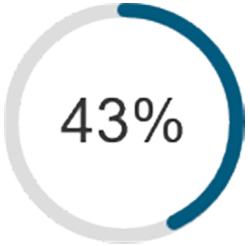
I fondamenti della sicurezza per PMI

Mantieni il controllo della sicurezza

Scopri come si presenta l'attuale panorama delle minacce informatiche per le PMI in modo che la tua azienda possa sopravvivere; riduci i costi operativi e fai crescere il business in modo sicuro; fai sì che la sicurezza diventi una priorità per tutti e proteggi la tua azienda con Cisco.

Più l'azienda cresce, più attira l'attenzione, e non sempre si tratta di un'attenzione positiva: un numero crescente di sofisticate organizzazioni criminali è alla caccia di PMI.



Il 43%

degli attacchi informatici prende di mira le piccole imprese. [1]

Il 60%

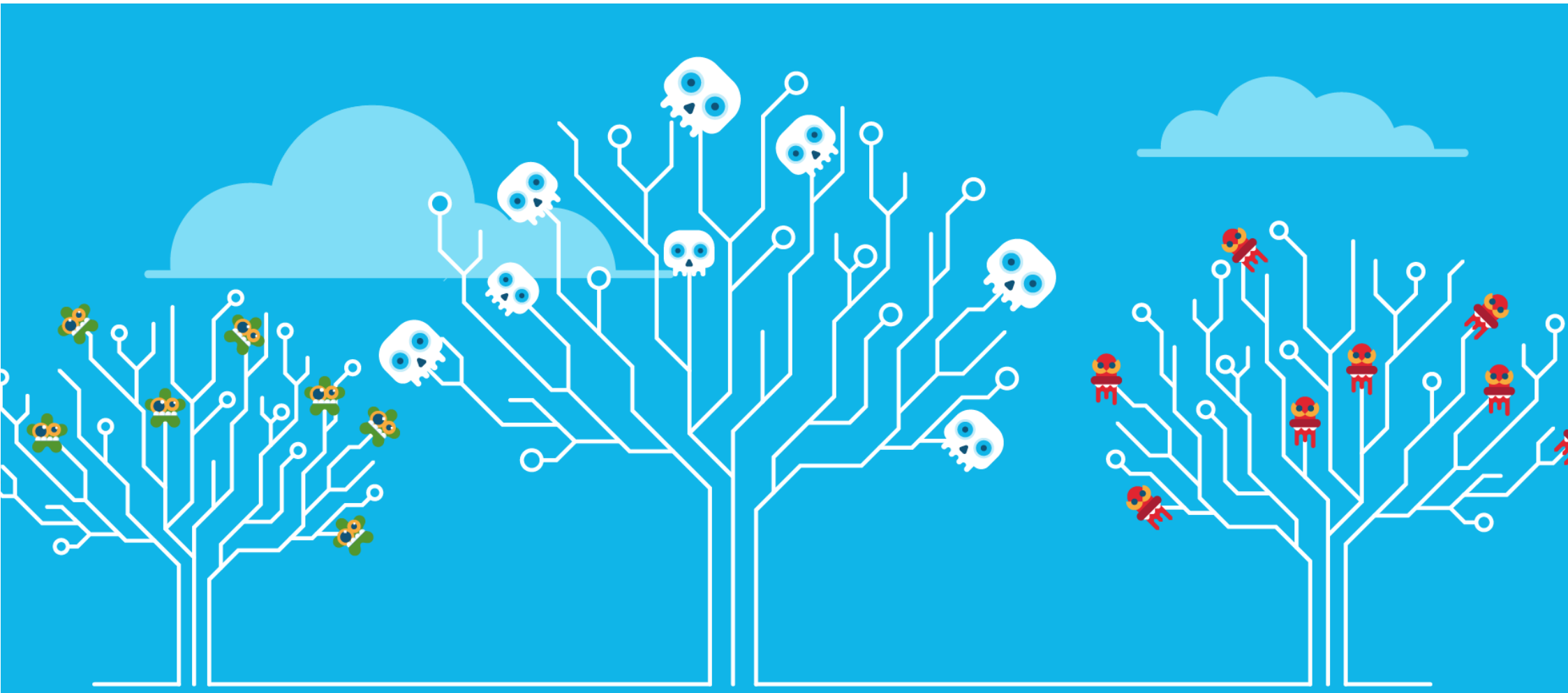
è costretta a chiudere per le conseguenze. [1]

Report annuale di Cisco sulla cybersecurity 2018 "Cisco ACR 2018"

$ 2.235.018 all'anno

La spesa media per le PMI in seguito a una violazione dei dati o a un attacco informatico a causa dei danni o del furto di risorse IT e all'interruzione delle normali operazioni.

È una dura verità: la sopravvivenza della tua azienda dipende dalla comprensione della sicurezza informatica.



Le minacce stanno diventando più sofisticate

Gli hacker conoscono i tuoi punti deboli e sanno come sfruttarli

Attualmente, solo una minoranza degli hacker agisce “solo per divertimento” o per sfida. La maggior parte sono spinti da motivazioni economiche, sono estremamente organizzati e raramente lavorano da soli. Gli hacker sono agili, mentre non si può sempre dire lo stesso delle aziende, soprattutto quando sono alle prime armi sul fronte della sicurezza.

L’obiettivo di un hacker è quello di rubare i dati delle carte di credito, gli indirizzi e-mail, i nomi utente e le password. Ossia tutto quello che possa essere venduto al miglior offerente. *Tra le tecniche* che sfruttano per raggiungere i loro obiettivi troviamo le seguenti.

