

## IN QUESTO NUMERO:

### CYBER ATTACK

pag. 4-6

• Attacchi alla sicurezza in Italia: più vittime che scampati

pag. 7-8

• 20 anni di cyber security con il Clusit: competenze cercasi

pag. 9-11

• Privacy GDPR e protezione dei dati baluardi della democrazia

pag. 12-13

• Trend Micro delinea il nuovo panorama delle minacce

### SOLUZIONI

pag. 14-16

• Le regole per applicazioni sempre sicure

pag. 17-19

• Endpoint al sicuro con la cifratura dei dati

pag. 20-21

• CyberArk Blueprint mette al sicuro gli accessi privilegiati

pag. 21-22

• Prevenire gli attacchi API controllando le credenziali

pag. 23-24

• Sottovalutare il Security Operations Center può costare caro

pag. 24-25

• Simulare previene gli attacchi e migliora la sicurezza



### 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

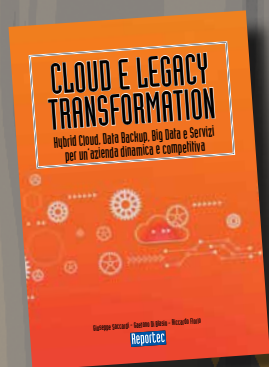
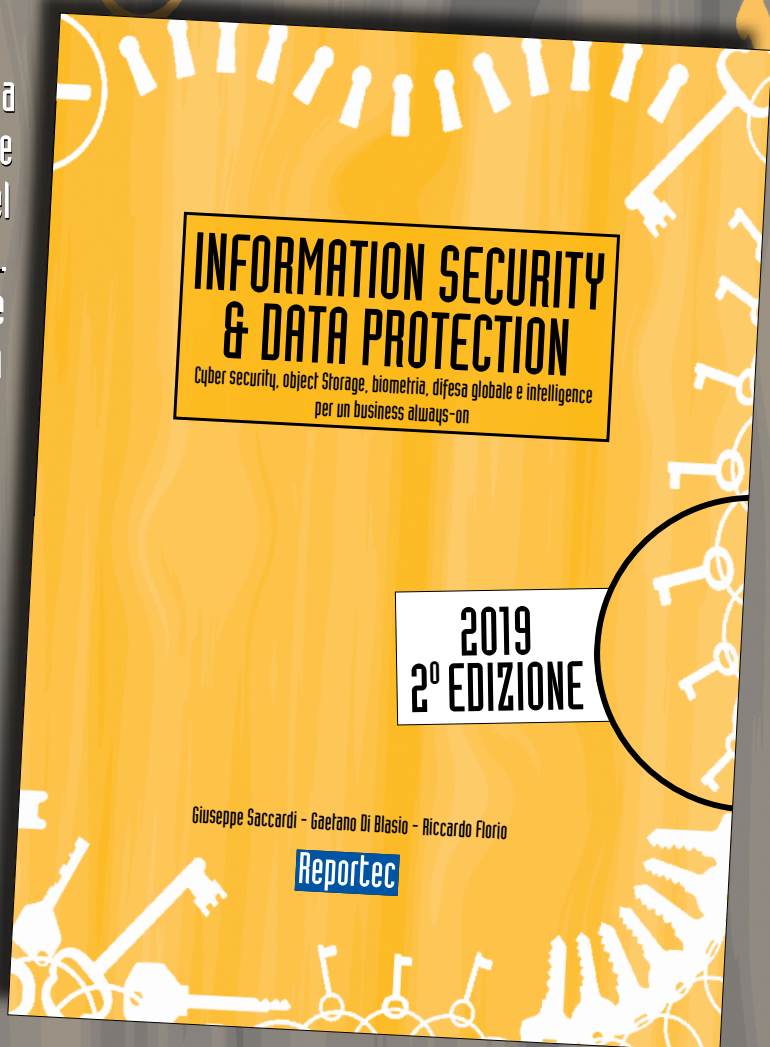
Proteggersi dalle vulnerabilità e scrivere codice sicuro richiede il coinvolgimento degli sviluppatori nel processo di sicurezza. È un compito che va proseguito nel tempo, reso più semplice dalle soluzioni Micro Focus Fortify.

**pag. 14-16**



# È disponibile il libro **SICUREZZA E PROTEZIONE DEI DATI**

In oltre 200 pagine il punto sulla situazione della cybersecurity e sulle dinamiche aziendali nella protezione del dato e della continuità del business. Una tematica sempre più vitale per le imprese, le quali devono mettere in conto che saranno attaccate. Ormai esistono sistemi automatici e pressioni da parte dei cybercriminali, tali per cui nessuno può sentirsi al sicuro: chi non è ancora stato attaccato lo sarà e, se non subirà danni gravi, sarà solo perché chi l'ha assalito cercava qualcos'altro.



È disponibili anche  
**CLOUD E LEGACY TRANSFORMATION**

Il libro è acquistabile al prezzo di 30 euro (IVA inclusa) richiedendolo a  
**info@reportec.it - tel 02 36580441 - fax 02 36580444**

## 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

Tutti i marchi sono  
registrati e di proprietà  
delle relative società

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 rubrica 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 Privacy, strumento di Democrazia.

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

## 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

**P**er 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 terzariizzata, 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 terzo posto i tool-kit. 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 l'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 grave, 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 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. ✱



## 20 ANNI DI CYBER SECURITY CON IL CLUSIT: COMPETENZE CERCASI

### *Capitalismo di Sorveglianza e Ransomware fra le minacce più pericolose del prossimo decennio*

di Gaetano Di Blasio

L'Associazione Italiana per la Sicurezza Informatica festeggia 20 anni dalla costituzione e lancia un appello per richiamare nuove professionalità. Il presidente del Clusit, Gabriele Faggioli, sottolinea: «La consapevolezza dei pericoli a cui è esposta la nostra società digitale è ormai a buoni livelli, grazie al lavoro di ricerca e comunicazione che ha visto i nostri esperti impegnati con professionisti, imprese, istituzioni e centri di ricerca, in maniera particolare negli ultimi cinque anni».

Tuttavia, aggiunge Faggioli, non è il caso di abbassare la guardia, visto il ritmo con cui si diffondono nuove minacce, come il Capitalismo di Sorveglianza e i Ransomware. Occorre, anzi, che tutte le imprese collaborino per diffondere la cultura della sicurezza informatica in tutti i suoi aspetti.

