Ottobre 2021

Non pagate il riscatto!

Una guida in tre passaggi per la protezione dal ransomware

Barracuda®
Your journey, secured.

Indice

Il ransomware e la sua evoluzione

Spiegato con semplicità, il ransomware è software dannoso che crittografa i dati o impedisce in altro modo di accedere ai propri sistemi. I criminali chiedono un riscatto in cambio della chiave di crittografia, ma ovviamente non esiste nessuna garanzia che la chiave poi funzioni e che sia possibile riavere i propri dati. Molte vittime, pur avendo pagato, non li hanno riavuti.

Barracuda

Rispetto all'approccio diretto di WannaCry, basato sui fattori "compromissione e crittografia" di qualche anno fa, gli attacchi ora adottano una strategia multivettoriale più sofisticata. Spesso iniziano con un'e-mail di spear-phishing, ma non si scatenano subito dopo che il destinatario ha fatto clic sul link dannoso.

Questo primo passo viene invece utilizzato per carpire le credenziali della vittima, al fine di utilizzarle in seguito per accedere alla rete dell'organizzazione e aggirarsi al suo interno, curiosando fra le risorse, i server, i database e la piattaforma e-mail. Questa fase di osservazione può durare settimane o anche mesi e solo dopo viene scatenato l'attacco. È esattamente questo quello che è successo con il ransomware ai danni del servizio sanitario irlandese, HSE. I criminali informatici hanno rivendicato di avere trascorso settimane all'interno della rete dell'HSE settimane all'interno della rete dell'HSE prima di sferrare l'attacco, nel quale 700 GB di dati dei pazienti sono stati crittografati e sottratti.

Uno dei motivi per cui oggi si sente parlare più spesso di ransomware è che sono cadute le barriere che bloccavano l'accesso. La tecnologia del crimine sta diventando più facilmente fruibile. Attualmente è possibile acquistare un kit ransomware e scegliere il bersaglio da colpire. Le bande di criminali informatici offrono supporto tecnico in cambio di una percentuale del riscatto e, se questo viene ritenuto troppo rischioso, l'aspirante hacker può assoldare veri hacker che portino a termine l'attacco in sua vece, stipulando una specie di contratto di servizio per il crimine. L'aumento del valore della criptovaluta e la diffusione delle assicurazioni per i rischi informatici hanno reso più redditizi gli attacchi ransomware per i criminali, attirando bande altamente organizzate, inoltre gli attacchi ransomware sponsorizzati da alcuni stati hanno incentivato la guerra cibernetica.

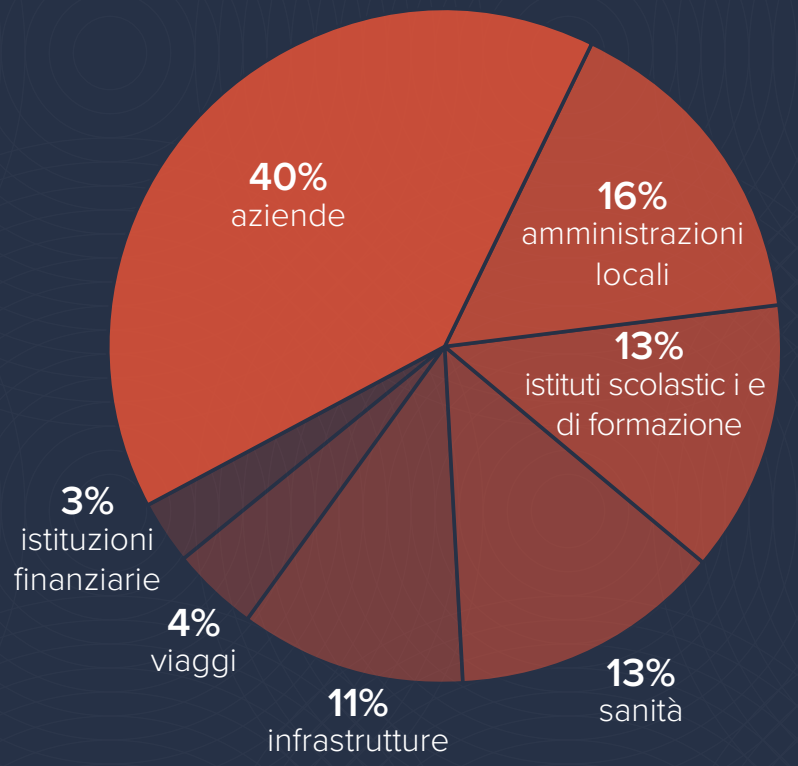
I criminali informatici alzano la posta

Gli attacchi ransomware hanno raggiunto un livello tale da essere considerati dai governi come veri e propri atti di terrorismo. Questa reazione non è eccessiva, in quanto hanno causato gravi problemi operativi ad amministrazioni locale, forze dell'ordine, istituzioni scolastiche, reti sanitarie, infrastrutture critiche e altro ancora. Nessun settore industriale, organizzazione o ente governativo ne è immune.

In base a una ricerca recente svolta da Barracuda, gli attacchi a infrastrutture, servizi di viaggio e finanziari e ad altre attività rappresentano fino al 57% degli attacchi ransomware totali effettuati tra agosto 2020 e luglio 2021, il 18% in più rispetto allo studio che abbiamo condotto nel 2020. Le aziende operanti nel settore delle infrastrutture sono le protagoniste dell'11% di tutti i casi che abbiamo preso in esame.

Anche le somme dei riscatti stanno salendo drasticamente e ora l'importo medio per incidente supera i 10 milioni di dollari. Solo nel 18% dei casi analizzati da Barracuda tra agosto 2020 e luglio 2021 il riscatto richiesto era inferiore a 10 milioni e nel 30% degli incidenti la richiesta ammontava a oltre 30 milioni di dollari.

