



LE MINACCE CRESCONO DA OGNI PARTE

I DATI DEL RAPPORTO
CLUSIT E ALTRE ANALISI

pag. 4

IN QUESTO NUMERO:

CYBER ATTACK

pag. 4

- Cybercrime ha via libera in Italia non s'investe in security

pag. 6

- Rischio sopravvivenza in metà delle aziende italiane

pag. 10

- Video giochi sotto la minaccia dei cyber criminali

SOLUZIONI

pag. 12

- Zero-Trust: che cosa significa e a che cosa serve

pag. 16

- Stop alle vulnerabilità applicative con Micro Focus Fortify

pag. 18

- Protezione runtime con la Container Security di Qualys

pag. 20

- Le best practice per la cyber security

pag. 22

- Come collaborare da remoto in modo sicuro

pag. 24

- La Enterprise Mobility nella ripartenza al tempo del Covid-19

pag. 26

- Workstation più sicure con Stormshield end point

OAD 2020

L'iniziativa OAD, Osservatorio Attacchi Digitali in Italia, con il 2020 è alla 12° edizione, con 12 anni consecutivi di indagini sugli attacchi digitali intenzionali ad aziende ed enti pubblici in Italia.

OAD è l'unica iniziativa in Italia per l'analisi sugli attacchi, realizzata tramite una indagine anonima con un questionario compilabile on line, indirizzata a tutte le aziende e alle Pubbliche Amministrazioni di ogni settore merceologico e dimensione. OAD collabora con la Polizia Postale e delle Comunicazioni, che fornisce significativi dati sugli attacchi digitali che costituiscono crimini informatici. Obiettivo principale di OAD è fornire reali e concrete indicazioni sugli attacchi ai sistemi informatici che possano essere di riferimento nazionale, autorevole e indipendente, per la sicurezza ICT in Italia e per l'analisi dei rischi ICT. La disponibilità di dati "locali all'Italia" sugli attacchi digitali intenzionali rilevati, sulla tipologia e sull'ampiezza del fenomeno è fondamentale anche per le organizzazioni di piccole e piccolissime dimensioni per valutare i possibili rischi e attivare le misure più idonee di prevenzione e protezione, così come richiesto da numerose normative nazionali ed internazionali, non ultimo il GDPR, il regolamento europeo sulla privacy. OAD, con la sua indagine e con lo stretto supporto di AIPSI, Associazione Italiana Professionisti Sicurezza Digitale (Capitolo italiano della mondiale ISSA), intende inoltre contribuire alla sensibilizzazione e alla consapevolezza, in Italia, sulla sicurezza digitale del personale a tutti i livelli, dai decisori di vertice agli utenti. Quest'ultimo obiettivo è particolarmente importante per creare una più diffusa cultura in materia di sicurezza digitale, che va oltre il mondo tecnico-informatico e toc-

ca anche i vertici dell'organizzazione e tutti coloro che decidono requisiti e budget della sicurezza digitale nei processi organizzativi delle proprie strutture.

Per la prima volta nell'edizione 2020, chi completa il questionario on line avrà anche in tempo reale una valutazione di sintesi di come le misure di sicurezza digitale indicate rispondano effettivamente alle esigenze di sicurezza digitale indicate per l'azienda/ente ed il suo sistema informatico: una macro valutazione qualitativa (e gratuita) del livello di sicurezza digitale del sistema informatico oggetto delle risposte fornite provè nel rispondere al questionario.

Per motivare il rispondente, a conclusione delle risposte fornite al questionario on line, oltre alla valutazione di cui sopra, è possibile scaricare gratuitamente il numero di maggio 2020 di ISSA Journal, la rivista mensile riservata ai soci AIPSI-ISSA, che tratta la crittografia quantistica, e l'intero volume "Information Security e Data Protection", pubblicato da Reportec, che è anche Publisher e Media Partner per OAD.

Il Rapporto finale di OAD 2020 è previsto per fine novembre 2020, e sarà scaricabile gratuitamente da parte di tutti gli interessati. Più compilazioni del questionario si avranno, provenienti dai vari settori merceologici e dalle Pubbliche Amministrazioni Centrali e Locali, più analitico, dettagliato, accurato e autorevole potrà essere il rapporto finale.

Si prega pertanto il lettore di questa nota di compilare, o di far compilare dai suoi tecnici, il questionario on line disponibile alla pagina: <https://www.oadweb.it/lime-survey2020/index.php/574592?lang=it>



Security & Business 56
novembre-dicembre 2020

Direttore responsabile:
Gaetano Di Blasio

In redazione:
Giuseppe Saccardi, Paola
Saccardi

Hanno collaborato:
Marco R. A. Bozzetti,
Riccardo Florio

Grafica: Aimone Bolliger
Immagini: dreamstime.com
www.securityebusiness.it

Editore: Reportec srl
Via Marco Aurelio 8
20127 Milano
tel. 02.36580441
Fax 02.36580444
www.reportec.it

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

Tutti i marchi sono
registrati e di proprietà
delle relative società

LE MINACCE CI CIRCONDANO: OCCORRONO STRATEGIE

Smart working, video giochi e la criticità di una pressione costante. Il Rapporto Clusit ha mostrato il consueto scenario di assedio cui le aziende prepararsi per fronteggiare le minacce del cybercrime.

La strategia può essere solo quella della resilienza. Ai dati del suddetto rapporto si aggiungono alcuni contributi provenienti dalle aziende che sempre più pubblicano indagini e informazioni di scenario, consapevoli dell'importanza della comunicazione, non solo per ridurre la superficie d'attacco attraverso la formazione, ma anche e soprattutto per aiutare le imprese a organizzare la risposta agli incidenti, pressoché inevitabili, considerando l'industrializzazione del cyber: un "mercato" in crescita costante.

L'analisi dei dati resta fondamentale, per questo realizziamo in partnership con l'associazione AIPSI (Associazione Italiana Professionisti Sicurezza Informatica) il rapporto OAD (Osservatorio Attacchi Digitali), che raccoglie i dati relativi alle violazioni verificatesi nel nostro Paese. Solo per questo numero sarà disponibile lo strumento di "assessment leggero" che fornisce un'indicazione del proprio stato della sicurezza. A fine anno, infatti saranno tirate le somme e si vedrà lo stato degli attacchi in Italia, confrontabile con i dati dei precedenti 12 anni di osservazioni.

La collaborazione con AIPSI si estende anche alla pubblicazione di contenuti importanti sotto il profilo tecnico/tutoriale.

In particolare su questo numero ospitiamo l'importantissimo tema dello Zero Trust, cioè, banalizzando il concetto: non fidarsi di nulla e nessuno.

Tornando al tema di dati presentiamo una ricerca piuttosto estesa realizzata dagli esperti di Bitdefender e relativa al mercato europeo, confrontato con la situazione italiana, da cui emerge una diffusa preoccupazione per l'industrializzazione degli attacchi.

Più di nicchia, ma interessanti sono i dati e i suggerimenti di Panda Security nonché quelli sulle soluzioni di Microfocus Security, CyberArk, Mobileiron, CIE Telematica.

CYBERCRIME HA VIA LIBERA IN ITALIA NON S'INVESTE IN SECURITY

Mancano ricerca e innovazione, secondo il rapporto Clusit

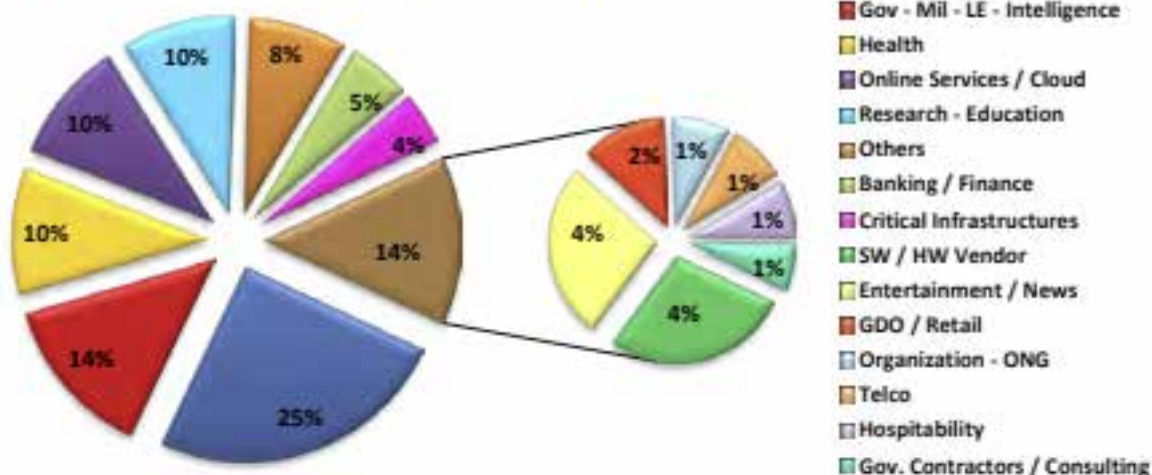
di Gaetano Di Blasio

I dati presentati dagli esperti del Clusit, relativi secondo semestre 2020 mostrano uno sconcertante risultato, con un aumento degli attacchi. In particolare sono cresciuti gli attacchi rivolti alle infrastrutture critiche, che segnano un +85%, cui si aggiunge la crescita degli attacchi rivolti verso il settore della ricerca e della scuola con un incremento del 63%. Da segnalare che sono stati analizzati 850 attacchi gravi nel primo semestre 2020: si tratta di una tendenza che risulta in costante crescita, definendo il semestre peggiore di sempre a livello globale. Nello

stesso periodo sono aumentati gli attacchi contro i Gov Contractors del 73,3%. In particolare Nel semestre si è inoltre registrato un incremento degli attacchi rivolti alle stesse istituzioni governative pari al 5,6%, sempre rispetto allo stesso semestre dello scorso anno.