In particolare, rimarca il presidente del Clusit: «È fondamentale che, all'inizio del nuovo decennio, si mettano concretamente in campo tutte le competenze diversificate di cui la cyber security ha bisogno per mitigare i rischi», aggiungendo: «Solitamente gli anniversari sono il momento dei bilanci: noi abbiamo imparato che da ora in poi potremo solo alzare la guardia. Celebriamo quindi i 20 anni di Clusit



consapevoli di trovarci di fronte a un nuovo punto di partenza, in cui è necessario mettere insieme le forze di chi crede nella società digitale e nella responsabilità che la stessa deve necessariamente assumersi per la propria sopravvivenza».

### **Capitalismo di Sorveglianza e diffusione del Ransomware**

Anno dopo anno gli esperti del Clusit analizzano i dati a livello globale per cogliere le tendenze sulle minacce presenti e future. In particolare, Capitalismo di Sorveglianza e la diffusione del Ransomware sono indicati come le minacce più allarmanti in questo inizio 2020. In attesa dei primi dati forniti usualmente in anticipo rispetto al rilascio del Rapporto Clusit, vogliamo segnalare la preoccupazione per la crescita degli attacchi che hanno un impatto diretto sulla democrazia. Oltre ad allargarsi il divario tra chi ha accesso alle informazioni ed è in grado di

comprenderne il significato e di chi è privo di strumenti per discernere la realtà in un contesto spesso inquinato da fake news.

Il punto è che le imprese sono alla ricerca dei dati e noi saremo sempre più invogliati a fornirli in cambio di "benefit", cedendo un po' della propria privacy. L'importante è poterlo fare supportati da una legge che ci tutela, permettendoci di fare marcia indietro e di riprenderci i nostri dati, ma non ovunque è così. Il capitalismo di sorveglianza uso dei dati che consente a chi "li possiede o acquisisce" di e ne ricavarne ulteriore vantaggio, magari con una buona posizione privilegiata. Si pensi ai dati di un supermercato che conosce i nostri gusti. Oppure pensiamo a una casa automobilistica, che può incrociare i dati della vettura acquistata per "vendere" le informazioni a un partner. Così come per il capitalismo in generale, si possono prevedere risvolti positivi per chi fornisce i dati. La logica degli Open Data può essere vista in questa direzione, purché sussistano strumenti di garanzie.

La protezione dei dati diventa un baluardo per il cittadino, ma il pericolo è rappresentato dai molti (troppi) paesi dove non esiste un regolamento per la protezione della privacy o, peggio, dove sono promosse regole che consentono ingerenze illiberali. Un dato di fatto aggravato dall'importanza del dato nell'età dei social media, come recentemente ha spiegato Antonello Soro, Presidente del Garante della Privacy, intervenuto in Parlamento sul tema della protezione dei dati e sulle Smart City.

Un ulteriore appello viene riservato a iscriversi all'associazione Italiana per la Sicurezza Informatica, che apre concretamente le porte a professionisti ed aziende, con l'obiettivo di mettere a fattor comune competenze e risorse, invitandoli ad associarsi

e a partecipare al programma di Clusit, che oggi rappresenta oltre 500 organizzazioni appartenenti a tutti i settori del Sistema-Paese e può contare su un importante network di relazioni professionali. Il Clusit, in particolare, mette a disposizione dei soci ogni anno decine di ore di formazione (sono previsti oltre 30 i webinar in agenda nel 2020) e l'accesso a risorse di supporto, quali lo sportello legale. Sono poi previsti gruppi di lavoro tematici, come la Clusit Community for Security, un punto di incontro pre-competitivo e aperto alla condivisione per professionisti multidisciplinari attenti ai temi della sicurezza e della compliance.

I soci possono anche contribuire al Rapporto Clusit, lo studio indipendente italiano che presenta ogni anno lo scenario completo degli eventi di cyber-crime più significativi degli ultimi 12 mesi e ne fornisce l'interpretazione.

A ciò si aggiungono gli appuntamenti del Security Summit, il convegno che ogni anno si svolge sul territorio italiano con l'obiettivo di analizzare lo stato dell'arte della cybersecurity e proporre nuovi temi di discussione su evoluzione tecnologica del mercato e nuove sfide della sicurezza. Tali incontri sono anche un'importante occasione per accedere a formazione e momenti di networking e crescita professionale. Il 2020 vede già a calendario le tappe di Security Summit di Milano (17-19 marzo); Treviso (21 maggio); Verona (7 ottobre) e Roma (5 novembre).

Clusit è inoltre promotore in Italia del mese per la sicurezza informatica - European CyberSecurity Month, una campagna dell'Unione Europea che si svolge ogni anno in ottobre con l'obiettivo di sensibilizzare, informare e formare cittadini e organizzazioni attraverso eventi sul territorio sui temi della cyber security come responsabilità condivisa. ✨

## PRIVACY GDPR E PROTEZIONE DEI DATI BALUARDI DELLA DEMOCRAZIA

*Il Presidente del Garante per la privacy, Antonello Soro interviene in parlamento sui pericoli delle smart city e dell'intelligenza artificiale*

*di Gaetano Di Blasio*



**A**ntonello Soro, presidente del Garante per la protezione dei dati personali, sottolinea come, in un periodo di rapidi cambiamenti quale l'attuale, sia necessario rinnovare il lessico e il diritto. Quest'ultimo deve colmare i vuoti che le nuove tecnologie rischiano di aprire quotidianamente. Più precisamente Soro ricorda che servono regole che affermino i principi di territorialità e sovranità.

Ci sono poi Interrogativi, molti generati dall'artificial intelligence, come, per esempio, valutare la soggettività giuridica relativa a un robot.

L'era digitale, continua Soro, rende più profondo il rapporto fra regola, società e diritto, ponendosi la questione dei confini che è lecito superare, senza "cadere nell'umana tracotanza. Per esempio, parlando di robot, quali possono essere i limiti da porre a

un'intelligenza artificiale, le cui decisioni si basano su algoritmi che sono, per definizione, perfettibili? Ma, "volando basso" appaiono urgenti anche questioni annose, come la "democraticità" di Internet. «La Rete, come ogni sistema relazionale, rischia di alimentare quelle asimmetrie anzitutto di potere, che dovrebbero, invece, scomparire per mezzo suo ell digitale diventa esso stesso confine», sostiene

Soro. Un confine "poroso" del nostro stesso essere persone, segnando il limite che separa la libertà dal determinismo.

