Cloud & Business

n.67
Gennaio 2018

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

IN QUESTO NUMERO

COVER STORY

L'ANALISI PREDITTIVA RENDE SICURI DATI E APPLICAZIONI

L'analisi comportamentale predittiva permette di ridurre i tempi di intervento per la sicurezza e di concentrarsi sugli utenti a più alto rischio

Il diffondersi del concetto di Smart IT e l'impatto che su di esso ha la sicurezza, ha come corollario negativo l'intensificarsi dell'intelligenza degli attacchi cibernetici. È pur vero che le soluzioni che li contrastano vengono immesse sul mercato da parte delle aziende specializzate in sicurezza abbastanza rapidamente ma si tratta comunque di una questione di tempi.

Secondo Gartner, il tempo medio per rilevare una violazione è di oltre tre mesi, cosa che lascia a malware e ad altri tipi di attacchi il tempo di infiltrarsi e localizzarsi in attesa di essere richiamati in vita dagli hacker o di trovare un modo di contrastare i successivi aggiornamenti dei software di sicurezza.

Un modo per ridurre questo intervallo consiste nello sfrutta-

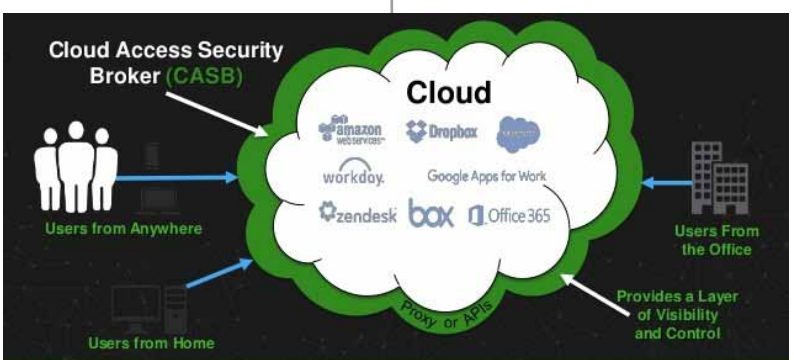
Luca Mairani di Forcepoint

Reportec Cloud&Business - Numero 67 - Gennaio 2018 - Registrazione al tribunale n°574 del 5 Novembre 2010 - Tutti i marchi sono di proprietà delle relative società- Editore: Reportec Srl (www.reportec.it) - Direttore responsabile: Giuseppe Saccardi - In redazione: Gaetano Di Blasio - Grafica: Paola Saccardi - Immagini: Dreamstime.com

re dati ed analitiche. La società di ricerca prevede in proposito che entro il 2018 l'80 per cento delle piattaforme di protezione degli endpoint includerà il monitoraggio delle attività e le capacità forensi e stima che almeno un quarto delle violazioni verrà evidenziato attraverso l'analisi del comportamento degli utenti e degli asset.

La criticità del cloud e degli ambienti ibridi

Il problema dei tempi intercorrenti tra il primo rilevamento di un nuovo tipo di attacco e il momento in cui le patch sono disponibili risulta enfatizzato quando da un ambiente esclusivamente privato, e quindi che offre la possibilità di pianificare interventi rapidi connaturati anche alle proprie capacità di investimento e di percezione del rischio, si passa ad un ambiente completamente migrato sul cloud pubblico o a uno scenario cloud di tipo ibrido o ancor meglio, si fa per dire, multi cloud.



La combinazione di ambienti IT caratterizzati da una forte presenza di dispositivi mobili che si collegano alle applicazioni business tramite infrastrutture cloud ibride e multi-cloud apre la strada a problematiche connesse allo stato di aggiornamento delle infrastrutture di terzi che si interpongono tra il dispositivo end user e il data center o i data center dove risiedono dati e applicazioni.

Non che i service provider non siano più che intenzionati ad apportare rapidamente le necessarie correzioni ma la realtà è caratterizzata dal fatto che non pochi degli operatori hanno sviluppato le loro infrastrutture quando gli attacchi apportati da cyber hacker non erano così sofisticati come lo sono ora, con la capacità che hanno di far leva su attacchi distribuiti, complessi e strutturati, attacchi che richiedono per essere rilevati da analisi approfondite non solo del traffico, ma anche di come questo si scosta per il singolo cliente da quello che è l'usuale comportamento delle applicazioni business fruite.

In sostanza, può avvenire che per mettersi al passo con la sofisticatezza degli attacchi e delle capacità elaborative e di analisi richieste si renda necessario apportare modifiche significative alla infrastruttura che data la scala di intervento richiesta ad un provider possono finire con il ritardare l'entrata in funzione delle contromisure di sicurezza atte a contrastarli.

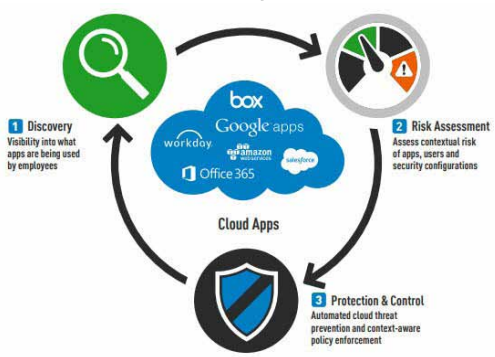
Per rimuovere questo potenziale vulnus, Forcepoint, bypassando e compensando le eventuali carenze dell'infrastruttura cloud dei provider, ha spiegato **Luca Mairani**, Senior Sales Engineer di Forcepoint in Italia, ha puntato sull'analisi comportamentale estesa a livello di end-point.

La società, che è un'azienda che sviluppa software di sicurezza operante a livello mondiale e con un solido background in due dei temi più all'attenzione dei manager, la cyber security e il cloud, ha con questo obiettivo di recente aggiunto al proprio peraltro già ampio portfolio di soluzioni per la sicurezza in cloud, nuove funzionalità che abilitano ulteriori controlli comportamentali previsionali che semplificano la protezione dei dipendenti, dei dati aziendali critici e della proprietà intellettuale.

Sicurezza più 'smart' con l'analisi comportamentale

La vision strategica è consistita nel rendere disponibili funzionalità basate sull'analisi del comportamento e sull'analisi predittiva, volte a rafforzare le policy di sicurezza per quanto concerne lo scambio dei dati tra ambiente informatico legacy da e verso il cloud esterno (CASB: Cloud Access Security Broker), come ad esempio nel caso delle banche i cui dipendenti utilizzano Microsoft Office 365, la sicurezza su Web e quella della posta elettronica.

Approcciare la security attraverso un filtro human-centric, osserva Forcepoint, aiuta le organizzazioni a comprendere meglio gli indicatori del normale comportamento informatico e identificare rapidamente attività e operazioni, quali la shadow IT, che rappresentano i maggiori rischi.



Il rafforzamento delle policy di sicurezza è stato perseguito con lo sviluppo di funzionalità che permettono di valutare il rischio di condivisione di file e di altre applicazioni cloud e proteggono dalla perdita di dati sensibili non archiviati nella rete aziendale, analizzando parametri quali il comportamento dell'utente e le caratteristiche dell'applicazione, ad esempio i dati, il dispositivo e la posizione da cui si accede.