Ha commentato Gabriele Faggioli, presidente del Clusit: «Di fronte a questo scenario, che sottende un'accelerazione del cyber crimine con logiche industriali, crediamo che sia fondamentale sviluppare Ricerca e l'Innovazione, anche attraverso il finanziamento a startup e iniziative imprenditoriali italiane nel settore della cyber security. L'avvio di imprese nel settore della cybersecurity sembra incontrare maggiori criticità nel nostro Paese rispetto al resto del mondo. I dati dell'Osservatorio Cyber Security &

Tipologia e distribuzione delle vittime (1H 2020)



Data Protection del Politecnico di Milano evidenziano infatti che su un totale di 254 start up nell'ambito della cybersecurity avviate nel mondo a partire dal 2015, solo il 2% è italiano; in termini di finanziamento, la media italiana è stata di un milione di dollari, a fronte dei 15 milioni di dollari ricevuti in media nel resto del mondo».

Il presidente del Clusit continua: «Per attuare una strategia efficace di cyber difesa occorrono adeguati investimenti in Ricerca e Innovazione dovrebbero prevedere anche forme condivise di sapere e collaborazione tra pubblico e privato, così come la proposizione di un programma formativo nazionale che sviluppi a lungo termine le competenze necessarie. In particolare, le tecnologie "dual use" oggi disponibili sul mercato e il loro utilizzo da parte dei diversi stakeholder rappresentano l'asset emblematico di questa cooperazione. Pensiamo che questi siano i primi e urgenti passi da compiere per mettere in moto un processo virtuoso di crescita non solo tecnologica, ma anche economica dell'intero sistema Paese Lavoriamo in questa direzione anche con le istituzioni; in gioco ci sono continuità sociale ed economica».

Riportiamo alcuni dei dati compresi nel rapporto, evidenziando alcuni risutati più eclatanti.

Oltre ai danni direttamente conseguenti agli attacchi compiuti, gli esperti Clusit evidenziano che il tema Covid-19 ha alimentato anche la diffusione di fake-news, fomentando la confusione sulla pandemia che si è venuta a creare a livello globale soprattutto nei primi mesi.

Gli attacchi a tema Covid-19 sono stati condotti nel 61% dei casi con campagne di "Phishing" e "Social Engineering", anche in associazione a "Malware" (21%), colpendo tipicamente i cosiddetti "bersagli

multipli" (64% dei casi): si tratta di attacchi strutturati per danneggiare rapidamente e in parallelo il maggior numero possibile di persone ed organizzazioni. Il 12% degli attacchi a tema.

Cyber attacchi nel primo semestre 2020: chi viene colpito e perché.

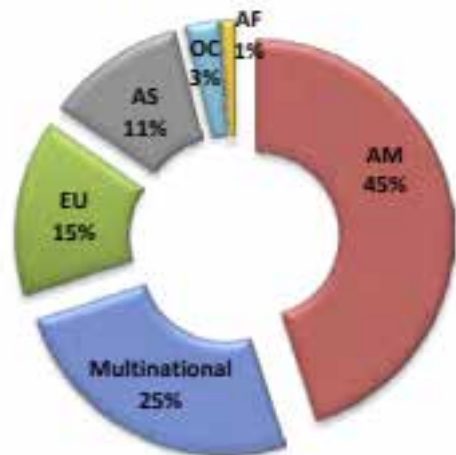
Nei primi sei mesi del 2020 gli esperti Clusit hanno registrato in prevalenza attacchi verso la categoria "Multiple Targets" che, come nel caso specifico degli attacchi a tema Covid-19, risulta la categoria più colpita, in crescita del 26% rispetto allo stesso periodo dello scorso anno.

A crescere maggiormente sono tuttavia gli attacchi verso le categorie "Critical Infrastructures" (+85%), "Gov Contractors" (+73,3%) e "Research / Education" (63%). Sono anche aumentati gli attacchi verso la categoria "Government" (+5,6%).

In termini assoluti, il settore "Government - Military - Intelligence" è stato il secondo settore nel mirino degli attaccanti (con il 14% degli attacchi), seguono i settori "Healthcare" e "Online Services" (10% degli attacchi).



Appartenenza geografica delle vittime per continente (1H 2020)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia - aggiornamento giugno 2020

RISCHIO SOPRAVVIVENZA IN METÀ DELLE AZIENDE ITALIANE

Un 46% dei manager teme i rischi indotti dall'industrializzazione del cyber crime

di Gaetano Di Blasio

L'impatto economico che il Covid ha determinato s'incrocia con le problematiche di sicurezza che sono tornate prepotentemente sul tavolo dei decisori aziendali. Ciò, in particolare, a causa dell'ampliarsi degli attacchi e, al contempo, delle difficoltà che le società incontrano nell'occuparsi adeguatamente della cybersecurity. Si evidenzia, osservano gli esperti di Bitdefender, che hanno diffuso una nuova indagine sui fenomeni legati alle violazioni dei dati, una superficie d'attacco maggiore, attraverso la quale il cybercrime ha così potuto proliferare nel 2020.

Se risulta difficile per tante aziende integrare i tool e le practice per combattere le minacce, ancor più critico è portare in azienda le competenze, sempre più eterogenee, che occorrono per contrastare le attività malevole e sviluppare i processi che migliorano la sicurezza.

Purtroppo, ci svela Denis Cassinerio, Director Regional Sales Director SEUR di Bitdefender: «Sono molti i recenti attacchi, anche sul piano nazionale che hanno mostrato le carenze delle imprese, quali Geox e Carraro oppure Bonfiglioli, cui va il merito dell'aver avvisato il mercato relativamente a come l'attacco subito avrebbe potuto far danni sulla filiera».

In tale contesto, pertanto, non stupisce che il 46%

delle società italiane coinvolte in un sondaggio da Bitdefender abbia dichiarato di temere per la sopravvivenza della propria azienda.

D'altro canto, rivela ancora il manager: «Gli attaccanti continuano ad attrezzarsi con incredibile velocità, già nella prima parte dell'anno si era notato un evolversi delle minacce ransomware, che maturavano di sette volte, secondo la telemetria di Bitdefender, sfruttando i temi del Covid».

È andato crescendo inoltre, l'uso di tecniche avanzate per entrare nei sistemi della vittima, per esempio cercando e crittografando i backup in modo da impedirne il ripristino e rendere efficaci le richieste di riscatto.

Attacchi di questo genere sono tanti, il che, evidenzia Cassinerio, dà l'idea dell'industrializzazione sviluppatasi con il RaaS ovvero ransomware as a service.

La Nuova Normalità tra le minacce previste per il 2021

Il report "Business Threat Landscape" realizzato dagli esperti di Bitdefender illustra il quadro delle minacce indirizzate alle aziende, le quali comprendono attacchi alle vulnerabilità, che fanno leva sulle patch mancanti, e la crescita di attacchi noti, alcuni dei

quali sempre più condotti anche attraverso la filiera degli MSP (Managed Service Provider). Le imprese avranno l'opportunità di imparare e adattarsi a una nuova normalità in quanto saranno costrette ad affrontare i cambiamenti nel panorama minacce e le molte che saranno riutilizzate, come, per esempio quelle che sfruttano vulnerabilità non risolte..

«Configurazioni errate, attacchi mirati commissionati a pagamento, attacchi di tipo 0-day per cui non sono ancora disponibili patch, aumento delle tattiche di esecuzione "stealth" sono solo la punta di un iceberg.

La telemetria di Bitdefender mostra che il 63,63% di tutte le vulnerabilità segnalate e non ancora identificate coinvolge falle di sicurezza note più vecchie del 2018, segnalando che le aziende hanno, potenzialmente, un'ampia superficie di attacco che gli hacker potrebbero sfruttare. Se l'apice delle minacce opportunistiche nel 2020 si è focalizzato intorno alle email di spear-phishing che sfruttavano i temi della pandemia, è probabile che le vulnerabilità non ancora identificate finiranno sotto i riflettori nel 2021. Quindi le aziende devono adottare rapidamente soluzioni di mitigazione e patch management che valutano lo stato dei dispositivi in dotazione ai dipendenti, per diminuire la crescente esposizione al rischio di un attacco di tipo cyber.

Rivalutazione dello stack di sicurezza aziendale

Durante la fase di esecuzione degli attacchi, l'uso di comandi e script PowerShell rimane la sotto-tecnica

preferita dai criminali informatici: rappresenta infatti ben il 42,52% di tutte le sotto-tecniche segnalate. Gli hacker prediligono quelle tattiche che si muovono al di sotto delle soglie di rilevazione delle soluzioni di sicurezza tradizionali, perciò è probabile che le aziende dovranno rivalutare il loro stack di sicurezza per il 2021 e includere soluzioni efficaci che non si limitino a fornire funzionalità antimalware.

