Cloud & Business

n.95
Novembre 2020

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

IN QUESTO NUMERO>>>

LE BEST PRACTICE PER LA CYBER SECURITY DI END-POINT E NEL CLOUD

di Giuseppe Saccardi

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

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

La crisi sanitaria, evidenzia **Paolo Lossa**, Country Sales Manager di CyberArk Italia (cyberark.com), ha influenzato e influenzerà in modo significativo la nostra vita quotidiana e ci ha spinti a un utilizzo sempre più intenso delle tecnologie. E' una combinazione di fattori che ha stimolato la

Paolo Lossa - CyberArk Italia

Reportec Cloud&Business - N.95 Ottobre-Novembre 2020 - società- Editore: Reportec Srl (**www.reportec.it**) - Direttore responsabile: Giuseppe Saccardi - In redazione: Gaetano Di Blasio - Paola Saccardi - Immagini: Dreamstime.com

creatività dei cyber criminali che hanno sviluppato nuove tecniche di attacco volte a catturare i nostri dati sensibili, la cui vendita sul dark web è molto redditizia.
Ma cosa suggerisce Lossa? Innanzitutto che gli utenti devono conoscere i rischi informatici in cui potrebbero incorrere al fine di adottare l'approccio più appropriato per proteggere se stessi e i propri dispositivi. Molti aspetti della nostra vita quotidiana possono infatti diventare un punto di accesso per i cyber criminali, ma non tutti ne sono consapevoli.
Cinque i consigli suggeriti da Lossa per incrementare il livello di protezione. Vediamoli in sintesi:

1. Non fidarsi degli estranei: non bisognerebbe mai aprire messaggi o cliccare su link ricevuti da persone che non si conoscono, che si tratti di e-mail, messaggi su Slack, Teams o Google Chat.
2. Monitorare la salute va bene, farsi rubare i dati, no: Fitness tracker e orologi "intelligenti" sono un modo semplice per tenere sotto controllo la propria forma fisica, purtroppo però raccolgono molti dati personali. Chi li utilizza deve quindi assicurarsi di sapere esattamente come vengono utilizzati, archiviati e protetti i dati personali dalle differenti aziende.
3. Non raccontare troppo sui social network: Se questi canali permettono di condividere le passioni e i bei momenti con le persone care, bisogna fare attenzione a non condividere informazioni personali che potrebbero essere utilizzate per determinare password e domande di sicurezza, indicare un luogo o prevedere il comportamento.
4. Proteggere lo smartphone. I cellulari hanno assunto il ruolo di assistente personale, sia in ambito privato che professionale, ma sono vulnerabili agli attacchi. Pertanto, è importante verificare a quali dati ogni applicazione ha accesso. Inoltre, processi di autenticazione come l'autenticazione a più fattori aiutano a garantire che gli smartphone non vengano sfruttati dagli aggressori per rubare dati personali.
5. Proteggere l'Internet of Things. Nei prossimi dieci anni, ogni consumatore avrà almeno 10 dispositivi collegati e, se non sono sicuri, ognuno di essi rappresenterà un modo per rubare dati sensibili. I dispositivi IoT, come le smart TV e i contatori collegati, sono sicuramente utili, ma richiedono molte informazioni e connessioni per funzionare correttamente. Per metterli in sicurezza e chiudere tutti gli accessi alla rete, è necessario fidarsi solo di produttori rinomati, applicare ogni patch di sicurezza disponibile e aggiornare le loro password di default.

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

LA CRITICITÀ DI AMBIENTI SAAS

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

SI prenda ad esempio gli attacchi di phishing di Office 365. Negli ultimi mesi si è osservato che questo approccio mira a token temporanei (aka access token) generati per consentire il Single Sign-On per Microsoft 365 e tutte le applicazioni Microsoft.

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

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

All'interno di queste applicazioni SaaS, possono rubare le credenziali e compromettere le identità digitali dei dipendenti, in particolare di utenti privilegiati, accedere ai dati sensibili inclusi in questi strumenti di collaborazione, report giornalieri e dati finanziari.

