

IN QUESTO NUMERO:

COVER STORY MICRO FOCUS

pag. 4

- La sicurezza resiliente di Micro Focus

pag. 5

- Dalla sicurezza reattiva a quella resiliente: come cambiano i paradigmi di protezione

pag. 08

- Un tool online per valutare il grado di resilienza

pag. 10

- Soluzioni intelligenti per proteggere dati, applicazioni, identità

CYBER ATTACK

pag. 13

- Una piattaforma per assicurare la continuità del business

pag. 16

- Il Rapporto 2020 OAD

SOLUZIONI

pag. 17

- La nuova piattaforma di rete intelligente Aruba ESP

pag. 18

- BenQ Instashow è la soluzione plug & play ideale per l'ufficio e non solo

pag. 21

- L'innovazione che nasce dalle applicazioni creando servizi

pag. 24

- Il supporto di Westcon

pag. 25

- RSA tutela la sicurezza nel lavoro da remoto



COVER STORY
LA SICUREZZA RESILIENTE
DI MICRO FOCUS

pag. 4

È disponibile il nuovo libro
CYBER SECURITY e DATA PROTECTION



Il libro è acquistabile al prezzo di 30 euro +IVA,
scrivendo a: **shop@reportec.it**

Security & Business 57
Gennaio 2021

Direttore responsabile:
Gaetano Di Blasio

In redazione:
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
www.reportec.it

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

Tutti i marchi sono
registrati e di proprietà
delle relative società

LA STRATEGIA PER LA RESILIENZA

Il numero 57 di Security & Business si apre con una cover story dedicata a Micro Focus, marchio storico della cyber security, che approfondisce la vision e le soluzioni del vendor, presentando un tema quanto mai attuale: la strategia per la resilienza.

A seguire la più ampia indagine sugli attacchi digitali avvenuti in Italia nel corso del 2020. L'osservatorio OAD è particolarmente prezioso, in quanto, giunto al 12esimo anno, consente di effettuare delle analisi nel tempo e si avvale della collaborazione della Polizia Postale e delle Telecomunicazioni. Infine si basa esclusivamente su attacchi realizzati in Italia.

Il rapporto, opera di Marco Bozzetti, è patrocinato da AIPSI (Associazione Italiana Professionisti della Sicurezza Informatica), capitolo italiano di ISSA, la più grande associazione di specialisti del settore nel mondo.

Il numero presenta anche altri dati, come quelli di Trend Micro e altri vendor del settore.

Soprattutto il numero offre visibilità a una cospicua serie di soluzioni per la security, che sempre più deve essere introdotta in ogni strumento digitale, al fine di contrastare il cybercrime. Ne è un esempio la soluzione di Aruba Networks, società del gruppo HPE, che propone una soluzione di rete in grado di anticipare i guasti, grazie a sistemi di machine learning e artificial intelligence che potrebbero bloccare le infrastrutture o penalizzarne le prestazioni.

Pure di grande attualità è il tema della sicurezza sul luogo di lavoro. BenQ ha sviluppato la soluzione InstantShow per le presentazioni, che, non solo risulta facile da utilizzare, grazie a logiche plug and play, ma, soprattutto, dispone di una serie di sistemi certificati per la sicurezza della comunicazione. Sono sempre BenQ i display interattivi per sale riunioni che tutelano anche la sicurezza ambientale grazie ai sensori di controllo dell'aerazione dei locali e agli schermi antibatterici che limitano la propagazione dei germi da contatto

Come appena mostrato, i rischi possono essere tanti e vari, ma, riallacciandoci al concetto di resilienza, che apre la cover story, la questione riguarda il rischio che i manager sono abituati a gestire. Certo che, come evidenziano in RSA, oggi occorrono strumenti per gestirla vista la rapidità con cui avvengono i cambiamenti e la numerosità degli eventi.

LA SICUREZZA RESILIENTE DI MICRO FOCUS

Pierpaolo Ali, Director CyberSecurity Southern Europe di Micro Focus delinea i principi e le soluzioni per realizzare una “resilient security”

di Riccardo Florio

Cosa significa sicurezza resiliente?

Significa predisporre un modello integrato di governance della sicurezza pensato per garantire la continuità operativa mentre l'infrastruttura aziendale si trova a dover affrontare continue minacce e attacchi. Significa organizzare sistemi, tecnologie e processi in modo tale che sia possibile predisporre le contromisure necessarie per bloccare attacchi, eliminare vulnerabilità e impedire minacce prima ancora che l'infrastruttura ne sia interessata.

Perché è necessaria?

È necessaria per due ragioni fondamentali.

La prima è che le minacce sono così numerose ed evolvono così rapidamente che non c'è tempo per analizzare tutti gli “alert” né per affrontarle efficacemente una volta che sono arrivate alle porte dell'infrastruttura aziendale.

La seconda ragione è che il costo per una violazione della sicurezza è talmente elevato che, dopo la fase di ripristino della normalità, un'azienda può trovarsi in grande sofferenza, se non addirittura non riuscire più a riprendersi.



Come si consegue un elevato livello di resilienza?

Il primo passaggio è quello di effettuare un assessment del proprio livello di cyber resilienza, in base al quale poter effettuare una pianificazione tattica e strategica.

Servono poi tecnologie innovative e automatizzate capaci di intervenire in tempo reale ma, soprattutto, una visione unitaria della sicurezza.

In che modo Micro Focus abilita una sicurezza resiliente?

La strategia di Micro Focus parte da tre considerazioni fondamentali:

- il nuovo perimetro aziendale è delineato dalle identità digitali;
- i dati sono il vero valore per ogni tipologia di azienda;
- le applicazioni sono uno strumento critico per il business, ma anche uno dei principali vettori per i nuovi attacchi.

Pertanto, la sicurezza resiliente di Micro Focus è costruita attorno a tre principi.

Il primo è la protezione da ogni tipo di minaccia

Pierpaolo Ali, Director CyberSecurity Southern Europe di Micro Focus

informatica attraverso: una governance delle identità e modelli avanzati di autenticazione; una protezione dei dati persistente attraverso il loro intero ciclo di vita; il costante rilevamento delle vulnerabilità applicative.

Il secondo aspetto è il rilevamento delle minacce, che deve essere accelerato attraverso soluzioni di data discovery e affiancato da tecnologie di automazione capaci di attivare risposte rapide, riducendo al minimo i falsi positivi.

Infine, la predisposizione aziendale verso una costante evoluzione, per stare al passo con minacce e rischi informatici. Questo richiede l'uso di soluzioni di sicurezza intelligenti e adattabili, di modelli ibridi di distribuzione e l'utilizzo di competenze provenienti dal mondo della data science.

Quali sono le soluzioni Micro Focus che permettono di conseguire questi obiettivi?

Le soluzioni di sicurezza Micro Focus sono organizzate in quattro famiglie di prodotti: ArcSight per la protezione intelligente e automatizzata dalle minacce di ogni tipo, NetIQ per la gestione sicura di identità e accesso, Voltage SecureData per la protezione cifrata dei dati, Fortify per lo sviluppo sicuro e il test delle applicazioni.

