WHITE PAPER

COME DIVENTARE FORNITORI DI SERVIZI DI SICUREZZA GESTITA:
PERCHÉ È ESSENZIALE UN APPROCCIO ALLA SICUREZZA SU PIÙ LIVELLI

solarwinds msp

N4B NETWORK for BUSINESS

Distributore Autorizzato

INTRODUZIONE

I provider di servizi gestiti in grado di concentrarsi sulla sicurezza informatica potranno sfruttare diverse opportunità per incrementare il proprio fatturato. Nello specifico, implementando diversi livelli di sicurezza presso i propri clienti, potranno ridurre i costosi problemi legati alla sicurezza. Comprendere che un'efficace difesa dagli attacchi informatici coinvolge più livelli di tecnologia è fondamentale, così come essere consapevoli del fatto che le interruzioni di servizio per i clienti dei provider di servizi gestiti (MSP) rappresentano un vero e proprio disastro economico.

Il destino degli MSP e quello dei loro clienti, infatti, sono profondamente intrecciati. Di conseguenza, gli MSP devono garantire ai propri clienti un'operatività senza problemi, se desiderano che questi siano soddisfatti e paghino.

Ecco perché devono poter offrire ai propri clienti servizi di sicurezza. Aggiungendo questi servizi alle proprie offerte, gli MSP potranno sfruttare nuove opportunità di consulenza, guadagnare visibilità con i clienti di fascia alta e offrire premium suite di sicurezza conformi.

Con l'aumento degli attacchi informatici distruttivi e dei costi necessari al Disaster Recovery successivo a tali attacchi, in particolare ransomware, tutti gli MSP potranno beneficiare dall'implementazione di più livelli di difesa. In questo modo, i clienti saranno tranquilli e soddisfatti e gli MSP avranno la possibilità di incrementare il proprio fatturato.

Nel corso del presente white paper vengono illustrate le tipologie di servizi che gli MSP possono includere nella propria offerta per garantire ai propri clienti servizi di sicurezza realmente gestiti. Vengono inoltre analizzati i tipi di attacchi che i provider di servizi possono evitare ai clienti e vengono delineate alcune linee guida sui basilari principi di progettazione e metodologia della sicurezza necessari agli MSP che desiderino considerare questa nuova opportunità di guadagno.

SOMMARIO

Le prime pagine dei giornali sono piene di notizie su violazioni di dati e di dettagli su come ancora un'altra organizzazione o impresa abbia perso informazioni critiche sui propri clienti, subito spiacevoli e imbarazzanti inconvenienti e affrontato una perdita economica significativa.

HACKING: PERCHÉ LA SICUREZZA È UN ASPETTO FONDAMENTALE

Ogni mese, le prime pagine dei giornali sono piene di notizie su violazioni di dati e di dettagli su come ancora un'altra organizzazione o impresa abbia perso informazioni critiche sui propri clienti, subito spiacevoli e imbarazzanti inconvenienti e affrontato una perdita economica significativa, a causa di un attacco informatico. Nella sezione seguente vengono forniti alcuni esempi e sottolineati i punti deboli dell'infrastruttura aziendale a causa dei quali si sono verificati tali disastri. Tali informazioni sono particolarmente utili per progettare una soluzione di sicurezza finalizzata alla protezione dei propri clienti.

· JAPAN AIRLINES

La Japan Airlines si è resa conto di aver subito un attacco solo in seguito all'analisi dei motivi per cui le prestazioni di rete risultavano stranamente scarse. L'azienda ha rilevato che gli hacker erano riusciti a introdursi nei sistemi aziendali e a estrarre informazioni sui clienti, quali nomi, sesso, date di nascita, indirizzi postali e e-mail, nonché le sedi di lavoro dei partecipanti al programma fedeltà di JAL[1]. Quasi 750.000 clienti sono stati interessati dall'attacco informatico, che ha infettato 23 computer presenti sulla rete con malware. Si pensa che l'attacco sia stato sferrato mediante un'e-mail di phishing.

VETTORI DI ATTACCO:

- E-mail di phishing
- Drive-by-download o allegati nocivi
- Trojan horse

· JAPAN PENSION SERVICE

Il Japan Pension Service ha perso 1,25 milioni di record di clienti a causa di allegati e-mail con malware inviati dagli hacker sotto forma di documenti provenienti dal ministero della salute. Secondo fonti ufficiali, sono stati compromessi dati sul cassetto previdenziale, nomi, date di nascita e indirizzi.

