SECURITY
& BUSINESS

n. 50

RAPPORTO OAD, GLI ATTACCHI INFORMATICI IN ITALIA

pag. 4-6

CYBER ATTACK

CYBER ATTACK: L'IMPORTANZA DELLA PRIVACY

Il Presidente del Garante per la Privacy, Antonello Soro, interviene in parlamento sui pericoli delle smart city e dell'intelligenza artificiale. **pag. 9-11**

SOLUZIONI

LE REGOLE PER APPLICAZIONI SEMPRE SICURE

Proteggersi dalle vulnerabilità e scrivere codice sicuro richiede il coinvolgimento degli sviluppatori nel processo di sicurezza. È un compito che va proseguito nel tempo, reso più semplice dalle soluzioni Micro Focus Fortify.

pag. 14-16

IN QUESTO NUMERO:

Reportec

EDITORIALE

Security & Business 50 Genn-Febb 2020

Direttore responsabile: Gaetano Di Blasio

In redazione: Giuseppe Saccardi, Paola Saccardi

Hanno collaborato: Riccardo Florio

Grafica: Aimone Bolliger

Immagini: dreamstime.com

www.securityebusiness.it

Editore: Reportec srl
Via Marco Aurelio 8
20127 Milano
tel. 02.36580441
www.reportec.it

Registrazione al tribunale n.585 del 5/11/2010

Una ricca serie di analisi sugli attacchi alla sicurezza apre il numero 50 di Security & Business di gennaio/febbraio 2020.

Il primo contributo è quello del Rapporto OAD (Osservatorio Attacchi Digitali in Italia), realizzato da Malabo, sotto l'egida di Aipsi (Associazione Italiana dei Professionisti della Sicurezza Informatica, capitolo italiano di ISSA, la più grande associazione internazionale di settore).

Giunto alla 12 edizione il rapporto raffigura un'analisi dinamica dell'andamento della sicurezza informatica italiana, poiché tutti i rispondenti, rigorosamente anonimi, sono italiani.

La nuova edizione presenta delle conferme, ma anche sorprese e novità.. in particolare, per la prima volta, il numero di aziende che hanno registrato almeno una violazione alla sicurezza è superiore a quello delle aziende che non hanno registrato attacchi. Potrebbe essere un interessante dato su una crescita della maturità, poiché in passato era probabile che in molte organizzazioni piccole e medie, gli attacchi passassero inosservati.

Il rapporto è gratuitamente scaricabile dal sito AIPSI.org. Su Security & Business trovate una sintesi di alcuni risultati.

Le analisi della brubrica Cyber Attack continuano con i 20 anni di compleanno per la associazione Clusit, il cui atteso rapporto parlerà di Capitalismo di Sorveglianza, tra molte altre cose, ovviamente.

I dati di Trend Micro accendono altre luci sulle minacce, mentre il presidente del Garante per la Privacy, Antonello Soro, sottolinea i rischi legati a una non sufficiente cura della Privasy, strumento di Democrazia.

Non mancano, infine, alcune delle più recenti soluzioni per la sicurezza informatica, come quelle di MicroFocus, CyberArk e altre ancora.

CYBER ATTACK

ATTACCHI ALLA SICUREZZA IN ITALIA: PIÙ VITTIME CHE SCAMPATI

Nuova edizione del rapporto OAD (Osservatorio Attacchi Digitali), l'unica indagine che si concentra sulle violazioni nelle aziende italiane con un'indagine rigorosamente anonima

di Gaetano Di Blasio

Per la prima volta, dopo 12 anni consecutivi, il numero delle imprese che hanno subito un attacco sono più di quelli che non l'hanno subito. L'indagine è disponibile gratuitamente (https://www.oadweb.it/it/oad2019/per-scaricare-il-rapporto-2019-oad.html).

I rispondenti, pur non rappresentando la totalità delle imprese, sono distribuiti coerentemente con i dati statistici dell'ISTAT, con una quota importante di aziende appartenenti al settore ICT. Più precisamente, il bacino di rispondenti emerso nel 2019 risulta costituito, in termini di numero di dipendenti, per il 62,6% da strutture sotto i 250, e di queste il 37,4% sotto i 50. Per le grandi organizzazioni, il 9% dei rispondenti ha più di 5000 dipendenti. Rispetto ai settori merceologici, i rispondenti al 18% appartengono a pubbliche amministrazioni, istruzione statale inclusa, il resto al settore privato: di questo, la maggior parte di aziende appartiene al settore ICT (25,7%) e a quello manifatturiero e delle costruzioni (16,4%), cui seguono con percentuali inferiori organizzazioni appartenenti a tutti gli altri settori merceologici, classificati secondo il codice ATECO2. In sostanza, risulta quindi abbastanza ben bilanciato tra piccole strutture e quelle medio grandi; per i vari settori merceologici il I compilatori del questionario 2019 sono per il 18,3% i responsabili dei sistemi informatici (CIO), per il 17% il personale di terze parti cui è terziarizzata, in tutto o in parte, la gestione del sistema informatico e della sua sicurezza, e con una identica percentuale il personale di vertice dell'azienda/ente. Seguono con percentuali a scalare altri ruoli, incluso con il 7,2% quello di responsabile della sicurezza digitale (CISO).