A queste problematiche CyberArk ha risposto rendendo disponibili le proprie soluzioni di security tramite Cloud dal Marketplace Microsoft Azure. In pratica, i clienti Microsoft Azure hanno accesso alla soluzione di protezione degli accessi privilegiati di CyberArk e possono fruirne per definire le strategie aziendali

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

Il digital workplace nel portfolio BT con Zoom

L'accordo con Zoom Video Communications permette a BT di offrire un servizio gestito con rete integrata in grado di garantire una user experience ottimale

BT ha annunciato l'ampliamento delle proprie proposte di servizi gestiti di collaboration audio e video cloud-based riservate ai suoi clienti multinazionali, con l'inserimento a portfolio di Zoom Meetings. Fa seguito alla firma di un nuovo carrier agreement tra BT e Zoom Video Communications.

Con l'accordo BT, osserva l'azienda, diventa il primo provider globale ad offrire un servizio gestito di Zoom Meetings, caratterizzato dalla scelta di connettività e di integrazione con la propria rete voce globale.

Il servizio comprende anche il monitoraggio dell'esperienza end-to-end e garanzie di maggiore sicurezza.

Le diverse opzioni di connettività includono internet, SIP, PSTN o MPLS. BT offre anche opzioni di sicurezza come la crittografia delle comunicazioni, la protezione degli ID utente dei clienti, la connettività MPLS sicura, privata e resiliente, gateway di rete dedicati e programmi di adozione delle migliori pratiche di sicurezza.

L'accordo consente inoltre a BT di offrire Zoom Rooms, il sistema di sale conferenze modulabile basato su software Zoom.

«Stiamo semplificando le cose per i clienti, aiutandoli a creare ambienti di lavoro digitali sicuri e produttivi per i loro dipendenti, ovunque essi siano. Il nostro nuovo servizio gestito consente alle aziende globali, tipicamente con una complessa infrastruttura di rete e IT, di utilizzare Zoom Meetings in modo semplice, costante e sicuro con esperienze ottimizzate per le loro persone in tutto il mondo», ha commentato **Andrew Small**, direttore Global Portfolio di BT.

Difendere tutti con una protezione avanzata per Windows

Le migliorie apportate da ESET ai propri prodotti includono il rilevamento di malware e il supporto per la smart home, oltre alla protezione delle operazioni bancarie

ESET, attore globale nel mercato della cybersecurity, ha presentato al mercato le nuove versioni di prodotto dedicate alla sicurezza Windows per il settore consumer.

Va considerato che nell'epoca dello smart working la distinzione tra consumer e azienda si sta facendo sempre più labile e sono richieste soluzioni dalle prestazioni comunque elevate.

Le nuove release potenziano la sicurezza nelle soluzioni ESET Internet Security, ESET NOD32 Antivirus e ESET Smart Security Premium.

La gamma di migliorie alla sicurezza include il rilevamento di malware, la sicurezza delle password e il supporto per la smart home, in linea con l'obiettivo di ESET di creare un mondo digitale più sicuro per tutti e proteggere maggiormente gli utenti nelle loro attività online.

Gli upgrade dei software coinvolgono temi chiave, tra cui i pagamenti online e le minacce che coinvolgono operazioni bancarie, furto di identità e perdita dei dati personali, furto di password e sicurezza dei dispositivi connessi.

Altri aggiornamenti includono i nuovi scanner Windows Management Instrumentation (WMI) e System Registry in grado di rilevare malware che utilizzano WMI o il Registro di Sistema in modo malevolo.

Il modulo Connected Home, ha osservato ESET, è stato inoltre migliorato con una maggiore risoluzione dei problemi di sicurezza e rilevamento dei dispositivi connessi.

La sicurezza delle operazioni con le banche dispone di una speciale modalità browser protetta attraverso la quale è possibile effettuare transazioni online in sicurezza. La nuova funzionalità consente agli utenti di utilizzare qualsiasi browser supportato in modalità protetta per impostazione predefinita, assicurando che la comunicazione da tastiera e mouse al browser venga crittografata per scongiurare il keylogging.

Inoltre, Banking & Payment Protection ora avvisa gli utenti quando il Remote Desktop Protocol (RDP) è attivo per allertarli sul pericolo di un utilizzo malevolo.

Infine, ESET Password Manager è stato completamente riprogettato con nuove funzionalità come la disconnessione dai siti web e la cancellazione remota della cronologia di navigazione, sia tramite estensioni del browser sia per le app mobili native.