Queste famiglie sono costituite da prodotti modulari, integrabili sia tra loro sia con soluzioni di terze parti. Inoltre, si avvalgono di tecnologie innovative come il machine learning non supervisionato di ArcSight Intelligence o la tecnica brevettata Hyper FPE per la cifratura dei dati anche durante l'uso.

DALLA SICUREZZA REATTIVA A QUELLA RESILIENTE: COME CAMBIANO I PARADIGMI DI PROTEZIONE

Nel corso del tempo a ogni scenario di minaccia ha fatto seguito un corrispondente modello di sicurezza. Finora è stata la sicurezza a inseguire, ma ora prova ad anticipare

Le tecnologie per la sicurezza informatica hanno cominciato ad affermarsi seguendo un paradigma di tipo reattivo. I tempi erano diversi e gli attacchi meno sofisticati, estremamente meno numerosi in numero e non così diversificati e, inoltre, tutto avveniva più lentamente.

La sicurezza reattiva interveniva dopo che era stato individuato un problema: un compito, peraltro, non difficile come oggi, poiché gli attacchi erano pensati per dare dimostrazione di sé. Se i tempi di ripristino erano ragionevoli i danni restavano tutto sommato accettabili. Inoltre, le aziende erano meno esposte a problematiche legate al rispetto delle normative. Le tecnologie di sicurezza non godevano di grande popolarità: erano considerate un puro costo e, da alcuni, addirittura un costo inutile.

Con il cambiare dello scenario tecnologico tutto è aumentato: i dati, i volumi di informazioni, il numero degli attacchi, il numero degli accessi alle risorse aziendali, il numero di sistemi e processi e così via. La storia recente si è riempita di stalle chiuse dopo che i proverbiali buoi sono scappati ed è apparso evidente che le perdite e i danni di un attacco andato a buon fine non erano più facilmente assorbibili e, anzi, a volte, non assorbibili del tutto, fino a decretare persino la chiusura di un'azienda.

I limiti dei modelli preventivi e predittivi

Questo nuovo scenario ha portato a rivedere il modello della sicurezza in una rinnovata ottica di tipo preventivo.

Tuttavia, l'iniziale idea di prevenzione, basata essenzialmente sul controllo di minacce note, si è dimostrata efficace per un tempo piuttosto breve. Un tempo che ha coinciso con un contestuale mutamento nella natura del cyber crimine secondo modelli organizzati su larga scala e logiche imprenditoriali, dove l'unico obiettivo è il massimo profitto.

Dal modello preventivo si è, quindi, passati a un modello predittivo in cui l'obiettivo era ancora quello di prevenire, ma con metodi che fossero un passo avanti e non uno indietro a quelli dei cyber criminali. Questo obiettivo ambizioso ha portato allo sviluppo di nuove classi di software come i SIEM, capaci di rilevare e gestire avvisi di sicurezza provenienti da tutte le soluzioni implementate e relativi a dati di ogni tipo. L'efficacia di questo modello di protezione richiede però un significativo contributo umano nel costante adeguamento delle impostazioni di sicurezza, di gestione dell'accesso, di protezione dei dati e di definizione delle policy.

Con l'ulteriore crescita esponenziale del numero di minacce, gli avvisi di sicurezza si sono trasformati in veri e propri big data e la richiesta di capacità di analisi, di prestazioni, di competenze e risorse tecnologiche è arrivata a saturare la capacità delle aziende. Mai come negli ultimi due anni i costi per la sicurezza sono cresciuti, arrivando a un livello considerato ormai dalle aziende non più sostenibile. Oltretutto, in molte aree di sicurezza gli investimenti in nuove tecnologie si sono dimostrati inefficaci perché non si è riusciti a realizzare il livello di integrazione necessario o perlomeno non nei tempi richiesti.

La sicurezza resiliente

Il nuovo approccio alla sicurezza si chiama resilienza. La resilienza è la caratteristica in base al quale un sistema o un processo continua a supportare la propria missione ovvero svolgere il suo compito mentre si trova a dover affrontare una serie di minacce.

In caso di un attacco gli aspetti che concorrono a rendere un sistema resiliente comprendono la ridondanza, la semplicità, la riduzione della superficie di attacco, restrizione dell'accesso e capacità di coordinamento e di comprensione della situazione in corso. Il principio cardine alla base di un modello di sicurezza resiliente è l'adattabilità, con un approccio predittivo che sfrutta tecnologie di machine learning e intelligenza artificiale capaci di automatizzare i compiti di analisi e di adeguare dinamicamente e autonomamente il modello di protezione in base

all'evoluzione dello scenario.

L'obiettivo è individuare in tempi più rapidi le possibili vulnerabilità, acquisire la capacità per risolverle più rapidamente, riconoscere un numero superiore di attacchi e avere le difese in atto ancor prima che l'attacco venga sferrato.

Insomma, non si tratta più di aspettare l'invasore sotto le mura del castello per difendersi, né di prepararsi sapendo che arriverà il giorno dopo, ma di spostare continuamente il castello in modo che il nemico non lo riesca mai a trovare.



UN TOOL ONLINE PER VALUTARE IL GRADO DI RESILIENZA

Micro Focus mette a disposizione gratuitamente sul Web uno strumento per effettuare l'assessment del livello di cyber resilienza

di Riccardo Florio

Valutare il grado di resilienza della propria azienda rappresenta il primo passo verso un'efficace modello di protezione. Tuttavia non si tratta di un compito banale. Per aiutare le aziende in questo compito Micro Focus ha realizzato un tool per effettuare un assessment del livello di cyber resilienza che ha reso disponibile gratuitamente online all'indirizzo. <https://www.microfocus.com/en-us/cyberresilient/cyber-assessment>.

Come funziona

Lo strumento è stato pensato per aiutare le aziende a identificare le loro carenze nell'approccio alla cyber security e per aiutarle a comprendere meglio come definire le corrette priorità di intervento.

Si tratta di un questionario che analizza aspetti quali il livello di prontezza e il modello di pianificazione strategica organizzato in tre aree.

La prima analizza le tematiche di protezione di dati, identità e applicazioni dalle minacce mettendole in relazione alle azioni strategiche, di sostegno e di difesa.

Una seconda area riguarda la capacità di rilevamento delle minacce e del modo in cui è declinato nelle attività di osservazione e ispezione.

La terza area esamina la capacità dell'azienda di adattarsi dinamicamente all'evoluzione degli scenari di attacco e di predisporre azioni di ripristino efficaci, rapide e automatizzate, Al termine della valutazione viene consegnato un

rapporto che include il punteggio per ognuna delle tre aree di valutazione e il confronto con la media globale (e per settore). A ciò si aggiungono indicazioni strategiche per rafforzare la resilienza informatica generale.

Micro Focus 360° of Cyber Resilience



Il modello di Cyber resilienza di Micro Focus

SOLUZIONI INTELLIGENTI PER PROTEGGERE DATI, APPLICAZIONI, IDENTITÀ

Micro Focus propone un insieme di prodotti e tecnologie per rispondere alle minacce in modo intelligente, adattabile e proattivo e per garantire la business continuity anche in caso di attacco

di Riccardo Florio

Conseguire la cyber resilienza significa predisporre le condizioni per avere un'infrastruttura IT in grado di continuare a svolgere le principali attività di business anche in caso di attacco informatico e mantenere l'accesso agli strumenti necessari per avviare procedure di salvataggio dei dati, di eliminazione delle minacce e di ripristino così da minimizzare i danni e accelerare la ripresa.