VETTORI DI ATTACCO:

- E-mail di spear phishing
- Allegati dannosi
- Trojan horse

· ANTHEM

All'inizio del 2015, il colosso assicurativo nel settore sanitario Anthem ha perso le informazioni personali, inclusi numeri di previdenza sociale, date di nascita, indirizzi postali e numeri di telefono, di circa 80 milioni di clienti. Gli hacker hanno configurato un dominio fittizio su cui era ospitato malware. I dipendenti di Anthem venivano invogliati a visitare il sito dannoso tramite e-mail di phishing mirate con link incorporati.

VETTORI DI ATTACCO:

- E-mail di phishing
- Drive-by-download
- Trojan horse

Per le proprie attività fraudolente, gli hacker si avvalgono di un'ampia gamma di vettori e di approcci di attacco.

· AUSTRALIAN BROADCASTING CORPORATION

La Australian Broadcasting Corporation è stata colpita da un attacco ransomware che ha interrotto il palinsesto dei notiziari per 24 ore. Gli hacker avevano inviato ai dipendenti della rete televisiva allegati con malware, tramite e-mail che sembravano provenire da Australia Post.

Quando i dipendenti dell'azienda aprivano le e-mail visualizzavano un messaggio che li informava del mancato recapito di un pacco. Nel momento in cui aprivano l'allegato per saperne di più, le loro macchine venivano infettate da ransomware[2].

Gli attacchi crypto-ransomware rappresentano una minaccia sempre più pericolosa per le imprese. Si tratta infatti di malware che crittografano i documenti memorizzati sull'hard disk delle vittime, rendendoli inaccessibili fino al pagamento di un "riscatto" (ransom) in denaro (generalmente tramite bitcoin). Sebbene si tratti di una minaccia ancora relativamente rara rispetto ad altre tipologie di malware, si sta diffondendo rapidamente. Secondo l'Internet Security Threat Report di Symantec del 2015, alla fine del 2014 gli attacchi crypto-ransomware flagellavano circa 1.000 computer ogni giorno[3]. Da allora il numero è cresciuto.

VETTORI DI ATTACCO:

- E-mail con payload ransomware allegato

· ATTACCO WEB DRUPAL 7

Nell'ottobre 2014, gli hacker hanno individuato e sfruttato a loro vantaggio un bug presente nel popolare sistema di gestione contenuti, Drupal 7. Durante questi attacchi, venivano inviate richieste opportunamente preparate che causavano esecuzioni SQL arbitrarie, compromettendo il sito ospitato. A causa del bug, è stato possibile prendere il controllo di un server su cui è ospitato un sito basato su tecnologia Drupal, eseguire il download dei dati memorizzati sul server e utilizzare il sito per distribuire malware agli ignari visitatori.

Durante l'attacco, i server Drupal interessati hanno funzionato come un'armata di bot. I visitatori hanno subito i danni di uno script di software dannoso che li ha usati per tentare di individuare altri server Drupal vulnerabili e infettare ancora più siti Web.

Sebbene sarebbe stato possibile evitare l'attacco poiché gli sviluppatori software di Drupal avevano già risolto il bug, molti amministratori del sito non avevano caricato la patch necessaria.

VETTORI DI ATTACCO:

- Software senza patch
- Attacco di tipo SQL injection
- Exploitation automatica
- Sito di drive-by-download

Per un'efficacia ancora maggiore, gli MSP devono conoscere l'azienda e le relative procedure operative fondamentali.

COME EVITARE ATTACCHI AI CLIENTI

Gli MSP hanno l'opportunità di offrire servizi più efficaci ai propri clienti, rendendo i loro sistemi informatici meno vulnerabili agli attacchi, installando una suite di strumenti utilizzabili per proteggere computer e reti dei clienti.

Per un'efficacia ancora maggiore, gli MSP devono conoscere l'azienda e le relative procedure operative fondamentali. I sistemi critici vanno protetti a fondo con più livelli di sicurezza rispetto ai sistemi generici. Gli MSP, inoltre, possono implementare misure di protezione per ogni fase di un eventuale attacco: prima, durante e dopo.