Attacchi ransomware per settore

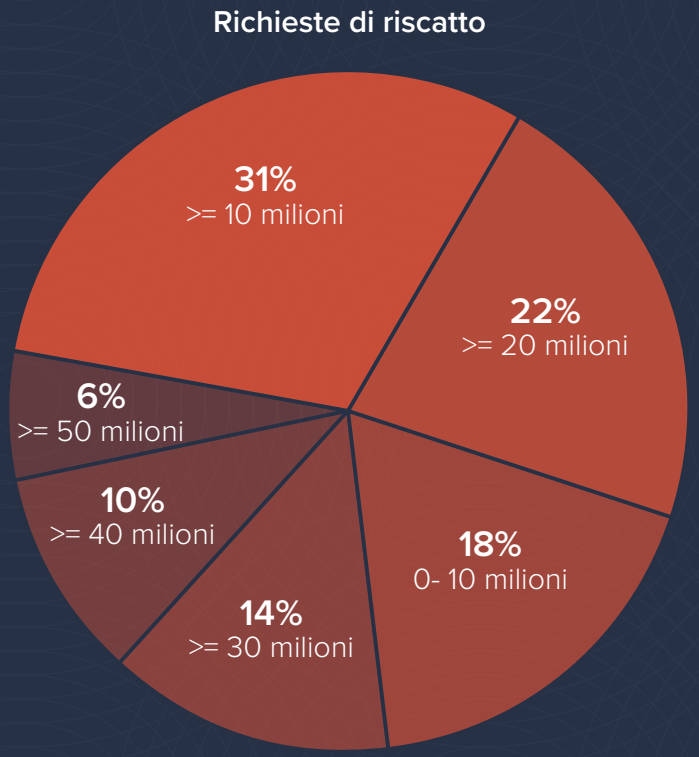


Il ransomware non è una nuova minaccia, ma si è evoluto in modo tale da divenire più distruttivo. I criminali hanno affinato le loro capacità e tattiche, arrivando a creare uno schema a doppia estorsione. In pratica, basano le richieste di riscatto su ricerche eseguite prima dell'attacco. Rubano dati sensibili alle vittime e richiedono un pagamento in cambio dell'impegno a non pubblicare o vendere tali dati ad altri malintenzionati. Come è ovvio aspettarsi dai criminali, le vittime che pagano spesso vengono ricontattate dopo alcuni mesi con la richiesta di un altro pagamento per mantenere segreti i dati rubati. Alcuni criminali informatici accettano il pagamento per poi concludere comunque la vendita dei dati.

Pagando il riscatto, non si ha mai la garanzia di poter recuperare tutti i dati crittografati. Le vittime ormai si rendono conto che i dati carpiti in un attacco ransomware sono compromessi per sempre. Semplicemente non c'è motivo di pagare i criminali per le violazioni che commettono.

Bisogna mettere in conto che qualsiasi azienda può essere oggetto di un attacco ransomware e, se questo colpisce nel segno, è necessario avere un piano di riserva per non pagare il riscatto.

Per proteggere l'azienda dagli attacchi ransomware occorre proteggere i dati e questo aspetto può essere suddiviso in tre settori di interesse: proteggere le credenziali, mettere in sicurezza le applicazioni Web ed eseguire il backup dei dati. Vediamo singolarmente in maggior dettaglio questi tre punti.



Passaggio 1: proteggere le credenziali

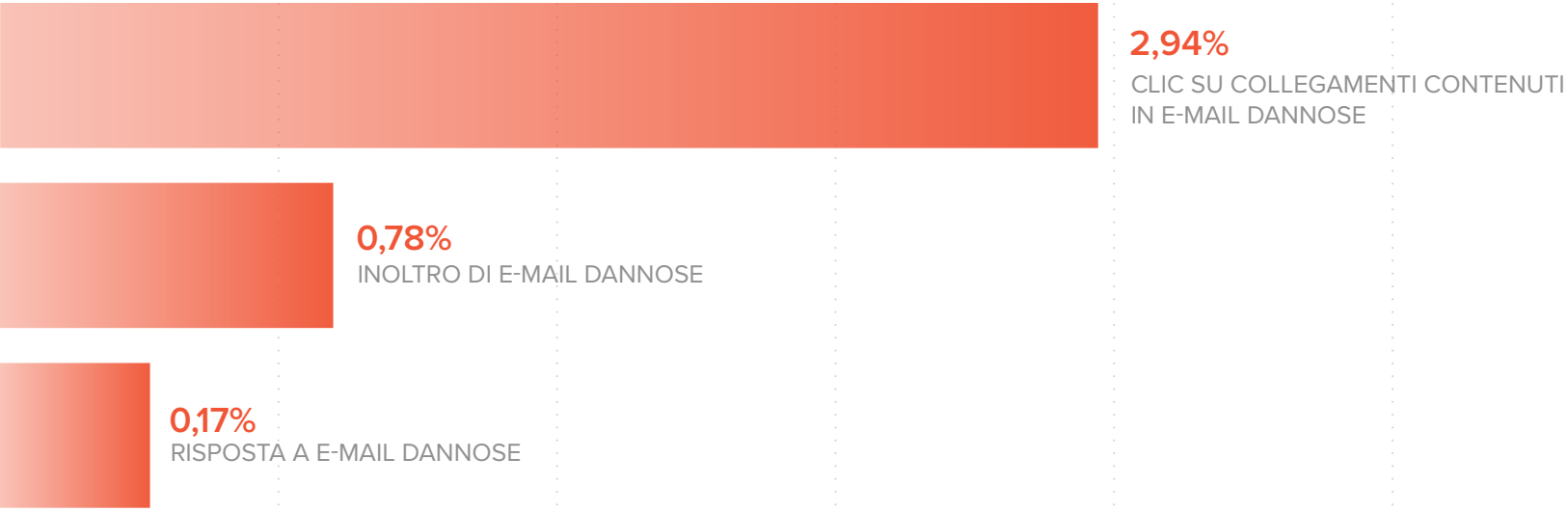
Per prima cosa, il ransomware tenta di far breccia nell'e-mail o di appropriarsi delle credenziali in altro modo. Con decine di migliaia di nomi utenti e password prontamente disponibili online, questo primo passo può essere spaventosamente facile. Spesso gli autori degli attacchi utilizzano le credenziali rubate per accedere ai sistemi aziendali.

Barracuda

Dato che il phishing è il principale vettore di attacco per il ransomware, è essenziale suscitare consapevolezza sull'importanza di mantenere al sicuro le credenziali, sviluppando procedure di formazione per gli utenti sulla sicurezza dell'e-mail e implementando una tecnologia anti-phishing che sia in grado di identificare e segnalare le attività insolite. Se i criminali non riescono ad appropriarsi delle credenziali, diventa più difficile per loro passare dal phishing al ransomware.

Gli attacchi di phishing funzionano perché alle persone piace fare clic per vedere le cose. Gli hacker confezionano con cura gli attacchi raccogliendo informazioni personali disponibili pubblicamente sulle vittime e facendo leva sull'urgenza di avere una risposta. Per i criminali informatici è sufficiente che una persona all'interno dell'organizzazione faccia clic su un link o apra un allegato. Da una recente ricerca condotta da Barracuda è emerso che, in media, il 3% delle persone che riceve un'e-mail di phishing fa clic sul link. In genere lo scopo dell'attacco è appropriarsi delle credenziali dell'account, il che consente all'hacker di muoversi lateralmente all'interno dell'azienda e ricattare l'intera organizzazione.