Aumentare la cyber resilienza significa, innanzitutto, mettere in atto strategie pensate per identificare e monitorare le componenti che hanno un impatto sui rischi, creando le condizioni per evitarli e prevenirli adattandosi dinamicamente all'evoluzione degli scenari di minaccia.

Per il conseguimento di questi obiettivi Micro Focus ha sviluppato un modello di "resilient security" che fornisce tutti gli strumenti per predisporre un livello di

protezione completo ed efficace, adattabile in modo intelligente e dinamico all'evoluzione delle minacce.

Una strategia per la cyber resilienza

Micro Focus abilita la cyber resilienza attraverso un'ampia gamma di soluzioni e tecnologie integrate, organizzate in famiglie specifiche e guidate da una strategia comune incentrata su tre principi fondamentali.

Il primo è di aumentare il livello di protezione attraverso soluzioni pensate per la sicurezza delle identità digitali, delle applicazioni e dei dati. A ciò si affianca l'integrazione della sicurezza all'interno dei modelli di sviluppo come DevOps. L'ultimo tassello è un percorso costante di evoluzione basato su intelligenza artificiale e machine learning che permetta di individuare costantemente le minacce, di determinare chi ha accesso a quali risorse e di adattarsi dinamicamente alle nuove condizioni.

"L'insieme delle soluzioni di resilient security di Micro Focus fornisce gli elementi per implementare una protezione efficace, predittiva e intelligente necessaria per garantire la cyber resilienza richiesta dal nuovo mondo digitale – spiega Pierpaolo Alì, Director CyberSecurity Southern Europe di Micro Focus - Le soluzioni software di Micro Focus sono



organizzate in famiglie specifiche, integrabili tra loro e con soluzioni di terze parti, che abilitano un approccio di sicurezza efficace favorendo, nel contempo, un percorso di aggiornamento che garantisce la protezione degli investimenti già effettuati. ”

Protezione intelligente e governance della sicurezza

Un tassello importante nel modello di cyber resilienza proposto da Micro Focus è svolto da **ArcSight Intelligence** (in precedenza Interset), un software per l'analisi di sicurezza di tipo predittivo che utilizza tecnologie di machine learning non supervisionato per effettuare analisi comportamentale degli utenti e delle entità. ArcSight Intelligence dispone di un motore di analytics che integra oltre 200 algoritmi ed è stato sviluppato sulla base dell'analisi di casi reali. La tecnologia di machine learning non supervisionato

di Micro Focus abilita la predisposizione di meccanismi capaci di modificare la superficie di attacco in base all'analisi di uno scenario di rischio che muta, indipendentemente dall'effettivo rilevamento di una minaccia: di fatto prevenendo potenziali minacce anche se queste minacce non sono state individuate. Questa soluzione è completamente integrata con **Enterprise Security Manager di ArcSight**, che permette di analizzare in tempo reale grossi flussi di dati per un'analisi completa degli eventi di sicurezza e una protezione in tempo reale contro attacchi noti e sconosciuti.

Ad accelerare ulteriormente il rilevamento e la risposta efficace alle minacce concorre **ArcSight SOAR**, la piattaforma di Security Orchestration, Automation and Response che consente di radunare centralmente gli avvisi sulle minacce, riducendo i tempi di indagine a pochi minuti e attivando

automaticamente azioni di risposta e ripristino. La tecnologia SOAR è integrata e inclusa gratuitamente nella soluzione SIEM di ArcSight.

Soluzioni per proteggere identità,

Nell'attuale modello di azienda aperta e delocalizzata, dove il nuovo perimetro aziendale è definito dalle identità digitali degli utenti, la cyber resilienza richiede la predisposizione di una gestione centralizzata di identità e accesso che copra utenti, dispositivi, cose e servizi. A questa esigenza Micro Focus indirizza la famiglia **NetIQ** con cui è possibile gestire il "chi" (dipendenti, clienti) e il "cosa" (dispositivi, servizi) accede a sistemi e dati. Conoscere i modelli normali di queste identità rende più facile identificare la comparsa di modelli anormali di comportamento.

La famiglia di prodotti NetIQ favorisce la predisposizione di **un modello di sicurezza Zero Trust** verso cui tutti si stanno orientando e basato sul principio che non esistano situazioni, sistemi o utenti che possano essere considerati affidabili a priori. In un modello Zero Trust tutte le attività devono essere monitorate, il livello di accesso fornito deve essere sempre quello minimo necessario allo svolgimento del proprio compito e si devono monitorare costantemente anche gli utenti con privilegi come, per esempio, l'amministratore delegato.

Proteggere dati e applicazioni attraverso l'intero ciclo di vita

La famiglia **Voltage SecureData** di Micro Focus mette a disposizione una serie di tecnologie innovative e brevettate di cifratura e di accesso sicuro per la protezione dei dati sia strutturati sia destrutturati. Alla base di queste soluzioni vi è un modello di sicurezza che prevede di implementare il meccanismo di difesa e protezione direttamente sul dato o sui sistemi che lo trattano. Con le soluzioni Voltage SecureData i dati restano sempre cifrati dal momento della loro creazione fino alla loro cancellazione sicura. Persino durante l'utilizzo, grazie a tecniche di mascheramento brevettate e uniche sul mercato, le soluzioni Micro Focus permettono di mantenere cifrati i dati anche all'operatore che li sta trattando. La sicurezza delle applicazioni deve partire dalla fase di sviluppo integrando strumenti di controllo e test di sicurezza direttamente nelle piattaforme di sviluppo per poi estendersi all'intero ciclo di vita. Alla protezione delle applicazioni Micro Focus indirizza la consolidata gamma di soluzioni **Fortify** giunta alla ventesima release e inserita per il settimo anno consecutivo tra i leader nel Gartner Magic Quadrant for Application Security Testing oltre a figurare al primo posto nel rapporto 2020 Gartner Critical Capabilities for Application Security Testing per i casi d'uso Enterprise e Mobile and Client. Le soluzioni Fortify abilitano test di sicurezza delle applicazioni in modalità statica sul codice sorgente, in modalità dinamica mentre sono in esecuzione e in ambiente mobile. Sono disponibili anche come servizio in cloud (Fortify on Demand). ❖

UNA PIATTAFORMA PER ASSICURARE LA CONTINUITÀ DEL BUSINESS

La visione della sicurezza 2020 con Trend Micro

di Gaetano Di Blasio

Nel 2020 abbiamo assistito a una corsa per la digitalizzazione scatenatesi per il bisogno di utilizzare lo smart working o l'home working, a causa delle limitazioni indotte dalla pandemia. Una indagine realizzata da Trend Micro con l'istituto Ponemon, mostra che L'88% delle aziende ha accelerato l'aggiornamento del digitale. Un riscontro in tal senso arriva anche dal boom degli acquisti in dispositivi, servizi e applicazioni in cloud.