Commentando gli aggiornamenti, **Matej Krištofík**, Product Manager di ESET, ha affermato: «Poiché le minacce informatiche sono sempre più sofisticate e diffuse, è fondamentale che i consumatori e i loro dispositivi siano protetti a tutti i livelli. La tecnologia è al centro della nostra vita, dall'home banking alla smart home, quindi è più che mai importante che questa sia sicura e protetta. Siamo orgogliosi di offrire agli utenti i nostri ultimi aggiornamenti dei prodotti di sicurezza di Windows, che riflettono la nostra dedizione a migliorare e innovare costantemente al fine di fornire un'esperienza digitale più sicura per tutti».

Con Stormshield Endpoint Security Evolution più protette le workstation

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

In un mondo in cui la mobilità è diventata la norma e la tecnologia digitale permea ormai ogni settore aziendale, è sempre più importante garantire la costante protezione delle workstation, indipendentemente dal contesto in cui vengono utilizzate. E' però un obiettivo, osserva Stormshield, che comporta l'adozione di un nuovo approccio volto ad affrontare i tentativi dei cybercriminali di aggirare le soluzioni di sicurezza in essere, sfruttandone direttamente le eventuali falle.
E' quello che si è proposta di ottenere con Stormshield Endpoint Security (SES) Evolution per la messa in sicurezza delle postazioni di lavoro Windows combinando la protezione adattiva comportamentale e la tecnologia di analisi dei dispositivi fornita da SES con la capacità di identificare e investigare sull'origine degli attacchi.
«La nuova generazione di attacchi avanzati, (per esempio quelli che sfruttano le vulnerabilità zero-day) evidenzia l'incapacità della maggior parte delle soluzioni esistenti

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

Considerazione di base è che quando si è in movimento, la connettività non è sempre scontata. A differenza di soluzioni che utilizzano motori di analisi ospitati su server, i cui tempi di risposta possono essere troppo lunghi in presenza di un attacco o che non sono utilizzabili se il computer è offline o al di fuori della rete aziendale, Stormshield Endpoint Security Evolution si propone di fornire una difesa permanente, che il computer sia connesso o meno.

Inoltre, in alcuni ambienti sensibili, l'uso di soluzioni di sicurezza basate sul cloud può presentare rischi per la protezione dei dati. E' a queste situazioni che vuole permettere di far fronte Stormshield Endpoint Security Evolution.

L'obiettivo, spiega l'azienda, è perseguito combinando le funzioni di protezione delle workstation e di rilevamento. In pratica, Stormshield Endpoint Security Evolution blocca in modo proattivo il malware, gli attacchi alla memoria e gli exploit. La soluzione fornisce inoltre agli amministratori informazioni che consentono di comprendere meglio come si è verificato l'attacco al fine di risalire alle sue origini

Protezione sensibile al contesto

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

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

IN particolare, l'agente di SES Evolution modifica dinamicamente le proprie politiche di sicurezza adattandosi al proprio ambiente, in modo da dare un accesso più granulare alle applicazioni e alle risorse dell'azienda in base all'utilizzo.

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

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

Il servizio VoipCloud favorisce la digitalizzazione delle TLC aziendali

VoipCloud di VoipVoice è una piattaforma dedicata ai centralini VoIP che favorisce la transizione a infrastrutture digitali della telefonia aziendale

Il mercato del VoIP sta subendo - anche a fronte delle difficoltà oggettive riscontrate durante la prima ondata della pandemia - forti spinte verso la digitalizzazione. Un trend che non è sfuggito a VoipVoice, che ha rilevato quanto negli ultimi sei mesi il classico centralino fisico installato presso le sedi aziendali, e per molte organizzazioni ancora sinonimo di maggior sicurezza, sia risultato incapace di fornire la necessaria flessibilità e mobilità per garantire la continuità del business.

«Poter essere reperibili al proprio numero aziendale senza dover condividere i propri recapiti personali e utilizzare anche da remoto l'intera gamma di funzionalità di comunicazione e collaborazione delle moderne soluzioni per la telefonia ha fatto la differenza per molte imprese» ha osservato **Simone Terreni**, CEO di VoipVoice. E proprio l'esigenza di continuità e di maggior mobilità, unita alla sensibile riduzione dei costi di manutenzione tipica delle soluzioni virtualizzate, è assurta a driver essenziale per la migrazione a infrastrutture telefoniche ospitate nel cloud.