Per proteggere le credenziali e gli accessi è necessario un duplice approccio: in primo luogo investire in strumenti di rilevamento e risposta e quindi dedicarsi alla formazione degli utenti.



Fonte: Threat Spotlight: Post-delivery email threats

Barracuda

Strumenti di rilevamento e risposta

La tecnologia di protezione dell'e-mail prescelta non deve concentrarsi solo sul rilevamento di payload dannosi forniti mediante link o collegamenti, ma anche sulla capacità di riconoscere quando per l'attacco vengono utilizzate tattiche di social engineering, pensate per aggirare la tecnologia di filtraggio e indurre gli utenti ad agire. Deve saper ricercare i pericoli contenuti nelle e-mail, anche in assenza di un payload dannoso. Un sistema di sicurezza dell'e-mail che utilizza algoritmi di apprendimento automatico è in grado di rilevare gli attacchi di social engineering con un maggiore grado di precisione, identificando scostamenti anche minimi dai consueti schemi di comunicazione.

Non è possibile proteggere le credenziali degli utenti senza un'adeguata protezione dal furto di account. L'autenticazione a più fattori (MFA) resta una best practice e oggi dovrebbe essere adottata da tutte le organizzazioni. Tuttavia non è infallibile e non sempre è sufficiente. Gli autori degli attacchi cercano modi per aggirarla, inducendo gli utenti a installare malware sui dispositivi di verifica o fornendo l'accesso a false app ai loro account. Le organizzazioni devono disporre di sistemi di protezione dal furto di account in grado di identificare rapidamente attività dannose quali accessi sospetti o attacchi sferrati da account compromessi, e segnalarle.

Per proteggere le credenziali e gli accessi è necessario un duplice approccio: in primo luogo investire in strumenti di rilevamento e risposta e quindi dedicarsi alla formazione degli utenti.

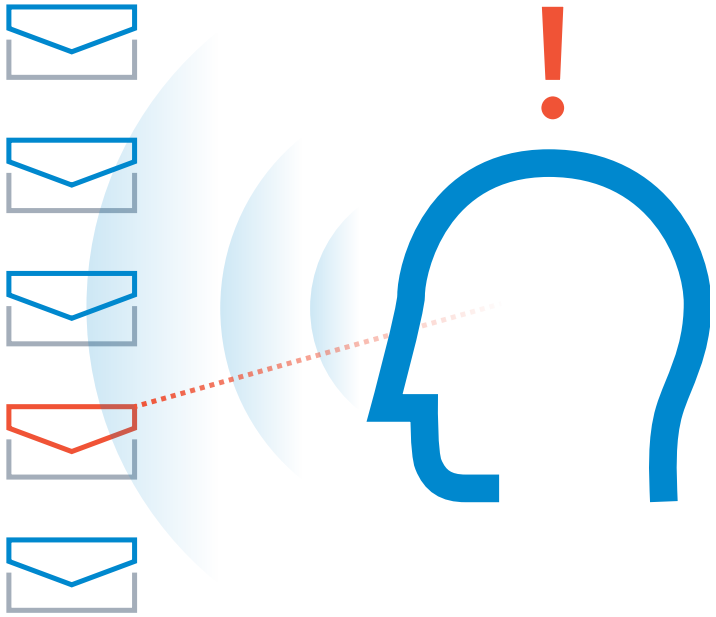
Barracuda

Formazione per gli utenti

Come ultima linea di difesa, è importante insegnare ai dipendenti a riconoscere e segnalare gli attacchi. Per questo occorre integrare nella strategia di protezione dell'e-mail formazione atta a sensibilizzare gli utenti sul tema della sicurezza e simulazioni di phishing. In passato gli attacchi di phishing erano associati unicamente all'e-mail, ma oggi i criminali informatici utilizzano anche altre canali, quali gli SMS e le chiamate vocali. La simulazione di phishing deve pertanto comprendere e-mail, caselle vocali e SMS per abituare gli utenti a identificare gli attacchi informatici, verificando in seguito l'efficacia della formazione erogata e valutando quali sono gli utenti più vulnerabili agli attacchi.

La formazione sulla sicurezza informatica inoltre non va riservata soltanto ai nuovi assunti il primo giorno di lavoro. Deve essere un processo continuo per mantenere il personale aggiornato sulle minacce in evoluzione. Ad esempio, oggigiorno le bande di criminali utilizzano tecniche di social engineering difficili da riconoscere. Gli attacchi di spear-phishing prendono di mira una sola persona o alcuni componenti di un reparto, ad esempio l'area finance, con messaggi estremamente mirati.

È essenziale che le iniziative di formazione si conquistino la fiducia del personale e rendano i dipendenti disponibili a dare l'allarme anche qualora abbiano commesso accidentalmente un errore in prima persona. Può essere necessaria anche formazione su come rimediare, ma bisogna evitare di punire chi esce allo scoperto per avvertire. Molti attacchi non vengono segnalati perché le persone temono di essere incolpate per avere fatto clic su un link o avere aperto un allegato. Gli avvisi precoci sono invece estremamente utili e devono essere valorizzati.



Barracuda

Passaggio 2: proteggere le applicazioni Web e l'accesso

Il passaggio al lavoro a distanza ha spostato un numero ancora maggiore di applicazioni dai data center a internet. Alcune volte, la fretta di mantenere in funzione i servizi aziendali ha portato in secondo piano la sicurezza e i criminali informatici sono pronti a sfruttare queste vulnerabilità.