- **PRIMA**

  Prima di un attacco, è necessario potenziare l'infrastruttura IT e implementare criteri di protezione ancora più severi. Per proteggere i clienti da potenziali minacce, è necessario implementare una serie adeguata di strumenti e formare il personale in modo opportuno. È fondamentale progettare un solido sistema di backup cloud e locale. Per gli attacchi comuni, è sufficiente rimuovere i privilegi amministrativi locali e applicare patch e aggiornamenti al sistema.

- **DURANTE**

  Potenziare i sistemi per proteggerli da eventuali attacchi non impedirà agli hacker di tentare di penetrare i sistemi dei clienti e di accedere ai dati su di essi presenti. Ecco perché gli MSP devono essere in grado di individuare un attacco nel momento stesso in cui viene sferrato, di bloccarlo per evitare danni ai sistemi presi di mira e, infine, di difendere i sistemi da ulteriori intrusioni dell'hacker. Le regole firewall per il traffico in uscita che consentono di rilevare attività inconsuete su workstation e server e la registrazione degli eventi sono fondamentali per rilevare attività sospette e dannose. Inoltre, antivirus, filtri e-mail e protezione Web sono tutte tecnologie attive che consentono di sconfiggere e arginare gli attacchi informatici.

  Ad esempio, per ostacolare un attacco zero-day è possibile abilitare i controlli del registro eventi per analizzare eventuali attività sospette sulla rete del cliente.

  È possibile impostare un controllo specifico per osservare le macchine presenti sulla rete e individuare se Acrobat.exe o Flash.exe generano un errore di protezione generale. Se quando si apre un file PDF o si fa clic su un video online, Adobe Reader smette di funzionare, è possibile che si sia verificato un errore critico a livello software e ciò potrebbe indicare un attacco zero-day. .

  Il computer viene utilizzato come punto di appoggio per accedere ad altre componenti della rete e sferrare un attacco ad ampio raggio sulla rete.

È importante capire come comportarsi al termine di un attacco e migliorare il proprio approccio imparando dall'accaduto.

· DOPO

Gli MSP che offrono servizi a diversi clienti potrebbero rilevare vari attacchi durante un singolo anno. È importante capire come comportarsi al termine di un attacco e migliorare il proprio approccio imparando dall'accaduto. Dopo aver respinto con successo un attacco, è necessario comprenderne la portata, contenere eventuali danni, in modo da proteggere gli altri sistemi, e ripristinare eventuali danni. Nella maggior parte dei casi, questo implica il ripristino dei dati e/o la creazione di una nuova immagine del sistema. Gli MSP devono sempre e senza eccezioni garantire ai propri clienti la resilienza operativa.

Essi inoltre dovranno raccogliere dati e informazioni sui sistemi interessati dall'attacco e utilizzarli in modo proattivo per irrobustire ulteriormente i propri sistemi e migliorare costantemente i servizi offerti ai clienti. Non sempre è necessario implementare le tecnologie più all'avanguardia nell'immediato: talvolta per mitigare un attacco è sufficiente eliminare il software dannoso (ad esempio, Adobe Flash) o applicare opportuni privilegi per i software scaricati. A volte, per evitare molti dei più comuni attacchi informatici, basta impedire agli utenti di installare software sulle macchine.

Proprio come gli intrusi nei nostri appartamenti, molti hacker sono estremamente calcolatori e scelgono l'obiettivo meno protetto.

IMPORTANZA DI UN APPROCCIO DI SICUREZZA SU PIÙ LIVELLI

A supporto di tutte queste procedure di sicurezza è il concetto di sicurezza su più livelli. Si tratta di un metodo che impiega diverse linee di difesa per respingere eventuali attacchi e si basa sul principio per cui nessuna forma di protezione singola è sufficiente a fermare un criminale informatico risoluto.

Per comprendere al meglio tale approccio, basta considerare un sistema IT come un'abitazione, all'interno della quale sono presenti tutti i nostri oggetti di valore. È abbastanza semplice installare un chiavistello alla porta per tenere lontani eventuali malintenzionati durante la notte. Ma questa misura non è utile quando in casa non c'è nessuno, quindi è necessario montare una serratura di sicurezza, che comunque non protegge le finestre, facilmente raggiungibili data la loro altezza rispetto al suolo ed anche estremamente fragili. Per proteggere quest'altra via di accesso, è necessario installare delle barre di ferro, ma, ancora meglio, un allarme antifurto nel caso in cui i malintenzionati trovino comunque il modo di entrare. Infine, installare luci di sicurezza sul retro dell'abitazione impedirà a eventuali malintenzionati di avvicinarsi durante la notte, scoraggiando ulteriormente gli intrusi. A questo punto, ai ladri non rimane che scegliere un'altra abitazione con meno difese.