Simone Terreni, CEO di VoipVoice

Tuttavia, non tutte le PMI si avvalgono già di architetture cloud, né dispongono internamente di competenze sufficienti per calibrare un eventuale server virtuale in maniera adeguata a garantire il funzionamento di un centralino IP. Con VoipCloud, VoipVoice ha voluto mettere a disposizione delle imprese un servizio cloud TLC as-a-service perfezionato per l'hosting di IP-PBX.

«Con questo strumento, le aziende possono avviare con serenità il processo di transizione dalle tradizionali soluzioni hardware-based ad una completa digitalizzazione della propria infrastruttura per le

telecomunicazioni, assicurandosi nel contempo rapidamente un vantaggio competitivo, ovvero essere reperibili per i propri clienti e fornitori in qualunque situazione», ha aggiunto Terreni.
I server preposti all'erogazione del servizio VoipCloud sono ubicati al MIX (Milan-Internet-Exchange), principale centro di interscambio degli operatori TLC e garante di un'elevata qualità delle chiamate VoIP.
L'assistenza, il supporto per il setup e l'archiviazione dei dati hanno tutti luogo in Italia, per garantire la compliance con il GDPR.
Il servizio viene fornito a canone mensile con profili basati sul numero di chiamate contemporanee da condurre (4, 8 o 16), oltre che sicuro grazie a un firewall dedicato e personalizzabile in base alle esigenze. Ciascun taglio del VoipCloud dispone di un IP statico pubblico e è compatibile con i principali IP-PBX. L'azienda può infatti selezionare insieme al proprio partner il centralino che ritiene più adeguato alle proprie esigenze. Ma non solo. Osserva Terreni, VoipCloud è fruibile in maniera adattabile alle effettive necessità e il passaggio ad un profilo superiore è attuabile in qualsiasi momento.

CASE STUDY

La Digital Enterprise Transformation di TIM è firmata SAP S/4HANA

TIM aggiorna il sistema gestionale e punta sulla tecnologia intelligente di SAP e il cloud per una trasformazione digitale integrata in tutte le 24 società

Il Gruppo TIM ha fatto un passo verso l'innovazione e la digital transformation dell'intera organizzazione e ha scelto per farlo l'ERP SAP S/4HANA al fine di migliorare la gestione dei processi aziendali e supportare la crescita del business attraverso una semplificazione dei sistemi e una maggiore ottimizzazione delle risorse.
Il precedente sistema su cui poggiava l'infrastruttura del Gruppo, sempre basato su soluzioni SAP, non rispondeva più in modo adeguato ai processi di business, avendo raggiunto il suo potenziale di utilizzo, appesantito anche da una intensa customizzazione e un'eccessiva richiesta di manualità.
Tutto questo impediva all'area Finance di sfruttare leve e strumenti offerti oggi da SAP S/4HANA per prendere decisioni pertinenti e tempestive per una gestione più dinamica e agile del business.
Per rendere i processi più efficienti in un contesto technology driven, l'area Finance ha incaricato il team IT di **Gabriele Chiesa** (Chief Information Officer) di TIM di disegnare e sviluppare un

progetto di digitalizzazione che permettesse alla divisione di aumentare la produttività delle risorse.

«In soli 10 mesi si è passati dall'idea all'entrata in funzione del nuovo sistema gestionale avvenuta lo scorso 2 settembre mettendo di fatto le basi per quello che, con la seconda fase del programma, è diventato uno dei progetti più importanti ed estesi di trasformazione digitale del Gruppo», ha commentato **Pierpaolo Taccini,** Responsabile Revenue Assurance & Digital Finance di TIM.

I risultati positivi raggiunti, insieme alla capacità organizzativa e operativa del team IT, hanno convinto il management del Gruppo TIM ad ampliare il target all'interno dell'organizzazione estendendo di fatto il programma in un'ottica di Digital Enterprise Transformation e coinvolgendo anche altre aree di business tra cui quelle che fanno capo a HR, Real Estate, Purchasing, Legal, Logistica.