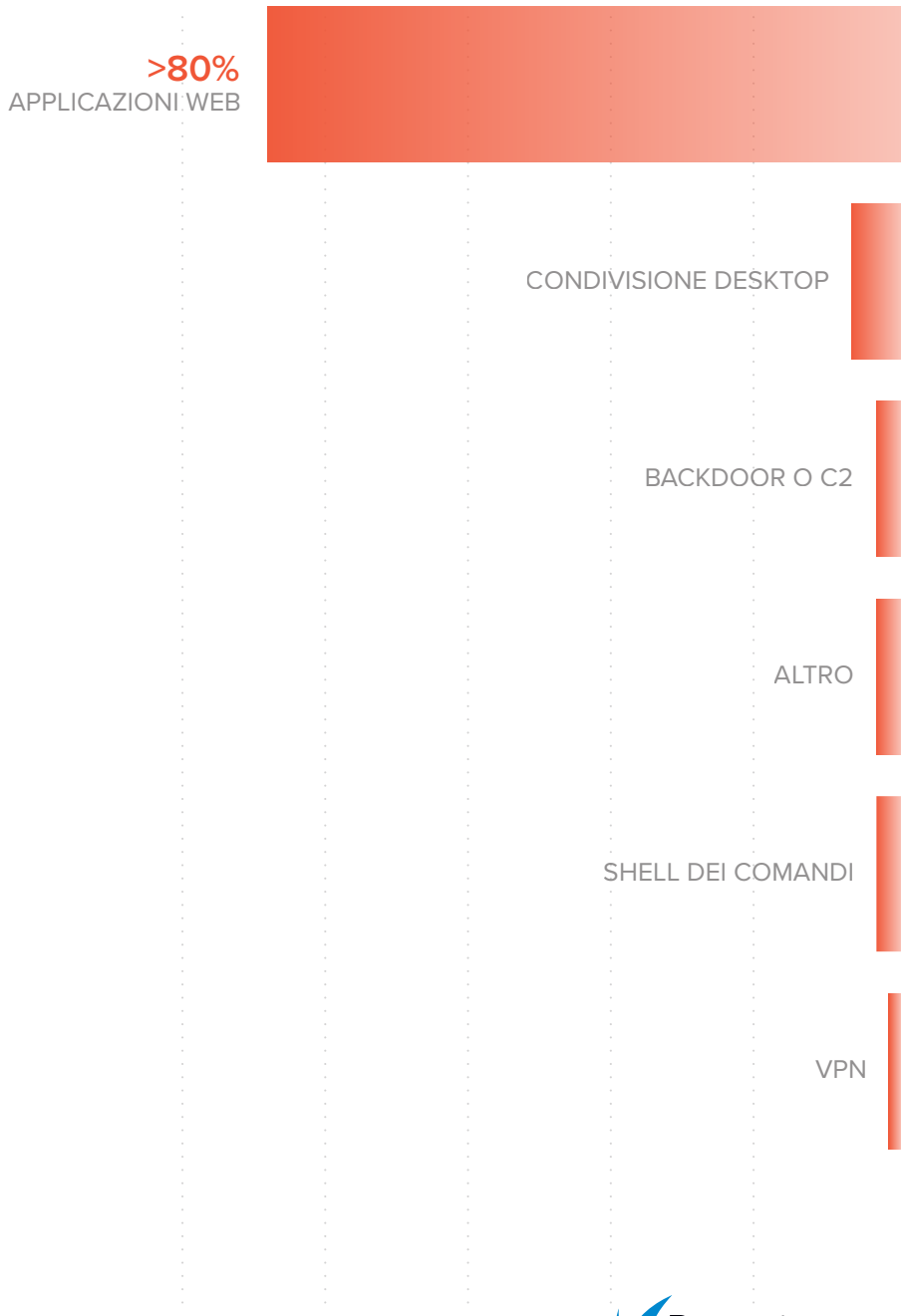
Barracuda

Il report di indagine sulle violazioni di dati di Verizon del 2021 evidenzia che le applicazioni Web sono il vettore di attacco più usato negli hackeraggi, responsabile di oltre l'80% delle violazioni di dati.

Le applicazioni online, come i servizi di condivisione file, i moduli Web e i siti di e-commerce possono essere compromessi da malintenzionati. Le applicazioni Web vengono attaccate tramite l'interfaccia utente o un'interfaccia API. Spesso si tratta di attacchi di tipo credential stuffing o brute-force, oppure vengono sfruttate le vulnerabilità citate dall'OWASP. Quando l'applicazione è compromessa, i criminali possono introdurre nel sistema ransomware e altri tipi di malware, per poi muoversi lateralmente e procedere infettando la rete e gli utenti dell'applicazione.

È importante capire che, per difendersi dal ransomware e da altri malware, la protezione delle applicazioni e dell'accesso è critica quanto la sicurezza dell'email. L'OWASP (Open Web Application Security Project) si adopera per incentivare la consapevolezza del pubblico sulle vulnerabilità più comuni delle applicazioni che possono essere sfruttate in un attacco ransomware.

Fonte: report di indagine sulle violazioni di dati di Verizon del 2021



Un esempio recente è l'hackeraggio alla supply chain da parte del ransomware REvil che è stato scoperto nel luglio 2021. Sono state sfruttate le vulnerabilità di un'applicazione MSP internet rivolta al pubblico per diffondere ransomware ai clienti. In questo caso, dato che l'applicazione disponeva di autorizzazioni profonde, il ransomware si è potuto diffondere piuttosto facilmente e ha avuto un impatto significativo prima di essere bloccato. Questo tipo di hackeraggio potrebbe avvenire tramite qualunque applicazione esposta a internet: gli autori dell'attacco si infiltrano nell'applicazione e quindi si muovono lateralmente per gettare scompiglio. Una situazione del genere può concretizzarsi se si lasciano aperti i sistemi RDP a internet, anche cambiando la porta predefinita. I criminali hanno raccolto le credenziali da questi sistemi RDP per tentare di infettare l'intera rete con ransomware veicolato tramite questo vettore di attacco non protetto.

Fino a

1500

aziende colpite dall'attacco alla supply chain REvil

Barracuda.

Quattro vettori di attacco per le applicazioni Web

Le applicazioni sono ora uno dei principali bersagli per il ransomware, quindi è importante proteggere i seguenti quattro vettori di attacco: accesso alle applicazioni, vulnerabilità delle applicazioni Web, accesso all'infrastruttura e movimento laterale.

1. Accesso alle applicazioni

Per stabilire se l'accesso alle applicazioni è una falla che potrebbe essere sfruttata ai danni dell'organizzazione, è necessario rispondere a qualche domanda fondamentale.

- **I dipendenti che lavorano a distanza e i collaboratori esterni utilizzano dispositivi non gestiti o personali (BYOD, Bring Your Own Device)?** I dispositivi mobili ne sono l'esempio più comune. Un dispositivo non gestito o BYOD può essere compromesso e quindi utilizzato per estrarre credenziali o attaccare ulteriormente un'applicazione.
- **Si ha visibilità sugli utenti e i dispositivi in rete?** Ad esempio, è necessario sapere chi si connette alla rete guest e se questa è segmentata correttamente.
- **È disponibile un audit trail di chi accede a cosa e quando?** Si deve poter guardare indietro e vedere chi accede alle applicazioni, come vi accede e se questi utenti dispongono di autorizzazioni corrette.