Una mira più accurata

Come accennato, gli attacchi rilevati quest'anno sono andati a segno più che in passato. Precisamente, la percentuale di rispondenti che ha subito/ rilevato attacchi è stata del 55,7%,superiore a chi non li ha subiti. Le cinque principali tipologie di attacco più diffuse tra i sistemi informatici dei rispondenti sono state, in ordine, di diffusione tra i rispondenti: 1.gli attacchi ai sistemi IAA per il controllo degli accessi, con un 54,21%; 2.gli attacchi all'intero sistema ICT target, con un 41%; 3.gli attacchi alle reti di comunicazione, con un 34,65%; 4.il furto di dispositivi mobili d'utente, con un 33,62; 5.saturazione sistemi e risorse ICT (DoS, DDoS), con un 30,93%. Tutte le altre tipologie di attacco hanno registrato un'incidenza sotto il 30%. La tecnica più diffusa e

più usata, secondo i rispondenti, è stata la raccolta malevole e non autorizzata di informazioni, tipicamente tramite social engineering, cui segue l'uso di codici maligni e script. Al al terzo posto i toolkit. Poi a seguire le altre tecniche, ben distanziate.

Le misure di sicurezza

Per quanto possibile, il rapporto ha cercato di verificare quali misure di sicurezza sono state adottate dalle aziende dei rispondenti. Questo con l'obiettivo di capire, a livello generale, se i sistemi informatici dei rispondenti abbiano saputo e in che misura, reagire/ contenere gli attacchi. Le risposte raccolte hanno mostrato che 'equipaggiamento in dotazione presso i rispondenti appartiene alla fascia medio alta in termini di livello di sicurezza digitale, attuato, pur con qualche elemento di eccellenza e, più numerosi, elementi di debolezza. Aspetto negativo: in diversi casi mancano le più elementari e basilari misure per la security. Questo sia dal punto di vista delle misure tecniche sia da quello delle misure organizzative. Per molti versi una mancanza, quest'ultima, molto gravve, in quanto indice di potenziali problemi con la conformità con il GDPR. Una mancanza che si registra non solo nelle microimprese o nelle PMI (piccole e medie imprese), ma anche in alcune realtà medio grandi.

Qualche curiosità

Ricordando che il rapporto è scaricabile gratuitamente, riportiamo qualche dato tra i più interessanti. Per esempio, si nota che sono sostanzialmente poche (13%) le aziende/ enti dei rispondenti che seguono un approccio architetturale, basato su standard e best practice per la sicurezza digitale. Inoltre, il 29,59% dichiara di possedere almeno le risorse ICT più critiche in alta affidabilità (99,9%). Tuttavia, la la mancanza di una architettura per la sicurezza digitale porta alla non interazione e coordinamento tra i diversi Strumenti. Sono poi assai limitate le misure di sicurezza fisica. per la protezione delle reti, il 54,3% usa firewall di rete e DMZ, il 49,8% usa

VPN, il 27,6% utilizza sistemi IPS/IDS e di analisi. Per il controllo degli accessi si utilizza il solo username e password nella maggior parte delle aziende (60,2% dei rispondenti). Per quanto riguarda la protezione delle applicazioni e dei dati trattati, risulta ancora molto limitato l'utilizzo della crittografia sia, nella trasmissione dati, (38,9%,) sia nella archiviazione dei dati più critici, quelli sensibili inclusi (27,6%). Le misure e gli strumenti per la gestione della sicurezza utilizzati nei sistemi informatici dei rispondenti sono percentualmente basse, anche per la forte incidenza delle piccole e medie organizzazioni. Gli strumenti più diffusi sono il monitoraggio ed il controllo centralizzato delle funzionalità e delle prestazioni dei sistemi ICT con un 37,1% dei rispondenti. Il 42% dei rispondenti affida a terzi, parte o in toto il sistema informatico e la gestione della sua sicurezza. In particolare, l'11,8% utilizza SOC e/o SCC. Un tema interessante riguarda la responsabilità della sicurezza digitale. Circa tre quarti delle organizzazioni sostengono di avere un responsabile, ma le misure organizzative sono meno avanzate di quelle tecniche, tanto è vero che il responsabile tecnico è ufficiale solo in un terzo delle aziende. Altre note dolenti sono : per il 40% circa sono definite e in uso policy per la sicurezza digitale, percentuali inferiori, a partire da 37,1%, per le relative procedure organizzative; scarse attività di sensibilizzazione e formazione sulla sicurezza digitale; scarso interesse sulle certificazioni professionali per la sicurezza digitale a livello aziendale e personale, sia all'interno della propria organizzazione sia verso i fornitori. ❄