Il cambio di passo punta a sfruttare la tecnologia SAP in tutte le sue componenti e soluzioni con l'obiettivo di abilitare una semplificazione dei sistemi e raggiungere un'importante efficienza delle risorse.

Apripista della seconda fase è ancora la divisione Finance insieme alla divisione Purchasing, con l'adozione delle soluzioni SAP ERP/SAP EPM e SAP Ariba per il controllo end-to-end delle spese del gruppo e che dal 2021 saranno estese anche in ambito Logistica e Real Estate.

Peraltro,la divisione Finance sta anche lanciando l'implementazione di SAP Analytics Cloud, per accelerare il passaggio da "insight" ad "azione", affidando i dati alla combinazione di business intelligence, analisi aumentata e funzionalità di pianificazione collaborativa, e

SAP Cloud Platform, per sviluppare rapidamente applicazioni robuste e scalabili native per il cloud.

Il programma intrapreso dall'azienda abbraccia le 24 società del gruppo e interessa oltre 8.000 utenti che avranno accesso a SAP S/4HANA, dei quali circa 600 hanno testato e collaudato la piattaforma prima della sua entrata in esercizio eseguendo più di 3.600 casi di test con la Linea Utente.

«E' indubbiamente esaltante vedere come un'azienda del calibro del Gruppo TIM punti con determinazione sulla tecnologia core di SAP per impostare un percorso importante di trasformazione digitale dei processi aziendali, recuperando efficienza e produttività per indirizzare le persone verso compiti di maggior valore e funzionali alla crescita del business», ha commentato **Enzo Pagliaroli**, Services and Public Sector Sales Director di SAP Italia. «Questa è un'ulteriore dimostrazione di come SAP supporti le aziende a diventare Imprese Intelligenti e le aiuti a sfruttare le tecnologie più innovative per accelerare cambiamenti basati sui dati, prendere decisioni complesse più velocemente, individuare opportunità nascoste e anticipare i trend di mercato».

Come essere pronti per il lavoro del futuro e l'azienda diffusa

Si va verso l'azienda diffusa e la riorganizzazione delle interazioni personali. Il perché e i problemi da affrontare li illustra Simon Biddiscombe di MobileIron

di Simon Biddiscombe,
President and Chief Executive Officer di MobileIron

L'azienda diffusa e lo smart working stanno cambiando il modo di realizzare e gestire gli spazi aziendali. Un esempio è fornito analizzando quanto accaduto in casa MobileIron.

A marzo, MobileIron era pronta a firmare un contratto di locazione per alcuni spazi ad uso ufficio, quando la crisi del Coronavirus si è trasformata in un'ondata di panico che ha investito tutto il mondo. La società ha fatto un passo indietro, e abbiamo fatto bene.

«Siamo un'azienda in crescita, quindi spesso sottoscriviamo contratti di locazione per nuovi uffici, ma la pandemia ha imposto un cambiamento radicale, a noi come a molti altri. Dall'oggi al domani, il luogo, le dimensioni e la struttura dell'immobile scelto non erano più idonei. Il tipo di ambiente di cui avevamo bisogno e, di fatto, il modo di lavorare in futuro, sono cambiati in una notte. In un istante siamo dovuti passare da una forza lavoro diffusa a livello globale con una policy rigorosa per il lavoro remoto a una Azienda diffusa», ha commentato **Simon Biddiscombe**, President and Chief Executive Officer di MobileIron

Uno dei cambiamenti più evidenti che ci aspettano, osserva il manager, riguarderà il luogo di lavoro. Alcune aziende permettono già ai dipendenti di lavorare permanentemente da casa. Per le aziende questa è un'opportunità. Facebook adeguerà i salari dei dipendenti in base al luogo di lavoro e sarà quindi potenzialmente in grado di ridurre i costi. Fujitsu prevede di dimezzare gli spazi ufficio in Giappone se i dipendenti sceglieranno di lavorare altrove.

Cambia l'ufficio e il modo di lavorare

Gli uffici forse non spariranno del tutto, ma saranno differenti e situati in luoghi diversi. Diventeranno sempre più spazi per incontrarsi e collaborare, piuttosto che per lavorare da soli. Pensati come luoghi di aggregazione sociale, saranno più piccoli e con meno scrivanie.