Contro misure per gli hacker APT "in affitto" - Focus sulle PMI

Uno dei più grandi cambiamenti nel panorama internazionale delle minacce riguarda la comparsa di hacker APT "in affitto", che ha costretto le aziende

La metodologia dello studio

In particolare ha preso in considerazione i punti di vista e le opinioni di oltre 6.700 professionisti del settore, tra cui CISO, CSO e CIO, in diversi Paesi: Regno Unito, Stati Uniti, Australia/Nuova Zelanda, Germania, Francia, Italia, Spagna, Danimarca e Svezia. Gli intervistati rappresentano un ampio spaccato di aziende che vanno dalle PMI fino a imprese quotate in borsa con 10.000 e oltre dipendenti in un'ampia varietà di settori, tra cui quello finanziario, governativo, sanitario e della tecnologia.



di tutte le dimensioni e settori a rivalutare le minacce che si trovano ad affrontare. Mentre gli attacchi APT tradizionali erano rivolti contro enti governativi e settori industriali specifici, oggi gli attacchi in stile APT da parte di hacker mercenari cambiano totalmente il paradigma della sicurezza per ogni azienda. Nel caso delle PMI, che sono maggioranza in Italia, sottolinea Cassinerio, le aziende devono cambiare l'approccio con cui disegnano i modelli di minaccia. Finora, per la maggior parte, le violazioni APT, facevano parte degli attacchi alla filiera, ma, spiegano in Bitdefender, ora, questa nuova dinamica potrebbe significare attacchi continui, con la conseguenza del dover alzare il livello di sicurezza con strumenti di visibilità sia a livello di endpoint che di rete. Per esempio, gli strumenti di rilevamento automatico a livello endpoint e di risposta che mettono in evidenza gli avvisi di sicurezza pertinenti, indicativi di una tattica o di una tecnica comunemente utilizzata dai gruppi APT, potrebbero facilmente segnalare potenziali intrusi.

Inoltre, la mancanza di personale di sicurezza qualificato potrebbe essere affrontata rivolgendosi a team di rilevamento e risposta gestiti o come team specializzato per la ricerca di minacce su eventi sospetti. Questi servizi, che includono gli stack tecnologici necessari di tipo Endpoint Detection and Response (EDR), prendono il nome di Managed Detection and Response (MDR). Sia le soluzioni EDR che MDR sono diventate accessibili alle piccole e medie imprese, offrendo una sicurezza di tipo SOC che solo le grandi aziende possono normalmente

permettersi, ma a una frazione del costo e con il beneficio di una partnership efficiente e specializzata.

La cyber war è una minaccia per il 71% dei Ciso secondo Bitdefender

Uno studio di Bit defender, che ha coinvolto anche manager italiani, evidenzia la crescita di nuove minacce ransomware, problemi di comunicazione e mancanza di competenze.

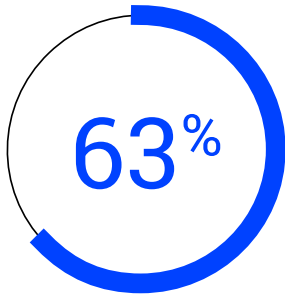
Una serie di problemi che vanno affrontati e che imporranno importanti cambiamenti nei prossimi mesi e anni.

Il 63% dei professionisti della sicurezza informatica a livello mondiale (47% in Italia) tra cui un 71% di Ciso nel mondo, ritiene che la guerra informatica sia una minaccia per la loro azienda, peraltro, solo il 22% degli esperti nel mondo e il 32% degli italiani) ammette di non avere una strategia in atto per mitigare questo rischio.

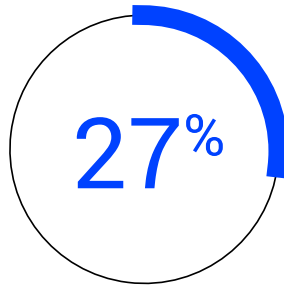
Ciò è allarmante in un periodo di sconvolgimento globale senza precedenti, affermano i manager di BitDefender poiché la metà dei professionisti della sicurezza informatica (dato globale 50% ma in Italia il) 53%) concorda sul fatto che l'inasprimento di una guerra informatica danneggerà l'economia nei prossimi 12 mesi.

I CISO e i professionisti della sicurezza informatica stanno comunque rafforzando le loro difese – come sostengono il nel 48% dei rispondenti a livello mondiale e del 43% in Italia.

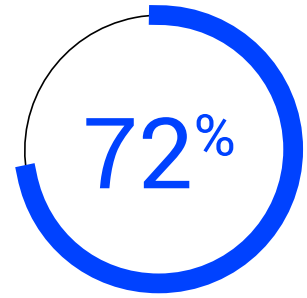
Questi e altri risultati sono raccolti nello studio internazionale "10 in 10" di Bitdefender. ❁



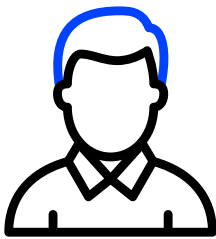
believe that the **state of cyberwarfare** is a threat to their organisation



of companies **don't have a strategy** to protect against cyberwarfare

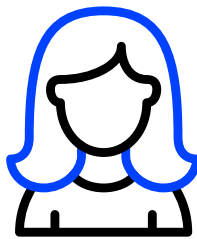


believe that there **is a need for a more diverse skill set** in cybersecurity



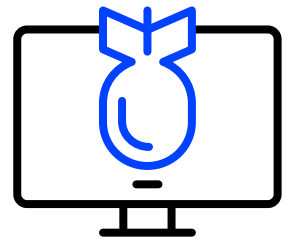
28%

CISOs and CIOs



22%

infosec professionals



50%

believe that the skills gap will be seriously disruptive



38%

Reputational damage



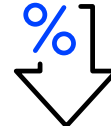
36%

Increased downtime and business continuity disruptions



35%

The personal impact on people (customers, staff, vendors)



33%

Loss of revenue



30%

Increased cost of cyber insurance



29%

Paying to have the ransomware deactivated



27%

Legal fines and penalties



0%

Other



3%

Don't know

VIDEO GIOCHI SOTTO LA MINACCIA DEI CYBER CRIMINALI

I dati di una ricerca Akamai e i suggerimenti degli esperti di Panda

di Gaetano Di Blasio

Tra le forme d'intrattenimento più in voga, i video giochi stanno prosperando, in un momento di restrizioni legate alla pandemia in corso.

Cresce pertanto una minaccia anche per le aziende, a causa dei tanti smart worker che, al termine del lavoro, dopo aver riposato gli occhi, possono rilassarsi e dedicarsi ai loro passatempi on line, fra cui campeggiano i videogiochi.

Stando a una ricerca commissionata da Akamai, già alla fine del 2019 gli account di gaming fruttavano ai cyber criminali oltre 12 miliardi di dollari, grazie ad attacchi basati sul credential stuffing.

I regimi di lockdown aumentano i rischi perché accrescono lo smartworking, che non sempre è supportato da politiche di sicurezza informatica adeguata. Chi usa dispositivi personali per lavorare dovrebbe essere equipaggiato e informato sui rischi a dovere. Gli attacchi di credential stuffing, approfittano di grandi database inseriti in reti botnet per accedere agli account senza il permesso dei loro possessori. In buona sostanza, molti utenti usano poche password per più servizi, anche per attività importanti e legate ad attività lavorative. Così facendo, tramite un processo automatizzato spesso è possibile arrivare illegalmente agli account, specialmente quelli legati alle carte di credito o ai conti correnti,

di ignari utenti.

Ci sono anche altre minacce rivolte ai gamer. Per esempio quelle che sfruttano l'interesse rendere unico un personaggio o un accessorio, più in generale per la customizzazione. Si può arrivare a spendere migliaia per rendere un personaggio più potente. Per esempio, sul sito 2G2 si permette di vendere e scambiare qualsiasi cosa relativa a un videogame, compresa, al costo di oltre 2mila euro, una gallina dalle uova d'oro da usare come se fosse un cavallo per spostarsi all'interno dell'ambientazione di World of Warcraft, uno degli MMORPG più famosi di tutti i tempi. Costumi, spade e altre personalizzazioni alimentano un mercato fiorente: calcolato in crescita, secondo la suddetta ricerca fino ad arrivare, entro il 2025, a 50 miliardi di euro.

Sia i dati personali contenuti negli account dei gamer, spesso associati alla carta di credito o PayPal del giocatore, sia gli oggetti e i personaggi ottenuti nell'ambito di uno o più giochi, sono ormai posti sullo stesso piano dai cybercriminali.

Come fanno gli hacker a violare gli account dei gamer

Gli esperti di Panda Security ci svelano le tecniche di attacco, partendo, innanzitutto, distinguendo

tra due grandi tipi di attacchi. Il primo attacco è il credential stuffing già descritto in precedenza, che sfrutta un database di credenziali rubate .

Il secondo tipo di attacchi, invece, sono quelli mirati, che, hanno come bersaglio un determinato giocatore che il criminale ha individuato all'interno del gioco (in questo caso la gran parte di questi cybercriminali è rappresentata da altri giocatori). L'attacco può prendere la forma di una truffa, per esempio facendo amicizia con l'avatar della vittima e consigliando un sito web dove acquistare crediti a prezzi stracciati, quindi con un attacco di tipo phishing :Il giocatore potrebbe, collegandosi al sito, involontariamente scaricare uno spyware che registrerà i suoi dati di accesso durante il login.

Come proteggere l'account di gioco

Sempre gli esperti di Panda Security ci forniscono dei consigli per ridurre al minimo i rischi e proteggere il proprio account di gioco online.



Il primo passaggio consiste nell'attivare una verifica a due fattori

Attivare la verifica in due fattori. Diversi account prevedono questo strumento di sicurezza che da solo è sufficiente per sventare la maggior parte dei furti di credenziali. Viene consigliato, in particolare, di impostare il secondo passaggio su un dispositivo diverso da quello su cui si effettua il login. Successivamente, va installato un antivirus, che ovviamente, gli esperti di Panda consigliano sia, Panda Dome, che nel "Real-World Protection Test" condotto da AV Comparatives ha raggiunto il 100% di rilevamento di virus e minacce, consente di continuare a giocare senza rinunciare alla qualità video e senza impegnare una quantità eccessiva di larghezza di banda, mentre ti protegge da eventuali minacce online.