Microsoft 365 e Azure sicure con Forcepoint CASB

L'obiettivo di rafforzare e rendere sicure le attività in Cloud e in ambienti quali Microsoft 365 e Azure si è concretizzato, come in precedenza evidenziato, con il recente rilascio di ulteriori controlli di analisi comportamentale che permettono di semplificare la protezione di dipendenti, dati aziendali critici e proprietà intellettuale.

Le funzionalità, disponibili per Forcepoint CASB, Forcepoint Web Security e Forcepoint Email Security, hanno l'obiettivo primario di fruire del cloud come motore per lo sviluppo del proprio business in modo sicuro e affidabile. L'obiettivo, per le specifiche soluzioni, è stato perseguito apportando aggiornamenti che comprendono rispettivamente:

- **Forcepoint Web Security:** funzionalità che consentono un controllo più granulare delle applicazioni cloud e bloccano eventuali attività di shadow IT.
- **Forcepoint Web Security:** strumenti di migrazione in cloud che consentono agli utilizzatori di Forcepoint Web Security con installazioni locali di migrare in ambiente Cloud in qualsiasi momento.
- **Advanced Malware Detection (AMD) Powered by Lastline:** disponibile per le piattaforme on-premise e in Cloud Forcepoint Web Security e Forcepoint email security. L'integrazione della tecnologia AMD sandbox consente poi di proteggere in tempo reale gli utenti ovunque si trovino.

In pratica, la analisi comportamentali di Forcepoint CASB analizzano il comportamento dell'utente e le caratteristiche dell'applicazione, ad esempio i dati, il dispositivo e la posizione da dove si accede. A questo Forcepoint ha aggiunto una rinnovata User Risk Dashboard single-view che evidenzia sia le attività dei dipendenti che il potenziale impatto sul business basato sulle autorizzazioni che l'utente detiene all'interno dell'organizzazione.

Una combinazione perfetta

FUJITSU Server PRIMERGY
e Windows Server 2016

FUJITSU

Microsoft

Windows Server: Power your business

Iperconvergenza, qualità e affidabilità: i Server PRIMERGY e Windows Server 2016 sono la perfetta combinazione per vincere le sfide del futuro. Cosa stai aspettando?

Info:

www.fujitsu.com/windowsserver2016
Numero verde: 800 466 820
customerinfo.point@ts.fujitsu.com
blog.it.fujitsu.com

shaping tomorrow with you

PALO ALTO NETWORKS PORTA IL LOGGING SERVICE NEL CLOUD

Lee Klarich di Palo Alto Networks

Con il Logging Service di Palo Alto Networks non si è limitati dalla capacità del proprio hardware per rispondere alla necessità del business

Palo Alto Networks, società attiva nella sicurezza, ha annunciato il lancio del suo servizio di Logging Service cloud-based in Europa. Il servizio consente ai clienti di raccogliere dalla Next-Generation Security Platform di Palo Alto Networks grandi quantità di dati relativi alla propria sicurezza.

Tutti i dati inviati al Logging Serice in Europa verranno immagazzinati presso un data center collocato nell'Unione Europea.

L'esigenza di un tale servizio deriva dal fatto, ha spiegato l'azienda, che i prodotti di cybersecurity generano enormi quantità di dati, sotto forma di log che possono essere utilizzati per combattere minacce sofisticate.

Oggi, le organizzazioni necessitano della capacità di immagazzinare, elaborare e analizzare più dati di log possibile per ottenere una ampia e esaustiva visibilità su tutta la propria infrastruttura e trasformare questi dati in informazioni concrete, sui cui prendere decisioni efficaci.

Una raccolta di log tradizionale, basata sull'hardware, porta con sé difficoltà amministrative e limitazioni di scala che possono addirittura rendere difficilmente utilizzabili o non indisponibili dati potenzialmente utili.

Con il Logging Service di Palo Alto Networks, le organizzazioni non sono più limitate dalla capacità del proprio hardware per rispondere alla necessità del business. In essenza, il Logging Service fornisce un'infrastruttura di logging centralizzata e scalabile, senza difficoltà amministrative, che consente ai clienti di raccogliere dati di log senza limitazioni locali legate allo storage o alle capacità elaborative. In sostanza, il servizio cloud-based cambia le dinamiche economiche e semplifica le operazioni di raccolta di log su ampia scala.

Inoltre, il prossimo Palo Alto Networks Application Framework permetterà di utilizzare strumenti avanzati di analisi sui propri utili dati di log, e di utilizzare una serie di applicazioni di sicurezza cloud-based sviluppate da Palo Alto Networks, da sviluppatori indipendenti e dagli stessi clienti. La nuova funzionalità estenderà in pratica le capacità della Next-Generation Security Platform di Palo Alto Networks, senza necessità di infrastrutture aggiuntive.

«Il Logging Service consente di rispondere a necessità di business in costante evoluzione, semplificare le operazioni e incrementare i livelli di automazione. Rendere il Logging Service disponibile in Europa permette ai nostri clienti di avere a disposizione queste funzionalità di raccolta dati, garantendo al tempo stesso che i dati rimangano in Europa, rispondendo così alle loro esigenze di confidenzialità», ha spiegato **Lee Klarich**, chief product officer di Palo Alto Networks.

NUVIAS RAFFORZA LA DIVISIONE PRACTICE DI CYBER SECURITY

Piera Loche di Nuvias Italia

Nuvias ha ampliato l'offerta e dato ai partner di canale l'accesso a tecnologie e servizi a valore per la Digital Transformation e il cloud

Nuvias ha completato la gamma dei prodotti selezionati e certificati inseriti nella Practice di Cyber Security, divisione che raggruppa soluzioni e servizi professionali volti a garantire ai partner un'offerta ampia ed integrata. Il nuovo portfolio include in particolare:

- **Arbor Networks**, che contrasta attacchi DDoS e altre minacce.
- **Barracuda Networks**, che fornisce soluzioni di sicurezza e connettività per il cloud.
- **HID Global** che propone soluzioni di Strong Authentication e Identity Management.
- **Juniper Networks** che garantisce una elevata protezione della rete grazie alla Software Defined Secure Network.
- **Malwarebytes**, con soluzioni di disinfestazione e protezione dati.
- **VASCO**, con strumenti di e-signature per documenti e transazioni online.

L'arricchimento del portfolio deriva dalla constatazione che innovazione digitale, trasformazione del business ed implicazioni tecnologiche comportano continui aggiornamenti delle infrastrutture IT.

Il 2017 verrà ad esempio ricordato come l'anno dell'estorsione digitale, con gli attacchi WannaCry e NotPetya perpetrati a livello mondiale, così come è stato l'anno nero del Data Breach, ovvero del furto e della diffusione di dati sensibili. Come se non bastasse, l'inarrestabile domanda di nuove tecnologie e il rapido aumento di vendor emergenti, sottolinea quanto il canale debba tenere il passo con tassi di innovazione senza precedenti. Nuvias, ha spiegato **Piera Loche**, Managing Director di Nuvias Italy, si è proposta di rispondere in modo puntuale a queste esigenze, fornendo un portfolio molto ampio di soluzioni progettate e sviluppate per adattarsi a tali trasformazioni, siano queste legate a cambi di piattaforma, migrazioni sul cloud o difesa da rischi finora sconosciuti.