Ransomware

Gli hacker possono virtualmente tenere in ostaggio le aziende con il ransomware, una pratica spietata che cripta da remoto i file senza il tuo consenso. Alcune forme di ransomware sono programmate per diffondersi nella rete.

Invece di richiedere che un destinatario apra l’allegato di un’e-mail o faccia clic su un link, la tendenza attuale è diversa. Il ransomware abilita la trasmissione del codice dannoso tra le reti senza l'interazione dell'utente (come ad esempio WannaCry, che ha iniziato a diffondersi nel maggio 2017). “WannaCry è il primo ransomware completamente automatizzato”, spiega Craig Williams, responsabile senior del programma di sicurezza di Talos, il ramo di Cisco dedicato alle ricerche sulla sicurezza.

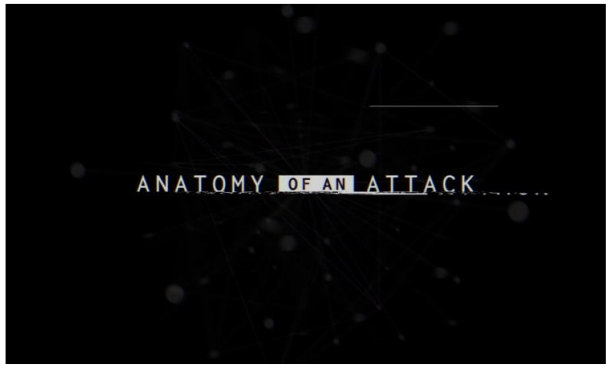
WannaCry ha interessato più di 200.000 computer in tutto il mondo e si stimano perdite per circa 4 miliardi di dollari. Questo ransomware viene installato sfruttando una vulnerabilità del protocollo SMB di Microsoft ed è particolarmente efficace in ambienti Windows più vecchi, come Windows XP, Windows Server 2003 e Windows 8. Microsoft aveva già rilasciato un aggiornamento della sicurezza per correggere questa vulnerabilità, ma non tutti gli utenti erano protetti automaticamente.

PMI tenute in ostaggio

Secondo i risultati del report “2017 State of Cybersecurity in Small and Medium-Sized Businesses (SMB)” del Ponemon Institute, il 52% delle PMI intervistate ha subito un attacco ransomware (andato o meno a segno) in un lasso di tempo di 12 mesi. Una volta completata l’infezione, sullo schermo compare un messaggio con la richiesta di pagare un riscatto in bitcoin per riavere i propri dati. In genere la cifra del riscatto varia dalle £ 200 (circa € 225) alle £ 10.000 (circa € 11.230), ma alcune vittime hanno pagato molto di più.
Notizie recenti mettono in luce l’esistenza di una nuova generazione di minacce ormai virale su scala globale e che prolifera con una rapidità senza precedenti. Il gruppo di ricerca sulle minacce Cisco Talos ha scoperto una minaccia, chiamata VPNFilter, che ha compromesso oltre 500.000 router o dispositivi Network Attached

Storage di piccole sedi o uffici domestici a livello globale. I dispositivi Cisco non sono stati colpiti. Questa minaccia complessa consente all'autore di analizzare il traffico che passa attraverso i dispositivi, di rubare i file da unità di backup della rete e potenzialmente di sfruttarli per accedere alle reti aziendali connesse.

I criminali informatici conoscono a fondo i loro bersagli, compresi i loro gusti e il modo in cui conducono gli affari. Sanno quanto pagheranno per il rilascio dei loro dati e sfruttano senza pietà tutti i punti deboli che riescono a individuare.



BEC (Business E-mail Compromise)

Gli attacchi BEC sono il 75% più redditizi del ransomware. Eppure non se ne parla così tanto.

I BEC (Business E-Mail Compromise) sono attacchi mirati che utilizzano tecniche di social engineering per indurre le persone a trasferire denaro a favore degli hacker. Non c'è nessun malware, non ci sono allegati. A differenza degli attacchi ransomware, non sottraggono alcun dato alle vittime. Tutto si basa su false dichiarazioni e istruzioni fraudolente.

Di solito gli hacker studiano per qualche tempo l'azienda target e iniziano a costruire un profilo. Quando hanno raccolto abbastanza informazioni, inviano e-mail di spear-phishing ai ranghi più alti del personale, spesso del dipartimento finanziario. In ogni caso deve trattarsi di una persona in grado di autorizzare trasferimenti di denaro. Più è grande l'azienda, più soldi possono ottenere. Tuttavia, gli attacchi rivolti a piccole e medie imprese sono in aumento.

Più è grande l'azienda, più soldi possono ottenere. Tuttavia, gli attacchi rivolti a piccole e medie imprese sono in aumento.

Violazione dei dati

I dati sono al centro di tutte le attività dell'azienda: si tratta di proprietà intellettuale, della prossima grande occasione, dei record dei clienti, del fatturato. I costi di una violazione vanno ben oltre la correzione delle interruzioni e dei sistemi danneggiati.

Costruire una postura della sicurezza solida può aiutare a proteggere la proprietà intellettuale e la reputazione della tua azienda. In media, le aziende impiegano 191 giorni per rilevare una violazione e 66 giorni per contenerla. (Fonte: Ponemon Institute). Eppure la soluzione per limitare i danni è il rilevamento precoce.

La media dei tempi di rilevamento di Cisco è pari a 3,5 ore. Se si verifica una violazione, gli esperti dei Cisco Incident Response Services sono disponibili nel giro di poche ore per aiutarti a contenere e risolvere le cause profonde.