Più in generale consigli importanti sono: creare password sicure, non utilizzare gli stessi dati di login per più account, non utilizzare la mail personale e la relativa password per accedere alle piattaforme di gioco. Consigliabile, per la gestione di molte password, un password manager come quello della stessa Panda Security . Inoltre è importante non condividere dati personali né accedere a link che millantano, di offerte incredibili e soprattutto non associare la carta di credito all'account. . altra prassi importante riguarda i minori Infine, se la passione per i videogiochi riguarda anche dei minori, gli esperti di Panda consigliano vivamente calorosamente di utilizzare il Parental control e iniziare un percorso di educazione all'uso sicuro di Internet e dei videogiochi. ❄

ZERO-TRUST: CHE COSA SIGNIFICA E A CHE COSA SERVE

Un articolo a opera di un esperto del settore: Di Marco R. A. Bozzetti di Malabo e presidente del Consiglio direttivo di AIPSI, associazione di professionisti della cyber security, capitolo Italiano della ISSA staunitense

di Marco R. A. Bozzetti

Su un numero crescente di di articoli e di pubblicazioni sulla sicurezza digitale sono usati i termini Zero Trust (ZT), Zero Trust Networks, Zero Trust Network Architecture (ZTNA), Zero Trust Security Model, etc. Ma che cosa significa "zero trust"? Significa "zero fiducia", ossia di non fidarsi della sicurezza digitale dei vari dispositivi e servizi, ad esempio in cloud, che costituiscono il sistema informatico di una azienda/ente.

Gli attuali sistemi informatici sono molto complessi ed eterogenei: distribuiti ed interconnessi via Internet, utilizzano servizi in cloud, sistemi e dispositivi mobili, sistemi OT ed IoT. In questa poliedricità di ambienti e di collegamenti via Internet, tutti questi devono essere considerati intrinsecamente insicuri, e la logica zero trust richiede in primo luogo il controllo dell'identità e dell'integrità dei dispositivi indipendentemente dalla loro posizione e dal loro ambito operativo. L'accesso ad applicazioni e servizi deve quindi basarsi sull'identità ed integrità dei

dispositivi e dell'autenticazione forte dell'utente.

La logica e l'approccio ZT vede sia varie proposte commerciali di prodotti e soluzioni sia, soprattutto, la specifica NIST (SP) 800-207, "Zero Trust Architecture" di agosto 2020 (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>) Lo standard NIST specifica che un approccio ZT si concentra principalmente sulla protezione dei dati e dei servizi, ma può e dovrebbe essere ampliato per includere tutte le risorse aziendali (dispositivi, componenti dell'infrastruttura, applicazioni, componenti virtuali e cloud) e soggetti (utenti finali, applicazioni e altre entità non umane che richiedono informazioni dalle risorse).

I modelli di sicurezza ZT presuppongono che ogni ambiente informatico è insicuro e inaffidabile, anche quello di proprietà aziendale che non deve essere ritenuto più affidabile e sicuro di qualsiasi ambiente non di proprietà, come ad esempio gli ambiti in cloud. In questo nuovo paradigma, un'impresa non deve assumere alcuna fiducia implicita e analizzare e valutare continuamente il rischi per le sue risorse e funzioni aziendali e quindi attuare protezioni per mitigare questi rischi. Nella logica ZT, queste protezioni comportano la riduzione al minimo necessario del diritto di accesso alle risorse (come dati e risorse di calcolo e applicazioni/servizi) ai soli soggetti e asset identificati che abbiano necessità di accesso, nonché un sistematico e sicuro controllo, con identificazione, autenticazione e autorizzazioni, per

le varie risorse ed utenti.

I principi di base della logica ZT sono indipendenti dal tipo di tecniche e misure di sicurezza usate, ed includono:

1. Tutte le fonti di dati e i servizi di elaborazione sono considerati risorse
2. Tutte le comunicazioni sono protette indipendentemente dalla loro posizione
3. L'accesso alle singole risorse aziendali viene concesso per sessione. La fiducia nel richiedente viene valutata prima che venga concesso l'accesso, e questo dovrebbe essere concesso con i privilegi minimi necessari per completare l'attività.
4. L'accesso alle risorse è determinato da una policy dinamica, che includa dinamicamente lo stato osservabile dell'identità del cliente, dell'applicazione/servizio e della risorsa richiedente, e che possa includere altri attributi comportamentali e ambientali.
5. L'azienda monitora e misura l'integrità e la sicurezza di tutti i beni di proprietà e associati. Nessuna risorsa è intrinsecamente affidabile.
6. Tutte le autorizzazioni e l'autenticazione delle risorse sono dinamiche e applicate rigorosamente

prima che l'accesso sia consentito.

7. Devono essere raccolte quante più informazioni possibili sullo stato attuale delle risorse, dell'infrastruttura di rete e delle comunicazioni, che devono essere utilizzate per migliorare il livello di sicurezza.

Una architettura zero trust (ZTA) è un'architettura di sicurezza informatica aziendale basata sui principi ZT sopra elencati, progettata per prevenire violazioni dei dati e limitare i movimenti laterali interni. Essa non è sostitutiva, ma complementare e da integrare con la preesistente architettura del sistema informatico e della sua sicurezza digitale, le cui misure e tecniche fanno riferimento a standard quali quello dell'architettura delle contromisure NIST schematizzata nella fig. 2.

Quindi ZT non deve essere considerata come una nuova singola architettura sostitutiva di altre, ma come un insieme di principi guida per implementare e gestire in maniera più sicura le operazioni ed i flussi di lavoro dei sistemi informatici, basandosi sulla classificazione delle informazioni, e quindi dei sistemi informatici a loro supporto.

La fig. 1 evidenzia i principali elementi logici di una

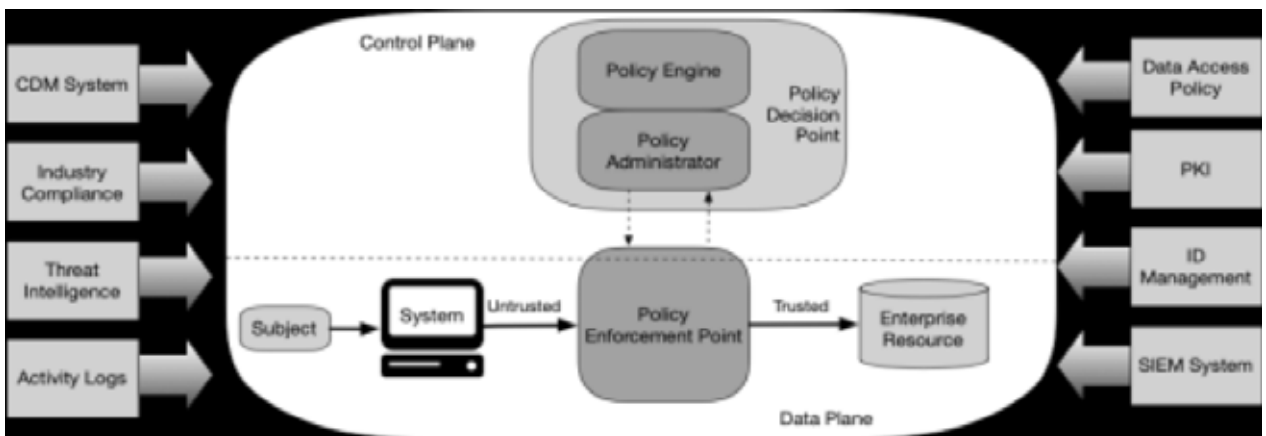


Fig. 1 Principali componenti ZT (CDM=Continuous Diagnostics and Mitigations, PKI=Public Key Infrastructure, SIEM= Security information and Event Management)

soluzione ZT, e schematizza il suo funzionamento. La fig. 1 mostra un nucleo centrale diviso su due piani: quello dei dati, Data Plane, e quello del controllo, Control Plane. Questo nucleo riceve un insieme di regole e di informazioni, derivanti e generate da normative, da policy, da sistemi informatici quali il CDM, il SIEM, la PKI, il gestore dei log di sistema e quello delle identità di utenti e risorse ICT (es. LDAP, Active Directory).

Il Policy Engine (PE) è responsabile della decisione finale per la concessione dell'accesso a una risorsa per un determinato soggetto. Il PE utilizza la politica aziendale e le informazioni da fonti esterne, ad esempio dai sistemi CDM ai servizi di intelligence sulle minacce, come input per un algoritmo (trust algorithm) per concedere, negare o revocare l'accesso alla risorsa. Il PE è abbinato al componente dell'amministratore della policy, il Policy Administrator (PA), che esegue quanto deciso dal PE. PA è responsabile della creazione o dell'interruzione della comunicazione tra un soggetto e una risorsa (tramite comandi ai PEP pertinenti). Genererebbe qualsiasi autenticazione specifica della sessione ed i token di autenticazione o credenziali utilizzati da un client per accedere a una risorsa aziendale. PA è strettamente legata al PE e si basa sulla sua decisione di consentire o negare alla fine una sessione. Se la sessione è autorizzata e la richiesta autenticata, la PA configura il PEP per consentire l'avvio della sessione. Se la sessione viene negata (o una precedente approvazione è revocata), la PA segnala