La società, spinta dai recenti cambiamenti del settore, si è attivata per rinnovare la propria offerta e garantire ai partner di canale l'accesso alla più ampia gamma di tecnologie ad alto valore e ad una serie di servizi di supporto innovativi, per consentire ai partner di incrementare il loro business e di entrare in nuovi mercati. Il portfolio di prodotti si basa sul concetto di Practice, un'area di specializzazione e competenza, che riunisce soluzioni leader di settore e servizi professionali di supporto in modo da creare un'offerta ampia e coesa. Ad oggi le Practice attive in Nuvias sono Cyber Security, Advanced Networking e Unified Communication, cui si andranno ad affiancare nei prossimi mesi anche quelle di Application Performance, System Infrastructure, Cloud e Mobility. «L'ampliamento della gamma dei prodotti, insieme al nostro team offre le migliori soluzioni per aiutare le imprese a costruire solide difese che annullano ogni cyberattack» ha dichiarato Loche.

APPLIANCE DI JUNIPER NETWORKS RICONOSCE IL MALWARE ON PREMISE E NEL CLOUD

Gli aggiornamenti della piattaforma Software-Defined Secure Networks automatizzano le operazioni e danno visibilità nelle fasi del contrasto al cybercrimine

Juniper Networks, società specializzata nelle reti e nella loro sicurezza, ha annunciato nuovi aggiornamenti alla sua piattaforma di cyber-security, con l'obiettivo di permettere ai team preposti alla sicurezza di semplificare la gestione e ridurre i tempi di soluzione dei problemi.

Gli aggiornamenti prendono atto che gli attacchi mirati stanno diventando sempre più sofisticati e le organizzazioni di ogni dimensione sono oggetto di minaccia a tutto campo, indipendentemente dal luogo, dal cloud e dalle funzioni.

In pratica i cyber criminali non si fermano mai e aumentano costantemente le pressioni sul team dedito di sicurezza che non solo è generalmente carente di personale qualificato ma è anche coinvolto nella gestione di policy complesse e processi manuali. Per rispondere a queste minacce Juniper ha apportato aggiornamenti alla sua piattaforma di cyber sicurezza che, con l'obiettivo di far risparmiare tempo, si propongono di permettere la semplificazione delle operazioni grazie a una più efficiente gestione delle policy e la difesa dal malware on-premise mediante l'analisi del comportamento delle minacce, la mitigazione one touch e l'applicazione adattiva su diversi ambienti. Vediamoli in sintesi.

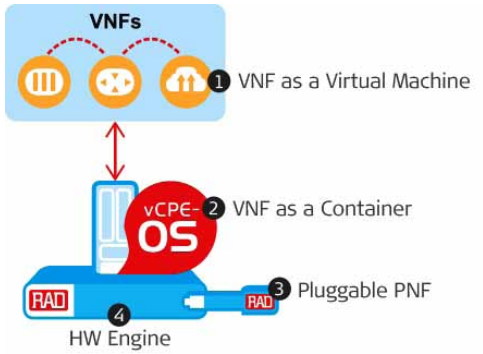
Junos Space Security Director: è una funzione che permette di eliminare il lavoro manuale tramite un framework intent-based che crea e applica le policy in base al mutare delle condizioni di rete. In pratica, permette ai team della sicurezza di definire policy di sicurezza basate sui metadati che vengono forniti dai diversi ambienti. Con questa nuova funzione il tempo dedicato alla gestione delle regole del firewall, evidenzia l'azienda, può essere ridotto di oltre l'80%.

- **Advanced Threat Prevention Appliance con One-Touch Mitigation:** è un nuovo dispositivo che costituisce il complemento on-premise del prodotto Sky Advanced Threat Prevention disponibile via cloud. Entrambi sfruttano le tecnologie di remediation e analytics di Cyphort per fornire visibilità sui comportamenti delle minacce e mitigazione one touch, riducendo i tempi di reazione agli incidenti.
- **SRX4600 Next-Generation Firewall:** è un firewall di nuova generazione SRX Series, ottimizzato per la protezione degli ambienti di cloud privato, caratterizzato da alte prestazioni e che è integrato con Security Director per disporre di una visione unificata degli ambienti di sicurezza aziendali.

«Questi aggiornamenti alla nostra piattaforma di cyber sicurezza SDSN permetteranno ai team preposti alla sicurezza di risparmiare tempo e denaro grazie all'automazione pur continuando a poter contare sull'esperienza dei professionisti della sicurezza», ha commentato Mihir Maniar, Vice President per il Security Product Management di Juniper Networks

RAD SEMPLIFICA SVILUPPO E INTEGRAZIONE DI SOLUZIONI VNF

Un sistema operativo per i vCPE permette ad aziende e operatori di fruire facilmente di nuove funzioni VNF e di semplificare la gestione end-to-end



Con l'obiettivo di permettere la realizzazione di reti in modo semplice e adattabili facilmente alle esigenze di fornitori di servizi a valore aggiunto e degli utilizzator, RAD ha espanso il suo portfolio di soluzioni di rete geografica con nuove funzionalità di software defined WAN, con l'obiettivo ulteriore di consolidare e rafforzare la propria posizione di fornitore di soluzioni per reti di accesso nel campo delle reti virtuali.

In pratica, alla base dell'approccio RAD c'è un sistema operativo carrier class unico per tutti gli uCPE del suo portfolio.

Tramite questa e altre funzionalità e caratteristiche delle soluzioni RAD, i cui prodotti sono distribuiti e supportati in Italia da CIE Telematica, osserva l'azienda, diventa possibile realizzare una integrazione morbida con qualsiasi orchestratore di servizi di rete, disporre di una Service Assurance per quanto concerne WAN e VNF (Virtual Network Function), disporre di dispositivi "pluggable" atti a semplificare il rollout a livello globale direte e servizi nonché controllare i dispositivi di rete tramite RADview e un apposito portale.

Ampie le possibilità che si aprono in termini di funzioni virtuali atte ad arricchire i servizi di rete. Ad esempio, ha illustrato l'azienda, è possibile incorporare nel dispositivo RAD come l'ETX 2i/2V, soluzioni SD-WAN di terze parti come Riverbed, Cloudgenix , nuagen networks o Citrix.

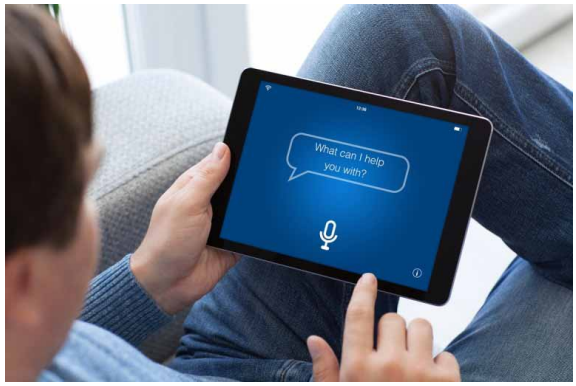
Il sistema operativo per i virtual CPE (vCPE-OS) abilita anche diverse possibilità di implementazione di VNF basate su software (ad esempio sotto forma di virtual machine o di container) così come diverse possibilità per quanto concerne PNF (Physical Network Function) basate su hardware e, nello specifico, sia sotto forma di hardware integrato che sotto forma di dispositivo "pluggable".