Ma tutto ciò, ancorché positivo, si limita in parte a spostare confusamente risorse in cloud senza attenzione per la sicurezza né una reale consapevolezza del cloud, afferma Alessandro Fontana Head of Sales Trend Micro Italia, commentando: «Basti pensare alla scarsa consapevolezza del concetto stesso di share responsibility, che implica la messa in sicurezza di quanto è "in the cloud"».

Il manager continua, riprendendo i dati dell'indagine: «A dimostrazione della mancanza di consapevolezza, solo il 55% degli intervistati ha previsto di implementare strumenti di protezione. Ciò è ancora più grave, poiché il cloud prevede un processo continuo e infinito che impone capacità di automazione». Sul fronte degli attacchi la pressione resta alta, come dimostrano i dati della Smart Protection



inquadrare per approfondimenti online



Network di Trend Micro. Covid 19 è tuttora l'esca del momento, in varie declinazioni: malware, phishing, attacchi mirati e così via presentano quasi sempre la parola Covid, hanno osservato in Trend Micro. Tornando ai dati della ricerca Ponemon, il 51% degli intervistati sostiene di aver capito che occorre investire di più in sicurezza, l'87% ritiene di avere il pieno controllo, l'83% è fiducioso di poter gestire la sicurezza nell'immediato futuro. In generale, cresce una certa consapevolezza. D'altro canto, resiste un 45% di rispondenti che considera la sicurezza un ostacolo. Eppure, basterebbe un metodo critico, come suggerito nel GDPR, che impone semplicemente di considerare la security, monitorare e valutare il da farsi. In questo non si è soli: l'utente finale è normalmente supportato da un system integrator: «Il nostro approccio - evidenzia Fontana - non parte dal voler vendere un prodotto, ma dall'aiutare il cliente e supportarlo a tutto tondo. Sappiamo quali sono le

preoccupazioni delle aziende, come, per esempio, la coerenza delle policy, le applicazioni delle patch, la protezione dei flussi network, così come pure la privacy e la compliance. Oggi non esiste un perimetro aziendale, non ci sono confini, pertanto l'obiettivo è supportare il cliente al 100%.».

Attenzione al cloud

Come accennato, spiega il manager c'è stata una rincorsa al cloud confusa e occorre fare attenzione, mette in guardia l'Head of Sales di Trend Micro: «Noi abbiamo una piattaforma di cloud ibrido in grado di soddisfare le esigenze dei nostri clienti. Non tutti sono pronti a gestire le complessità, senza strumenti di automazione è impossibile e gli ICT manager tornano a preoccuparsi per la sicurezza.

Le aziende, sottolinea Fontana devono comprendere che la continuità del business dipende dalla sicurezza informatica, perché un attacco informatico blocca l'azienda, cioè il business.

Sul mercato ci sono tante aziende e startup di security e altre ne arriveranno ma poche possono vantare trent'anni di storia, durante i quali c'è stato, sottolinea Fontana, un costante rinnovamento. Il manager ricorda come prima del cloud fosse stato necessario aggiungere la sicurezza della rete

e altro ancora. Ora è il momento della Endpoint Detection and Response, ma si tratta "solo" di un altro pezzo di un progetto di sicurezza, mentre è necessario riuscire a vedere l'insieme. In altre parole, la visione di Trend Micro presume la capacità di Detection and Response non sull'end point, ma sull'intero progetto di sicurezza, che sia on premise, presso un cloud privato, pubblico o ibrido. Non si può perdere la visibilità del progetto di sicurezza. Si deve proteggere il dato che si trova su Office 365 come i servizi dei vari fornitori come Google o altri, sottolinea Fontana, aggiungendo «Ci sono poi altri aspetti che devono essere considerati: per esempio c'è chi pensa di poter mettere in esercizio un data lake in cloud, trascurando i vincoli, come quelli im-

posti dall'amministrazione pubblica, rispetto alla movimentazione di tutta una serie dati».

Un'altra situazione critica è quella di una tecnologia che è fisicamente on premise, ma si avvale di un sistema di controllo in cloud. In questi casi, di fatto, il problema è il poter garantire sia la privacy che la compliance.

Nel cloud ci si espone a delle minacce, perché non siamo soli, ma condividiamo spazi. come sottolineato pocanzi.

Questi aspetti si allacciano a quelli della privacy, della formazione e della compliance. Senza una share



*Alessandro Fontana Head of Sales
Trend Micro Italia*

responsability ci si espone a delle minacce L'event configuration di Trend Micro, permette di comprendere cosa realmente accade nel cloud.

fondamentale che questo sia basato su: progetto, servizi e formazione per garantire la propria privacy, e quella dei dipendenti e di ciò che si fa entrare nel cloud. Serve una visione accurata.

La pressione degli attacchi è notevole come dimostra il rapporto sulle previsioni per la cybersecurity nel 2021, realizzato dagli esperti dell'azienda, che si aspettano un massiccio attacco all'home working.

Cresce l'esigenza del management detection and response, cioè esperti che hanno una visione dall'alto grazie a strumenti per prevedere le minacce.

In termini di prevenzione, Fontana ricorda anche le soluzioni di awareness che Trend Micro regala ai propri clienti per diffondere la conoscenza dei rischi e per educare alla protezione.

Per questo in Trend Micro hanno realizzato uno strumento per simulare attacchi in ufficio, in modo da far comprendere come possa essere facile sbagliare. Con un po' di conoscenza e attenzione si rende più difficile l'azione malevola.

A tal proposito, tornando al cloud è importante verificare l'aggiornamento delle applicazioni. Queste ultime, se non "aggiornate" possono compromettere un sistema: «È più facile per un hacker sfruttare una



inquadra per approfondimenti online

vulnerabilità, piuttosto che creare un attacco zero day. D'altro canto, è pressoché impossibile stare al passo col patching, senza automatismi. Con le soluzioni di Trend Micro è possibile effettuare una scansione delle vulnerabilità e verificare quando è il momento

migliore per applicarle virtualmente, cioè, precisa il manager, senza che possano generare conflitti, anche perché nulla viene installato sulla macchina. Sono diversi gli esempi di business continuity risolti dagli esperti di Trend Micro, come il caso che ha coinvolto un cliente con 40mila utenti che per ragioni di compliance non potevano utilizzare dispositivi personali, ma dovevano usufruire di tutti i contenuti da lunedì al venerdì.

In generale osserviamo che l'approccio di Trend Micro è basato sul concetto di platform company, che abbraccia l'intera azienda, in sostanza, ci spiega Lisa Dolcini, Head of Marketing di Trend Micro Italia "L'obiettivo è fornire una piattaforma di sicurezza condividendo una base comune, che consiste nel sistema di Threats intelligence e nelle analisi condivise con i ricercatori di Trend Micro, oltre che in un'infrastruttura comune. importante è molto importante anche la nostra capacità di integrazione con altri fornitori, che arricchisce l'intero ecosistema". ❖

OAD

Osservatorio
Attacchi Digitali
in Italia

Disponibile e scaricabile il Rapporto 2020 OAD

Reportec è l'editore del Rapporto 2020 OAD, Osservatorio Attacchi Digitali in Italia, iniziativa giunta al dodicesimo anno consecutivo di indagini sugli attacchi digitali intenzionali ad aziende ed enti pubblici in Italia, e che si avvale della preziosa collaborazione della **Polizia Postale e delle Comunicazioni**, che ha fornite interessanti dati sugli attacchi alle infrastrutture critiche ed agli ambiti di e-banking nazionali.