Attacchi alla filiera di approvvigionamento

Gli attacchi alla filiera di approvvigionamento costituiscono una minaccia informatica emergente e in crescita, il che dimostra la competenza raggiunta dai criminali informatici. Essi infatti compromettono i meccanismi di aggiornamento software di pacchetti altrimenti legittimi. Ciò, in un secondo momento, consente loro di sfruttare la distribuzione di software lecito.

Fondamentalmente, i criminali informatici prenderanno di mira le aziende della filiera di approvvigionamento con procedure di sicurezza informatiche deboli, soprattutto quando si tratta di condivisione delle informazioni. Ecco perché spesso le vittime sono PMI.

Una volta identificato l'anello debole, l'hacker può quindi concentrarsi sullo sfruttamento dell'obiettivo finale prefissato.

Difese contro attacchi ovunque

Difendi il tuo business dagli hacker. Combattili ovunque tentino di infiltrarsi. Le nostre soluzioni ti proteggono dal livello DNS, all'e-mail fino all'endpoint e sono supportate dalle ricerche sulle minacce leader del settore di Talos.

Cosa fare

Se la tua azienda appartiene a una filiera di approvvigionamento, chiedi ai fornitori/partner in che modo proteggono le loro rispettive filiere di approvvigionamento. Chiedi informazioni sulle loro procedure di sviluppo e sui controlli di sicurezza interni. Come implementano le patch e gli aggiornamenti nei sistemi interni e con quale frequenza? Come segmentano e proteggono gli ambienti di sviluppo, QA e produzione? Come controllano partner e fornitori?

E non dimenticarti di porti tutte queste domande anche in merito alla tua azienda, o potresti scoprire che è proprio questo l'anello più debole della filiera di approvvigionamento.

Ulteriori informazioni sugli attacchi alla filiera di approvvigionamento sono disponibili a questo link: https://gblogs.cisco.com/uki/protecting-...

Troppe aziende hanno un “problema di stacking”

Alcune aziende semplicemente non hanno una strategia di sicurezza informatica chiara. Si arrangiano con una soluzione finché non diventa un ostacolo.

Altre tentano di far fronte a tutto e finiscono per dover affrontare un problema di stacking: uno stack di diverse soluzioni di sicurezza puntuali di vari fornitori, installate tutte insieme. Entrambe le situazioni implicano problemi.

Il miscuglio di tecnologie di sicurezza incompatibili lascia lacune, crea difficoltà di gestione e crea inefficienze che fanno prosperare gli hacker. Ogni nuova soluzione di sicurezza è dotata di un'altra interfaccia di gestione. Inoltre esige risorse umane, ore di gestione per la configurazione, la definizione di policy, la risposta agli avvisi e non è sempre chiaro se la sicurezza supplementare che ne risulta valga tutto lo sforzo ulteriore destinato alla gestione della soluzione stessa, quando sarebbe forse più opportuno concentrarsi su altri problemi di maggior rilievo.

Le aziende in questo modo si trovano ad aumentare la complessità senza incrementare più di tanto l'efficacia complessiva. Questa situazione è aggravata dal fatto che la sicurezza è considerata ancora soprattutto come un “problema IT”. Secondo lo Studio comparativo di Cisco sulla sicurezza, alcune aziende non sono del tutto convinte che i responsabili delle line-of-business debbano essere coinvolti nella questione della sicurezza. L'atteggiamento è troppo spesso: “La sicurezza è un problema dell’IT”. Si tratta di un problema reale, perché significa che la sicurezza spesso viene “aggiunta” anziché essere integrata nell'ecosistema di un'azienda. Smussare gli angoli crea più lavoro.

Se implementata nel modo giusto, la sicurezza può essere uno strumento di business. Una piattaforma di crescita.

La “superficie di attacco” è sempre più ampia e complessa

Lavoriamo ovunque: a casa, in ufficio, negli aeroporti, nelle caffetterie. Eppure le soluzioni di sicurezza tradizionali si focalizzano ancora sulla protezione dei dipendenti solo quando si trovano nella rete aziendale.

Lo scenario è questo:

- Gli utenti accedono alla rete dai propri dispositivi intelligenti, ovunque si trovino

- Le app, i server e i dati aziendali sono nel cloud

- Dispositivi che non sembrano nemmeno computer si connettono alle tue reti (pensa ai contatori, ai termostati, alle stampanti, alle telecamere intelligenti...)

- E, per complicare ulteriormente la situazione, devi pensare a come garantire la sicurezza ovunque in modo da proteggere questa infrastruttura complessa

IT fantasma

L’IT fantasma è la pratica per cui i dipendenti utilizzano tutte le applicazioni che vogliono senza l'approvazione del reparto IT. Questa pratica può esplicarsi in una miriade di modalità, dall'installazione di un servizio di messaggistica istantanea su un dispositivo aziendale, al download di un software di condivisione di file personale e al suo utilizzo per il trasferimento di dati sensibili.

Nel report “2017 State of Cybersecurity in Small and Medium-Sized Businesses (SMB)” del Ponemon Institute, il 54% degli intervistati afferma che i dipendenti negligenti sono stati la causa profonda della violazione dei dati subita dall’azienda, in aumento rispetto al 48% riportato nello studio dell'anno precedente.

L’IT fantasma può creare enormi vulnerabilità di sicurezza, soprattutto se ignora quanto sia esteso il problema. Questo tipo di attività è come fare una nuotata in acque infestate da squali indossando un costume fatto di carne. Eppure è incredibilmente diffuso nelle aziende. Quindi perché esiste?