Il rilascio rafforza la posizione di RAD nel campo dei fornitori di soluzioni per reti virtuali, che costituiscono la nuova frontiera del networking per favorire la trasformazione digitale in atto e amplia le possibilità a disposizione della D-NFV Alliance (RAD's Distributed NFV Alliance), un ecosistema di sviluppatori di applicazioni e di fornitori di funzioni virtuali per reti che indirizza il mercato Enterprise, così come venditori di soluzioni di orchestrazione che forniscono software di gestione di reti e funzioni su base end-to-end, dal cloud alla sede dell'utente.

Una volta che le varie applicazioni sviluppate sono state testaste e approvate da RAD, vengono rese disponibili ai service provider su scala mondiale tramite le piattaforme vCPE in modo da abilitare una espansione dei servizi offerti al mondo Enterprise e alle SMB.

CITRIX 2018, SICUREZZA, CLOUD, INTELLIGENZA ARTIFICIALE E IOT

L'innovazione tecnologica che farà tendenza nei prossimi dodici mesi, secondo le previsioni di Citrix



Protagonista della trasformazione tecnologica inarrestabile è il cloud ibrido, secondo le previsioni degli esperti di Citrix, che tracciano le tendenze per il 2018. Anche se l'hybrid cloud è cresciuto meno delle aspettative nel 2017, per il prossimo anno gli analisti sono più positivi.

In particolare, PJ Houg, senior vice presidente Chief Product Officer di Citrix sostiene: «C'è una convergenza reale tra le tecnologie che agiscono con l'obiettivo di unificare i migliori luoghi di lavoro attraverso il cloud».

Il manager aggiunge: «Il cloud ibrido unifica tutte le applicazioni, sia enterprise sia on-premise e sia cloud o mobili, provenienti da tutte le piattaforme e le distribuisce in maniera coerente su qualsiasi dispositivo».

Quanto sostenuto da Citrix è che il cloud fornirà alle persone la flessibilità di cui necessitano e all'IT il livello di sicurezza indispensabile.

Inoltre, il luogo di lavoro sarà sempre meno legato a uno spazio fisico e l'uso del cloud semplificherà «il movimento delle persone non solo nello spazio, ma all'interno dei progetti e permetterà di trasferire facilmente gli skill da una parte dell'azienda all'altra», afferma Hough.

Christian Reilly, vice president, Global Product and Tech Strategy di Citrix sancisce, ma nel lungo termine, la fine di mouse e tastiere: «La voce sarà la principale "interfaccia" uomo-macchina, rappresentando un fattore determinante per l'innovazione nel 2018. Per le imprese che vogliono innovare, saper usare la voce, abbinata all'intelligenza artificiale per interagire con dati complessi sarà un fattore critico di successo».

Gli analytics, secondo il manager, consentiranno di essere sempre più produttivi. Inoltre, i tool di analytics sono utili anche per la sicurezza, afferma il manager: «Si può pensare agli analytics come a una forma di apprendimento automatico che crea la fotografia dei comportamenti usuali di un utente e rileva eventuali anomalie applicando controlli di sicurezza nel momento in cui si rendono necessari».

Anche l'IoT (Internet of Things) può essere visto come strumento utile alla sicurezza, invece che come elemento di rischio, sostiene Steve Wilson, vice president Cloud and IoT di Citrix: «Dispositivi come tecnologie beacon Bluetooth, GPS, biometria, riconoscimento facciale, insieme con analytics pervasivi sul comportamento dell'utente, daranno un contributo decisivo alla sicurezza facendo in modo che le persone accedano alle informazioni cui devono accedere».

CYBERARK AUTOMATIZZA LA PROTEZIONE ON-PREMISE E NEL CLOUD DEGLI ACCOUNT

Proteggere le credenziali è un punto chiave per la sicurezza degli utenti privilegiati, sia on-premise che nel cloud. A garantirla ci ha pensato CyberArk

Per garantire la sicurezza degli account privilegiati CyberArk, società specializzata nella protezione ad alto livello di questo tipo di utenti business critici per le aziende a causa dei dati riservati di cui sono sovente in possesso, sia quando operano dal loro ufficio che quando si trovano in mobility e accedono alle applicazioni e ai dati mediante dispositivi mobili, ha inglobato nel suo portfolio numerosi sviluppi che permettono di accelerare l'adozione di soluzioni di sicurezza che si posizionano tra quelle più avanzate disponibili sul mercato.

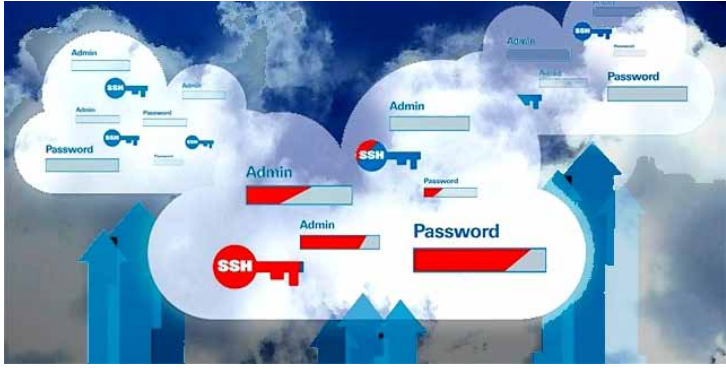
Le funzionalità hanno l'obiettivo primario di rendere più semplici le modalità necessarie per rafforzare la sicurezza, migliorare l'automazione dei processi di security e ridurre il rischio complessivo in cui possono incorrere gli utenti privilegiati.

Nel loro insieme, evidenzia CyberArk, fanno di CyberArk Privileged Account Security Solution V10 (CyberArk V10) una piattaforma di sicurezza che può facilmente scalare in funzionalità al fine di proteggere da exploit critici gli account privilegiati ovunque si trovino, sia quando utilizzano infrastrutture ICT on-premise che quando accedono ad applicazioni e dati tramite ambienti cloud ibrido o attraverso workflow DevOps.

Accelerazione dei processi di sicurezza

Un punto chiave di CyberArk v10 è di accelerare fortemente il deployment di una soluzione di sicurezza e semplificare i processi di protezione degli account privilegiati. L'obiettivo è perseguito tramite:

- **User experience semplice e snella:** gli aggiornamenti apportati con la V10 hanno perseguito l'obiettivo di ridurre di un ordine di grandezza il tempo che deve essere dedicato per garantire la protezione dei privileged account e allo stesso tempo ridurre di un fattore 5 l'impegno che deve essere dedicato dagli auditor IT nell'analisi delle registrazioni delle sessioni. La nuova user interface semplifica anche i workflow, visualizza i rischi, monitorizza le attività privilegiate ed è compliant con quanto prescritto da policy e Audit.
- **Strategia Customer-Driven basata su API:** Si basa su API funzionalmente estese che permettono di accelerare l'integrazione della soluzione CyberArk Privileged Account Security all'interno dell'architettura di sicurezza esistente, delle Operation e degli strumenti DevOps. Ad esempio, nuove REST API danno la possibilità ai responsabili IT di ridurre di sino al 90% il tempo necessario per inserire nel sistema di sicurezza gli account, un aspetto questo molto critico in aziende di ampie dimensioni che devono distribuire e fornire la sicurezza a migliaia di utenti contemporaneamente.