Se un dispositivo che non dovrebbe essere autorizzato ad accedere è connesso alla rete e qualcuno vi ha impostato strumenti di hackeraggio, il problema è grave. Non avendo visibilità su tutto ciò, diventa difficile identificare chi accede a cosa e qual è la vulnerabilità, perché in questo modo non è possibile arginare la superficie vulnerabile o bloccare l'accesso ai malintenzionati.

2. Vulnerabilità delle applicazioni Web

Le vulnerabilità delle applicazioni Web sono il successivo vettore di attacco da valutare per stabilire quanto queste siano sicure in realtà.

Le domande da porsi sono le seguenti:

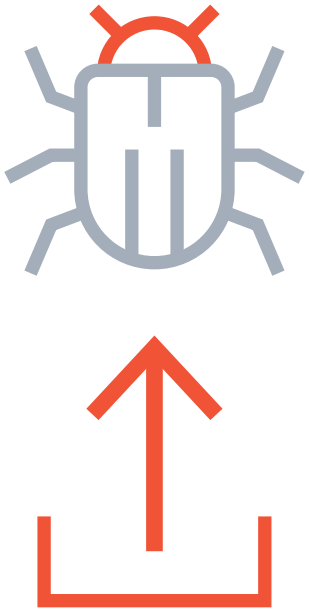
- Quanto è sicuro il sito Web aziendale? Quando è stato aggiornato l'ultima volta?
- Il sito utilizza moduli? È in atto una prevenzione dagli attacchi tramite i moduli?
- Il sito Web accetta il caricamento di file? Che tipo di protezione contro il malware utilizza?

Per proteggere il sito non è sufficiente attivare il protocollo HTTPS, implica soltanto che i criminali informatici non possano intercettare gli utenti che vi accedono per impossessarsi delle loro credenziali, ma potrebbero comunque sferrare un attacco brute-force all'interno di quel frame HTTPS per tentare di estrapolare i dati di accesso corretti per il sito.

Anche l'uso di CAPTCHA o reCAPTCHA prima dei moduli di accesso al sito non è sufficiente, perché è facile automatizzare questi servizi ed eluderli.

Gli accessi o gli indirizzi IP con limitazione della frequenza sono un'altra misura di sicurezza facilmente aggirabile dagli hacker mediante attacchi low-and-slow e vari sistemi di automazione.

Se si accetta il caricamento di file, anche questo è un problema da tenere in considerazione. È abbastanza comune che gli autori degli attacchi tentino di violare un sito Web caricando malware, come virus o ransomware.



3. Accesso all'infrastruttura

Sin dall'inizio della pandemia di COVID-19, molte organizzazioni hanno introdotto l'uso di VPN per fornire l'accesso alle applicazioni ospitate internamente. Questa scelta viene fatta quando non esistono servizi SaaS sostitutivi per alcune applicazioni in self-hosting. Fornire l'accesso mediante VPN da casa è il solo modo per continuare a operare. Senza prassi adeguate per il controllo degli accessi e delle identità però questo approccio è come una bomba a orologeria che prima o poi esploderà. Molte delle credenziali già sottratte potrebbero avere in comune nomi utenti e password utilizzati per accedere all'infrastruttura e introdurre di fatto un rischio reale che potrebbe esporre la rete, le applicazioni e i dati.

4. Movimenti laterali

Dopo avere compromesso le applicazioni o l'infrastruttura con le credenziali rubate, i criminali potrebbero spingersi più in profondità nella rete e sferrare altri attacchi da lì, quindi questo è il quarto vettore di attacco da contenere. Le seguenti domande possono essere utili a questo proposito:

- La rete aziendale è suddivisa in segmenti adeguatamente protetti?
- È abilitata l'autenticazione a più fattori per l'accesso alla rete?

L'impostazione di una segmentazione corretta per la rete richiede molto tempo e lavoro, per cui sussistono spesso motivazioni valide per aprire due segmenti e consentire l'accesso dall'uno all'altro ma, in ultima analisi, questo comporta un'apertura dell'accesso secondo modalità indesiderate.

L'autenticazione a più fattori aggiunge un altro importante livello di protezione, che contribuisce a impedire l'accesso alla rete a malintenzionati.

Barracuda

In che modo un attacco ransomware sfrutta le vulnerabilità delle applicazioni Web

Qui è descritto un altro scenario: una serie immaginaria, ma realistica, di passaggi che un criminale informatico può eseguire per sfruttare falle nella sicurezza delle applicazioni e mettere a segno un attacco ransomware, tentando di attuare un tipo di frode abbastanza diffuso, quello dei coupon, sfruttando l'onda riemergente di plugin per i browser.

Passaggio 1

Il criminale crea un falso sito Web che riproduce un sito di coupon legittimo. Quindi impersonifica un sito di coupon conosciuto, operazione relativamente semplice da compiere utilizzando l'impersonificazione del dominio e il Web scraping automatizzato. Chiamiamo questo sito falso "sito Web X".

Passaggio 2

Il criminale sonda una o più delle 10 principali vulnerabilità evidenziate dall'OWASP per rubare le credenziali di un sito Web aziendale legittimo scarsamente protetto, che chiameremo "sito Web Y". Vulnerabilità quali l'infrazione dell'autenticazione e l'esposizione di dati sensibili consentono all'hacker di raccogliere le credenziali degli utenti e altre informazioni riservate dal sito Web Y.

Passaggio 3

Il criminale utilizza le credenziali rubate per dare inizio a un attacco di credential stuffing diretto contro un sito Web di e-commerce legittimo, che chiameremo "sito Web Z". Questo attacco automatizzato può essere eseguito lentamente nell'arco di diverse settimane ed è finalizzato a trovare corrispondenze tra credenziali carpite e account reali esistenti presso questi siti.

Passaggio 4

Se nell'attacco viene riscontrata una corrispondenza, l'hacker può accedere all'account della vittima e il passaggio successivo consiste nell'utilizzare tale account per pubblicare recensioni recensioni di prodotti conosciuti sul sito Web Z, scrivendo ad esempio "Questo prodotto è fantastico!. Risparmia il 50% sul prezzo di acquisto con questo coupon facendo clic qui". Il link per avere il coupon porta il visitatore al sito Web X, ovvero il sito falso creato al passaggio 1.

Barracuda

Passaggio 5

Le potenziali vittime accedono al sito Web Z e poi fanno clic sulla recensione del prodotto seguendo il link al sito Web X, inconsapevoli di essere approdati a un sito truffaldino, a meno che non facciano estrema attenzione a nome di dominio, URL, certificato del sito e altri dettagli. Le vittime che si fidano del sito forniscono i loro dati di contatto in cambio del coupon. Il criminale a questo punto ha a disposizione gli indirizzi di persone che si aspettano un'e-mail da quel sito Web e si guadagna la loro fiducia, intanto le vittime abbassano la guardia.