Per la verità, il personale agisce con le migliori intenzioni. I lavoratori vogliono migliorare i propri livelli di produttività e utilizzare gli strumenti digitali più recenti. Di solito non pensano alle implicazioni per la sicurezza quando accedono a queste applicazioni. In alcuni casi i dipendenti utilizzano gli strumenti di IT fantasma perché erano abituati a usare determinati sistemi nell’azienda in cui lavoravano precedentemente. Dopotutto, è più facile che imparare qualcosa di nuovo.

Fai luce sull’IT fantasma

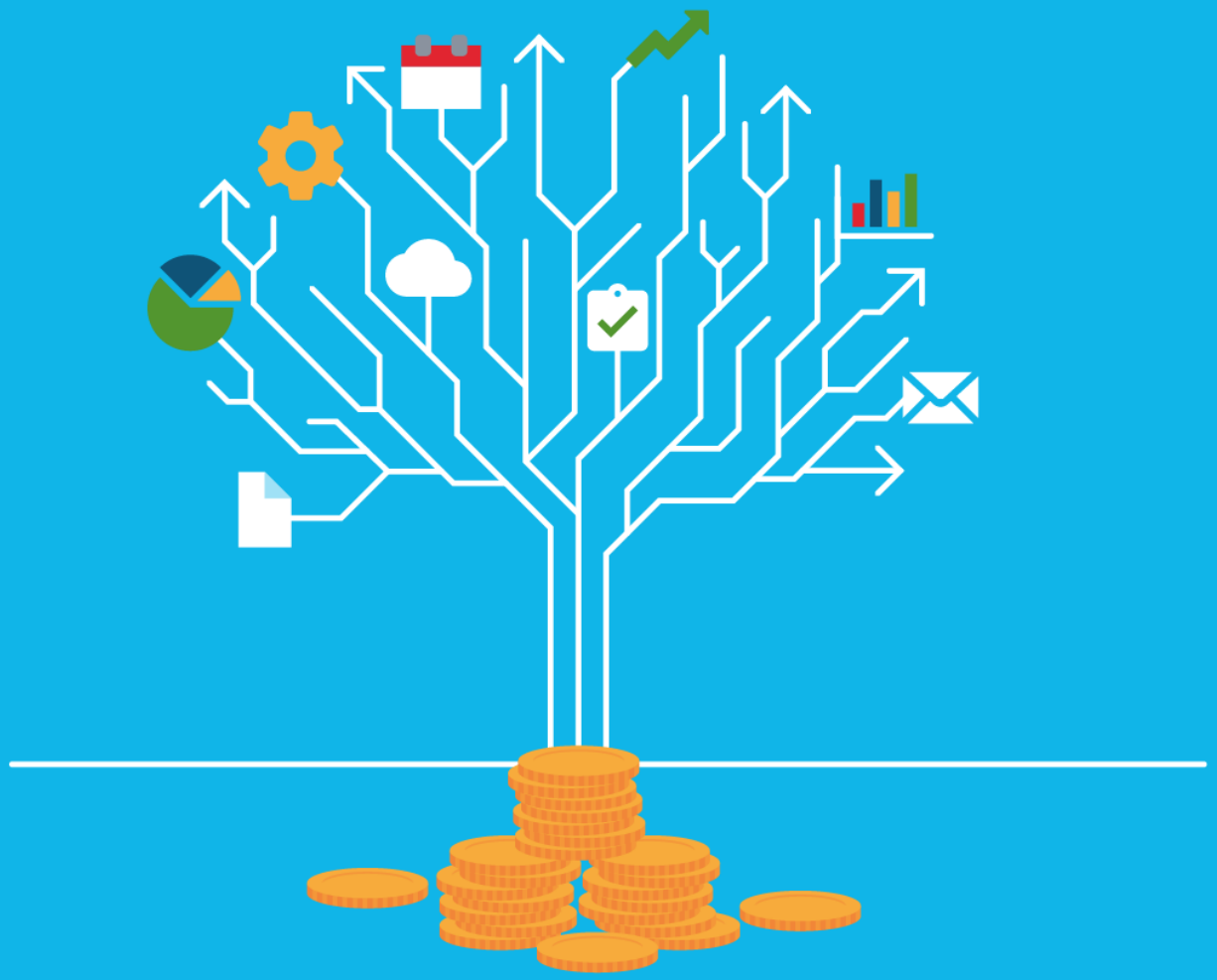
È possibile trasformare l’IT fantasma in un contributo positivo per la tua azienda:

- Se non esiste già, crea un forum o uno strumento per i suggerimenti che consenta ai dipendenti di esprimere idee che potrebbero migliorare la gestione dell'azienda. Premia le persone per i loro interventi e festeggia quando un'idea diventa realtà.
- Una sicurezza efficace non riguarda solo la tecnologia: si tratta anche di impostare i processi giusti. Fai sì che la sensibilizzazione sulla sicurezza diventi una parte fondamentale del programma di formazione, così che le persone possano capire le conseguenze dell'utilizzo di dispositivi e programmi non sicuri.
- Sapere cosa sta accadendo nella tua rete è una priorità assoluta nell'ambito della sicurezza IT. Purtroppo, la maggior parte delle aziende non sa quando una violazione ha avuto luogo, come è riuscita a infiltrarsi e quanto sia grave il danno. Ribalta la situazione.

Policy delle password

Le password solide continuano a svolgere un ruolo essenziale per la cybersecurity delle PMI. Eppure il 59% degli intervistati dell’attuale report di Ponemon (la stessa percentuale di quello precedente) afferma di non avere visibilità sulle procedure di creazione delle password dei dipendenti, incluso l'utilizzo di password univoche o complesse.

Gli intervistati affermano anche che le policy delle password non vengono applicate rigorosamente. Nel caso di aziende che dispongono di una policy delle password (si tratta del 43% degli intervistati), il 68% afferma che questa non viene applicata con rigore o di non sapere con certezza se sia amministrata efficacemente.