«Se prive di regole, le nuove tecnologie possono alimentare un regime di sorveglianza rendendo un individuo una "non persona", cioè un individuo da normalizzare, addestrare o escludere.

Nell'era Digitale il dato diventa sempre più elemento che definisce la persona, ma la sua



*Antonello Soro, Presidente del Garante per la privacy*

mercificazione in una rincorsa alla svalutazione, ne svilisce l'individualità. spesso a opera dello stesso individuo.

In quest'ottica è necessario considerare l'importanza di una "educazione" alla Rete, perché la futura generazione sappia porre la tecnica al servizio dell'uomo.

Soro, facendo diretto riferimento all'Internet delle Cose e all'intelligenza artificiale, che è e sarà sempre più motore di una realtà connessa, che alimenta le città intelligenti, mette in guardia dall'abuso potenzialmente critico dei dati degli individui, laddove è labile il confine tra lecito e illecito, seppure il GDPR è chiaro al riguardo.

«Internet, da mezzo qual era, al pari di ogni tecnologia, è divenuta la nuova dimensione entro cui si svolge la personalità di ciascuno».

In questa dimensione, però, la percezione di libertà può essere distorta. Al riguardo Soro riporta l'esempio, per non guardare come sempre agli Usa, dell'Estonia, che ha sviluppato e investito nel digitale, ma più recentemente ha adottato leggi illiberali. Oppure cita Singapore, dove da un lato si sono sperimentati droni postino e taxi a guida autonoma, ma, dall'altro ha legittimato ampie deroghe alle regole della disciplina dati (che, in ogni caso ha varato), arrivando a consentire una sorta di monitoraggio delle persone, anche attraverso tecniche di sentimental analysis applicate ai post pubblicati sui social network.

In Cina, afferma inoltre il presidente del Garante per la protezione dei dati personali, si trovano oltre un



quarto delle 2mila aziende di intelligenza artificiale del mondo. Queste hanno un vantaggio competitivo rappresentato dalla disponibilità di dati pressoché fuori da ogni controllo da parte degli individui. I grandi provider, d'altro canto sono obbligati a consegnare al governo tutti i dati dei loro clienti, senza vincoli, in base a generiche esigenze di sicurezza.

Le tecnologie per il riconoscimento facciale sono utilizzate senza regole per controllare il e il crimine, ma in una regione è impiegato per pubblicare e mostrare su appositi schermi i debitori insolventi, in pratica come in una gogna digitale.

Agli individui non sono riconosciuti diritti, in cambio di una generica promessa di benessere sociale.

Se si considera lo sviluppo dei computer quantistici e i primati su tecnologie critiche come il 5G, si può paragonare la Cina al "monopolio" petrolifero degli anni 60'. In sostanza, l'intreccio fra reti e intelligenza artificiale rappresenta una questione vitale per lo



sviluppo sociale, di cui ancora non si comprende le dimensioni e le conseguenze, anche in considerazione delle difficoltà a trovare un'architettura sulle reti condivisa a livello occidentale.

Internet diventa la nuova catena di montaggio, che da un lato fornisce lavoro e sostentamento, ma dall'altro sviscerisce gli individui.

Ancor più preoccupante sembra essere il Social Credit System, introdotto dal governo Cinese, dapprima su base volontaria e dal 2020 obbligatoria, il quale, spiega Soro: «È stato istituito per valutare l'affidabilità dei cittadini, migliorare la fiducia nel Paese e promuovere una cultura di sincerità e credibilità giudiziaria. Un punteggio che viene assegnato controllando tutti i dati disponibili sull'individuo, dalle frequentazioni ai post in rete. Tale punteggio, se alto, agevola l'accesso a servizi pubblici e privati, mentre un punteggio basso impedisce l'accesso al credito, a determinate professioni e anche a

prestazioni di welfare». È evidente la deformazione implicita possibile in un sistema totalitario, che, nel nome di una maggiore sicurezza, annulla le logiche liberali. Soro vi contrappone appunto il diritto alla privacy paragonandolo alla mancanza di privacy imposta dalle ingerenze dei regimi totalitari del secondo dopoguerra.

Oggi la guerra diventa "cyber war", dove il dato digitale è l'estensione dell'individuo. Combattere il cyber crime annullando ogni diritto alla riservatezza non può essere una strategia di difesa.

D'altro canto, non si ha la certezza che una deregulation possa aiutare i "buoni".

Un attacco avvenuto a dicembre del 2019, ha colpito circa 3mila soggetti pubblici e privati, con l'interruzione dei servizi informatici degli uffici giudiziari distrettuali di tutta Italia. Anche nel resto d'Europa sono stati registrati attacchi gravi e i volumi raggiunti dal cyber crime crescono costantemente interessando il 74% dei affari mondiali.

La tutela dei dati diventa cardine della democrazia insieme grazie a una resilienza indispensabile, considerando l'influenza che i dati apportano nelle strategie di propaganda utilizzate quali strumenti di guerra della disinformazione.

La protezione dei dati è lo strumento basilare per fondare le smart city e far crescere la cultura digitale e produttiva del sistema Paese in Europa. La facilità, come su accennato, con cui si cedono i propri dati, senza realmente valutare cosa ci viene dato in cambio è il primo passo per l'insicurezza propria e del proprio paese. ❁

## TREND MICRO DELINEA IL NUOVO PANORAMA DELLE MINACCE

*Le minacce alla sicurezza non calano, anzi, aumentano con la diffusione delle nuove tecnologie. Lo rivela il Report 2020 della società*

di Paola Saccardi

**D**a 32 anni Trend Micro si impegna per contrastare le minacce informatiche in continua evoluzione. Oggi si assiste a un'ampia varietà di applicazioni, servizi e piattaforme e tutto va protetto. Le minacce sempre più complesse avranno la tendenza a combinare i rischi tradizionali con le nuove tecnologie, come l'intelligenza artificiale.

Restano sempre presenti alcune minacce che si ripetono da anni, come estorsioni e phishing, ma i rischi maggiori arriveranno dalle migrazioni cloud e dagli ambienti DevOps, che esporranno le organizzazioni a rischi anche di terze parti.