Passaggio 6

Le vittime ricevono un'e-mail personalizzata riguardante il prodotto e il coupon, con un allegato da installare per attivare il coupon. L'allegato può essere un eseguibile o un'estensione del browser che si serve di JavaScript per portare a termine l'attacco. Dato che il messaggio e-mail è altamente personalizzato e il destinatario se lo aspetta, è probabile che filtri attraverso le tradizionali difese dell'e-mail. Il sistema operativo avverte di non installare eseguibili non attendibili, ma a questo punto la vittima potrebbe fidarsi completamente e fare clic per procedere.

Barracuda

Passaggio 7

La vittima installa l'allegato avviando l'attacco ransomware. Una volta installato l'eseguibile, possono essere sferrati alcuni tipi di attacchi, ad esempio infettando il record di avvio principale, crittografando la tabella del file system e anche impedendo l'avvio del sistema operativo. Poco dopo questo, la vittima riceve la richiesta di riscatto. I criminali di norma cercano di espandere l'attacco e raccogliere altre credenziali e dati che riescono a trovare nella rete. Una volta terminato, il ransomware crittografa i dati di rete.

In questo esempio, il ransomware raggiunge il suo obiettivo soltanto perché è stato possibile realizzare uno scenario convincente per via di alcune vulnerabilità di sicurezza delle applicazioni su più siti: il Web scraping di un sito legittimo nel passaggio 1, il furto di credenziali nel passaggio 2, il credential stuffing nel passaggio 3, il commento spam e l'URL dannoso nei passaggi 4 e 5 e infine l'installazione dell'eseguibile nel passaggio 7. Una sicurezza delle applicazioni adeguata in ciascuno di questi passaggi avrebbe potuto bloccare l'attacco.

Barracuda

Come proteggere le applicazioni e l'accesso

Protezione della rete

Occorre evitare che il ransomware si diffonda all'interno della rete segmentandola e attuando la prevenzione delle intrusioni con una soluzione firewall di nuova generazione che:

- Fornisca sicurezza a più livelli bloccando le minacce avanzate, inclusi gli attacchi zero-day
- Includa la prevenzione delle intrusioni e il sandboxing del malware
- Fornisca una solida segmentazione della rete in modo da evitare il movimento laterale

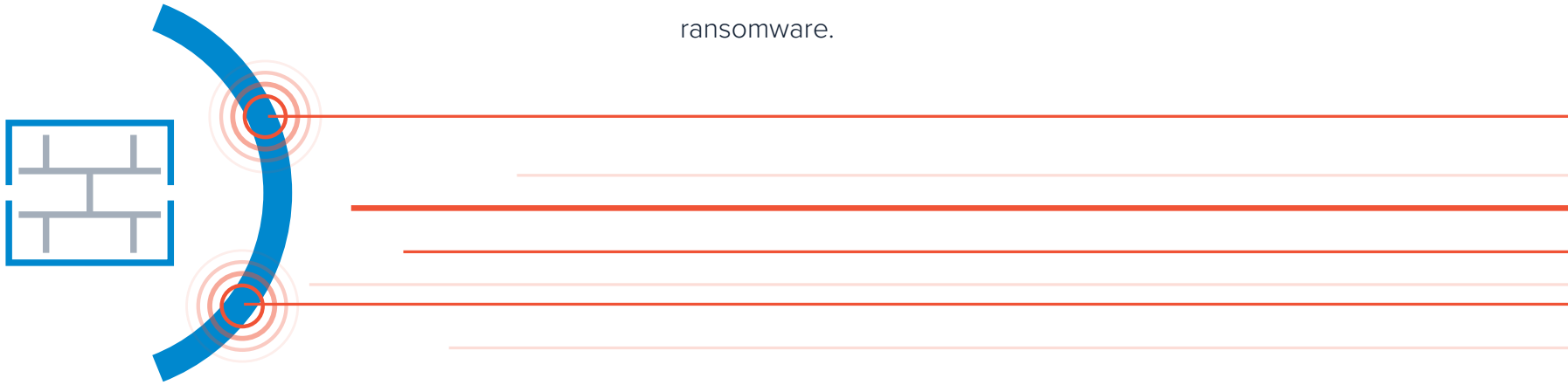
Protezione dell'accesso alle applicazioni

È necessario proteggere l'accesso alle applicazioni con una soluzione Zero Trust Network Access (ZTNA) in grado di fornire l'accesso sicuro ad applicazioni e carichi di lavoro da qualsiasi dispositivo e postazione.

La soluzione prescelta deve:

- Verificare continuamente che le risorse aziendali siano accessibili solo alle persone giuste con il dispositivo giusto
- Applicare il controllo degli accessi basato su ruoli e attributi per fornire privilegi minimi

Bloccando gli accessi non autorizzati, la tecnologia ZTNA blocca i criminali che tentano di far breccia nelle applicazioni e diffondere ransomware.



Barracuda

Protezione delle applicazioni Web

Uno dei modi migliori per implementare la sicurezza delle applicazioni è dotarsi di un Web Application Firewall (WAF) per proteggere il software, gli utenti e i relativi dati, ovunque questi si trovino. In questo modo si arrestano sia gli attacchi dei bot che di tipo denial-of-serviceye si ottiene anche una visibilità molto maggiore su ciò che accade. Una buona soluzione deve disporre delle seguenti caratteristiche:

Facilità di implementazione e personalizzabilità in base all'ambiente

Un WAF non è in grado di fornire una protezione completa se non si riesce a configurarlo per l'ambiente.

Scalabilità

La crescita dell'azienda, la trasformazione digitale e altri fattori possono incrementare i carichi delle applicazioni e dei siti Web. Il WAF prescelto deve essere in grado di crescere secondo necessità, in base ai ritmi dell'azienda.

Protezione completa dalle minacce avanzate

La protezione specificata dalla Top Ten dell'OWASP e la protezione DDoS al livello delle applicazioni costituiscono il minimo che ci si deve aspettare da un buon WAF. Per una protezione completa è possibile affidarsi a una soluzione in grado di difendere da attacchi zero-day, credential stuffing, fuga di dati, bot dannosi e altro.

Aggiornamenti semplici

Il firmware del WAF deve essere regolarmente aggiornato per migliorare la sicurezza e le funzionalità del dispositivo. Una soluzione in hosting che si aggiorna automaticamente senza l'intervento dell'amministratore è l'ideale.