La crescita richiede sicurezza

La debolezza informatica danneggia l'innovazione

Di sicuro la prevenzione degli attacchi informatici costituisce un motivo impellente di preoccupazione, ma un risultato ancora più fastidioso di una cybersecurity debole è l'impatto sulla crescita e l'innovazione dell'azienda.

In un recente studio di Cisco, uno scioccante 71 per cento dei dirigenti ha dichiarato che i timori relativi alla cybersecurity avevano impedito l'innovazione nelle rispettive aziende. Tra gli intervistati, il 39 per cento ha dichiarato di aver sospeso iniziative mission-critical a causa di problemi di cybersecurity. Queste risposte evidenziano come la debolezza della cybersecurity ostacoli la capacità delle aziende di innovare proprio nel momento in cui ne hanno bisogno per poter competere.

La digitalizzazione, le turbative e i cambiamenti radicali sono diventati la nuova normalità di un ambiente aziendale altamente competitivo. Le aziende agili possono stabilire un chiaro vantaggio rispetto alla concorrenza se possono innovare, agire rapidamente e premiare la sperimentazione.

L'impatto di una violazione va ben oltre i profitti

L'incapacità di proteggere la rete può avere conseguenze di vasta portata, tra cui: interruzione dell'operatività, danni e sostituzione di attrezzature, reazione agli incidenti, analisi forense, comunicazioni e controlli interni.

La perdita di fiducia dei clienti può danneggiare in modo permanente un flusso di entrate che prima era consistente. La perdita di dati dei clienti può comportare azioni legali, sanzioni, normative più severe e costi delle misure correttive. Eppure il danno non si limita a questo. Ad esempio, se un rivenditore subisce una violazione dei dati, i clienti potrebbero non sentirsi più sicuri di condividere le informazioni personali.

La tua azienda può trarre un vantaggio decisivo sfruttando:

- Tecnologie consolidate come il Web, i dispositivi mobili, il cloud, la gestione delle risorse aziendali e la gestione delle relazioni con i clienti

- Le tecnologie in rapido sviluppo come l'intelligenza artificiale e l'analisi dei dati

Queste tecnologie aiutano le aziende a entrare meglio in contatto con i clienti, a raggiungere nuovi mercati e a migliorare la produttività dei dipendenti, aumentando al contempo i profitti e riducendo i costi. I timori nei confronti della sicurezza informatica possono ostacolare il perseguimento di alcuni modelli di business e innovazioni digitali.

Agire è rischioso, non agire anche

Molti imprenditori devono affrontare un'ardua scelta: prendersi il rischio di sbagliare o quello di

rimanere indietro. Sentono di dover continuare ad andare avanti per non rischiare di soccombere agli innovatori digitali e ad altri concorrenti agili. Il 73 per cento degli intervistati del nostro sondaggio ha infatti ammesso di aver adottato spesso nuove tecnologie e processi aziendali, nonostante i rischi di cybersecurity.

Una cybersecurity inadeguata lascia le aziende nella peggiore posizione possibile rispetto alla concorrenza: non si innovano abbastanza rapidamente per competere, ma non sono neanche abbastanza al sicuro dagli attacchi informatici nonostante abbiano ritardato le innovazioni digitali.

In che modo una violazione della sicurezza o un attacco ransomware comprometterebbero la tua azienda?

Qual è il potenziale impatto finanziario di un'interruzione della rete provocata da una violazione della sicurezza o dalla perdita di accesso ai dati e ai sistemi a causa di un attacco ransomware?

- Una violazione della sicurezza o un attacco ransomware potrebbero provocare problemi alla filiera di approvvigionamento?
- Che cosa accadrebbe se un attacco bloccasse il sito Web della tua azienda?
- La tua azienda sfrutta funzionalità di e-commerce sul proprio sito Web?
- Per quanto tempo il sito può rimanere inaccessibile prima che la tua azienda inizi a subire perdite?
- La tua azienda è assicurata contro gli attacchi informatici o contro l'uso improprio dei dati dei clienti? La polizza di assicurazione è adeguata?
- La tua azienda dispone di funzionalità di backup e recupero per ripristinare le informazioni in caso di necessità dopo una violazione della sicurezza o la perdita di dati a causa di un attacco ransomware?

Valore potenziale digitale

Il valore potenziale digitale permette di attribuire un valore alla sicurezza. Esso si basa su fonti di valore completamente nuove provenienti da investimenti e innovazioni digitali e sul valore trasferito tra le aziende a seconda della loro capacità di sfruttare il potenziale digitale.

Parte del valore digitale potenziale deriva dall'aspetto difensivo della cybersecurity, come:

- La tutela della proprietà intellettuale
- La riduzione dei dati compromessi (sia informazioni interne che dei clienti), maggiore operatività aziendale e minori interruzioni dell'operatività della rete
- La protezione delle risorse finanziarie
- La protezione delle informazioni riservate della pubblica amministrazione, nazionali e politiche
- La difesa della reputazione aziendale

Scopri il quadro completo. Leggi Ultimate Guide to Cybersecurity to Drive Profitability di Cisco.

Una piattaforma sicura per la crescita

L'architettura di sicurezza integrata di Cisco aiuta le aziende a migliorare l'efficacia della sicurezza riducendo al minimo i tempi per rilevare le minacce e risolvere gli incidenti, a risparmiare di più (sia per le spese in conto capitale che per quelle operative) e a migliorare la produttività del personale IT.