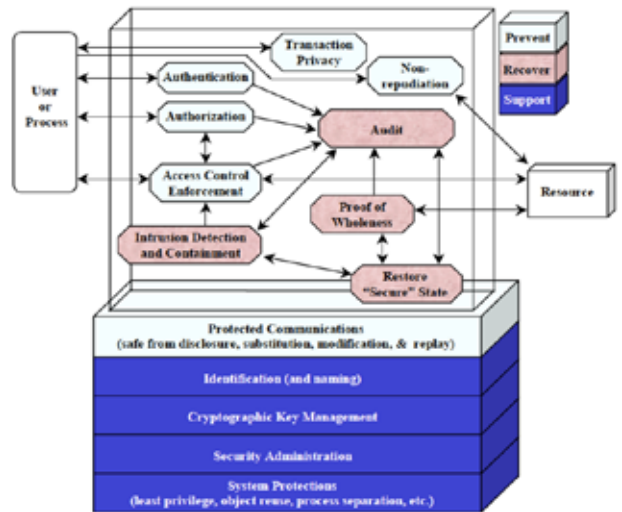


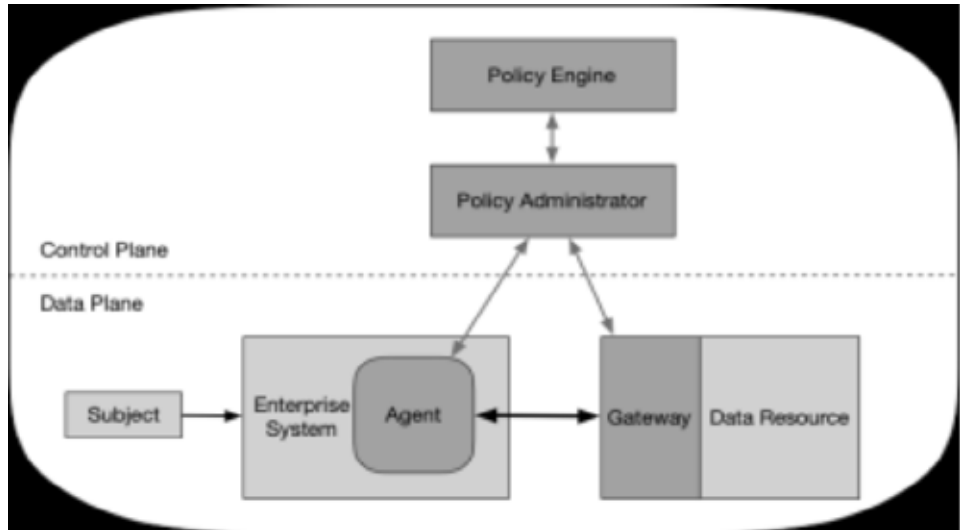
Fig. 2 Architettura NIST delle contromisure per la sicurezza digitale (NIST SP 800-30)

al PEP di interrompere la connessione. Il PEP, Policy Enforcement Point, è l'elemento per l'abilitazione, il monitoraggio e la terminazione delle connessioni tra un soggetto e una risorsa. Il PEP comunica con la PA per inoltrare richieste e / o ricevere aggiornamenti delle policy. Oltre il PEP si crea la zona sicura (di fiducia) che ospita la risorsa richiesta.

L'implementazione di una logica ZT può essere attuata in diversi modi, tenendo conto anche della realtà esistente del sistema informatico dell'azienda/ente, in primo luogo dalle policy e dai sistemi di controllo e monitoraggio in uso: ma dovrebbero essere sempre assicurati i 7 principi fondamentali in precedenza elencati. Il documento NIST elenca, ad esempio, implementazioni basate su Enhanced Identity Governance, su Micro-Segmentation protette da gateway intelligenti, su Network Infrastructure and Software Defined Perimeters.

La fig. 3 mostra l'esempio implementativo di ZT basato sull'interazione agent-gateway. In questo tipico, un soggetto con un laptop fornito dall'azienda desidera connettersi ad una applicazione

Fig. 3 Modello implementativo ZT Agente/Gateway



del sistema informatico dell'azienda. La richiesta di accesso viene presa dall'agente locale e la richiesta viene inoltrata all'amministratore dei criteri. L'amministratore e il motore dei criteri potrebbero essere una risorsa locale dell'organizzazione o un servizio ospitato in cloud. L'amministratore dei criteri inoltra la richiesta al motore dei criteri per la valutazione. Se la richiesta è autorizzata, l'amministratore della politica configura un canale di comunicazione tra l'agente del dispositivo e il gateway di risorse pertinente tramite il piano di controllo. Ciò può includere informazioni quali un indirizzo IP, informazioni sulla porta, la chiave di sessione, etc. L'agente del dispositivo e il gateway si connettono

e iniziano i flussi di dati crittografati. La connessione tra l'agente del dispositivo e il gateway delle risorse viene interrotta quando il flusso di lavoro viene completato o quando viene attivato dall'amministratore dei criteri a causa di un evento di sicurezza (ad esempio una mancata autenticazione o un time-out della sessione).

La fig. 4 schematizza il ciclo di vita della realizzazione di una logica ZT, associato ai vari step del RMF, Risk Management Framework (si veda in particolare SP800-37 [1]). La figura evidenzia l'importanza e la

basilare necessità di disporre dell'aggiornato inventario di utenti, risorse, processi, cui deve seguire l'analisi dei rischi e la definizione delle varie policy.*

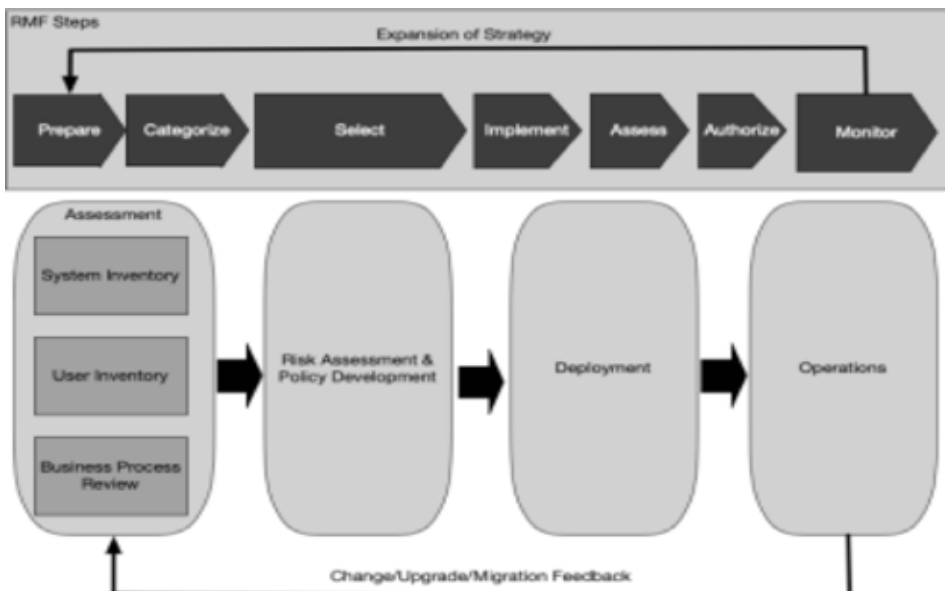


Fig. 4 Il ciclo di vita di realizzazione di una ZTA

STOP ALLE VULNERABILITÀ APPLICATIVE CON MICRO FOCUS FORTIFY

La protezione stratificata di Micro Focus Fortify protegge le applicazioni durante il loro ciclo di vita combinando test applicativi statici e dinamici

di Riccardo Florio

Micro Focus Fortify è la famiglia di soluzioni per la sicurezza delle applicazioni che combina la flessibilità di test in locale e on-demand. Punto di forza delle soluzioni Micro Focus Fortify è la capacità di fornire una visibilità completa della situazione di rischio applicativo combinando test di sicurezza delle applicazioni di tipo statico (Static Application Security Testing o SAST), dinamico (Dynamic Application Security Testing o DAST), autoprotezione delle applicazioni runtime (RASP) e test di sicurezza delle applicazioni mobili (Mobile Application Security Testing o MAST). Gli strumenti di analisi statica forniscono un feedback completo nelle prime fasi del ciclo di vita dello sviluppo del software, mentre gli strumenti di analisi dinamica consentono ai team di sicurezza di individuare immediatamente le vulnerabilità sfruttabili negli ambienti di produzione o di pre-produzione. Eseguire test con entrambi le modalità è il modo per ottenere la visione più completa del rischio e porre rimedio in modo preventivo a possibili attacchi. Analizziamo più in dettaglio le ragioni per cui questo approccio risulta vantaggioso.

Difesa a più livelli

L'analisi statica fornisce una copertura eccellente, ma non può essere eseguita in ambienti di produzione in cui le configurazioni e le opzioni di distribuzione possono avere un impatto enorme sulla situazione generale del rischio delle applicazioni. L'analisi dinamica è quella che consente di identificare i problemi in un successivo stadio del ciclo di vita applicativo, quello della produzione in cui i rischi diventano più consistenti.

Nelle attuali logiche di mercato, caratterizzate da cicli di sviluppo del software applicativo più brevi ma con rilasci molto frequenti, di nuove release, i test dinamici possono efficacemente identificare le vulnerabilità legate a flussi di lavoro affrettati e a errori dello sviluppatore o di implementazione.

Sfruttando l'analisi statica per identificare le vulnerabilità nelle prime fasi dello sviluppo e l'analisi dinamica per identificare le vulnerabilità che si presentano in produzione, i team di sicurezza possono dunque implementare un approccio a più livelli che fornisce maggiore sicurezza, in cui il DAST funge da rete di sicurezza per le vulnerabilità non identificati dal SAST.

“La capacità di coniugare test applicativi statici, dinamici e di simulare i principali attacchi per ambienti mobile, unitamente alla flessibilità di scegliere un'implementazione locale oppure on-demand, è ciò che rende Fortify una soluzione unica sul mercato - spiega Pierpaolo Alì, Director CyberSecurity Southern Europe di Micro Focus -. Nessun'altra soluzione permette di fornire un livello di protezione così completo e flessibile

delle applicazioni, che sono sempre più spesso l'anello debole nella catena della sicurezza aziendale.”