Intelligence continua delle minacce

Ogni giorno vengono sviluppati nuovi attacchi, che possono diffondersi nel mondo nel giro di poche ore. Il WAF deve ricevere aggiornamenti in tempo reale su questi attacchi e utilizzare l'apprendimento automatico per adattarsi alle varianti.

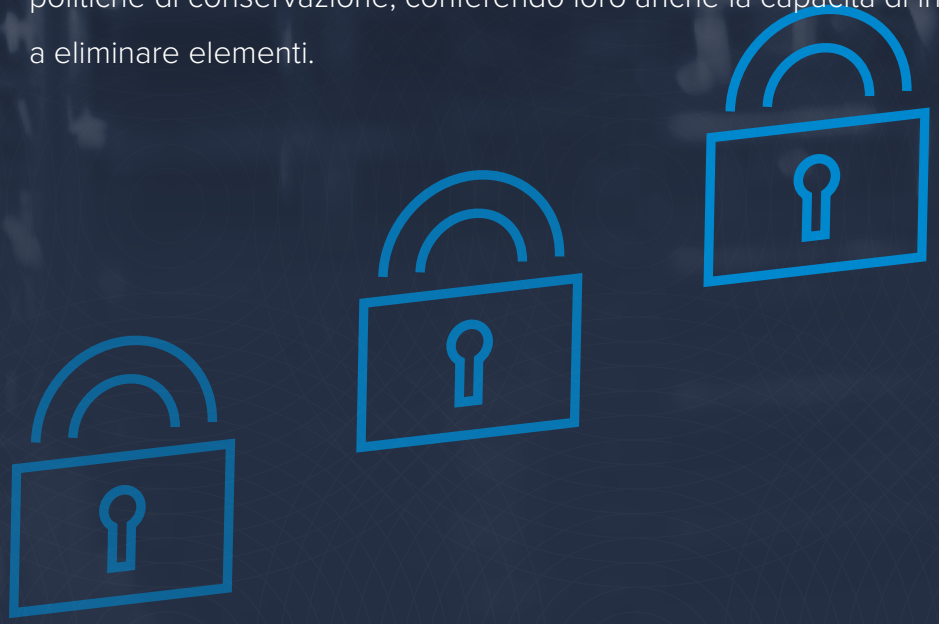
Bloccando vulnerabilità comuni delle applicazioni Web e minacce zero-day, un buon Web Application Firewall evita che il ransomware riesca a infiltrarsi nei sistemi.

Barracuda.

Passaggio 3: eseguire il backup dei dati

Una strategia di protezione da ransomware efficace dovrebbe partire dal concetto di backup e ripristino di emergenza. Il problema è che lo sanno anche i criminali.

Le soluzioni di backup sono nel mirino degli autori degli attacchi durante il periodo di “appostamento” in cui esplorano la rete. La console di amministrazione dei backup è particolarmente importante, in quanto potrebbe fornire l’accesso alle pianificazioni, alla configurazione e alle politiche di conservazione, conferendo loro anche la capacità di iniziare a eliminare elementi.



Barracuda

Prendono di mira anche l'archivio dei backup, sperando di arrivare a eliminare le copie dei file conservate sul server di backup primario e quelle secondarie per il ripristino di emergenza. Una volta carpite le password di Active Directory in modo che nessuno possa accedere al proprio account, arriva il momento di premere il grilletto e assumere il controllo.

Un concetto errato ancora fin troppo diffuso è che il ransomware non possa influire anche sui dati in cloud. Assolutamente falso.

Ad esempio, un ragazzino che naviga sul Web dal computer laptop o dal tablet che usa da casa per la scuola può essere facilmente indotto a fare clic accidentalmente su un link dannoso. Se il dispositivo utilizzato è connesso o sincronizzato con OneDrive mediante l'account Office 365 della scuola, è possibile che il file del ransomware venga caricato automaticamente in OneDrive e finisca per crittografare i file e i dati della scuola conservati nel cloud Microsoft.

Il ripristino di emergenza dev'essere considerato un componente strategico di importanza cruciale dell'infrastruttura. Va testato regolarmente e in maniera realistica, ovvero eseguendo un ripristino vero e proprio, e non soltanto verificando che sia in esecuzione.

Barracuda

Abbiamo assistito a casi in cui sono stati colpiti anche SharePoint, Exchange e altre origini dati. E se le unità di rete sono mappate a librerie di documenti residenti in Office 365, utilizzando la funzione “Apri con Esplora risorse” il ransomware può anche eseguire la scansione dei file in unità connesse e infettarli.

Anche i dati in cloud e SaaS possono essere crittografati dal ransomware. Microsoft garantisce la disponibilità del servizio, ma consiglia di eseguire il backup dei dati utilizzando una soluzione di terze parti. I dati possono essere salvati in Microsoft Office 365, ma Office 365 non è pensato per recuperare intere istanze come invece potrebbe essere necessario fare dopo un attacco ransomware.

Quindi è necessario difendere e isolare adeguatamente i dati di backup. Pensiamo alla frequenza con cui si deve eseguire il mirroring dei dati e alla velocità con cui queste immagini consentono di ricostruire i sistemi.

Occorre accertarsi che sia effettivamente possibile ripristinare i sistemi da versioni di backup in tempi accettabili e con informazioni sufficientemente aggiornate. Vale a dire che bisogna assumere il controllo e farlo davvero, non basta controllare i registri e vedere se i dati vengono replicati con una frequenza e una precisione sufficienti.

Si devono eseguire approfondimenti reali per avere le prove che i sistemi funzionino. Si può ad esempio scegliere un reparto o anche una sola applicazione anziché arrestare tutto, ma è essenziale potersi affidare completamente alla possibilità di ripristinare i sistemi in tempi accettabili.

Questo è l'ultimo baluardo di difesa. Anche se tutto il resto fallisce, se si dispone di backup veramente aggiornati e protetti i criminali non l'avranno vinta.

Il ripristino di emergenza dev'essere considerato un componente strategico di importanza cruciale dell'infrastruttura. Va testato regolarmente e in maniera realistica, ovvero eseguendo un ripristino vero e proprio, e non soltanto verificando che sia in esecuzione.

Barracuda.

Cosa serve in una soluzione di backup

Per ridurre i rischi associati al ransomware serve una soluzione di backup completa in grado di fornire quanto segue:

Archivio non modificabile

Anche qualora un criminale arrivi ai backup, non deve poter modificare o eliminare i dati.

Isolamento del cloud

Conservare una copia dei backup in un cloud sicuro residente in una rete isolata.

Autenticazione a più fattori (MFA)

Proteggere gli account e le credenziali utilizzate per l'accesso ai backup.