Proprio come gli intrusi nei nostri appartamenti, molti hacker sono estremamente calcolatori e scelgono l'obiettivo meno protetto. Implementare diverse misure di difesa può scoraggiare i malintenzionati virtuali, tuttavia valutare i punti deboli di un sistema IT potrebbe risultare più problematico che identificare i possibili punti di accesso di un'abitazione. Ed ecco l'importanza di un approccio su più livelli.

Sono sette gli elementi che costituiscono una strategia di difesa su più livelli efficace; tali elementi interagiscono fra loro e formano una rete di protezione intorno ai sistemi dei clienti.

Solitamente, infatti, prendono di mira un software non ancora aggiornato per la protezione da vulnerabilità note.

DEFINIZIONE DI UN APPROCCIO DI SICUREZZA SU PIÙ LIVELLI

1. GESTIONE DELLE PATCH

Una tecnica comunemente utilizzata dagli hacker è quella di prendere di mira un software non ancora aggiornato per la protezione da vulnerabilità note.

Molti attacchi utilizzano software cui non sono ancora state applicate le patch, anche quando i difetti dell'applicazione sono ormai noti. I difetti dei software sono catalogati nel database Common Exposures and Vulnerabilities (CVE) gestito da MITRE Corp. Secondo Verizon, il 99,99% degli exploit utilizzati nel 2014 ha sfruttato le vulnerabilità cui era stata assegnata una classificazione CVE almeno un anno prima4.

Di fatto, la situazione è ancora peggiore di quella appena delineata. Secondo il rapporto di Verizon, infatti, sono oltre 30 gli exploit responsabili di violazioni dei dati nel 2014 che hanno avuto origine da minacce aggiunte al database CVE per la prima volta nel 1999. Proprio così: le aziende continuano a perdere dati a causa di hacker che utilizzano difetti di sicurezza segnalati prima ancora della diffusione del famoso worm ILOVEYOU. L'importanza di applicare le opportune patch ai software è tale che l'Australian Signals Directorate lo segnala come un requisito obbligatorio per ridurre le intrusioni informatiche5.

Se gli operatori di Drupal 7 menzionati in precedenza avessero correttamente applicato le patch ai propri sistemi, i loro siti Web non sarebbero stati compromessi e gli ignari visitatori non avrebbero subito alcun attacco. Invece, gli hacker che hanno progettato l'attacco sfruttando un bug noto di Drupal hanno potuto contare sul fatto che tanti operatori non avevano aggiornato i propri software per eliminare il bug.

Una volta individuato un difetto in una particolare porzione di software (ad esempio, un sistema operativo, un motore di database, un framework applicativo o un'applicazione software), i criminali informatici sono in grado di scrivere senza problemi script per cercare su Internet le versioni del software in esecuzione e tentare di comprometterle. I toolkit di attacco progettati per le ricerche degli hacker contengono i cataloghi di tali difetti aggiornati regolarmente, insieme a codici progettati per sfruttare tali falle, cosa che offre a persone senza scrupoli armi informatiche già pronte all'uso.

La gestione delle patch rappresenta una misura di sicurezza di facile utilizzo per gli amministratori IT, che possono automatizzare in una certa misura le procedure di applicazione di tali patch al software tramite strumenti di scripting o sistemi più sofisticati che documentano, scaricano, testano e gestiscono le patch di diversi fornitori software.

Prima di applicare le patch, è buona prassi consultare i social media e testare le patch su un solo sistema per un giorno intero prima dell'implementazione su larga scala. Talvolta, infatti le patch risultano difettose anche se sottoposte a opportuni test da parte del fornitore. Sebbene una patch possa causare problemi sul sito di un cliente, è decisamente preferibile installare una patch problematica piuttosto che subire un attacco informatico; nel caso di una patch difettosa, infatti, si conosce perfettamente l'origine di un'interruzione

Con tutti questi attacchi che sfruttano i malware come punto di accesso alle reti aziendali, installare un buon software antivirus non è soltanto una possibilità, ma un vero e proprio obbligo.