I vantaggi di una tassonomia unificata

Specialmente con la diffusione delle metodologie DevOps, la sicurezza delle applicazioni è un tema che coinvolge un team di persone ed è, quindi, importante che gli strumenti utilizzati nelle varie fasi dello sviluppo forniscano dettagli coerenti sulle vulnerabilità.

Disporre di una tassonomia unificata per i diversi metodi di test è ciò che consente una visione completa sullo stato di vulnerabilità.

Di fatto, i test statici e dinamici della sicurezza delle applicazioni sono tecnologie complementari nella loro capacità di identificare le vulnerabilità nell'intero ciclo di vita di sviluppo del software, dalla scrittura, al controllo qualità, alla produzione. Quando questi due metodi di test sono riuniti in una tassonomia comune, si potenziano a vicenda per fornire una soluzione completa.

Sfruttando una tassonomia unificata tra test statici, dinamici e runtime, la soluzione Fortify può rilevare un punto debole nel codice sorgente con Fortify Static Code Analyzer (SCA) per poi analizzare le ricadute in ambienti di produzione (dove il punto debole può diventare una vulnerabilità vera e propria) tramite l'analisi dinamica di Fortify WebInspect.

Inoltre, le tecnologie di test statico e dinamico Fortify, sostenute da una tassonomia comune delle vulnerabilità, forniscono ai team di sviluppo suggerimenti e mappature di sicurezza comuni e condivisi, favorendo la collaborazione per la risoluzione dei problemi.

Definire le priorità

Le vulnerabilità non sono tutte uguali e, peraltro, non è realistico pensare di correggere tutti i potenziali

problemi. Gli odierni professionisti della sicurezza delle applicazioni devono, pertanto, prendere decisioni difficili e definire livelli di priorità di intervento per decidere quali problemi risolvere e quali differire.

La sovrapposizione dell'analisi dinamica e di quella statica, fornisce una metrica di rischio per scegliere quali problemi debbano essere corretti per primi. Ne consegue un approccio generale alla sicurezza migliorato, che consente agli sviluppatori di utilizzare il loro tempo in modo più efficiente concentrandosi prima sui risultati più importanti.

Gestione unificata delle vulnerabilità

I team di sicurezza e sviluppo sono sommersi da avvisi di sicurezza e devono considerare un'ampia gamma di fattori nell'identificazione e riduzione dei rischi. Gli strumenti Micro Focus Fortify forniscono una piattaforma di gestione unificata delle vulnerabilità per analizzare facilmente i risultati.

Disporre di una piattaforma unificata di gestione delle vulnerabilità della sicurezza delle applicazioni non è solo fondamentale per semplificare i flussi di lavoro di assegnazione delle priorità, ma anche per mettere a punto modelli di lavoro più efficienti e sicuri.

Per esempio, se un'analisi statica evidenzia una vulnerabilità è di fondamentale importanza creare cicli di feedback in grado di identificare quando tale problematica si presenta negli ambienti di produzione tramite un'analisi dinamica. Solo così è possibile mettere a punto le proprie metodologie di formazione e sviluppo per affrontare i problemi sistemici. ❁



Pierpaolo Ali, Director CyberSecurity Southern Europe di Micro Focus

PROTEZIONE RUNTIME CON LA CONTAINER SECURITY DI QUALYS

La nuova soluzione assicura elevata visibilità e protezione delle applicazioni in esecuzione negli ambienti basati sui container, anche in modalità as-a-service

di Giuseppe Saccardi

Qualys, pioniera e fornitore di soluzioni IT di sicurezza e compliance basate sul cloud, ha presentato Container Runtime Security, una funzionalità che è volta ad assicurare capacità di difesa a livello di esecuzione per le applicazioni containerizzate.

L'approccio utilizza una piccola porzione di codice Qualys nell'immagine del Container, consentendo di controllarne lo stato e bloccarne comportamenti non desiderati.

La funzionalità elimina la necessità di ricorrere a container privilegiati che sono complessi da gestire e non possono funzionare in ambienti as-a-service.

La soluzione, una volta attivata, spiega Quali, funziona in qualunque ambiente senza richiedere ulteriori elementi. Questo consente di indirizzare in tempo reale casi tipici della Container security quali, ad esempio, il controllo degli accessi ai file, micro segmentazioni di rete, mitigazioni delle vulnerabilità e degli exploit e virtual patching.

La soluzione permette di:

- Verificare il comportamento dei container in esecuzione, potendo decidere cosa controllare e bloccare, per esempio, in relazione all'accesso ai file, le comunicazioni di rete e i comportamenti dei singoli processi.
- Creare policy granulari e personalizzate, oppure utilizzare la library integrata piuttosto che impostare una policy sulla base dei comportamenti osservati dal sistema
- Equipaggiare le immagini dei container nella pipeline di sviluppo CI/CD con un approccio "follow the image" che abilita una sicurezza



Philippe Courtot, CEO di Qualys



standardizzata e garantita dei container in esecuzione in ogni ambiente (Docker, Kubernetes, AWS EKS/ECS, Azure AKS, Google GKE), inclusi quelli privi di server come Azure Container Instances, AWS Fargate e Google CloudRun.

“Le funzioni di rilevamento e risposta in una singola applicazione attraverso la pipeline di sviluppo dei container è la chiave per rendere sicure le applicazioni containerizzate, in quanto questa stessa pipeline ad alta velocità può essere sfruttata da malintenzionati durante l’esecuzione”, sostiene Philippe Courtot, Chairman and CEO di Qualys. “Pertanto, dobbiamo aumentare la sicurezza nei carichi di lavoro in cloud ed estendere la protezione ai container in funzione”. Qualys estende le capacità

di difesa nella nostra soluzione Container Security con l’aggiunta di funzioni di rilevamento del comportamento e di risposta guidate da policy-driven per proteggere i container in funzione negli ambienti on-premise, nei public cloud o nei container cloud public as-a-service”.

Realizzata sulla piattaforma Qualys Cloud Platform, ha spiegato la società, Qualys Container Security scopre, traccia e protegge i container dalle fasi di sviluppo al runtime. Container Security effettua continue segnalazioni e risponde ai problemi di sicurezza e conformità nei container in tutto l’ambiente IT ibrido.

L’implementazione della runtime protection estende queste capacità e provvede ad avere una granulare visibilità durante un’esecuzione del container permettendo di controllare e monitorare l’esecuzione secondo diverse regole. In pratica, è possibile riconoscere una deviazione dal comportamento atteso che potenzialmente crea un rischio di sicurezza a causa di una vulnerabilità o di errate configurazioni. ❁



LE BEST PRACTICE PER LA CYBER SECURITY

Paolo Lossa, Country Sales Manager di CyberArk Italia, suggerisce i cinque punti critici della cyber security nell'era del Covid-19 e dello smart working

di Giuseppe Saccardi

Si si sta avviando alla fine del 2020, un anno di certo difficile per le aziende, che hanno dovuto ricorrere allo smart working e così facendo a dover rispondere ai problemi intrinseci nel lavoro da remoto, soprattutto nel caso di utenti privilegiati i cui dati sono tra i più ambiti dai criminali cibernetici.

La crisi sanitaria, evidenzia Paolo Lossa, Country Sales Manager di CyberArk Italia (cyberark.com), ha influenzato e influenzerà in modo significativo la nostra vita quotidiana e ci ha spinti a un utilizzo sempre più intenso delle tecnologie. È una combinazione di fattori che ha stimolato la creatività dei cyber criminali che hanno sviluppato nuove tecniche di attacco volte a catturare i nostri dati sensibili, la cui vendita sul dark web è molto redditizia.

Cosa suggerisce Lossa a tal proposito? Innanzitutto che gli utenti devono conoscere i rischi informatici in cui potrebbero incorrere al fine di adottare l'approccio più appropriato per proteggere se stessi e i propri dispositivi. Molti aspetti della nostra vita quotidiana possono infatti diventare un punto di accesso per i cyber criminali, ma non tutti ne sono consapevoli.

Cinque i consigli suggeriti da Lossa per incrementare il livello di protezione. Vediamoli in sintesi:

- 1. Non fidarsi degli estranei:** non bisognerebbe mai aprire messaggi o cliccare su link ricevuti da persone che non si conoscono, che si tratti di e-mail, messaggi su Slack, Teams o Google Chat.
- 2. Monitorare la salute va bene, farsi rubare i dati, no:** Fitness tracker e orologi "intelligenti" sono un modo semplice per tenere sotto controllo la propria forma fisica, purtroppo però raccolgono molti dati personali. Chi li utilizza deve quindi assicurarsi di sapere esattamente come vengono utilizzati, archiviati e protetti i dati personali dalle differenti aziende.
- 3. Non raccontare troppo sui social network:** Se questi canali permettono di condividere le passioni e i bei momenti con le persone care, bisogna fare attenzione a non condividere informazioni personali che potrebbero essere utilizzate per determinare password e domande di sicurezza, indicare un luogo o prevedere il comportamento.
- 4. Proteggere lo smartphone.** I cellulari hanno assunto il ruolo di assistente personale, sia in ambito privato che professionale, ma sono vulnerabili agli attacchi. Pertanto, è importante verificare a quali dati ogni applicazione ha accesso. Inoltre, processi di autenticazione come l'autenticazione a più fattori aiutano a garantire che gli smartphone non vengano sfruttati dagli aggressori per rubare dati personali.