OAD costituisce l'unica indagine indipendente online in Italia sugli attacchi digitali intenzionali ai sistemi informatici delle aziende e degli enti pubblici operanti in Italia. L'indagine non prevede un predefinito insieme di rispondenti, ma consente ai potenziali interessati un pieno e libero accesso al questionario online, in maniera totalmente anonima; grazie al numero di risposte raccolte e alla loro bilanciata distribuzione tra organizzazioni di varie di-



mensioni e appartenenti a vari settori merceologici, l'indagine OAD fornisce un preciso quadro sul fenomeno degli attacchi digitali intenzionali in Italia, relativo anche alle medie e piccole organizzazioni sia private (PMI) che pubbliche. Quadro molto utile ad ogni Azienda ed Ente per meglio contestualizzare la propria analisi dei rischi informatici, necessaria ad esempio per la compliance a GDPR per la privacy.

Il Rapporto 2020 OAD è costituito da 11 Capitoli (147 pagine A4), tra i quali, oltre a quello sui dati della Polizia Postale, i due principali riguardano la rilevazione degli attacchi digitali, e le misure di sicurezza digitale in atto, e da 9 Allegati (39 pagine A4), che includono le schede degli Sponsor e dei Patrocinatori, la metodica usata, un glossario degli acronimi e dei termini tipici della sicurezza digitale e della sua gestione.



Il Rapporto 2020 OAD è gratuitamente scaricabile da
<https://www.oadweb.it/it/oad-2020/per-scaricare-il-rapporto-2020-oad.html>
o inquadrando il QR Code

LA NUOVA PIATTAFORMA DI RETE INTELLIGENTE ARUBA ESP

La piattaforma di rete intelligente Aruba ESP (Edge Services Platform) consente l'individuazione e risoluzione automatica dei problemi di rete e supporta la trasformazione digitale nell'era del Covid-19

di Gaetano Di Blasio

La soluzione Aruba ESP di Aruba Networks, società che fa parte della Hewlett Packard Enterprise, ben si colloca all'interno dello scenario mondiale attuale in cui la pandemia di Covid-19 sta portando cambiamenti repentini in diversi ambiti e nel mondo delle aziende, modificando le modalità con cui queste lavorano e utilizzano la tecnologia.

Secondo un recente sondaggio di Aruba, sempre più responsabili IT stanno progettando di aumentare gli investimenti nella tecnologia di rete basata sull'intelligenza artificiale (35%) dopo la pandemia anziché ridimensionarli (17%).

Si assiste a un'accelerazione della trasformazione digitale, con i clienti che hanno maturato nuove esigenze e sviluppano i propri modelli aziendali per adeguarsi a un ambiente che si è profondamente modificato. Il cambiamento dipende in massima parte dalla disponibilità di strumenti per la gestione della rete agili, scalabili, cloud native e sicuri.

Caratteristiche e funzionalità di Aruba ESP

La nuova soluzione Aruba ESP è una piattaforma di rete intelligente supportata dall'IA (intelligenza artificiale) ed è progettata per individuare e risolvere

automaticamente i problemi di rete, spesso effettuando le regolazioni necessarie prima che si verifichi un problema.

Considerando che, come spiegano gli esperti dell'azienda, attualmente solo il 18% delle modifiche alle reti viene effettuato in questo modo. La capacità interessante della piattaforma è proprio quella riuscire a prevedere le modifiche che si rendono necessarie, quasi come se possedesse un "sesto senso". ESP sta per "Edge Services Platform", ma la sua denominazione è stata appunto ispirata dall'idea di percezione extrasensoriale che è in grado di offrire ai clienti.

È una capacità unica basata sull'esperienza decennale di Aruba nello sviluppo di soluzioni IA e sul data lake cronologico a cui attinge per addestrare gli algoritmi di machine learning.

Aruba è in grado di accedere a dati importanti e



comparabili, consentendo un miglior funzionamento delle sue soluzioni AI e una maggiore precisione nell'individuazione dei problemi. Se ad oggi, molti tecnici di rete necessitano di ore per collegare i punti manualmente e individuare i problemi, Aruba ESP ha il vantaggio di procedere allo stesso modo, ma automaticamente, con una precisione del 95%. Oltre a questa funzionalità, altre due caratteristiche di Aruba ESP sono molto utili.

La prima l'infrastruttura unificata, che consente la gestione centralizzata dell'intera rete da Aruba Central in un solo punto di gestione cloud-native, anziché da piattaforme separate attraverso

reti cablate, wireless e WAN, senza la necessità di replicare manualmente le modifiche fra tutti i vari domini campus, filiale, data center, lavoratori da remoto e così via.

La seconda consiste nella protezione della rete Zero Trust attraverso una combinazione di strumenti di sicurezza Aruba, consentendo alle organizzazioni di rilevare, prevenire, isolare e bloccare automaticamente le violazioni della rete, preferibilmente prima che si verifichino. ❖

Per saperne di più, scarica il white paper gratuito [QUI](#)

BENQ INSTASHOW È LA SOLUZIONE PLUG & PLAY IDEALE PER L'UFFICIO E NON SOLO

Tecnologia evoluta a prova di utente, senza dimenticare la sicurezza e la salute nell'ambiente di lavoro

di Gaetano Di Blasio

Mai come in questo momento è importante per le aziende operare in un contesto digitalmente al passo con i cambiamenti e soprattutto sicuro. Queste esigenze, che riguardano sia il lavoro in presenza che lo smart working, hanno messo in evidenza le soluzioni proposte da BenQ, il cui core business in Italia si rivolge ai segmenti monitor e videoproiettori, sia per il consumatore finale che per i settori business ed education.



Le proposte del brand taiwanese si distinguono per il design di prodotto e la semplicità di utilizzo: non sono necessarie competenze tecniche per collegare dispositivi wireless Plug & Play, come ci spiega con soddisfazione **Giacomo Rocchi**, Sales and Marketing Director di BenQ Italy: «Basta una breve dimostrazione per comprendere l'utilizzo di tutti i nostri prodotti pensati per il settore Business, dai display interattivi ai videoproiettori smart, senza dimenticare i sistemi di wireless presentation. Per esempio, il BenQ Instashow» sottolinea Rocchi, «un dispositivo WPS (Wireless Presentation System) che consente di organizzare una riunione in pochi semplici passi, eliminando il fastidioso problema del cavo da collegare al PC. Basta premere un pulsante per far sì che uno dei partecipanti alla riunione abbia la possibilità di presentare utilizzando il proprio PC, il tutto wireless. Non servono cavi né alcun software da installare».