Coinvolgere tutti con la cybersecurity

Rendere la sicurezza una priorità per tutti

A volte bisogna prendere un grosso colpo prima di intraprendere iniziative di cybersecurity.

Tuttavia, il 60% delle PMI che subiscono una violazione della cybersecurity sono costrette a chiudere. Il che indica, soprattutto per te, che prevenire è meglio che curare.

Presenta i fattori di rischio specifici della tua azienda

Aiuta il consiglio di amministrazione a capire le minacce alla sicurezza che potrebbero riguardare la tua azienda. Non sprecare troppo tempo a presentare statistiche e tendenze generali. Aiutali invece a capire il collegamento tra quelle tendenze di sicurezza e le sfide specifiche per la tua azienda e il settore a cui appartiene. Più contesto sei in grado di fornire, più il consiglio lo troverà interessante.

Ad esempio, puoi parlare della maggior fonte di fatturato della tua azienda e descrivere in concreto come le minacce alla sicurezza come il ransomware potrebbero costituire una minaccia. Se la tua azienda conserva dati sensibili come record finanziari, puoi illustrare con esempi le implicazioni legali e le sanzioni che la tua azienda potrebbe subire se tali dati fossero resi pubblici.

Illustra come funziona un attacco e come può essere facile compromettere la sicurezza. Presenta esempi reali dei problemi che stai già affrontando nonché i rischi e gli effetti a lungo termine che tali problemi potrebbero causare.

Quantifica tutto

Ai dirigenti piacciono le metriche e i numeri. Perciò, è importante che allinei le priorità della sicurezza agli obiettivi e alle scadenze della tua azienda. Conferma le priorità aziendali e dell'IT e mostra come la sicurezza consentirà di rispettarle.

Mostra anche il rovescio della medaglia: come un incidente di sicurezza potrebbe mettere a rischio i loro piani. Ad esempio, se stai per lanciare un nuovo prodotto, quale sarebbe il danno potenziale per l'azienda se la proprietà intellettuale venisse resa pubblica o distrutta?

In realtà, non serve un problema ipotetico. Se sei in grado di quantificare quanto stanno già costando all'azienda i problemi di sicurezza esistenti, hai un argomento ancora migliore a tuo favore.

Ripeti, ripeti, ripeti

È improbabile che otterrai tutto quello che ti serve da un'unica conversazione. Le tue comunicazioni devono essere semplici e frequenti. Stabilisci aggiornamenti regolari e fornisci spesso resoconti su metriche rilevanti. Non temere di ripeterti e prova a presentare la questione da prospettive diverse fino a quando il messaggio non verrà capito e otterrai i finanziamenti e il supporto che ti servono.

L'aiuto del GDPR

In molti casi, gli esperti della sicurezza faticano a parlare la stessa lingua del consiglio di amministrazione e a fargli capire perché debba dare priorità agli investimenti nella sicurezza. Quando si verifica un attacco informatico di dominio pubblico e i dirigenti vedono i molteplici effetti dei danni che causa, i motivi per investire diventano chiarissimi. Le conversazioni (e i cambiamenti) avvengono a un ritmo molto più sostenuto quando tutti capiscono il problema.

Ecco in che modo leggi come il Regolamento generale sulla protezione dei dati (GDPR), entrato in vigore nel maggio 2018, possono contribuire a migliorare la sicurezza.

Le aziende che investono già in sicurezza potrebbero non doversi preoccupare molto, poiché probabilmente sono sulla strada giusta verso la conformità (dal punto di vista della sicurezza del GDPR). D'altro canto, per quanto concerne le aziende che hanno avuto difficoltà a ottenere i fondi da investire, il GDPR offre una grande opportunità affinché gli esperti della sicurezza e i massimi dirigenti si allineino. Nuove normative come questa stanno costringendo le aziende ad avere standard di base, il che fornirà il supporto per una maggiore innovazione tecnologica nel futuro.

La privacy dei dati e la sicurezza IT non costituiscono solo requisiti normativi, ma sono anche un'esigenza dei clienti. È sempre più frequente che i clienti domandino alle aziende come gestiscono i loro dati. C'è un rapporto di fiducia, si presuppone che l'azienda che riceve i dati ne avrà cura. La legge serve solo a garantire che le aziende stiano facendo tutto il possibile per onorare tale fiducia.

Proteggi la tua azienda con Cisco

Sicurezza di rete

Che cos'è la sicurezza di rete?

La sicurezza di rete comprende ogni attività pensata per proteggere l'usabilità e l'integrità della rete e dei dati. Include sia tecnologie hardware che software. Una sicurezza di rete efficace gestisce l'accesso alla rete. Mira a varie minacce e impedisce che penetrino o si diffondano nella rete.

Come funziona la sicurezza di rete?

La sicurezza di rete combina più livelli di difesa alla periferia e all'interno della rete stessa. Ogni livello di sicurezza della rete implementa policy e controlli. Gli utenti autorizzati ottengono l'accesso alle risorse di rete, ma viene impedito agli hacker di eseguire exploit e minacce.

Come traggo vantaggio dalla sicurezza di rete?

La digitalizzazione ha trasformato il nostro mondo: come viviamo, lavoriamo, giochiamo e impariamo. Tutte le aziende che vogliono offrire i servizi richiesti da clienti e dipendenti devono proteggere la propria rete e le relative informazioni proprietarie dagli attacchi. Di fatto è questa che protegge la reputazione dell'azienda.