Trend Micro ha realizzato il nuovo report dal titolo "La nuova normalità: previsioni Trend Micro sulla sicurezza per il 2020" presentato nel corso della quinta edizione del suo Security Barcamp, un evento organizzato per fare luce sulle tendenze per il nuovo anno. Lisa Dolcini, marketing manager della società in Italia, ha introdotto alla platea presente gli ospiti sul palco, tra i quali Rik Ferguson, Vice President Security Research di Trend Micro e Gastone Nencini, Country

Manager di Trend Micro Italia. Al loro fianco anche la Polizia postale e il Politecnico di Milano.

Nik Ferguson ha ricordato che 7 anni fa veniva presentato il Project2020, un documento che portava alla luce le previsioni sul futuro della tecnologia. Ferguson, che ha commentato i trend in corso, ha ironizzato: «Ora che siamo nel 2020 possiamo vedere cosa abbiamo indovinato e cosa è andato diversamente» riferendosi per esempio alla diffusione della augmented reality di cui si era previsto un maggiore utilizzo e potenziali pericoli. Il ricercatore ha anche sottolineato che il mondo online e quello reale sono sempre più "vicini" tanto che in futuro gli hacker potranno riuscire a «minacciare la percezione della realtà delle persone».

Gastone Nencini, invece, ha ricordato l'importanza di fare informazione alle persone, ai cittadini, per istruirle sui potenziali rischi informatici. Trend Micro in questo senso si sta impegnando in Italia per diffondere questa cultura, anche tra i giovani attraverso un programma di volontariato presso le scuole.

La Polizia postale ha sottolineato come il fenomeno della truffa si basi spesso sulla falsificazione e simulazione. «Un soggetto che finge di essere un altro, solitamente tramite e-mail rubate, per ingannare qualcuno che opera all'interno di aziende o istituti bancari» ha spiegato Salvatore La Barbera, dirigente della Polizia Postale di Milano, con una vasta esperienza nel settore della criminalità, che lo ha portato ad occuparsi di financial hacking, frodi telematiche su

**Le previsioni di Trend Micro elencate in breve:****Il futuro è complesso**

- Gli attaccanti non avranno problemi ad aggirare patch incomplete e applicate in modo affrettato
- I cybercriminali utilizzeranno le piattaforme blockchain per le transazioni clandestine
- I sistemi bancari saranno nel mirino con open banking e malware per bancomat
- I deepfake creati con l'intelligenza artificiale saranno la nuova frontiera delle frodi aziendali
- I Managed Service Provider saranno colpiti per distribuire malware e scatenare attacchi supply chain
- Gli attaccanti approfitteranno dei bug trasformabili in worm e deserializzazione

**Il futuro è esposto**

- I cyber criminali utilizzeranno dispositivi IoT per azioni di spionaggio ed estorsione
- Chi adotterà il 5G dovrà mettere al sicuro le reti software-defined
- Le infrastrutture critiche saranno colpite da ulteriori attacchi e fermi della produzione
- Gli ambienti home office e di lavoro da remoto ridefiniranno gli attacchi supply chain

**Il futuro è mal configurato**

- Le vulnerabilità dei container saranno tra i principali problemi di sicurezza per i team DevOps
- Le piattaforme serverless aumenteranno la superficie di attacco a causa di errori di configurazione e codici vulnerabili
- Errori di configurazione da parte degli utenti e il coinvolgimento di terze parti non sicure, aumenteranno i rischi nelle piattaforme cloud
- Le piattaforme cloud saranno preda di attacchi basati sulle loro vulnerabilità come gli SQL injection, attraverso librerie di terze parti

larga scala, uso fraudolento dei mezzi elettronici di pagamento e attacchi informatici. La Barbera ha spiegato che la Polizia postale ha intrapreso un progetto con il mondo bancario per raccogliere informazioni sui destinatari delle frodi e per inserire all'interno di un'apposita banca dati gli iban che risultano sospetti e verso i quali vengono a priori congelati i trasferimenti di denaro, per evitare possibili truffe.

La tecnologia è sempre più pervasiva e abbraccia tutti i settori, da quello aziendale, a quello bancario, ai

cittadini privati alla pubblica amministrazione, perché consente evidenti vantaggi, ma allo stesso tempo non è immune da possibili attacchi informatici.

**Dove aumentano i rischi**

Con la diffusione del cloud computing in un numero sempre maggiore di aziende, ma non solo, soprattutto in quelle di dimensioni minori che grazie al cloud possono ottenere vantaggi prima insperati, i rischi per la sicurezza saranno in aumento.

Lo studio di Trend Micro evidenzia che i cyber criminali cercheranno di impadronirsi sempre più dei dati custoditi nel cloud, attraverso attacchi basati su immissioni di codice che prenderanno di mira sia i cloud provider sia le librerie di terze parti.

Secondo quanto suggerito dal report, il maggior utilizzo di codice di terze parti che alimenta la cultura DevOps farà aumentare i rischi. I componenti compromessi dei container e delle librerie utilizzate in architetture serverless e di microservizi, fanno aumentare la superficie dell'azienda esposta ai rischi e i metodi di difesa tradizionali faranno fatica a tenere il passo. Un altro settore a rischio è quello dei Managed Service Provider, che i criminali informatici sarebbero interessati a colpire per raggiungere altre organizzazioni e non soltanto per rubare i dati critici, ma anche per installare malware e sabotare fabbriche intelligenti oppure estorcere denaro attraverso il ransomware. Infine, un altro ambito in cui bisognerà fare attenzione sarà quello della supply chain. Spesso i lavoratori si connettono da remoto attraverso reti Wi-fi poco protette oppure creando dei potenziali rischi alla sicurezza ma anche le aziende che interscambiano i dati in modo digitale. Anche le vulnerabilità nei dispositivi domestici connessi potranno essere utilizzate come punto di accesso alle reti aziendali. ❁

## 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*

*di Riccardo Florio*



**P**revenire è meglio che curare: è un concetto condiviso ma, spesso, non applicato nell'IT security. Focalizzandosi sul tema della sicurezza applicativa, il processo di prevenzione dovrebbe avere inizio durante la fase di sviluppo, ma questo richiede che gli sviluppatori siano coinvolti nelle fasi di "security testing". Si tratta di un passaggio tanto importante quanto sottovalutato.

Infatti, tutti gli ambienti di sviluppo prevedono strumenti integrati di controllo sul codice (da quello di tipo ortografico al diagramma di flusso) ma un codice privo di errori non è necessariamente anche sicuro.

Attraverso la famiglia di soluzioni Fortify, Micro Focus mette a disposizione gli strumenti per prevenire le vulnerabilità e affrontare in modo efficace e strutturato il processo di controllo applicativo attraverso l'intero ciclo di vita.