Questo piccolo dettaglio non è un caso, bensì l'applicazione della filosofia stessa di BenQ, il cui nome deriva dall'acronimo della promessa del marchio "Bringing Enjoyment 'n Quality to life": la tecnologia, anche la più complessa, deve avvicinarsi agli utenti garantendo la massima semplicità di utilizzo.

Tecnologia e sicurezza con Instashow

Fra le diverse proposte B2B fornite da BenQ, ci soffermiamo proprio sulla soluzione Instashow, che unisce la semplicità della tecnologia wireless a complessi sistemi che garantiscono la totale sicurezza dei dati.

Instashow è composto da due button e un host centrale dotato di porte HDMI, LAN, USB, più il relativo contenitore cradle. Il sistema è conforme HDMI 1.4 con HDCP e può quindi essere connesso con facilità a qualsiasi PC/notebook e riprodurre video DVD/Blu-ray. Non solo: consente di condividere

contemporaneamente fino a quattro presentazioni diverse, suddividendo lo schermo in 4 quadranti.

La semplicità di utilizzo di Instashow, tuttavia, non pone in secondo piano la totale sicurezza dei dati, garantita dalla protezione WPA2-PSK con crittografia AES a 128 bit.

In virtù di queste caratteristiche, evidenzia Giacomo Rocchi, InstaShow è stato certificato CVSS - Common Vulnerability Security System e ha ottenuto la certificazione ISO27001 per i sistemi di gestione della sicurezza delle informazioni (ISMS), a dimostrazione delle sue funzioni, che garantiscono la totale sicurezza dei dati e protezione della privacy degli utenti.

Garantire la tutela della salute nell'ambiente di lavoro

Oltre alla sicurezza dei dati, un altro pilastro della filosofia BenQ è sicuramente quello legato alla salute e al benessere dei suoi utenti. Ad esempio, sullo schermo dei display interattivi IFP (Interactive Flat Panels) viene applicato uno strato nanoionico d'argento, che li rende antibatterici e diminuisce così il rischio di diffusione dei germi.

Di fatto, la pandemia cambierà per sempre le abitudini dei lavoratori, sostiene Rocchi. Anche quando sarà superata, le aziende dovranno confrontarsi con le sue conseguenze e già molte si stanno interrogando sulla questione della sicurezza nelle sale riunioni e negli open space. Uno dei problemi principali riguarda la ventilazione e la nebulizzazione negli spazi chiusi. L'OMS afferma che soprattutto

inquadra per approfondimenti online



inquadra per approfondimenti online



le stanze con scarsa ventilazione corrono un rischio elevato: mantenere una buona qualità dell'aria e ridurre la trasmissione di germi è fondamentale per fornire un ambiente di lavoro sicuro e anche più produttivo.

A questo proposito, i display interattivi IFP BenQ sono dotati di sensori di controllo per la qualità dell'aria: i sensori integrati forniscono dati in tempo reale sui parametri ambientali circostanti, rilevando la temperatura e l'umidità e monitorando il livello di concentrazione di PM 2,5, PM 10 e CO2. In questo modo sarà più facile controllare la qualità dell'aria circostante, così da adottare le contromisure giuste per favorire un ambiente di lavoro o studio più sano. Conclude infine Rocchi con un ultimo accenno alla tecnologia Eye-care presente in tutti i Display Interattivi di BenQ: «I nostri schermi garantiscono un livello minimo di emissione di luce blu e offrono la tecnologia anti sfarfallio, riducendo così l'affaticamento e l'irritazione degli occhi e migliorando notevolmente il comfort visivo».



L'INNOVAZIONE CHE NASCE DALLE APPLICAZIONI CREANDO SERVIZI

La sicurezza alla base del processo di realizzazione di app e servizi

di Gaetano Di Blasio

In F5 l'importanza delle applicazioni è da sempre il fulcro di una strategia aziendale di lungo termine; lo dimostrano i grandi investimenti degli ultimi quattro anni, volti a potenziare l'offerta sul fronte delle applicazioni cloud native: come evidenza Maurizio Desiderio, Country Manager Italia e Malta, l'acquisizione di NGINX, la piattaforma di application delivery più utilizzata a livello mondiale, è forse il segno più chiaro di questa strategia che mantiene alta l'attenzione anche sul fenomeno del software Open Source.

Poter contare sulla solidità del supporto di F5 in tanti ambiti, compreso il settore pubblico, è una forte garanzia per tutte le imprese che stanno incrementando sempre di più l'utilizzo dei canali digitali.

Ma la strategia di lungo termine di F5 non si è fermata all'application delivery: con il recente investimento da un miliardo di dollari per l'acquisizione della soluzione Shape Security, basata principalmente su soluzioni di machine learning e AI, F5 punta a cambiare le modalità di identificazione dei rischi informatici, riuscendo a identificare un altissimo numero di tipologie d'attacco.

Queste acquisizioni rispondono alle esigenze di un mercato oggi pronto a sviluppare applicazioni con



Maurizio Desiderio, Country Manager Italia e Malta di F5

nuove modalità di sviluppo, in grado di supportare i bisogni dei clienti finali, senza rinunciare a adeguati livelli di sicurezza applicativa.

Rispetto al passato, quando lo sviluppo e il rilascio di nuove versioni delle applicazioni aziendali richiedeva dai sei mesi in su, oggi la rapidità del time to market è cruciale: l'adozione dei cloud e l'impiego di moderne metodologie di sviluppo sono la risposta. «Oggi, grazie alle nostre soluzioni di application delivery e security, siamo in grado di fornire un servizio che cresce con gli utenti, aumentando la user experience di ognuna delle app da essi utilizzate», afferma Desiderio.

È naturale chiedersi come si sia potuto raggiungere questo risultato e quali criticità si possano incontrare: «Il tutto è stato reso possibile dall'evoluzione della programmazione, che non richiede più di scrivere linee e linee di codice, ma consente di usare

degli elementi che funzionano come i mattoncini di Lego, che possono essere assemblati facilmente, con cui creare varie funzionalità aggiuntive. Tra i primi esempi di questo approccio», aggiunge Desiderio, «possiamo ricordare le tecnologie come Javascript, ma il cambiamento è stato soprattutto nell'impulso a condividere le esperienze e gli stessi "mattoncini di Lego", in pieno spirito Open Source». Senza entrare nel tecnico, le API hanno rappresentato e rappresentano un chiaro esempio di questa evoluzione: esse sono un passo fondamentale nella semplificazione e nella trasparenza dello sviluppo applicativo moderno, ma se non adeguatamente protette con sistemi dedicati di sicurezza possono causare grossi danni a causa della possibile perdita di messaggi, degli errori di "traduzione" dei vari linguaggi di programmazione o della consegna dei messaggi in mani sbagliate. Come sottolinea Desiderio, «Le API sono oggi una delle basi fondamentali dello sviluppo applicativo, ma posso facilmente diventare anche il punto più debole della sicurezza nelle applicazioni».