Machine learning per una protezione ubiqua delle credenziali

La crescente mobilità di personale e manager che costituiscono account privilegiati e l'utilizzo di reti mobili e cloud per accedere ai dati e collaborare pone il problema di come proteggere adeguatamente le credenziali in contesti ad alto rischio, sia per le carenze nei criteri di security che possono essere native delle reti o del cloud pubblico utilizzato, che dell'ambiente pubblico in cui l'account privilegiato fisicamente si muove. Credenziali non adeguatamente protette costituiscono un target molto attraente per gli attaccanti esterni o per malintenzionati interni all'azienda stessa.

Si tratta di rischi che sono amplificati per quelle aziende che hanno fatto del cloud la loro strategia di digital transformation e hanno allo stesso tempo accelerato l'adozione di DevOps.

Indipendentemente dalle dimensioni dell'azienda, le nuove funzionalità presenti nella versione V10 di CyberArk Privileged Account Security Solution sono volte a permettere di :

- **Prevenire l'attacco ad account privilegiati sugli Endpoint:** Gli end-point costituiscono uno dei punti maggiormente critici per la sicurezza, soprattutto per la crescente mobility degli utenti privilegiati. Per eliminare il rischio connesso alla perdita di dati o credenziali, CyberArk ha sviluppato CyberArk Endpoint Privilege Manager, una soluzione che ha il compito di bloccare e contenere attacchi dannosi proteggendo l'end-point da exploit che mirano alle credenziali privilegiate. In pratica, tramite le funzionalità contenute in CyberArk Application Risk Analysis Service si ha la possibilità, mediante funzioni di machine learning e analitiche basate su cloud, di aiutare a bloccare gli attaccanti e impedire, rilevando le applicazioni potenzialmente dannose e in grado di accedere a dati e informazioni sensibili, che questi possano posizionarsi in un end-point.
- **Accelerare la sicurezza nel Cloud:** V10 estende il supporto per Amazon Web Services (AWS), automatizza il caricamento delle credenziali tramite l'integrazione con CloudWatch e Auto Scaling. In pratica, viene ridotto significativamente il rischio di credenziali non gestite in ambienti di elastic computing e il team dedito alla sicurezza ha la possibilità di ridurre sensibilmente il tempo che vi deve dedicare in modo da potersi meglio focalizzare sulla mitigazione dei potenziali rischi. CyberArk garantisce anche la sicurezza delle credenziali attraverso piattaforme cloud pubbliche quali AWS, Microsoft Azure e Google Cloud Platform (GCP) ed ha validato la sua capacità di attivare la sicurezza per account privilegiati su AWS in un massimo di 15 minuti.

Per quanto concerne il cloud e le funzionalità di CyberArk Privileged Account Security Solution v10 relativamente alla Google Cloud Platform (GCP), la tipica configurazione GCP comprende l'esecuzione delle vault primarie e di disaster recovery, nonché il monitoraggio della sessione in modo da rendere sicuro il workload che gira in un ambiente nativo GCP.

L'organizzazione aziendale può, in alternativa, estendere la propria installazione di CyberArk (ad esempio che gira su piattaforma on-premise, AWS o Azure) in modo che possa aiutare nel rendere sicuro anche l'accesso alla console GCP e a renderne sicuri i relativi workload.

CON VEEAM RECOVERY DATI AL SICURO SU MICROSOFT AZURE

Con la nuova soluzione, Veeam consente di sfruttare Microsoft Azure per la continuità operativa di eliminare il costo di un sito di ripristino dedicato

Albert Zammar di Veeam

Veeam Software, fornitore di soluzioni per l'Availability for the Always-On Enterprise, ha annunciato la disponibilità di Veeam Recovery to Microsoft Azure with Veeam PN (Powered Network).

La soluzione on-demand, che è già disponibile, ha l'obiettivo di assicurare una rapida continuità operativa e include anche il nuovo prodotto gratuito, Veeam PN, una soluzione software defined networking (SDN che elimina la necessità di creare VPN e semplifica la configurazione di rete quando si vuole creare un sito di ripristino su Microsoft Azure.

Veeam Recovery to Microsoft Azure fornisce in pratica, osserva Veeam, un mezzo semplice e sicuro per il recupero dei carichi di lavoro on-premises su cloud pubblico. Con Veeam Availability Suite, i responsabili IT possono avviare automaticamente un'istanza cloud Azure ed erogare in modo sicuro servizi a clienti, partner e dipendenti ovunque essi siano, il tutto senza il costo di un sistema ridondante di standby.

A livello funzionale la nuova soluzione, fornita pronta all'uso, abilita il ripristino cloud per i backup Veeam ed è arricchita come accennato da Veeam PN, una soluzione SDN per definire un sito di ripristino in Microsoft Azure.

Veeam Recovery to Microsoft Azure con Veeam PN fornisce un recupero dati basato su cloud e permette di evitare le spese connesse alla costruzione e manutenzione di un sito remoto di ripristino di proprietà.

«Con Veeam Recovery to Microsoft Azure, i dirigenti e gli imprenditori possono dormire sonni tranquilli, sapendo che, in caso di disastro, l'azienda continuerà ad operare nel cloud pubblico - senza spendere una fortuna od occupare tutto il tempo del personale IT», ha commentato **Danny Allan**, Vice President Product Strategy di Veeam.

Veeam Recovery to Microsoft Azure con Veeam PN è stato espressamente progettato, ha illustrato l'azienda, per semplificare e automatizzare la configurazione di un sito di ripristino in Microsoft Azure riducendo la complessità delle implementazioni di VPN, indipendentemente dalle dimensioni delle aziende o dei service provider e fornisce un collegamento di rete sicuro tra le risorse IT locali e quelle in Azure mediante una connettività da sito a sito.

Veeam assicura la business continuity ai clienti di KPNQwest

Una conferma del livello di sicurezza e di business continuity garantite dalle soluzioni Veeam arriva dalla decisione di KPNQwest di adottarne le soluzioni per garantire la continuità operativa ai propri clienti.

KPNQwest Italia, società nazionale che offre servizi di telecomunicazioni su tutto il territorio italiano, ha scelto Veeam Backup Replication Enterprise Plus per supportare l'efficienza, la visibilità e la scalabilità su diversi ambienti IT, oltre a supportare i propri clienti nel percorso di Digital Transformation caratterizzato dalla disponibilità dei dati "Always On" e dalla rapidità di ripristino.

KPNQwest Italia fornisce a migliaia di aziende italiane servizi di connettività in fibra ottica, data center e cloud computing ad altissima affidabilità e performance. Tali servizi sono erogati a partire da quattro data center proprietari, ubicati presso il "Fiber Hub" italiano di via Caldera a Milano ed attraverso una rete di accesso in larga banda nazionale.