### **Visualizzare in tempo reale le vulnerabilità**

Il primo passaggio per uno sviluppo privo di vulnerabilità è l'uso di strumenti che mettano in guardia lo sviluppatore, in tempo reale, sui potenziali problemi di sicurezza legati alle linee di codice che sta scrivendo.

Micro Focus ha realizzato Fortify Static Code Analyzer (SCA), uno strumento per il controllo statico delle applicazioni, che identifica le vulnerabilità di sicurezza durante la fase iniziale dello sviluppo ovvero quando l'eventuale correzione degli errori è

meno onerosa sia economicamente sia in termini di tempo.

Fortify SCA funziona in modo molto simile a un compilatore; legge i file di codice sorgente e li converte in una struttura intermedia, ottimizzata per l'analisi della sicurezza da parte di una serie di algoritmi specializzati capaci di individuare le violazioni delle procedure sicure di scrittura del codice. Fortify SCA prevede anche un sistema per la creazione di regole personalizzate per ampliare la capacità di rilevamento.

I risultati dell'analisi prodotta da questo software sono mostrati allo sviluppatore in tempo reale contribuendo a rafforzare la sua capacità di creare software più sicuro.

I risultati di Fortify SCA possono essere gestiti con Fortify Software Security, un sistema di gestione centralizzato che fornisce visibilità sul programma aziendale di revisione, controllo, assegnazione di priorità e correzione associato al processo di test di sicurezza del software.

### **Automatizzare il processo di audit**

Il secondo step per coinvolgere gli sviluppatori nei test di sicurezza consiste nell'automatizzare il processo di controllo.

L'audit automatizzato è molto più rapido rispetto a quello umano. In, tal modo, gli sviluppatori possono cominciare a lavorare su problemi che sono stati validati come vulnerabilità, pochi minuti dopo avere

ottenuti i risultati dell'analisi statica "grezza" del codice; questo senza correre il rischio di incappare in un falso positivo e disponendo già di una classificazione del livello di pericolosità della vulnerabilità. Fortify Static Code Analyzer è completato dal tool Audit Workbench, che fornisce un'interfaccia grafica utilizzabile dagli auditor della sicurezza per effettuare la scansione dei progetti software e per organizzare, investigare e predisporre i livelli di priorità sui risultati delle analisi.

Il sistema di auditing automatizzato di Fortify prevede prima ad anonimizzare i risultati, per poi effettuare un processo di analytics basato sul confronto con schemi di riferimento e infine eseguire analisi previsionali mediante algoritmi di machine learning. Il risultato di questo processo è estremamente accurato e minimizza la possibilità di incorrere in falsi positivi.

### **Formare gli sviluppatori sulle attività di sviluppo sicuro.**

Un terzo passaggio nel processo virtuoso di coinvolgimento degli sviluppatori nei processi di testing applicativo è quello di predisporre attività di formazione specifica.

In questo modo gli sviluppatori possono essere formati all'utilizzo delle best practice di codifica e abituarsi a scrivere codice privo di errori che introducano vulnerabilità.

Micro Focus mette a disposizione una vasta libreria

di corsi Web-based e prevede, nel suo portafoglio, una serie di soluzioni di formazione di enterprise security in diverse opzioni e modelli.

### **Esercitare un controllo costante delle applicazioni in produzione**

Lo scenario IT evolve nel tempo e, pertanto, l'approccio preventivo non può e non deve esaurirsi dopo la fase di rilascio. Inoltre, non tutte le aziende sviluppano autonomamente il proprio software così come non è quasi mai possibile esercitare alcun controllo sulle pratiche di sicurezza adottate nello sviluppo di software di terze parti.

Per rispondere a queste esigenze Fortify prevede una soluzione specifica chiamata WebInspect che si preoccupa di effettuare test dinamici di sicurezza sulle applicazioni in produzione, incluse quelle commerciali. WebInspect imita le tecniche di hacking e di attacco per identificare, classificare e riportare vulnerabilità applicative.

Un altro strumento della famiglia Fortify per esercitare una protezione costante sulle applicazioni è Fortify Application Defender, una soluzione RASP (Runtime Application Self-Protection) pensata per gestire e ridurre il rischio associato sia alle applicazioni sviluppate internamente sia di terze parti.



Fornisce visibilità in tempo reale sull'utilizzo (e l'eventuale abuso) di un'applicazione, mettendola al sicuro dai tentativi di sfruttamento delle vulnerabilità e da altri tipi di violazioni.

Application Defender può essere implementata come soluzione on-premise oppure sottoscritta come servizio; è caratterizzata da un

processo di installazione estremamente semplice e richiede solo pochi minuti per diventare operativa.

### **I vantaggi del modello on-demand**

Dotarsi di strumenti per il controllo applicativo, per le aziende che non hanno nel proprio core business le attività e le competenze di sviluppo può essere costoso. Anche qualora il budget non sia un problema, può risultare egualmente difficoltoso per la mancanza di figure competenti in grado di effettuare i controlli nei modi e tempi giusti e capaci di scegliere gli strumenti idonei.

A queste realtà Micro Focus indirizza Fortify on Demand, una piattaforma cloud che mette a disposizione tutta la potenza delle soluzioni Fortify in modalità automatizzata, consentendo anche a persone non esperte di svolgere controlli efficaci.

L'approccio as a service aiuta, inoltre, a contenere i costi e a predisporre attività di controllo e test in modo programmato.



## ENDPOINT AL SICURO CON LA CIFRATURA DEI DATI

*La cifratura e il monitoraggio dei dati permettono di migliorare la sicurezza degli endpoint e contrastare le minacce*

*di Giuseppe Saccardi*



Se la digitalizzazione dei processi di business, della produzione e delle relazioni umane apporta consistenti benefici, non c'è dubbio che la stessa apre la strada a concreti rischi per la sicurezza dei dati.

Generalmente si tende ad attribuire a cause esterne, tipicamente hacker, l'origine dei problemi, ma sovente questi sono invece da ricercare internamente, perlomeno come uno dei motivi che abilitano o rendono possibile un attacco. Un esempio in tal senso è la carenza o la totale mancanza di un piano per la sicurezza degli endpoint organico e ben strutturato. In sua mancanza risulta difficile contrastare attacchi portati su più piani, in profondità e a partire dai punti più deboli, gli endpoint.