Per tutti questi motivi, F5 ha sviluppato e introdotto tecnologie che proteggono le API dalle principali

minacce di sicurezza: il country manager italiano sostiene infatti che «siamo gli unici, da sempre, a porre le applicazioni al centro del business. Anche se oggi tutte le aziende che propongono soluzioni di sicurezza stanno correndo ai ripari per "mettersi al pari" sul fronte della protezione delle applicazioni». Questo "involucro" di sicurezza attorno all'applicazione deve però essere necessariamente trasparente agli utenti, che vogliono interagire con applicazioni semplici, intuitive ed efficaci e agli operatori, che devono preoccuparsi solo degli aspetti logistici o economici nello scegliere dove mettere le proprie applicazioni, avendo molto spesso a disposizione un ambiente multi-cloud o hybrid-cloud.

Da parte di F5, evidenzia il country manager italiano, c'è l'impegno a essere sempre all'avanguardia per garantire che la protezione e gli altri servizi costruiti intorno all'app siano costantemente aggiornati, nonché per estendere la sicurezza ad altre piattaforme in una logica multicloud.

Prestazioni sotto controllo con le performance proattive

Un ulteriore livello di affidabilità e sicurezza sarà aggiunto presto, ci svela Desiderio, grazie a un motore di analytics che consentirà di monitorare il funzionamento delle applicazioni, rendendo possibile mostrare, per esempio, quale esatto elemento di una architettura a microservizi presenta bassi livelli di prestazione.

L'obiettivo è l'ottimizzazione generale delle performance con una logica proattiva.



inquadra per approfondimenti online

Come sottolinea il country manager, si tratta di un risultato importante non solo per la sicurezza, ma, in generale, per tutto ciò che riguarda le prestazioni delle applicazioni, «il cui diffuso utilizzo fa in modo che esse siano sempre più indispensabili per gli utenti che, di conseguenza, hanno un livello di pazienza molto bassa e la situazione andrà peggiorando. Il rischio è perdere il cliente che, grazie all'ampia offerta di mercato, ha la possibilità di passare velocemente a un servizio della concorrenza». Tale aspetto è ulteriormente critico nel caso dei managed service provider, non necessariamente fornitori legati alla sicurezza, che devono gestire al meglio il cliente, rispettando come minimo le SLA (Service Level Agreement). Per questo molti managed service provider che utilizzano le tecnologie di F5 troveranno un vantaggio importante con i nuovi analytics. «La stessa cosa», sostiene Desiderio, «vale per il Public Cloud, poiché ogni fornitore ha logiche commerciali e logistiche che determinano un impatto sulle SLA. I controlli forniti da F5 sono un'ulteriore garanzia, anche nello specifico della sicurezza, rispetto alle credenziali e ai privilegi degli utenti». Un altro vantaggio dell'adozione di soluzioni di machine learning, infatti, consisterà nella capacità dei sistemi di autenticazione di definire un profilo abbinato all'utente. Tipicamente ciascuno di noi opera allo stesso modo: non solo possiamo capire se un utente "torna" sul nostro servizio, ma gli scostamenti dal profilo sono sospetti e meritano un approfondimento con operazioni preventive. Si tratta di logiche già applicate, per esempio, dalle

banche sulle transazioni con carte di credito, che avvisano se si sta effettuando un prelievo più alto del solito. In sostanza, scatta un controllo quando si verifica un'anomalia. In tal senso gli strumenti di machine learning sono fondamentali, perché non è umanamente possibile prevedere quali minacce possano nascondere grandi quantità di transazioni generate attraverso bot. Inoltre, è noto che persiste una carenza di tecnici specializzati nella sicurezza e ancora meno sono quelli che possono vantare grande esperienza.

Il manager ci lascia con un caso di successo: «Abbiamo realizzato un progetto con centinaia di utenti in una realtà italiana che ha scelto F5. Il suo sviluppo è stato emblematico perché ha permesso di evidenziare l'efficienza del modello a microservizi sia nella parte di progettazione sia in quella di messa in esercizio. Il progetto iniziale, infatti, è stato completamente rivoluzionato e non per rispondere alle esigenze tecniche di F5, bensì per migliorarlo a vantaggio del cliente».



IL SUPPORTO DI WESTCON

La relazione, il supporto e la formazione del distributore

di Gaetano Di Blasio



Westcon-Comstor è un distributore globale di soluzioni e sistemi digitali, in grado di offrire una conoscenza profonda delle tecnologie proposte: si tratta di un elemento cruciale, che parte dall'istruzione, fondamentale per l'adozione della tecnologia. Di questo si occupa Westcon, che garantisce la formazione di tecnici e utenti finali accreditati che possono ottenere le competenze e l'esperienza necessarie per fornire un'implementazione senza soluzione di continuità, per massimizzare l'utilizzo.

Come distributore di F5, Westcon ha diversi ruoli. «Certamente l'innovazione è il nostro pane quotidiano, per questo sono fondamentali l'informazione sulle nuove tecnologie e, soprattutto, la capacità di trasmettere le stesse in termini di formazione», afferma Alessandro Della Negra, Country Sales Director Italy, Greece, Cyprus, Malta and Adriatics di Westcon, che aggiunge, «a ciò si abbina il supporto in affiancamento alle risorse già formate. Più in dettaglio, la componente di Accademy, che vede per altro Westcon come l'unico Authorized Training



Alessandro Della Negra, Country Sales Director Italy, Greece, Cyprus, Malta and Adriatics di Westcon

Center di F5 in Italia, è certamente al centro delle importanti attività legate all'erogazione dei training ufficiali».

In quanto realtà internazionale, inoltre, i partner possono attingere alle competenze globali dei partner del distributore. «Per esempio, ricordo un episodio che mi è personalmente capitato», racconta Della Negra: «Un nostro partner italiano aveva bisogno di supporto relativamente a funzionalità particolari di NGINX e si è potuto appoggiare a un partner europeo con notevole esperienza specifica per realizzare, degli script appositi».

Più in generale emergono le potenzialità di abilitazione per i partner.

Westcon si occupa della soluzione di tutti i paradigmi tipici della filiera operativa che dal distributore arriva fino all'utente finale, in un contesto da gestire che è ben diverso dal rivendere hardware che è sempre più software defined, mentre queste nuove soluzioni si basano su micro-servizi, quindi su licenze. Dinamiche che prevedono gestioni degli approvvigionamenti diversi e così via.

Inoltre, Westcon si è dotata di una piattaforma cloud ad hoc per la gestione degli ordini di fulfillment delle risorse intangibili, ottimizzando la fatturazione ricorsiva, la gestione delle licenze multiple e multifornitore, il pagamento nel corso di utilizzo delle licenze anche nel caso non sia direttamente gestito dal fornitore, in un'ottica di semplificazione per il partner e per l'utente finale. Grazie ad un servizio

di intelligent demand progettato dal distributore è possibile analizzare l'utilizzo delle soluzioni per prevedere quale potrà essere l'evoluzione tecnica e le esigenze che i partner e i loro clienti potrebbero avere in futuro, in modo da agevolare e accelerare lo sviluppo. Infine, il distributore fornisce altre tecnologie complementari a F5 fornendo al canale un unico punto di riferimento progettuale. ❖

RSA TUTELA LA SICUREZZA NEL LAVORO DA REMOTO

La pandemia ha velocizzato il processo di trasformazione digitale e spinto l'adozione del lavoro da remoto, spesso sottovalutando i rischi alla sicurezza informatica

di Gaetano Di Blasio

La sicurezza in RSA, società storica del settore, parte dal concetto di digital risk che, ci spiega Roberto Branz, Channel Account Executive di RSA Security Italia rispetto ai rischi di business cui sono avvezzi i top manager, presenta due fattori differenzianti, la velocità con cui si concretizzano i fenomeni collegati ai rischi e si modificano nel tempo e i

volumi che li caratterizzano.

