclude un riutilizzo della stessa.

Per implementare queste soluzioni basta un tempo che va da 3 a 6 mesi ed un investimento che si aggira, per una banca comprensivo dei nuovi banconi "interattivi", intorno ai 25 milioni di euro, cifra che corrisponde a 1/3 di quanto spende la stessa banca all'anno per proteggere le distinte di versamento e prelievo. Dal secondo anno il costo è intorno ai €500.000.

Esistono già casi applicativi funzionanti. La Fiat lo sta utilizzando con soddisfazione per il caricamento delle bisarche. Da 2 mesi, in tutto il mondo, gli autisti sui piazzali firmano in modo biometrico le bolle di consegna in modo biometrico inviando poi la bolla direttamente in azienda senza creare documenti cartacei, se non copie conformi per il passaggio dalle dogane.

Velocità, risparmio, ecologia e soprattutto sicurezza a 360°!