Vi sono però situazioni dove i dipendenti, non possono lavorare da casa e hanno bisogno di misure di sicurezza aggiuntive. Nel commercio al dettaglio, ad esempio, è necessaria più distanza e meno interazione fisica con i clienti e tra i colleghi. Diverse persone ordinano da casa, perciò i servizi di consegna avranno un ruolo sempre più importante.

I dipendenti, continua Biddiscombe, lavoreranno da casa molto più spesso e tutto ciò comporterà nuovi problemi. Le persone possono aver tollerato condizioni di lavoro a distanza temporanee, ma se queste diventano una regola, avranno bisogno di un miglior supporto a lungo termine. Ciò significa più interazione sociale e tecnologie di gestione progettate per questa "nuova normalità", per promuovere il coinvolgimento dei dipendenti e mantenere la cultura aziendale.

Ogni dipendente avrà bisogno di una tecnologia collaborativa ancora più integrata, per un'esperienza agevole e protetta.

In sostanza, è il momento di vincere le sfide che hanno messo in crisi le aziende durante il lockdown. Molte aziende hanno avuto difficoltà a garantire accessi protetti alle risorse e nel fornire supporto IT da remoto. Hanno dovuto inoltre affrontare un aumento di minacce come furto delle credenziali, attacchi malware e di phishing.

Largo alle nuove tecnologie

Per eliminare questi problemi, le aziende, osserva Biddiscombe, devono creare posti di lavoro sicuri e offrire una connettività protetta, permettendo al reparto IT di distribuire rapidamente policy di sicurezza a dispositivi e applicazioni.

Per esempio, mentre Zoom migliorava le funzionalità di sicurezza a inizio pandemia, i reparti IT implementavano rapidamente le configurazioni per dispositivi e dipendenti tramite l'Unified Endpoint Management (UEM). Le aziende possono sfruttare l'UEM per proteggere molti altri servizi basati su cloud e on-premise.

L'altro miglioramento che le aziende devono implementare riguarda l'usabilità. Molti dipendenti utilizzano ancora le password per accedere alle applicazioni e ad altre risorse informatiche aziendali. Si tratta di una modalità di accesso poco sicura che diventerà sempre più obsoleta, con l'utilizzo crescente dei dispositivi mobile da parte dei dipendenti.

Ma non si può rinunciare alla sicurezza in nome dell'usabilità e delle funzionalità, ma serve immaginare un futuro in cui il dispositivo mobile sarà esso stesso una forma di accesso mediante sistemi di autenticazione senza password, basati su identificatori biometrici.

«L'uso dei lettori di impronte digitali e delle funzioni di rilevamento del volto dei dispositivi mobile migliorerà e semplificherà l'autenticazione, permettendo ai dipendenti di accedere in modo agevole alle applicazioni di lavoro da casa o in ufficio. I clienti sono già abituati a questo tipo di esperienza, che viene utilizzato dalle app di home banking e shopping: il passaggio al telelavoro eliminerà l'uso delle password molto rapidamente», considera Biddiscombe.

Lavorare in futuro sarà quindi molto diverso rispetto al passato e questo cambiamento porterà ai manager nuove sfide. Tuttavia, diventerà anche un'opportunità importante per rinnovare le modalità di lavoro, supportare i dipendenti che lavorano da casa con una migliore collaborazione e modalità di accesso più intuitive.

"Azienda diffusa" non è quindi una frase fatta, è la realtà attuale, un concetto in continua crescita ed espansione che va di pari passo con nuovi modi di lavorare, ovunque ci si trovi.

Mantenere la cybersecurity in prima linea è la nuova normalità

E il momento di mettere in campo le migliori pratiche di sicurezza e fare tutto il possibile per fornire la protezione più idonea. Il punto della situazione con SolarWinds

Tim Brown, SolarWinds

La prossima fase della trasformazione digitale è già alle porte, prima di quanto molti si aspettassero. Quest'anno ha spinto tutti a ripensare il proprio rapporto con la tecnologia, costringendo le aziende a creare nuovi modelli per il lavoro da remoto, da un giorno all'altro: una mossa che molte organizzazioni non erano ancora pronte a fare.