2. ANTIVIRUS

I servizi antivirus dovrebbero rappresentare una componente chiave dell'arsenale di ogni MSP. Sebbene da soli non rappresentino una protezione sufficiente in caso di attacchi, gli antivirus offrono una prima linea di difesa da software dannosi utilizzabili dagli hacker come punto d'appoggio per accedere ai sistemi aziendali. Le linee guida sulle buone prassi e i requisiti di conformità impongono l'implementazione di difese antimalware. Gli hacker, infatti, spesso utilizzano trojan horse e malware "noti" per colpire i propri obiettivi, pertanto, un antivirus aggiornato con le ultime definizioni dei virus è in grado di rilevare regolarmente e rimuovere eventuali trojan horse e malware.

Le tecnologie antivirus si sono evolute nel corso degli ultimi anni e ora dispongono di funzionalità euristiche e di altre caratteristiche avanzate in grado di rilevare virus e trojan horse fino a quel momento sconosciuti. Grazie agli aggiornamenti delle firme basati su cloud, i fornitori di soluzioni di sicurezza proteggono i clienti degli MSP dai nuovi ceppi di malware non appena si rendono disponibili. Poiché i fornitori di antivirus rilevano in media 200.000 nuovi ceppi malware ogni giorno, gli aggiornamenti in tempo reale rappresentano un aspetto critico del panorama antivirus odierno.

Con tutti questi attacchi che sfruttano i malware come punto di accesso alle reti aziendali, installare un buon software antivirus non è soltanto una possibilità, ma un vero e proprio obbligo.

3. PROTEZIONE WEB

Neanche le tecnologie antivirus sono perfette, purtroppo: potenzialmente sono in grado di identificare una firmamalware, ma non è detto che accada. Tali tecnologie potrebbero rilevare comportamenti sospetti di un'applicazione, ma talvolta li ignorano. Poiché molti ceppi malware vengono diffusi tramite browser, la protezione Web è un'altra componente fondamentale di un'efficace strategia di difesa multilivello.

Gli MSP possono utilizzare tali tecnologie per rilevare i siti visitati dai dipendenti del cliente o eventuali macchine infette che navigano su Internet senza autorizzazione. Proprio come ogni software antivirus, anche i servizi di protezione Web ricevono regolari aggiornamenti, quali i nomi di dominio e gli indirizzi IP associati a comportamenti dannosi, e possono essere utilizzati per bloccare la navigazione dalle reti aziendali.

I servizi di protezione Web, inoltre, consentono agli MSP di offrire un valore aggiunto ai propri clienti. Essi infatti sono utilizzabili come meccanismi di individuazione di eventuali attività di navigazione sospette, sintomi di un attacco in corso. Tali servizi di protezione Web sono inoltre utilizzabili per impedire ai dipendenti di visitare siti legittimi ma comunque sgraditi al datore di lavoro, ad esempio, pagine sportive o di intrattenimento, al fine di aumentare la produttività.

Secondo il Verizon Data Breach Incident Report (DBIR), il 54% delle infezioni da malware è dovuto alla navigazione sul Web. I browser interagiscono con i computer molto più dei client e-mail e spesso gli utenti vi installano un elevato numero di plug-in di terze parti per aggiungere altre funzionalità. Questo amplia la superficie di attacco del browser e lo rende un bersaglio particolarmente interessante.

Poiché tratta di uno dei più diffusi e importanti strumenti aziendali, la posta elettronica rappresenta ancora uno dei principali sistemi di diffusione di minacce da parte di hacker senza scrupoli.

4. PROTEZIONE E-MAIL

Poiché si tratta di uno dei più diffusi e importanti strumenti aziendali, la posta elettronica rappresenta ancora uno dei principali sistemi di diffusione di minacce da parte di hacker senza scrupoli, che, tramite questo mezzo, inviano link a siti Web dannosi o allegati contenenti malware direttamente ai dipendenti. Le e-mail rappresentano un potenziale veicolo di ingegneria sociale, vale a dire che gli hacker possono apprendere le informazioni su un'azienda e inserire dettagli pertinenti in un'e-mail destinata ai dipendenti.