Ridondanza

Replicare i backup on-premise e in cloud in un'altra posizione.

Controllo degli accessi basato su ruoli

Seguire il principio del "meno autorizzazioni possibile" per tutti gli utenti che hanno accesso al sistema di backup.

Barracuda.

Conclusione

Anche se l'azienda dispone di un'assicurazione per i rischi informatici o di altre risorse per pagare il riscatto, è estremamente pericoloso presupporre che pagando i dati verranno ripristinati. Non vi è alcuna garanzia che gli hacker li decrittograferanno una volta ricevuto il riscatto e, anche qualora lo facciano, dalle ricerche più recenti emerge che l'80% delle organizzazioni che hanno pagato vengono attaccate di nuovo.

Anche facendo tutto quanto sopra descritto, si può essere attaccati comunque e anche con la migliore protezione, è sensato prepararsi al peggio. I criminali hanno milioni da investire per introdursi nei sistemi. Il solo modo assennato per prepararsi è presupporre che prima o poi riusciranno a far breccia.

- Chi sono i componenti del team di risposta al ransomware?
- Chi si chiama se succede qualcosa durante un weekend o in un giorno festivo?
- Chi è l'incaricato?
- Quando informare clienti e fornitori?
- Chi fornisce consulenza legale?
- È il caso di informare le autorità o le forze dell'ordine?
- È il caso di informare sin dall'inizio qualcuno delle pubbliche relazioni?

Bisogna quindi pensare a quello che succederà in quel momento. Serve un piano per non pagare il riscatto.

È come per le esercitazioni antincendio: non è il momento di esercitarsi quando lo stabile è in fiamme. Ma gli attacchi più probabili e oggi più diffusi sono destinati a cambiare nel tempo, per cui la strategia e le tattiche di difesa devono essere aggiornate regolarmente. Scarica la nostra checklist sul ransomware come aiuto per iniziare una pianificazione.

Barracuda

Essere preparati a rispondere a un attacco

Occorre pensare a cosa succede nel momento in cui viene identificato un attacco e a cosa succederà qualora dovesse trasformarsi in una violazione. Sarà possibile contenerlo o limitarlo a una parte dell'infrastruttura interrompendo il traffico di rete? Sarà necessario portare temporaneamente offline i sistemi? In questo caso chi si assume la responsabilità?

Qui la tempestività e la lucidità sono elementi essenziali. Non c'è tempo per aspettare che il CTO richiami. Tutti devono sapere sin da subito cosa fare.

Se si agisce abbastanza in fretta, si può anche riuscire a evitare che i dati vengano crittografati. Occorre inoltre un piano per controllare rapidamente i sistemi in modo trasversale e avere un quadro definitivo di cosa sta succedendo.

I criminali di oggi tendono a utilizzare più tipi di attacchi contemporaneamente. Mentre da un lato si cerca di arginare un attacco denial-of-service, dall'altro può arrivare un attacco ransomware. Una volta capito cosa sta succedendo e dove, si può iniziare a pensare a cosa fare per debellare il malware e riportare online i sistemi.

Una volta ripristinati i sistemi e i dati, che sia dai backup o isolando in tempo l'attacco, e avere verificato se vi sono dati danneggiati o mancanti, arriva il momento di iniziare il riesame.

A questo punto si può valutare come è stata la risposta a un vero attacco e analizzare che cosa ha funzionato bene, che cosa è andato bene soltanto per fortuna e che cosa si è rivelato carente, considerando come migliorare e accelerare la risposta la prossima volta.

Avendo a disposizione i sistemi giusti, si avranno molti dati da valutare e anche da fornire alle forze dell'ordine affinché avviino le indagini. Quali che siano le informazioni a disposizione, è opportuno prendersi il tempo di parlare con il team di risposta e tirare le fila degli insegnamenti che è possibile trarne.

Ancora una volta, non si tratta solo di tecnologia, ma anche di persone e processi. È necessario rivedere la formazione del personale? Il team di risposta ha lavorato bene o è necessario potenziarlo?

Essere sempre informati

Le moderne strategie di difesa devono essere attive, non solo reattive. Serve la massima trasparenza possibile dei sistemi di sicurezza. Bisogna osservare quello che accade, quando e con che frequenza. Occorre prestare attenzione ai colleghi, negli attacchi ransomware spesso vengono presi di mira un mercato verticale specifico o una determinata area geografica. È inoltre necessario informarsi sempre sulle ultime minacce, le tendenze e le novità del settore con risorse quali il blog Barracuda.

I dati sono di importanza cruciale per una strategia di sicurezza di successo; la posizione o il profilo dell'organizzazione può variare nel tempo. È necessario essere pronti e informati per attuare il cambiamento quando è necessario farlo. La formula security-as-a-service può essere utile per eliminare il gravoso lavoro di tenersi al passo con i nuovi sviluppi, soprattutto visto che lo scenario della sicurezza informatica è oggi più che mai in evoluzione.

Per alcune aziende che adottano una posizione molto attiva o che hanno un elevato profilo di rischio, questo può significare dedicare personale full-time al lavoro di intelligence per sapere quanto prima di possibili attacchi.

Ma per molte organizzazioni questo può anche essere eccessivo. È sufficiente scegliere il partner giusto e dotarsi di misure di base. I criminali veri, a differenza di quello che si vede nei film e in TV, non sono dei geni del male che amano scandagliare minuziosamente i sistemi di sicurezza più elaborati. La maggioranza cerca soltanto un modo semplice per far soldi ai danni di chi trascura la sicurezza o non se ne occupa, oppure non investe nei sistemi giusti.

L'adozione delle tre misure di cui si è parlato, ovvero protezione delle credenziali, messa in sicurezza delle applicazioni Web e dell'accesso e backup dei dati, non garantisce di non essere attaccati da ransomware, ma garantisce di non dover mai pagare un riscatto per riavere indietro le proprie informazioni.

Informazioni su Barracuda

Barracuda si adopera per rendere il mondo più sicuro.

Crediamo che tutte le aziende meritino l'accesso a soluzioni di sicurezza di livello enterprise abilitate al cloud, che siano semplici da acquistare, implementare e utilizzare. Proteggiamo l'e-mail, le reti, i dati e le applicazioni con soluzioni innovative espandibili e adattabili lungo il percorso dei clienti.

Oltre 200.000 organizzazioni di tutto il mondo si affidano a Barracuda per essere protette in modi per cui non sanno nemmeno di essere a rischio, per potersi concentrare sulla propria attività e salire di livello. Ulteriori informazioni sono reperibili sul sito barracuda.com.

Barracuda
Your journey, secured.