6 azioni che puoi adottare per proteggere la rete

1. Monitora il traffico in entrata e in uscita dal firewall e leggi attentamente i report. Non affidarti agli avvisi per contrassegnare le attività pericolose. Assicurati che qualcuno del team comprenda i dati e sia in grado di adottare le misure necessarie.
2. Tieni d'occhio le nuove minacce che vengono scoperte e rese pubbliche online. Ad esempio, il blog di Cisco Talos fornisce aggiornamenti istantanei sulle nuove minacce e sulle vulnerabilità scoperte e un riassunto settimanale dettagliato delle minacce stesse. Il sito TrendWatch di Trend Micro monitora l'attività corrente delle minacce. Inoltre, puoi ricevere avvisi e-mail dallo U.S. Computer Emergency Readiness Team (US-CERT, una divisione della sicurezza nazionale degli USA) riguardo alle vulnerabilità e agli exploit software confermati di recente.
3. Abilita aggiornamenti regolari per il software di anti-virus e firewall.
4. Forma i dipendenti in modo continuativo così che possano comprendere tutte le modifiche alla policy dell'uso consentito. Inoltre, incoraggia un approccio alla sicurezza simile alle "ronde di quartiere". Se un dipendente nota qualcosa di sospetto, ad esempio non riesce ad accedere subito a un account e-mail, dovrebbe farlo immediatamente presente alla persona responsabile.
5. Installa una soluzione per la protezione dei dati. Questo tipo di dispositivo può proteggere la tua azienda dalla perdita di dati se viene violata la sicurezza della rete.
6. Valuta soluzioni di sicurezza aggiuntive che proteggano ulteriormente la rete e aumentino le capacità della tua azienda.

Tipi di sicurezza di rete

Controllo degli accessi

Non tutti gli utenti devono avere accesso alla rete. Per tener fuori potenziali hacker, devi riconoscere ogni utente e ogni dispositivo. A quel punto puoi applicare le policy di sicurezza. Puoi bloccare i dispositivi endpoint non conformi o consentirne solo un accesso limitato. Questo processo si definisce controllo dell'accesso alla rete (NAC).

Sicurezza delle applicazioni

Qualsiasi software utilizzato per gestire l'azienda deve essere protetto, sia che venga creato dal personale IT o che venga acquistato. Purtroppo, qualsiasi applicazione può presentare lacune o vulnerabilità che gli hacker possono sfruttare per infiltrarsi nella rete. La sicurezza delle applicazioni comprende l'hardware, il software e i processi che usi per colmare tali lacune.

Software antimalware e antivirus

"Malware", abbreviazione di "malicious software" (software dannoso), include virus, worm, Trojan, ransomware e spyware. A volte il malware infetta una rete ma poi rimane latente per giorni o addirittura settimane. I migliori programmi antimalware non solo cercano il malware in ingresso, ma continuano a monitorare i file anche in seguito per individuare le anomalie, rimuovere il malware e porre rimedio ai danni.

Data Loss Prevention

Le aziende devono essere certe che il proprio personale non invii informazioni sensibili all'esterno della rete. Le tecnologie di Data Loss Prevention, o DLP, possono impedire alle persone di caricare, inoltrare o perfino stampare informazioni critiche in modo non sicuro.

Analisi comportamentale

Per rilevare comportamenti anomali della rete bisogna conoscere il comportamento normale. Gli strumenti di analisi comportamentale distinguono automaticamente le attività che si scostano dalla norma. Il team di sicurezza può quindi identificare meglio gli indicatori di compromissione che costituiscono un potenziale problema e correggere rapidamente le minacce.

Sicurezza dei sistemi e-mail

I gateway e-mail sono il principale vettore di minaccia per una violazione della sicurezza. Gli hacker utilizzano informazioni personali e tattiche di social engineering per creare campagne di phishing sofisticate in modo da ingannare i destinatari e indirizzarli su siti che distribuiscono il malware. Un'applicazione di sicurezza dei sistemi e-mail blocca gli attacchi in arrivo e controlla i messaggi in uscita per prevenire la perdita di dati sensibili.

Firewall

I firewall creano una barriera tra la rete interna affidabile e le reti esterne non affidabili, come Internet. Utilizzano una serie di regole definite per consentire o bloccare il traffico. Un firewall

può essere costituito da un componente hardware, software o entrambi. Cisco offre dispositivi Unified Threat Management (UTM) e Next-Generation Firewall incentrati sulle minacce.

Intrusion Prevention System

Un Intrusion Prevention System (IPS) analizza il traffico di rete per bloccare attivamente gli attacchi. A tale scopo, le appliance Next-Generation IPS (NGIPS) di Cisco correlano moltissima intelligence globale sulle minacce non solo per bloccare attività dannose, ma anche per monitorare lo sviluppo di malware e file sospetti in tutta la rete e prevenire così la diffusione degli attacchi e la reinfezione.

Sicurezza dei dispositivi mobili

I criminali informatici prendono sempre più di mira i dispositivi mobili e le app. Entro i prossimi 3 anni, il 90 per cento delle aziende IT potrebbe supportare le applicazioni aziendali sui dispositivi mobili personali. Naturalmente, devi avere il controllo dei dispositivi che possono accedere alla rete. Inoltre, dovrai anche configurare le connessioni per mantenere il traffico di rete privato.

Segmentazione della rete

La segmentazione software-defined suddivide il traffico di rete in diverse classificazioni e semplifica l'applicazione delle policy di sicurezza. Idealmente, le classificazioni sono basate sull'identità degli endpoint, non sui meri indirizzi IP. Puoi assegnare i diritti di accesso in base al ruolo, alla posizione e ad altro ancora, in modo che il livello di accesso adeguato venga attribuito alle persone giuste e i dispositivi sospetti siano contenuti e corretti.