5. Proteggere l'Internet of Things. Nei prossimi dieci anni, ogni consumatore avrà almeno 10 dispositivi collegati e, se non sono sicuri, ognuno di essi rappresenterà un modo per rubare dati sensibili. I dispositivi IoT, come le smart TV e i contatori collegati, sono sicuramente utili, ma richiedono molte informazioni e connessioni per funzionare correttamente. Per metterli in sicurezza e chiudere tutti gli accessi alla rete, è necessario fidarsi solo di produttori rinomati, applicare ogni patch di sicurezza disponibile e aggiornare le loro password di default.

«La tecnologia sta entrando sempre più nelle nostre abitudini e gran parte delle nostre attività nel tempo libero, acquisti o operazioni amministrative ora includono la navigazione online. Pertanto, la protezione dei nostri dati personali e la prova della nostra identità saranno al centro di tutto ciò che facciamo fino al 2030. E, chissà, forse il nostro frigorifero connesso saprà più cose su di noi di noi stessi», mette in guardia Lossa.

La criticità di ambienti SaaS

Le criticità per gli utenti e soprattutto gli utenti privilegiati, sono enfatizzate anche dal fatto che gli attacchi e i rischi continuano a crescere anche in ambienti SaaS considerati sicuri. È con questo dato di fatto che CyberArk ha esaminato la tecnica di intrusione preferita dagli aggressori: il phishing.

Si prendano, per esempio, gli attacchi di phishing di Office 365. Negli ultimi mesi si è osservato che questo approccio mira a token temporanei (aka access token) generati per

consentire il Single Sign-On per Microsoft 365 e tutte le applicazioni Microsoft.

Rubando e utilizzando questi token temporanei, gli aggressori possono bypassare l'autenticazione multifattore (MFA) e persistere in rete "legittimamente" aggiornando il token. Inoltre, anche se un utente cambia la propria password, il token rimane valido e non può essere revocato.

Le applicazioni video e chat - come Microsoft Teams, Slack, WebEx, Zoom e Google Hangouts - sono diventate il nuovo volto dell'organizzazione in questo periodo di lavoro a distanza.

All'interno di queste applicazioni SaaS, si possono rubare le credenziali e compromettere le identità digitali dei dipendenti, in particolare di utenti privilegiati, accedere ai dati sensibili inclusi in questi strumenti di collaborazione, report giornalieri e dati finanziari. A queste problematiche CyberArk ha risposto rendendo disponibili le proprie soluzioni di security tramite Cloud dal Marketplace Microsoft Azure. In pratica, i clienti Microsoft Azure hanno accesso alla soluzione di protezione degli accessi privilegiati di CyberArk e possono fruirne per definire le strategie aziendali

«La soluzione CyberArk Privileged Access Security, offre un approccio esaustivo alla sicurezza e all'efficienza operativa nel cloud attraverso il rilevamento continuo e la protezione degli account privilegiati; funzionalità just-in-time per un accesso flessibile ai sistemi Windows sia in cloud che on-premise, un rilevamento e risposta alle minacce in grado di prioritizzare gli avvisi in base a comportamenti potenzialmente rischiosi, nonché la possibilità di prendere il controllo rapidamente degli account pericolosi», ha spiegato Lossa. ❄



Paolo Lossa, Country Sales Manager di CyberArk Italia

COME COLLABORARE DA REMOTO IN MODO SICURO

Lo smart working è uno dei punti chiave per affrontare la pandemia in corso, ma serve la garanzia di farlo in modo sicuro. Il come lo suggerisce CIE Telematica

di Giuseppe Saccardi

Nello scenario aziendale che si prospetta appare saliente il tema del come lavorare in team quando i partecipanti sono distribuiti su più sedi o in mobilità o presso la propria abitazione, e quali strumenti lo rendono possibile in modo sicuro.

Risolvere il problema dei dispositivi può infatti non essere sufficiente perché entrano in gioco anche altri fattori. Quella degli strumenti adatti, evidenzia Luigi Meregalli, general manager della società di ingegneria CIE Telematica (cietelematica.it), è di certo una condizione sine qua non per procedere, ma puntare solo su quello non basta. Assieme a un buon dispositivo serve anche quanto permette ai sistemi di collaborazione distribuiti di essere sempre operativi, ed esserlo in modo garantito, ed esenti da attacchi da parte di cyber criminali.

Se enunciare un principio è facile, i problemi con cui si scontrano i responsabili IT nel passare alla pratica sono consistenti. In primis c'è il fatto che sovente si dispone di personale di supporto limitato o non ancora formato sugli strumenti utilizzati, e poi la gamma di aspetti che devono essere considerati a corollario,

come il garantire la sicurezza remota, l'aggiornamento dei software, la manutenzione, la gestione, la garanzia del funzionamento e cos' via.

Apparati che smettono di funzionare nel mezzo di una conferenza, o una qualità della connessione insufficiente, o il mancato aggiornamento della sicurezza, sono aspetti che possono far perdere i benefici di un'evoluzione che ha permesso di affrontare l'attuale momento di criticità e lasciato intravedere un nuovo modo di lavorare e cooperare.

In pratica, si rischia di far seguire a una fase di entusiasmo una fase di disillusione. Inevitabile o quasi che a quel punto scatti la ricerca del colpevole, che inevitabilmente tende sempre ad essere considerato il responsabile IT, al quale sino a poco prima si negavano le risorse necessarie.

Per superare questi problemi e il fatto che si è spesso restii ad affidarsi ai suggerimenti di un produttore per il timore di incorrere in un lock-in tecnologico, CIE Telematica ha sviluppato una proposta risultante da una analisi terza del mercato che si è concretizzata in un portfolio di prodotti e servizi che ritiene adeguati a rispondere alle sfide che si prospettano.

Cooperazione flessibile e nel cloud

Cominciando dallo smart working e dalla collaborazione, grazie ad un'accordo con Lenovo, che a sua volta ha in corso una partnership con Microsoft, si è identificato uno strumento adatto per l'ambito aziendale in Microsoft Teams, una piattaforma che

permette di cooperare tramite chat, video meeting, file storage, abilita l'integrazione di applicazioni e che è disponibile in 26 lingue.

Aspetto saliente, osserva Meregalli, è che oltre a connettere in modo efficace gli utilizzatori in diverse modalità è una soluzione integrata anche con Microsoft Office 365 ed è integrato con app e servizi usati quotidianamente quali Word, Excel, PowerPoint, OneNote, SharePoint, Stream e PowerBI.

Semplificato, ha aggiunto Meregalli, è motivo della sua scelta, è anche l'editing simultaneo e in tempo reale con altri utenti di documenti, cosa che permette di evitare invii e reinvi di successive versioni via mail per la loro messa a punto.

La rilevanza dei servizi di security

Un secondo aspetto a cui porre attenzione è quello della garanzia di funzionamento e di sicurezza della soluzione adottata.

Le criticità derivano da diversi aspetti quali il dispositivo usato dagli utenti finali (aziendale o personale), i rischi connessi ai sistemi operativi dei dispositivi mobili, il malware e il phishing che hanno come obiettivo i social media e il rischio intrinseco all'utilizzo di software di terze parti.

La soluzione che CIE Telematica ha identificato e suggerisce nell'ambito delle proprie attività di società di ingegneria e in qualità di silver partner di Lenovo, è ThinkShield, uno strumento sviluppato da quest'ultima e che è utilizzabile per proteggere dati, i dispositivi, la identità e le attività on-line.

I servizi di protezione estesa di ThinkShield derivano dalla

considerazione che un'azienda non può permettersi di subire violazioni della protezione.

ThinkShield rappresenta sotto questo punto di vista una piattaforma di protezione personalizzabile che ha l'obiettivo di proteggere un'azienda nel suo complesso, dai dispositivi ai dati alle connessioni di rete, e dai criminali informatici sempre più agguerriti, anticipandone le mosse e bloccandone in modo preventivo e dinamico gli attacchi.

«Abbiamo verificato sul campo che Thinkshield è uno strumento estremamente efficace per la data security e la protezione dei dati, sia per quanto concerne l'utilizzo che viene fatto di un pc che nelle modalità di accesso ad Internet, con in aggiunta la possibilità di riconoscere reti wifi affidabili a cui connettersi, e dotata di funzioni di autenticazione a più fattori ed encryption», ha evidenziato Meregalli.

Ideato per il supporto e la gestione del personale che lavora da remoto è anche il servizio Premier Support, sottoscrivibile anche per un solo anno, che prevede l'accesso all'help-desk per i prodotti della famiglia Think di Lenovo. Unico requisito è che il dispositivo deve essere coperto dalla garanzia Onsite. Tra quello che prevede vi è anche il supporto hardware e software, un singolo punto di contatto e la reportistica standard sui livelli di servizio.

«CIE, come solution provider, è poi in grado di fornire assistenza nello sviluppo di soluzioni più complesse, non limitandosi solo ai prodotti Lenovo ma aggiungendo altre tecnologie utili a promuovere lo smart working, quali threat prevention su qualsiasi dispositivo (pc, smartphone e cloud), ottimizzazione della banda con soluzioni SD-WAN e strumenti di collaboration software e hardware», ha evidenziato Meregalli. ❁



*Luigi Meregalli,
general manager di CIE
Telematica*

LA ENTERPRISE MOBILITY NELLA RIPARTENZA AL TEMPO DEL COVID-19

Per garantire uno smart working efficace le aziende devono mutare l'approccio nella gestione e protezione dei dispositivi mobili. I suggerimenti di MobileIron

di Giuseppe Saccardi

Sono passati oltre sei mesi da quando è iniziato il lockdown a seguito del Covid-19 e oggi le aziende stanno cercando di riorganizzare le attività e i processi interni. In questo processo che ruolo avrà l'Enterprise Mobility?