«Ciò che ci contraddistingue nel settore dei Cloud Service Provider è l'alta specializzazione dell'infrastruttura. L'offerta KPNQwest Italia unisce l'affidabilità, la sicurezza, le prestazioni e la resilienza della propria infrastruttura di data center alle migliori tecnologie hardware e software per il cloud computing disponibili, per creare il servizio di Virtual Data Center tra i migliori presenti sul mercato», ha osservato Matteo Flavi, product manager di KPNQwest Italia.

Tra le soluzioni per l'always-on sul mercato, ha evidenziato l'azienda, la soluzione Veeam è stata quella che si è rivelata più matura ed idonea per il mondo degli Internet Service Provider rispetto a soluzioni più complesse ma carenti di funzionalità fondamentali, come ad esempio il restore agentless su qualunque sistema operativo ed ancora di più le funzionalità di multicloud.

«Siamo orgogliosi di essere stati scelti da KPNQwest Italia per tante ragioni diverse. Ci hanno scelto per la nostra indiscussa superiorità tecnologica e perché moltissimi dei loro clienti, che utilizzavano già la soluzione Veeam, ne hanno promosso presso KPNQwest la semplicità, la scalabilità e la perfetta integazione con gli ambienti cloud. Questo per noi è un apprezzamento molto importante per l nostra tecnologia da parte dei nostri clienti, e ci lusinga molto», ha commentato **Albert Zammar**, SEMEA Vice President di Veeam Software.

RETELIT RILASCIA LA TECNOLOGIA SOFTWARE DEFINED-WAN

La Software Defined WAN semplifica la gestione delle reti ibride e ottimizza le prestazioni nel cloud. E' Retelit la rete e il Virtual Data Center in Bonfiglioli

Federico Protto di Retelit

Retelit, uno dei principali operatori di servizi dati e infrastrutture nel settore delle telecomunicazioni, ha annunciato la disponibilità della tecnologia SD-WAN, una soluzione inserita nel portfolio per le aziende. La funzionalità di nuova generazione permette di trasformare le infrastrutture di rete in piattaforme dinamiche e intelligenti integrando tecnologie di accesso, compresi i servizi di rete internet, il routing dinamico, bandwidth on demand, QoS e servizi di Sicurezza informatica.

L'introduzione di questa nuova generazione di reti si inserisce nella strategia aziendale incentrata all'internazionalizzazione, alla qualità dei servizi e alla piena integrazione con l'hybrid cloud.

«Con questo lancio Retelit si conferma sempre più un provider di connettività e servizi ICT. Le organizzazioni oggi hanno infatti sempre più bisogno di flessibilità, reattività e sicurezza; negli ultimi anni si è assistito all'emergere di nuove necessità dovute per lo più alla delocalizzazione di utenti e data center. Retelit, grazie ad accordi con vari operatori esteri e all'implementazione di questa nuova tecnologia, risponde all'esigenza di controllare e proteggere le reti in Italia e all'estero semplificando la gestione e velocizzando i processi», ha commentato l'annuncio **Federico Protto**, Amministratore Delegato e Direttore Generale di Retelit.

La tecnologia SD-WAN, ha evidenziato l'azienda, porta infatti con sé alcuni importanti vantaggi. Fornisce ad esempio la possibilità di automatizzare il processo di delivery e la gestione dei collegamenti tra le differenti sedi, rendendoli autonomi nella configurazione di rete della propria WAN.

Ad esempio, la nuova rete SDWAN - grazie all'intelligenza in cloud - consente alle aziende di gestire i flussi di dati in maniera differenziata, quelli con un minor livello di priorità per il business possono essere riversati su una connettività meno pregiata, liberando la banda per i dati più importanti e accrescendo in questo modo la larghezza di banda totale.

«L'utente oggi vuole una trasmissione sicura senza però avere un aumento nei costi di implementazione. La tecnologia SD-WAN dà alle aziende la possibilità di ottenere prestazioni in maniera efficiente ed economica, perché consente di appoggiarsi a tecnologie di connessione diverse ed usufruire servizi di gestione della qualità del servizio, bandwidth on demand, cyber security e application performance in grado di reagire alle alterazioni della rete adattandosi ai cambiamenti e, infine, di dare la possibilità all'utente di confi-

gurarsi in autonomia la propria rete. Queste caratteristiche la rendono inoltre sicura, affidabile e flessibile ed automaticamente integrata verso il mondo del cloud», ha osservato **Luca Cardone,** Marketing Manager di Retelit.

Bonfiglioli migra in Retelit rete e Virtual Data Center

Una conferma di come l'approccio Retelit risponda alle esigenze di mercato delle aziende italiane viene dalla scelta fatta da Bonfiglioli Italia S.p.A., azienda italiana con una forte presenza a livello globale che realizza soluzioni per il controllo e la trasmissione di potenza nell'industria e nelle macchine operatrici semoventi. La società manifatturiera si è rivolta a Retelit per la rete in fibra e il virtual data center.

Nello specifico, con le soluzioni e i servizi di Retelit nella creazione di un servizio di Virtual Data Center dedicato a ospitare gli ambienti SAP, il gruppo Bonfiglioli ha voluto migrare da un'infrastruttura IBM Legacy a un'infrastruttura virtuale basata su architettura x86, database SQL e sistemi Windows.

«La collaborazione con Retelit ci ha permesso un aggiornamento modulare ed efficace delle nostre architetture informatiche senza rischi di salti nel vuoto. Grazie all'operatore possiamo, con più tranquillità, volgere lo sguardo al futuro per poterci adeguare facilmente ai sistemi operativi più all'avanguardia, sfruttando i servizi offerti da Retelit. Del team sales e operations dell'azienda abbiamo apprezzato soprattutto la velocità, la qualità del delivery, la reattività e il livello di customizzazione e cura dei servizi», ha dichiarato **Enrico Andrini,** CIO di Bonfiglioli.

La fornitura di Retelit ha permesso di ottenere un duplice risultato. Da un lato ha permesso a Bonfiglioli di continuare la digital transformation in atto senza stravolgere l'intera rete di servizi e mantenendo gli ambienti SAP preesistenti. Dall'altro, tramite la propria connettività di rete in fibra ottica ha collegato l'infrastruttura su cui poggia l'intera produzione della Bonfiglioli ai suoi Virtual Data Center.

La creazione di un pool di risorse di computing dedicato e di un cloud storage, uniti ad un servizio di backup gestito da tecnici e professionisti Retelit, permettono ai fini operativi e di business un controllo continuo dell'intera struttura e una migliore garanzia di ottenere gli obiettivi di business.

«Con quest'intervento Bonfiglioli può adottare soluzioni cloud attraverso un processo modulare, preservando gli investimenti e utilizzando infrastrutture tecnologiche qualitativamente elevate», ha commentato **Federico Protto**, Amministratore Delegato e Direttore Generale di Retelit -

Le soluzioni che fanno parte della fornitura di Retelit sono integrate anche con sistemi che contemplano la creazione di Virtual Firewall di protezione perimetrale degli ambienti SAP e prevedono la creazione di un Disaster Recovery plan nell'ottica della Business Continuity e della semplificazione del processo del recupero dati.