I dipendenti, manager in primis, di un'azienda, osserva Matrix42, azienda specializzata nella sicurezza degli endpoint, gestiscono necessariamente al fine di svolgere il loro compito un consistente volume di dati, e il problema è che complice la crescente mobilità questa gestione avviene in luoghi deputati diversi da quello aziendale che è relativamente più facile proteggere, ad esempio in aereo, in treno, in

hotel o nei momenti di home working.

La virtualizzazione del workspace apre in sostanza la strada a concreti rischi per la sicurezza e amplia anche notevolmente la superficie di attacco.

La cosa è resa più critica dal fatto che non solo i computer e i notebook, ma anche gli smart device e i dispositivi IoT o Industrial IoT finiscono con il costituire un serio rischio per le aziende.

### **Proteggere i dati con la cifratura**

I rischi, osserva Matrix42, in cui incorre un'azienda non sono solo dovuti alla perdita di dati ma anche agli aspetti legali e normativi in cui si può incorrere. In proposito, il regolamento europeo per la protezione dei dati personali prevede concrete conseguenze nel caso in cui accessi non autorizzati ai dati portino a infezioni da malware e perdita dei dati, soprattutto di clienti o terze parti.

Non a caso, per il rafforzamento delle difese, il regolamento in oggetto stabilisce che la protezione contro la perdita dei dati avvenga mediante la cifratura e il log degli accessi ai dati non cifrati.

In linea generale, persino la perdita di un singolo

file può costituire un danno considerevole per le imprese. Tuttavia, sebbene proteggere dati e file mediante cifratura fornisca una maggiore sicurezza, non tutte le aziende la applicano per il timore che l'operazione porti a una riduzione della produttività dei dipendenti.

Cifrare i dati, osserva Matrix42, e si può di certo essere d'accordo con lei, è oramai una procedura quasi inevitabile e il non implementarla può essere percepito come un colpevole vulnus.

A giustificarla può bastare citare i dati di un recente studio dell'associazione digitale Bitkom, che ha evidenziato come nel corso del 2018 circa l'84% delle imprese nel settore industriale sia stato vittima di attacchi informatici ancora più intensi che nel 2016. Circa il 70% di questi attacchi hanno avuto origine a livello di endpoint, e i due terzi di questi non sono stati rilevati. Nel 2019 le cose non sono di certo migliorate.

### **I benefici dell'analisi in tempo reale**

Altre ricerche evidenziano la crescente importanza della protezione degli endpoint. Le soluzioni di sicurezza per gli endpoint quali la cifratura d hoc, costituiscono un'ulteriore barriera a soluzioni quali i firewall nel confronto dell'esfiltrazione di dati e permettono agli amministratori IT di implementare e rafforzare le policy di sicurezza.

Il concetto trova applicazione anche nell'eventualità che gli end device vengano smarriti o rubati. Il criptaggio dei dati, la cui efficacia è massimizzata da smart card e eToken, garantisce che i criminali



informatici non abbiano accesso alle informazioni sensibili.

Sono quindi raccomandate, osserva Matrix42, soluzioni di Cloud Storage Encryption, iOS e Android Encryption, Full Disk Encryption, Local Folder Encryption, Network Share Encryption, così come di Removable Device Encryption e il criptaggio permanente file-base.

Per una difesa efficace contro gli attacchi, peraltro, la società suggerisce anche di utilizzare un sistema di difesa multilivello contro il trasferimento non autorizzato dei dati.

In questo caso, le soluzioni software devono però poter analizzare e classificare i processi in tempo reale, così come anche la migrazione dei dati e la loro archiviazione ai diversi livelli.

E, non ultimo, garantire che la cifratura e la relativa decifratura siano applicate non solo per le classiche workstation, come i sistemi Windows, ma anche per



macOS, Android, iOS e similari.

### Cifrare in modo sicuro

Va comunque osservato che la cifratura è un campo solo parzialmente esplorato ed utilizzato. Sin dalla ideazione della macchina Enigma si è assistito ad una rincorsa tra l'ideazione di nuovi metodi pubblici e privati, a più chiavi, eccetera, e chi cerca di trovare il modo di effrangere i dati cifrati.

Esiste poi una concezione diffusa, ma non del tutto corretta, evidenzia Matrix42, che le aziende debbano cifrare la comunicazione stessa solo quando si procede alla sincronizzazione dei dati.

I provider dei rispettivi servizi di sincronizzazione, generalmente, possiedono le chiavi per la cifratura. Tuttavia, i dati stessi non sono criptati: ciò significa che persone o organizzazioni non autorizzate, come ad esempio degli hacker, possono ottenere l'accesso alle chiavi segrete dei provider oppure accedere

direttamente all'archivio dei dati.

Di certo, la modalità più sicura si verifica quando sono le stesse imprese a detenere le chiavi e criptano i dati prima della sincronizzazione.

Le aziende dovrebbero cifrare le interfacce di dati che utilizzano, preferibilmente file-based e on-the-fly. Questa procedura ha il vantaggio di essere un metodo sostenibile, poiché le aziende non devono preparare un archivio dati in anticipo e non sono costrette a installare o gestire applicazioni aggiuntive per l'autenticazione, il decriptaggio o il criptaggio. In ultima istanza, un monitoraggio sistematico degli endpoint rende possibile implementare funzioni di alert a livello aziendale che sono accompagnate da risposte automatiche in caso di minaccia.

Il principio alla base è che l'IT controlla, accede e cripta gli accessi ai dati negli endpoint. Le nuove tecnologie basate sul Machine Learning (ML) e l'Intelligenza Artificiale (IA) forniscono in tal senso capacità potenziate correlate alle strategie di sicurezza degli endpoint.

Sono peraltro soluzioni che evolvono e apprendono da eventi passati e rendono persino possibile combattere minacce non solo già note ma anche sconosciute, e farlo in tempo reale.