Le aziende hanno reagito chiedendo ai dipendenti di lavorare da casa su dati e apparecchiature aziendali con tempistiche molto strette. Devono però rivedere le strategie per la sicurezza e individuare se e quali protocolli siano stati violati.

In più le aziende, osserva Riccardo Canetta, Regional Sales Director Mediterranean Area di MobileIron (www.mobileiron.com), a cui abbiamo chiesto quali ritiene siano i punti critici e come farvi fronte, devono rispondere a domande come: quali apparecchiature aziendali sono state utilizzate a domicilio e da chi? Quali dati contenevano? Dove si trovano adesso? Quali dipendenti utilizzano i propri dispositivi e quali sono le loro vulnerabilità?

Una forza lavoro più distribuita avrà bisogno di dispositivi ma l'introduzione di nuovi device non gestiti di varia provenienza comporta sfide inedite per l'IT. Un esempio

è lo Shadow IT, un problema serio che lo diventa ancor più con le nuove condizioni lavorative.

Le aziende devono in pratica fornire supporto ai dipendenti per i dispositivi che non controllano direttamente, ma in che modo possono farlo?

Cambiare la gestione IT per migliorare la sicurezza

«La gestione IT deve essere rivoluzionata. Molte tecniche e tecnologie perfezionate dalle aziende negli ultimi 30 anni non saranno più così efficaci. Probabilmente il sistema di prevenzione delle intrusioni non sarà eliminato del tutto ma non sarà più in grado di proteggere le risorse fondamentali o addirittura la maggior parte di esse», sottolinea Canetta.

In sostanza, l'IT dovrà ridefinire le esigenze di mobilità degli utenti. Ciò significa che dovrà conoscere molto bene il settore delle app e offrire soluzioni approvate che permettano di accedere facilmente ai servizi cloud. Inoltre, mettendo a disposizione uno spazio aziendale approvato i team IT saranno in grado di proteggere i dipendenti e i loro dispositivi, sia personali che aziendali. «I dispositivi mobile in dotazione ai dipendenti, sia in azienda che a casa, sono già predisposti per rendere questa esperienza ancora più semplice. In molte aziende, l'hardware dei dispositivi consentirà di eliminare password complesse che creavano problemi e rischi per la sicurezza. L'autenticazione mediante tecnologia biometrica integrata li trasformerà in una sorta di ID. I dispositivi mobile utilizzati dai dipendenti diventeranno

quindi il principale strumento di autenticazione», evidenzia Canetta.

Preservare la sicurezza e garantire le prestazioni con il cloud

«In MobileIron, abbiamo vissuto il cambiamento in prima persona perché i nostri clienti si sono rivolti a noi per richiedere assistenza su come accedere alle loro applicazioni e ai loro dati in modo sicuro.

Dunque, qual è stato l'effetto del lockdown sulla mobilità aziendale e quali i problemi che vanno affrontati?» osserva Canetta.

Un primo problema che MobileIron ha rilevato è che circa uno su tre dei propri clienti ha chiesto alle persone di accedere alle risorse aziendali dai loro dispositivi personali. Ciò ha però creato problemi di sicurezza perché i dati aziendali e personali tendono a "mischiarsi". Inoltre, le aziende non potevano avere alcun controllo sui dispositivi personali.

«Il nostro software le ha aiutate a risolvere questo problema delimitando aree sicure riservate al lavoro e controllate dall'azienda sui dispositivi mobili dei dipendenti e preservando la privacy personale di questi ultimi e la sicurezza del datore di lavoro», ha spiegato Canetta.

Una volta online, MobileIron ha rilevato che gli attacchi di phishing e di malware connessi al Covid-19 sono aumentati, una criticità che interessa soprattutto gli utenti di device che leggono le e-mail aziendali da questi strumenti con schermi relativamente piccoli.

«Per contenere i rischi abbiamo offerto ai nostri clienti funzionalità di sicurezza per dispositivi mobile che monitorano le attività sospette a livello, rete e applicazione. Inoltre, la nostra tecnologia anti-phishing è stata rinnovata per rilevare e porre rimedio ad attacchi



Riccardo Canetta, Regional Sales Director Mediterranean Area di MobileIron

di phishing su tutti i canali pericolosi, tra i quali: messaggi di testo e SMS, messaggi istantanei, social media e altre modalità di comunicazione diverse dalle semplici e-mail aziendali», ha spiegato Canetta.

Le aziende hanno anche dovuto affrontare un altro problema: i colli di bottiglia nella rete e nelle VPN, che sono di norma configurate in modo

da gestire un numero medio di collegamenti.

Le aziende che avevano già migrato le loro applicazioni e i loro dati nel cloud sono state in grado di far fronte all'aumento della domanda della rete in modo più efficiente e si sono adattate con facilità al grande flusso di nuovi lavoratori remoti.

«Le abbiamo aiutate mettendo loro a disposizione il nostro software per collegare in sicurezza i loro dispositivi mobile direttamente al cloud dalle loro posizioni remote senza dover instradare il traffico attraverso le loro reti aziendali. Ciò ha ridotto la pressione sui loro sistemi aziendali», ha spiegato il manager.

In questo mutamento però anche le modalità di accesso devono cambiare. Le password erano già obsolete ma in un mondo che deve convivere con un nuovo coronavirus gli utenti che lavorano da remoto avranno sempre meno voglia di digitare password su una tastiera.

«Occorrono meccanismi di accesso più efficaci che adottino soluzioni più pratiche come i dati biometrici basati sul telefono, l'autenticazione multifattore e gli accessi in base al contesto per semplificare il lavoro da remoto con i dispositivi mobile. Al momento solo il 10% circa delle aziende lo sta facendo. Riteniamo che il restante 90% inizierà a farlo presto. Una cosa è però certa: il posto di lavoro non sarà più lo stesso», ha considerato Canetta. ❁

WORKSTATION PIÙ SICURE CON STORMSHIELD END POINT

Stormshield Endpoint Security Evolution è una soluzione per la protezione delle workstation Windows dalle minacce informatiche, anche nel cloud e in mobilità

di Giuseppe Saccardi

In un mondo in cui la mobilità è diventata la norma e la tecnologia digitale permea ormai ogni settore aziendale, è sempre più importante garantire la costante protezione delle workstation, indipendentemente dal contesto in cui vengono utilizzate.

È però un obiettivo, osserva Stormshield, che comporta l'adozione di un nuovo approccio volto ad affrontare i tentativi dei cybercriminali di aggirare le soluzioni di sicurezza in essere, sfruttandone direttamente le eventuali falle.

È quello che si è proposta di ottenere con Stormshield Endpoint Security (SES) Evolution per la messa in sicurezza delle postazioni di lavoro Windows combinando la protezione adattiva comportamentale e la tecnologia di analisi dei dispositivi fornita da SES con la capacità di identificare e investigare sull'origine degli attacchi.

“La nuova generazione di attacchi avanzati – ad esempio, quelli che sfruttano le vulnerabilità zero-day – evidenzia l'incapacità della maggior parte delle soluzioni esistenti di adattarsi al contesto per

fornire una protezione efficace delle workstation. La nostra soluzione Stormshield Endpoint Security Evolution fornisce una risposta pragmatica e all'avanguardia per combattere attacchi noti e non noti, contribuendo ad una maggior comprensione dei team di sicurezza delle minacce che prendono di mira le loro organizzazioni”, ha osservato in proposito Adrien Brochet, Product Manager di Stormshield Endpoint Security.

Considerazione di base è che quando si è in movimento, la connettività non è sempre scontata. A differenza di soluzioni che utilizzano motori di analisi ospitati su server, i cui tempi di risposta possono essere troppo lunghi in presenza di un attacco o che non sono utilizzabili se il computer è offline o al di fuori della rete aziendale, Stormshield Endpoint Security Evolution si propone di fornire una difesa permanente, che il computer sia connesso o meno. Inoltre, in alcuni ambienti sensibili, l'uso di soluzioni di sicurezza basate sul cloud può presentare rischi per la protezione dei dati. È a queste situazioni che vuole permettere di far fronte Stormshield Endpoint Security Evolution.

L'obiettivo, spiega l'azienda, è perseguito combinando le funzioni di protezione delle workstation e di rilevamento.

In pratica, Stormshield Endpoint Security Evolution blocca in modo proattivo il malware, gli attacchi alla memoria e gli exploit.

La soluzione fornisce inoltre agli amministratori



informazioni che consentono di comprendere meglio come si è verificato l'attacco al fine di risalire alle sue origini

Protezione sensibile al contesto

L'approccio Zero Trust richiede che le workstation vengano tutelate in maniera diversificata a seconda del contesto d'impiego specifico (ubicazione all'interno o all'esterno della rete aziendale, utente registrato sul dispositivo, ecc.).

Stormshield Endpoint Security Evolution protegge da questo punto di vista i computer sia all'interno dell'azienda sia in un contesto di impiego mobile.

In particolare, l'agente di SES Evolution modifica dinamicamente le proprie politiche di sicurezza adattandosi al proprio ambiente, in modo da dare

un accesso più granulare alle applicazioni e alle risorse dell'azienda in base all'utilizzo.

Elevata la qualità della soluzione, aggiunge Stormshield. Questo perché è stata sviluppata secondo criteri di programmazione del software difensivi e basato su un'architettura di microservizi protetta, con una protezione di livello militare contro gli attacchi che prendono di mira la soluzione di sicurezza stessa.

"Con la trasformazione delle pratiche di lavoro, garantire una protezione ottimale delle workstation è diventata una questione rilevante. La nostra soluzione è stata progettata per consentire agli amministratori di svolgere questa missione e per consentire agli utenti di lavorare in modo efficiente in un ambiente affidabile", ha osservato Brochot.*