COSA HA INSEGNATO IL 2017 SULLA SICUREZZA NEL CLOUD?

La sicurezza nel cloud pubblico e privato è in continua evoluzione. Equinix ha fatto il punto su cosa ha insegnato il 2017 e che suggerimento se ne può trarre

La sicurezza in ambito cloud continua ad essere un argomento importante tra le aziende e, dato che oltre il 90% delle imprese utilizza una forma di cloud computing pubblico, continua a essere dibattuta tra i professionisti della sicurezza.

La sicurezza nel cloud pubblico e privato è però una tecnologia in evoluzione ed è un tema che abbiamo approfondito con gli esperti di Equinix, Vediamo le considerazioni salienti fatteci dall'azienda.

Nonostante le molteplici violazioni aziendali alla sicurezza informatica avvenute nel 2017, le principali piattaforme cloud pubbliche hanno mostrato una promettente capacità nel mantenere sicure le applicazioni e i dati aziendali.

L'intelligenza artificiale (AI) e il machine learning (ML) sono al centro di molte delle nuove funzionalità che i principali fornitori di servizi cloud stanno utilizzando per offrire un servizio di sicurezza più intuitivo e dinamico ai loro clienti.

Ad esempio, durante la sua recente conferenza Re:Invent, Amazon Web Services (AWS) ha annunciato funzionalità di sicurezza che sfruttano l'intelligenza artificiale per identificare indirizzi IP dannosi e rilevare anomalie.

Questa utilizza inoltre la tecnologia ML per riconoscere attività o comportamenti che indicano minacce, ad esempio un malintenzionato che esegue una scansione di server web in cerca di vulnerabilità di applicazioni conosciute. SI assiste al fatto che AI e ML continuano a svolgere un ruolo importante nella lotta proattiva alla sicurezza informatica nel cloud.

La gestione delle chiavi nel cloud ibrido e nel multicloud

La maggior parte dei CSP offre soluzioni di gestione delle chiavi d'identità ai propri clienti per aiutare a coordinare l'accesso ad applicazioni e dati all'interno di un'unica soluzione di piattaforma cloud.

Tuttavia, il crescente numero di infrastrutture aziendali ibride e multicloud, osserva Equinix, ha posto l'esigenza di avere soluzioni di gestione delle chiavi che forniscano copertura su più cloud e/o infrastrutture on-premise. In proposito, Equinix ha annunciato una beta pubblica per la sua soluzione SmartKey HSM-as-a-Service, un modulo di sicurezza hardware (HSM) indipendente dal cloud.

Sicurezza più vicina alle cose da proteggere

Mentre il perimetro IT aziendale si offusca e diventa più distribuito e di ampia portata, le aziende devono modificare il proprio approccio all'implementazione dei diversi controlli di sicurezza, e non solo per il cloud. Detto questo, il confine digitale di un'azienda, un luogo in cui il commercio, le persone e gli ecosistemi digitali si incontrano, deve essere preparato per applicazioni multicloud e flussi di dati che servono utenti e cose su più reti globali e servizi cloud. Adottando politiche di sicurezza cloud al confine e abbracciando una strategia di sicurezza del tipo "non fidarsi di nessuno", assicura che le protezioni critiche possano essere implementate laddove sono più efficaci e non abbiano alcun impatto sulle prestazioni o sulla qualità dell'esperienza dell'utente.

Una sicurezza basata su Governance, Rischio e Conformità

Il termine "governance, rischio e conformità", o GRC, descrive un insieme di attività o una piattaforma che pervade tutti i dipartimenti e le funzioni di un'organizzazione, consentendo a un'azienda di raggiungere i propri obiettivi aziendali, affrontare l'incertezza e agire con integrità. E il GRC non si ferma qui.
Può anche includere funzionalità di garanzia e gestione delle prestazioni rispetto a tali obiettivi di business. Secondo Scott Wisniewski, managing director presso la società di consulenza globale Protiviti, lo straordinario aumento della quantità di dati che le organizzazioni devono analizzare, insieme all'adozione diffusa delle tecnologie cloud e mobile, indica che una maggiore raccolta, condivisione e collaborazione delle informazioni porta le organizzazioni a "ripensare la loro intera infrastruttura GRC".

Prima o poi capita

L'anno passato da poco ha impartito lezioni senza precedenti sulla sicurezza. Letteralmente miliardi di account online sono stati violati e sono stati esposti dati personali sensibili per centinaia di milioni di persone. Anche gli animali di peluche "intelligenti" sono stati complici nel perdere milioni di registrazioni audio tra bambini e genitori. Le persone e le aziende, mette in guardia Equinix, devono essere consapevoli che qualsiasi tecnologia online è soggetta a compromessi. Applicare ciò che si è appreso dai primi quattro insegnamenti si rivelerà più importante che mai nel 2018.

VINCENTI E PROSPERE LE AZIENDE DATA VISIONARY

Abbracciare il cambiamento e la trasformazione digitale rende vincenti. Lo evidenzia una ricerca NetApp

NetApp ha annunciato i risultati di un programma di ricerca globale incentrato su come supportare le aziende ad abbracciare la trasformazione digitale. Realizzato in partnership con IDC, lo studio suggerisce azioni immediate e d'impatto che ogni azienda può mettere in campo per trasformarsi. I risultati della ricerca mostrano infatti cos'è che separa i Data Thriver (termine che indica chi ha successo sfruttando le potenzialità dei dati), aggressivi nell'uso delle tecnologie digitali per influenzare nuovi mercati, da coloro che sono semplicemente Data Survivor o addirittura Data Resister. Con solo l'11% di aziende che rientrano nel profilo di Data Thriver, mette in guardia NetApp, le aziende nei settori tradizionali rischiano di perdere una percentuale significativa delle loro entrate a favore di imprese più orientate verso i dati già nel 2018. I settori più a rischio sono quello dei servizi pubblici (29%), il commercio al dettaglio (> 25%), il settore delle attrezzature industriali (20%), i servizi finanziari (18%) e la pubblica amministrazione (18%). Le aziende che utilizzano dati per guidare il proprio business e soddisfare i clienti in modi nuovi e innovativi, hanno appena cominciato a rivoluzionare il mercato.

«I Data Visionary ispirano le loro organizzazioni ad essere Data Thriver. Riconoscono che i dati non sono più rinchiusi in dispositivi nascosti dietro firewall. Ora sono distribuiti, dinamici e diversificati», ha dichiarato **Jean English**, SVP e CMO di NetApp. «La nostra missione è supportare le aziende attraverso il processo di trasformazione digitale, offrendo servizi di cloud ibrido che migliorano radicalmente l'efficienza organizzativa e creano nuove opportunità di business».

Come aver successo

Ma come fanno i Data Thriver ad avere successo nel busness? In sostanza adottano misure per aumentare i ricavi, migliorare i risultati aziendali e trasformare i dati in denaro. Molte aziende Fortune 100 stanno costruendo in proposito laboratori di innovazione, oltre a creare nuovi ruoli manageriali che hanno come obiettivo l'innovazione e addetti al data management. Delle organizzazioni che hanno partecipato allo studio, quasi la metà ha già un Chief Data Officer.