Ma non solo. Il ricorso contemporaneo a ML e IA semplifica anche identificare ed evitare falsi positivi quali i falsi allarmi. Di certo nel prossimo futuro vi saranno ulteriori sviluppi in questo campo, ma una cosa è già certa, osserva la società: un concetto di sicurezza che non considera gli endpoint è incompleto. ❁

## CYBERARK BLUEPRINT METTE AL SICURO GLI ACCESSI PRIVILEGIATI

*Il Blueprint comprende strumenti e supporto normativo che permettono di innalzare i livelli di sicurezza e di concentrarsi sulle priorità della trasformazione digitale*

*di Giuseppe Saccardi*

CyberArk, azienda che sviluppa soluzioni per la protezione degli accessi privilegiati, ha annunciato il via al suo nuovo programma CyberArk Blueprint for Privileged Access Management Success, progettato per supportare le aziende nell'adottare un approccio flessibile, adattabile alle esigenze, modulare e misurabile che permetta di ridurre i rischi in cui possono incorrere gli utenti privilegiati. In base all'esperienza dei CyberArk Labs, di Red Team e degli sforzi per rispondere agli incidenti, osserva l'azienda di cyber security, praticamente tutti gli attacchi mirati seguono uno schema standard per la compromissione delle credenziali privilegiate. Questi modelli hanno avuto un'importante influenza nella definizione dei tre principi guida fondamentali del programma CyberArk Blueprint: prevenire il furto

di credenziali, fermare i movimenti laterali e verticali, limitare l'escalation dei privilegi e gli abusi.

### **Keep it simple**

La soluzione adotta in pratica un approccio semplice e prescrittivo basato sulle linee guida evidenziate al fine di contenere il rischio nelle cinque fasi di perfezionamento della gestione degli accessi privilegiati. CyberArk Blueprint dispone di modelli e sessioni di progettazione di roadmap personalizzabili in modo da permettere alle organizzazioni dei diversi settori di ampliare in modo progressivo i controlli e la strategia di accesso inerente gli account privilegiati.

In particolare diventa ad esempio possibile: Prevenire il furto di credenziali: Per mitigare i rischi interni ed esterni, le aziende devono prevenire il furto di credenziali critiche, per esempio quelle di amministratori IaaS, amministratori di dominio o le chiavi API, che potrebbero essere utilizzate per realizzare attacchi di acquisizione di rete o compromettere gli account delle infrastrutture principali. Tramite l'isolamento delle sessioni, la rimozione delle credenziali codificate e le strategie di rilevamento e blocco dei furti, diventa possibile proteggere l'accesso privilegiato da parte di persone, applicazioni e nei processi CI/CD. Blocco dei movimenti laterali e verticali: Il principio fa leva sul rafforzamento dei confini delle credenziali, sull'accesso just-in-time e sulla randomizzazione delle credenziali. L'obiettivo è di impedire ai



*Nir Gertner, chief security strategist di CyberArk*

malintenzionati di passare da dispositivi non affidabili a console cloud o controller di dominio di alto valore e bloccare e interrompere di conseguenza la catena di attacchi.

Limitare l'escalation di privilegi e abusi: Per impedire agli aggressori di abusare dei privilegi e ridurre la superficie complessiva dell'attacco, è importante implementare controlli forti sui privilegi minimi, disporre di analisi comportamentale e rispondere agli attacchi in modo adattativo.

«Semplice ma completo, CyberArk Blueprint offre

una guida imparziale che allinea le iniziative di gestione degli accessi privilegiati alla riduzione del rischio potenziale, aiutando le aziende ad affrontare le principali responsabilità il più rapidamente possibile. Indipendentemente dal loro livello di gestione degli accessi privilegiati, CyberArk Blueprint consente alle aziende di rendere gli investimenti in nuove tecnologie a prova di futuro, migliorando la sicurezza, riducendo la superficie di attacco e ottimizzando l'efficienza operativa», ha commentato Nir Gertner, chief security strategist di CyberArk. ✨

## PREVENIRE GLI ATTACCHI API CONTROLLANDO LE CREDENZIALI

*Uno scarso controllo delle credenziali tra applicativi e il non monitoraggio del traffico interno apre la strada a pericolosi attacchi*

*di Giuseppe Saccardi*

**G**li attacchi informatici stanno diventando sempre più sofisticati. Questo fenomeno è reso ancora più critico dal fatto che per gli hacker non è più sufficiente appropriarsi di credenziali aziendali o private, realizzare azioni dannose e rubare ingenti somme di denaro attraverso azioni di phishing. Il loro obiettivo è ora spostato sull'interazione tra applicazioni. Questo è un livello più profondo, osserva Di Massimo Carlotti, Presales Team Leader

di CyberArk, solo in apparenza più complesso da colpire, che è sempre più al centro dell'attenzione e degli attacchi.

Come confermato da un recente report, da maggio dello scorso anno il 75% degli attacchi è stato rivolto a livello API - acronimo di Application Programming Interface - in modo da superare i controlli di sicurezza e realizzare azioni più insidiose in modo ancor più efficace.

Il motivo di questo concentrarsi di interessi, malevoli, sul livello API è conseguenza del fatto che il controllo delle credenziali tra applicativi viene spesso effettuato in modo superficiale, con le aziende che non monitorano in modo efficace il traffico al loro interno, lasciando così finestre di accesso aperte ai malintenzionati.

Pensiamo, osserva Carlotti, ai reali ed effettivi pericoli che un'azienda potrebbe affrontare, qualora gli hacker riuscissero ad accedere ai sistemi e a pilotarne le attività: una banca vedrebbe la gestione dei pagamenti compromessa, un'industria potrebbe perdere il comando degli impianti e un magazzino potrebbe assistere a processi di logistica completamente sconvolti.

I rischi, non solo economici, sono realmente elevati ed è per questo che c'è un forte impegno da parte degli esperti in sicurezza informatica nel sensibilizzare imprese e responsabili di sicurezza sull'importanza di difendere gli accessi privilegiati, non solo a livello di identità umane, ma anche application-to-application, e farlo definendo metodi di autenticazione appropriati, senza complicare eccessivamente



*Massimo Carlotti, Presales  
Team Leader di CyberArk*

il processo.

Un altro passaggio fondamentale è quello di estendere le capacità aziendali di audit e monitoraggio agli ambienti DevOps, con l'adozione di nuove misure di protezione dedicate ad account privilegiati, credenziali e segreti, per avere una panoramica completa di chi accede a quali elementi ed essere in grado di analizzare e monitorare gli accessi in tutto l'ambiente.