Ma nella fretta di fornire ai dipendenti degli strumenti e delle connessioni necessarie per lavorare da remoto, osserva **Tim Brown**, Vice President of Security di SolarWinds MSP, alcune delle buone pratiche per la definizione dei protocolli di sicurezza e il relativo mantenimento possono essere state accantonate.

Questa situazione può aver portato a una maggiore esposizione al rischio in termini di cybersicurezza, in un momento in cui gli hacker stanno intensificando i loro sforzi, riconoscendo come l'improvviso aumento del telelavoro dia loro più opportunità per sferrare i loro attacchi.

Mentre il mondo cerca di adattarsi ad una nuova "normalità", cercando di contenere la diffusione del COVID-19, gli MSP, evidenzia il manager, dovrebbero discutere con i clienti sul come aiutarli a superare le fasi successive della pandemia e a prepararsi per un futuro post-pandemico.

Alcuni dei cambiamenti che la pandemia ha accelerato, diventeranno infatti permanenti: ad esempio, molti dipendenti non torneranno più in ufficio ma lavoreranno da remoto.

Tenendo presente questo, gli MSP, osserva Brown, devono impegnarsi nel contribuire a garantire la sicurezza in ambienti di lavoro decentralizzati.

Tanto per cominciare, qualsiasi "scorciatoia" relativa alle misure di sicurezza presa durante la pandemia deve essere corretta.

Oltre a questo, gli MSP hanno bisogno di strategie per la messa in sicurezza degli ambienti remoti, incluso il monitoraggio e l'aggiornamento delle infrastrutture software dei clienti.

Proteggere gli asset più importanti

Il punto di partenza è individuare gli asset più importanti in base al proprio core business e proteggerli tramite un livello più avanzato di sicurezza rispetto al resto.

Se non si è mai fatto questo esercizio in precedenza, questo è il momento giusto. Se si cerca di proteggere tutto non si avrà successo. Sviluppare una strategia di sicurezza efficace di questi tempi ha molto a che fare con la definizione delle priorità: gli asset e i flussi di lavoro più importanti richiedono una sicurezza maggiore rispetto a quelli meno critici per l'azienda.

Cercare di mettere tutto in sicurezza allo stesso livello è un compito praticamente impossibile che può portare ad abbassare il livello di sicurezza generale invece di proteggere gli asset che necessitano di maggiore protezione. «Non c'è mai stato un momento più importante come quello che stiamo vivendo per mettere la cyber hygiene al primo posto tra le priorità dell'azienda. Ritenere di non possedere alcunché di valore non basta per salvarsi. Stabilire le priorità di sicurezza non significa trascurare le basi. I fondamenti della cyber hygiene devono essere ancora affrontati, e ciò in pratica significa che tutti gli utenti debbano comprendere le politiche di sicurezza della loro azienda e che i clienti abbiano la capacità di far rispettare le politiche sulla gestione dell'identità e degli accessi, sulle patch e sul phishing», mette in guardia Brown.

Partire dalle basi aiuta a prevenire i cyber-attacchi. Un'azienda può disporre della tecnologia più sofisticata per sventare gli aggressori, ma se trascura di formare gli utenti su come identificare le e-mail phishing, questo la rende ancora più vulnerabile agli attacchi ransomware e altri tipi di malware.

Il più delle volte i criminali informatici si concentrano su bersagli facili, come sistemi senza patch e utenti ignari, dimostrando quindi perché sia così fondamentale non abbandonare mai le basi.

La singola rete non esiste più

Va poi considerato che gli endpoint sono diventati un punto di accesso da monitorare con attenzione perché la singola rete non esiste più.

È multi-tutto: multi-cloud, multi-reti, multi-endpoint. Ora ci sono più endpoint sotto il proprio controllo rispetto a prima, e hanno bisogno di z attenzione.

È il momento, suggerisce Brown, di mettere in campo le migliori pratiche di sicurezza e assicurarsi che si stia facendo tutto il possibile per fornire la protezione più idonea in sintonia con la trasformazione digitale che stiamo vivendo. Gli hacker stanno diventando sempre più aggressivi e gli utenti devono fare lo stesso.

È disponibile il nuovo libro

IL FUTURO DEL WORKSPACE E DELLO SMART WORKING

Chiedi la tua copia dell'e-book scrivendo a:
shop@reportec.it • Il prezzo del libro è di 20 euro (iva inclusa)