Oltre a far sentire i clienti più al sicuro, fornendo servizi di sicurezza e-mail ai clienti agli MSP potranno garantire loro alcuni vantaggi significativi. La ricerca di particolari schemi in grandi quantitativi di spam potrebbe fornire ai provider di servizi informazioni fondamentali sulle tipologie di attacchi diretti ai clienti per individuare, ad esempio, che un elevato numero di e-mail viene inviato a determinati dipendenti come parte di una campagna mirata.

Gli MSP possono inoltre garantire ai clienti migliori prestazioni di rete e costi di banda potenzialmente inferiori, offrendo loro un servizio basato su cloud per la protezione delle e-mail: l'MSP infatti si occuperà di analizzare e ripulire i flussi di posta elettronica prima di inoltrarli all'azienda. Questo permette anche di evitare che le reti dei clienti siano intasate da traffico indesiderato. È inoltre possibile configurare la rete perché accetti solo e-mail provenienti dal servizio basato su cloud dell'MSP, proteggendo ulteriormente i clienti da eventuali attacchi.

Secondo il Verizon Data Breach Incident Report (DBIR), il 77% delle infezioni da malware è causato da utenti che ricevono un'e-mail dannosa contenente un allegato o un link Web. Un servizio di protezione per la posta elettronica basato su cloud offrirà un ulteriore livello di sicurezza affidabile.

Bisogna essere onesti: gli incidenti di sicurezza possono essere davvero dispendiosi e danneggiare la reputazione degli MSP.

5. BACKUP

L'esecuzione di backup efficaci rappresenta il cardine finale della protezione e un servizio fondamentale in una strategia di sicurezza multilivello. Proteggere i clienti dagli attacchi può offrire loro tranquillità dal punto di vista della sicurezza, ma la sicurezza informatica non è un gioco a somma zero: persino i sistemi di protezione più all'avanguardia rischiano di essere compromessi. La minaccia di un attacco, insieme al rischio della perdita fisica di dati, rende il backup una componente cruciale di qualsiasi servizio di sicurezza informatica.

Gli MSP devono garantire di disporre di un servizio di backup comprovato e testato. I servizi di backup cloud frequenti e incrementali sono più semplici da testare e rappresentano una garanzia per i clienti; inoltre l'assenza di supporti fisici per il backup riduce il rischio di danneggiamento, perdita o furto dei dati di backup.

Non si è mai troppo scrupolosi con il backup. A causa della diffusione di attacchi di tipo ransomware, i clienti necessitano di un backup in loco e anche di un backup basato su cloud. Disporre di un backup cloud soddisfa i requisiti di conformità e le best practice per i backup off-site quotidiani e inoltre spesso le tecnologie impiegate non sono accessibili ai ransomware. Ciò consente di ripristinare i file in caso di diffusione di un attacco che superi le barriere difensive.

I backup in loco consentono il restore più rapido di file di grandi dimensioni o di un'elevata quantità di file. È davvero una buona prassi disporre della ridondanza locale e su cloud per il backup per evitare lo stress dei tempi di risposta a eventuali incidenti. Con la consapevolezza che il backup sia una buona norma, gli MSP avranno a disposizione efficienti capacità di risposta a eventuali incidenti per rendere il cliente nuovamente operativo.

Bisogna essere onesti: gli incidenti di sicurezza possono essere davvero dispendiosi e danneggiare la reputazione degli MSP

6. SERVIZI DI SICUREZZA SU PIÙ LIVELLI

Gli MSP che applicano tariffe per dispositivo o per utente dovrebbero prendere in considerazione la possibilità di implementare tutti i livelli di sicurezza possibili. Ogni volta che un MSP è costretto a rispondere a un incidente di sicurezza IT di un cliente, raramente la soluzione è semplice o rapida e, in genere, anche se non sempre, richiede una visita in loco. Il calcolo è semplice: sono i lavori effettivamente fatturabili a garantire un maggiore ritorno sull'investimento e non gli interventi di rimozione di malware dai sistemi, di ripristino dei dati o di reinstallazione di sistemi operativi. Meno tempo si perde a rispondere a complesse chiamate sulla sicurezza, meglio è.