A causa della pandemia si è accelerato il percorso delle aziende verso il digitale, ma non tutti sono stati al passo adottando tecnologie e modelli operativi corrispondenti.

Se, da un lato, il digitale amplia le potenzialità del business, dall'altro accresce in modo esponenziale il rischio: «La trasformazione digitale amplia il perimetro delle aziende e velocizza il commercio e i processi interni incrementando, i relativi rischi alla sicurezza dei dati - sottolinea Branz, che aggiunge - RSA aiuta a riconoscere per tempo questi rischi, a monitorarli e tenerne traccia, per mitigarli, fornendo le evidenze di quanto è accaduto. Questo è il nostro leit motif che cerchiamo di diffondere nelle aziende in modo di coinvolgere tre entità: l'IT tradizionale,

Roberto Branz, Channel Account Executive di RSA Security Italia



il team che si occupa di audit & compliance e i responsabili della security. Tutti insieme devono aiutare il Board nel prendere le decisioni giuste per la trasformazione digitale, a patto di condividere tali decisioni in modo corretto con il management».

Le priorità di sicurezza del 2021

Il manager evidenzia come le imprese nel 2020 abbiano cercato di mitigare la crisi indotta dal Coronavirus, usando la tecnologia e lavorando da casa. Sono state, così più disponibili a mettere contenuti in cloud, sia per i dipendenti sia per i clienti, aumentando il livello di digitalizzazione, superando vetuste impostazioni a silos, migliorando i propri prodotti e servizi, anche estendendosi al di fuori dei confini nazionali.

Chi era preparato, dal punto di vista delle soluzioni di sicurezza già adottate, è cresciuto anche in questo, aumentando, per esempio, il numero di utenti cui è stato elevato il livello di sicurezza. Tutto ciò è accaduto in modo piuttosto rapido, afferma Branz. In sostanza si è visto che il nuovo modello di smart working funziona e che sarà possibile accrescere la sicurezza assegnando una identità digitale sicura che certifichi l'ingresso digitale in azienda di chi è colui o colei che dice di essere.

L'identità della persona diventa il primo punto da proteggere anche perché le identità aziendali sono spesso collegate con quelle personali. Una buona pratica richiederebbe che a ogni utente siano assegnati specifici privilegi, pur considerando che in

troppe realtà non si controlla nemmeno che vengano cancellate le credenziali di un dipendente che lascia l'azienda.

Cresce l'importanza dell'identità digitale

In molte aziende nel prossimo anno si tornerà in ufficio, ma nulla sarà come prima, perché in tanti hanno sperimentato il lavoro da remoto con successo. Molti, a rotazione resteranno casa, per ottimizzare e risparmiare tempi di spostamento e costi. In tali contesti si troveranno ambienti di lavoro variegati con un perimetro esteso e sarà fondamentale certificare l'identità digitale delle persone perché ognuno dovrà conservare i propri privilegi all'interno del perimetro aziendale, senza che persone malintenzionate possano accedere a ogni contenitore d'informazioni.

Quindi certificare l'identità digitale delle persone è prioritario, perché molti attacchi si rivolgono all'utente come persona, il che si porta dietro un bagaglio digitale. «I cyber criminali possono accedere facilmente alle informazioni e a questo rischio - spiega Branz - poche aziende hanno pensato, perché la priorità era tornare al lavoro».

Un'altra fonte di rischio sono le frodi innescate dalla curiosità verso i temi attualità, che spesso nascondono contenuti malevoli, ma ci sono anche casi di persone che si presentano in una azienda spacciandosi per qualcun altro. Ognuno deve valutare la propria esposizione. Una possibilità interessante per numerose imprese è dotarsi di un sistema per il controllo dei rischi aziendali.

Le soluzioni di RSA Security

Soluzione storica di RSA, SecurID si occupa dell'identità digitale e la sua evoluzione ha allargato il concetto alla Identity Assurance. È disponibile un'ampia gamma di "autenticator" multifactor per soddisfare esigenze adatte a variegate applicazioni. Si va dal classico token, proseguendo alle impronte digitali, oppure una semplice operazione come accettare un messaggio o scuotere lo smartphone per dimostrare di possedere quello smartphone.

In RSA, oltre a questo hanno anche lavorato per semplificare l'utilizzo di queste tecnologie di authentication per gli utenti.

«La migliore tecnologia è quella che fa il lavoro in modo silenzioso. Noi monitoriamo il comportamento degli utenti e interveniamo soltanto quando c'è un fattore di rischio e chiediamo un'informazione in più per certificare l'utente - spiega Branz, che aggiunge - Se l'operazione che stai facendo è regolare, ti stai collegando da casa tua, col tuo pc e indirizzo, come fai tutti i giorni non ti chiediamo nessuna autenticazione agevolandoti nel tuo lavoro».

A questo si aggiunge una soluzione di Identity Governance per gestire persone e diritti in azienda e un sistema SIEM (Security Information and Event Management) evoluto, tra i più recenti strumenti di RSA, per il controllo di tutto quello che accade sull'infrastruttura, NetWitness. Raccogliendo molte informazioni, oltre a controllare, la soluzione è in grado di apportare i rimedi necessari usando le suddette informazioni e applicando modelli matematici ad hoc, fornendo un servizio di Detection e response



inquadra per approfondimenti online

in ambito esteso: «Ci spingiamo fino a proteggere le nuove reti basate su servizi e prodotti IoT che sono sempre più pervasive», sottolinea Branz.

Fraud&Risk affronta i temi antifrode insieme a NetWitness, monitorando la presenza sul web di siti con pagine social non ufficiali, quindi se qualcuno tentasse di registrare siti fake simili a quelli di un'azienda, RSA riesce a monitorarli ed, eventualmente, a bloccarli, grazie alle relazioni e alla expertise di RSA, producendo tutta la documentazione che dimostra la frode.

La storica suite Archer di RSA fornisce una piattaforma tecnologica per la gestione dei rischi e della conformità nel contesto del business.

50mila utenti in smart working nella PA

In RSA, durante il primo lockdown sono riusciti a implementare il lavoro da remoto su un perimetro di 50mila utenti. Il tutto in pochissimi giorni usando una app per l'autenticazione. Il progetto era già in corso, ma è stato inevitabilmente accelerato dall'emergenza sanitaria

Alle piccole e medie imprese, invece, è stato fornito un sistema di sicurezza gratuitamente per sei mesi. Qui la difficoltà è stata quella di superare le preoccupazioni degli IT manager, che non si fidano delle capacità dei loro stessi utenti, nel gestire lo strumento di autenticazione. La impossibilità di incontrarsi ci ha permesso di automatizzare molti dei processi per la sicurezza, come quelli per l'auditing.