«Il paragone potrebbe sembrare banale, ma ci sembra efficace. Se a casa investiamo in una porta blindata o in un sistema di videosorveglianza, consapevoli dei potenziali rischi ai quali siamo esposti, anche le aziende dovrebbero adottare lo stesso approccio. La buona notizia è che in molte lo stanno già facendo» ha evidenziato Carlotti. ❁

## SOTTOVALUTARE IL SECURITY OPERATIONS CENTER PUÒ COSTAR CARO

*In oltre il 40% delle grandi imprese italiane manca il SOC. È una carenza che, spiega Maurizio Tondi di Axitea, può mettere in forse la sicurezza aziendale*

*di Giuseppe Saccardi*

Una recente ricerca, condotta su 6.000 dipendenti di PMI e grandi aziende di vari paesi, tra cui anche l'Italia, ha analizzato la percezione di sicurezza negli ambienti aziendali. In Italia, il dato più interessante riguarda la scarsa presenza di SOC e, di conseguenza, la sensazione di arretratezza nello svolgimento delle pratiche inerenti la sicurezza informatica.

Ma, in primis, cos'è il SOC e perché è così importante? In sintesi, il Security Operations Center è un centro che comprende diversi team di esperti dal quale vengono erogati servizi di gestione, monitoraggio e, in alcuni casi, di incident response.

Il suo obiettivo è quello di garantire la sicurezza dei sistemi informativi aziendali o di clienti esterni.



*Maurizio Tondi, Director Security Strategy di Axitea*

Dall'indagine realizzata da Bitdefender è emerso che circa la metà dei dirigenti italiani ignora quali siano le policy essenziali della sicurezza informatica e ammette di non avere risorse economiche sufficienti da investire.

Oltre alle risorse limitate anche la percezione dei dipendenti sugli investimenti è negativa, infatti solo meno di un quarto degli intervistati ritiene che l'investimento della propria azienda in strategie di sicurezza sia adeguato.

In relazione con gli altri stati europei, il dato in cui l'Italia è fanalino di coda è la presenza di un SOC: è assente in oltre il 40% delle aziende è assente, a fronte di una media del 30%.

Avere un servizio di questo tipo, evidenzia Maurizio Tondi, Director Security Strategy di Axitea, aumenta la velocità di reazione a un attacco informatico o alla rilevazione di un problema nella propria infrastruttura, diminuendo notevolmente le conseguenze sui sistemi informativi, sulla produttività e sul "portafoglio" dell'azienda.

Più del 60% dei dipendenti del reparto IT, peraltro, crede che la propria azienda, in caso di un attacco malware, non sia pronta ad agire in modo corretto e tempestivo.


### **Diffusione limitata**

Quello che emerge dai freddi dati statistici, evidenzia Tondi, è che la diffusione e la conoscenza del SOC in Italia rispetto ad altri paesi è ancora troppo

bassa, le aziende non sanno cosa può offrire nello specifico, o credono che sia un servizio troppo costoso perché non possiedono la percezione di quali siano i reali vantaggi che può apportare.

Perlomeno, viene da considerare, sino a che non si è coinvolti in un incidente serio che obblighi, obtorto collo, a riconsiderare la propria postura nei confronti della cyber security.

«Non tutte le aziende hanno le risorse economiche e umane per crearne uno interno, ma aziende come Axitea possono offrirlo come servizio gestito, al fine di dare ai clienti tutta la visibilità e la protezione necessaria, condividendo la professionalità e il know-how acquisito con esperienza e mettendo a disposizione personale altamente specializzato. Il SOC rappresenta uno strumento prezioso per molte realtà, sia piccole che grandi, contribuendo alla difesa dei più importanti asset aziendali» ha osservato Tondi. ❁



## SIMULARE PREVIENE GLI ATTACCHI E MIGLIORA LA SICUREZZA

L'uso di tecniche d'attacco sempre più sofisticate richiede ai team dei fornitori di servizi di sicurezza gestita la costante capacità di individuare l'ampio panorama delle minacce dentro e fuori dal perimetro aziendale, di intercettare rapidamente i rischi e mettere in atto un approccio proattivo nell'affrontare le insorgenti minacce alle reti aziendali. Come fornitore di soluzioni digitali end-to-end per le medie e grandi aziende, il Gruppo Lutech, ha



## *Lutech adotta per il proprio SOC la piattaforma di sicurezza di Picus Security per le attività di simulazione di attacchi e le violazioni della rete aziendale*

*di Giuseppe Saccardi*

evidenziato l'azienda, considera la sicurezza informatica una componente fondamentale per garantire ai propri clienti la massima continuità aziendale. Per perseguire questo obiettivo ha attivato recentemente a Milano il suo Next Operations Generation Security Operations Center (NG SOC).

### **Simulare per prevenire**

Per mettere in atto e sviluppare attività di simulazione

preventiva Lutech ha adottato la piattaforma Picus Security Breach & Attack Simulation.

La piattaforma, ha spiegato, è in grado di testare migliaia di minacce sull'infrastruttura di sicurezza dei clienti senza richiedere alcun intervento manuale e in maniera automatizzata.

La piattaforma è in grado in sostanza di intercettare le falle di sicurezza e fornire soluzioni veloci tramite un ampio ecosistema di partnership.

Operativamente, Picus fornisce una console di gestione e un'infrastruttura di provisioning flessibile per i fornitori di servizi di sicurezza gestita, e li supporta nell'implementazione rapida dei più opportuni servizi di convalida continua della sicurezza.

E' tramite la console e le funzionalità relative che Lutech supporta i clienti nell'attività di simulazione di attacchi e violazioni alla rete aziendale.

«L'obiettivo principale di Lutech è di offrire le massime prestazioni ai propri clienti integrando nel suo nuovo NG SOC le tecnologie più innovative. Siamo rimasti particolarmente colpiti dalle capacità della piattaforma Picus BAS in termini di identificazione rapida delle falle di sicurezza in una rete aziendale. Una piattaforma che offre un solido contesto di mitigazione pienamente compatibile con l'offerta di un MSSP», ha commentato l'accordo Tullio Pirovano, Ceo del Gruppo Lutech.

Come accennato, i servizi di sicurezza sono erogati dal SOC da team di esperti di sicurezza informatica e ethical hacker che condividono 330 posti attivi h24. I servizi di sicurezza gestita erogati prevedono una protezione aziendale a 360 gradi. ✱

# È disponibile il nuovo libro **SMART & DIGITAL TRANSFORMATION**

## **SMART & DIGITAL TRANSFORMATION**

*Aziende, ambienti produttivi e città sono sempre più  
Smart, ma si deve garantire flessibilità, always-on,  
sicurezza e accesso al multcloud*

Giuseppe Saccardi

**Reportec**

Il libro è acquistabile al prezzo di 30 euro (IVA inclusa) richiedendolo a  
**info@reportec.it - tel 02 36580441 - fax 02 36580444**