Si tratta di numeri. La minaccia costituita dagli hacker è costante: dal semplice attacco di tipo brute force ai danni di VPN, RDP, Outlook Web Access e altri servizi esposti, ai sofisticati attacchi spear phishing. Gli MSP devono implementare quanti più servizi di sicurezza possibili, poiché essi, in modo economicamente vantaggioso, consentono di ridurre le probabilità di incidenti di sicurezza devastanti per i clienti.

Nel mercato odierno, il modello SaaS (Security as a Service, sicurezza come servizio) è davvero molto diffuso, secondo Gartner e altre società di analisi. I software di sicurezza offerti in abbonamento rappresentano la modalità più economicamente vantaggiosa per ridurre gli incidenti di sicurezza per i clienti. Bisogna essere onesti: gli incidenti di sicurezza possono essere davvero dispendiosi e danneggiare la reputazione degli MSP.

7. LA REPUTAZIONE È TUTTO

Eventuali interruzioni dovute a malware o altri attacchi sono considerate come un vero e proprio insuccesso dell'MSP. Parliamoci chiaro, questi incidenti potrebbero facilmente comportare per qualsiasi MSP il termine della collaborazione con il cliente, se quest'ultimo non ritorna più operativo e l'MSP in questione si barcamena nel tentativo di risolvere il problema. Di tutti i servizi illustrati, nessuno è tanto importante quanto il backup, che rappresenta il livello di sicurezza più rilevante, in quanto protegge da ogni tipologia di minaccia: fisiche, lato cliente, lato MSP e attacchi dei criminali informatici.

L'obiettivo ultimo di un'offerta di servizi di sicurezza gestita è rendere i clienti obiettivi difficili da colpire per gli hacker. Non sarebbe giusto né leale promettere ai propri clienti una sicurezza completa e inattaccabile, ma è possibile offrire loro una solida armatura in cambio di pagamenti regolari relativamente contenuti.

Grazie ai servizi di sicurezza implementati, i clienti degli MSP saranno soddisfatti e produttivi. Dato l'aumento delle minacce, è evidente che sia opportuno distribuire livelli di sicurezza in modo che gli MSP possano concentrarsi su altri progetti e sulla crescita dell'attività, anziché intervenire in loco presso i clienti per risolvere un costoso problema di sicurezza.

ALCUNE RIFLESSIONI FINALI

I servizi di sicurezza gestita rappresentano un nuovo e proficuo settore di attività per gli MSP. Infatti, con il continuo aumento di attacchi informatici, gli MSP che non offrono questa tipologia di servizi rischiano di perdere opportunità commerciali e di non restare al passo con la concorrenza. Per offrire servizi di sicurezza degni di tale nome, è necessario adottare un approccio multilivello. Con soluzioni antivirus, di gestione delle patch e di protezione Web, i clienti diventeranno bersagli davvero difficili da colpire; inoltre, grazie a sistemi di backup e ripristino, il restore dei dati e il ripristino della continuità operativa aziendale in caso di attacco informatico saranno molto più semplici.

In altre parole, offrire servizi di sicurezza su più livelli non solo dà accesso a nuovi introiti, ma garantisce la soddisfazione dei propri clienti che si sentiranno sicuri e protetti. E sappiamo bene che un cliente soddisfatto è un cliente fedele.

RIFERIMENTI

1. http://www.wsj.com/articles/japan-airlines-reports-hacker-attack-1412053828
2. http://www.csoonline.com/article/2692614/malware-cybercrime/ransomware-attack-knocks-tv-station-off-air.html
3. http://www.symantec.com/security_response/publications/threatreport.jsp
4. http://www.verizonenterprise.com/DBIR/2015/
5. http://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

SICUREZZA MULTILIVELLO

INTELLIGENCE COLLETTIVA

MULTIPIATTAFORMA

SolarWinds MSP offre agli MSP globali di qualsiasi dimensione gli strumenti più adatti per creare attività molto redditizie ed efficaci che apportino un vantaggio competitivo misurabile. Le soluzioni integrate per la gestione di automazione, sicurezza, reti e servizi, sia on-premise sia su cloud, supportate da approfondimenti fruibili sui dati, aiutano gli MSP a completare il proprio lavoro in modo più facile e veloce. Grazie a SolarWinds MSP, gli MSP possono finalmente occuparsi di ciò che conta: la conformità agli SLA e la creazione di attività redditizie.

Per ulteriori informazioni, visitare la pagina www.solarwindsmsp.com

RMWP00087IT0717