Come contraltare i Data Survivor stanno perdendo opportunità di guadagno, non utilizzando i dati per migliorare la soddisfazione dei

propri clienti e rischiando di essere sopraffatti da quelli che producono. Utilizzano gli strumenti più disparati per gestire i dati in diversi formati e diverse postazioni, aggiungendo una complessità ulteriore alla gestione di sicurezza, rischio, privacy e conformità.

Imparare dai Data Thriver

Le organizzazioni che mostrano comportamenti Data Thriver stanno adottando una serie diversificata di tecnologie, inclusi i servizi dati per cloud ibridi. Questi servizi comprendono diverse funzioni di protezione, sicurezza, integrazione e ottimizzazione dei dati per una gestione agile ed economica e analisi più rapide. Le tre cose principali che i Data Survivor possono imparare dai Data Thriver sono:

- Utilizzare i dati come asset organizzativi
- Permettere ad IT e manager di lavorare insieme
- Creare mappe per la visibilità e il controllo dei dati

Le organizzazioni che cercano di passare da Data Survivor a Data Thriver, suggerisce la società, devono trasformare in maniera olistica persone, processi e tecnologie e creare una roadmap di trasformazione digitale che dovrebbe includere:

- La creazione di nuovi ruoli
- L'impostazione di nuovi modelli di personale
- L'Istituzione di nuovi processi
- Nuovi investimenti
- L'utilizzo di servizi dati per cloud ibrido

Lo studio si è basato su un'indagine globale su 800 linee di dirigenti aziendali, leader IT e lavoratori esperti in tecnologia di grandi e medie imprese. Gli intervistati sono decision maker con controllo sul budget o capacità di influenzare la spesa di bilancio per progetti DX, che sono stati coinvolti in progetti DX per l'azienda e sono stati responsabili della valutazione o dell'architettura di almeno due servizi dati per il cloud ibrido.

COME ADEGUARE LA SICUREZZA ALLA RAPIDITÀ DEL BUSINESS

Le organizzazioni spendono di più in sicurezza ma le perdite non diminuiscono. Cosa fare lo suggerisce Rodolfo Rotondo di VMware

Rodolfo Rotondo di VMware

I modelli di business continuano a trasformarsi, le persone e i dispositivi stanno diventando sempre più connessi e le organizzazioni stanno ora cavalcando sia il mondo fisico che quello digitale. Ma quale approccio dovrebbe essere preso in risposta alle nuove esigenze via via emergenti? In che modo le organizzazioni possono garantire la sicurezza e la conformità dei dati e allo stesso tempo abilitare l'innovazione? Tre suggerimenti li propone **Rodolfo Rotondo**, Senior Business Solution Strategist EMEA VMware. Vediamoli in dettaglio.

Il problema del perimetro

La sicurezza, sin dall'inizio, si è concentrata sulla protezione del "perimetro": tutto, dai fossati nei castelli alle serrature sulla porta d'ingresso e, nel mondo moderno, alle telecamere a circuito chiuso e ai firewall. Nel mondo degli affari di oggi, tuttavia, la trasformazione digitale ha portato ad ambienti dinamici con dipendenti dislocati geograficamente, utilizzando molti dispositivi diversi con una mobilità abbastanza buona universalmente. In questo contesto, qual è l'equivalente del fossato per l'IT? Cosa dovrebbe effettivamente cercare di proteggere un'organizzazione in questo nuovo mondo?

L'approccio tradizionale alle esigenze di sicurezza deve essere rivolto verso l'interno. Non ci si può aspettare che la sicurezza della rete perimetrale protegga lo scenario sempre mutevole di applicazioni e utenti quando non è possibile definire dove sia il "perimetro", o anche se ne esistesse uno. Serve rivedere il concetto di base della sicurezza IT, inserendolo come una qualità intrinseca in tutta l'infrastruttura, piuttosto che solo ai suoi margini. Le aziende possono ottenere ciò sfruttando livelli software comuni come l'hypervisor per l'infrastruttura applicativa e una piattaforma di gestione della mobilità aziendale per endpoint e identità utente.

IT frammentato

Se i perimetri aziendali esterni si sono quasi dissolti, anche i perimetri interni stanno cambiando per quanto riguarda la proprietà dell'IT e della sicurezza. Il cloud computing offre agli utenti di tutto il business un accesso rapido e diretto a dati, applicazioni e servizi, quando lo desiderano, indipendentemente da dove si trovano e da quali dispositivi stanno utilizzando.
Tuttavia, poiché le line of business e i dipendenti sempre più spesso sono proprietari della tecnologia che utilizzano, diventa sempre più

difficile ottenere una reale visibilità dell'IT all'interno delle organizzazioni, il che significa che le aziende possono facilmente perdere il controllo.
Il movimento dei tradizionali silos tra l'IT e il business sta spostando ruoli e responsabilità, ma questo non può comportare una mancanza di chiarezza su chi "possiede" sicurezza e conformità. Ciò richiede una piattaforma unica e unificata in cui le aziende possono eseguire, gestire, connettere e proteggere le applicazioni, tra dispositivi e cloud, e da cui l'IT può gestirli tutti con un'unica vista.

l'IT di domani

Il modo in cui sviluppiamo, gestiamo e consumiamo IT è in continua evoluzione. Quindi, come si fa a sapere come sarà questo scenario domani, per non parlare di come proteggerlo?
Se le aziende non possono implementare la sicurezza alla velocità dell'azienda, la sicurezza diventa un inibitore per il progresso e l'innovazione, piuttosto che un fattore abilitante.
Questo essere 'a prova di futuro' della sicurezza IT richiede un altro cambiamento nel modo di pensare. Tradizionalmente, la maggior parte della sicurezza riguarda la ricerca di "cattivi": monitoraggio continuo dell'intera infrastruttura per malware e per le violazioni in generale. Il problema con questo approccio è che si basa sulla conoscenza di ciò che è "cattivo" - in un mondo in cui la maggior parte delle minacce emergenti sono i cosiddetti attacchi "zero-day" che non sono mai stati visti prima, un livello decrescente di efficacia dovrebbe difficilmente apparire come una sorpresa.
La natura mutevole del panorama delle minacce, unita al ritmo accelerato e alla complessità del business, richiede chiaramente un'altra soluzione: meno tentativi di inseguire l'ignoto "cattivo" e maggiore garanzia che venga eseguito solo il noto "buono", come ad esempio, osserva il manager quella rappresentata da VMware AppDefense, che esegue il monitoraggio in tempo reale.

Quale futuro

Cosa si può dedurre da quanto detto? In sostanza che osservazioni e sviluppi convergono in un unico obiettivo: la necessità di stabilire una fonte comune di verità tra una soluzione di sicurezza e l'ambiente che ha bisogno di protezione. L'ambiente continuerà ad evolversi: l'innovazione e la trasformazione accelereranno e diventeranno ancora più radicali.
Ma con questa "verità", che deriva da una maggiore visibilità e una maggiore comprensione del contesto, le aziende saranno maggiormente in grado di dare un senso alla loro sempre più frammentata e complessa impronta IT per offrire protezione alla velocità richiesta, per garantire, abilitare e innovare, per rimanere competitivi e guidare prestazioni sempre migliori.