VPN

Una Virtual Private Network cripta la connessione da un endpoint a una rete, spesso su Internet. In genere, una VPN ad accesso remoto utilizza IPsec o Secure Sockets Layer per autenticare la comunicazione tra il dispositivo e la rete.

Sicurezza Web

Una soluzione di sicurezza Web controllerà l'uso che il personale fa del Web, bloccherà le minacce basate sul Web e negherà l'accesso ai siti dannosi. Proteggerà il gateway Web in sede o nel cloud. “Sicurezza Web” si riferisce anche alle azioni che intraprendi per proteggere il sito Web della tua azienda.

Sicurezza wireless

Le reti wireless non sono sicure come quelle cablate. Senza misure di sicurezza rigorose, l'installazione di una LAN wireless può avere le stesse conseguenze di mettere porte Ethernet ovunque, incluso nel parcheggio. Per evitare che un exploit prenda piede, hai bisogno di prodotti elaborati appositamente per proteggere una rete wireless.

Intelligence sulle minacce di Talos

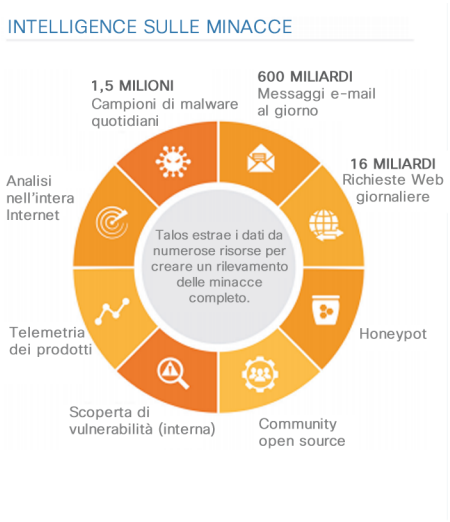
Talos è il team di intelligence e ricerca sulle minacce leader del settore e ogni prodotto per la sicurezza di Cisco è protetto tramite Talos. Talos ha più di 250 ricercatori delle minacce che

lavorano ventiquattro ore su ventiquattro e in tutto il mondo, con un repository di 100 terabyte di intelligence sulle minacce.

Analizziamo un terzo del traffico e-mail globale quotidiano e oltre il 2% delle richieste DNS nel mondo. Rileviamo oltre 1,1 milioni di campioni di malware univoco ogni giorno grazie alle nostre tecnologie Advanced Malware Protection (AMP) e ThreatGRID, che ci consentono di bloccare 19,7 miliardi di minacce quotidiane sulle reti dei nostri clienti.

Esattamente: 19,7 miliardi di minacce bloccate al giorno.

Funzionalità di ricerca e conoscenze così vaste supportano le soluzioni di cybersecurity di Cisco, che offrono la visibilità, l'automazione, la flessibilità e la scalabilità necessarie per proteggere l'ambiente di rete da minacce sempre più sofisticate.



Cisco Umbrella

Un servizio di sicurezza cloud che fornisce protezione integrata per il servizio Internet

Cisco Umbrella è un servizio di sicurezza cloud che fornisce protezione integrata contro gli attacchi alla connessione Internet, permettendoti di ridurre i tempi e i costi necessari per far fronte agli attacchi informatici.

La soluzione offre una protezione proattiva contro le minacce su Internet, come malware, botnet e attacchi phishing. Consente di proteggere l'azienda garantendo che il traffico sia pulito prima che raggiunga la rete interna, imparando in modo efficace dove vengono organizzati gli attacchi e bloccando le minacce su tutte le porte e i protocolli. Puoi stare certo che con un accesso a Internet sicuro, sei protetto da un primo livello di difesa contro il malware.

Cisco Umbrella offre visibilità su tutte le richieste Internet di tutta la rete e di ogni porta, protocollo o app per scoprire e bloccare le connessioni ai domini e agli IP dannosi. Scopri perché le piccole imprese stanno realizzando l'effetto moltiplicatore della sicurezza utilizzando il DNS per integrare le misure di sicurezza esistenti. Quali attacchi non rilevi?

Next-Generation Firewall

Un firewall tradizionale è in grado di controllare il traffico nel punto di entrata o di uscita all'interno della rete. In altre parole, è il ponte tra la tua azienda e la massa del resto di Internet.

Era uno strumento perfetto ai tempi in cui la vita era semplice e avevi visibilità su tutto ciò che si agganciava alla rete. Al giorno d'oggi, le aziende ospitano sempre più una miriade di dispositivi sconosciuti e un'oscura marea di applicazioni cloud che vengono scaricate dai dipendenti.

La differenza principale con un Next-Generation Firewall è che puoi impostare policy e controlli delle applicazioni. Ad esempio, se un membro del personale scarica un software per la condivisione dei file che potrebbe non essere sicuro, tu ne avrai visibilità automaticamente e potrai fare qualcosa all'istante.

Inoltre, avrai nel complesso molta più visibilità e controllo su utenti, dispositivi, minacce e vulnerabilità della rete. Così, quando il consiglio di amministrazione ti chiede "Siamo al sicuro?", puoi fornire una risposta molto più completa di quanto non faresti con un firewall tradizionale che controlla solo il traffico.

Scopri di più sui Next Generation Firewall o trova il Next Generation Firewall più adatto a te.

Advanced Malware Protection

Sicurezza degli endpoint di nuova generazione

La sicurezza degli endpoint di nuova generazione integra funzionalità di prevenzione, rilevamento e risposta in un'unica soluzione, sfruttando la potenza dell'analisi basata su cloud. Cisco AMP for Endpoints è un connettore leggero che funziona con i dispositivi Windows, Mac, Linux, Android e iOS.

Cisco AMP for Endpoints offre protezione completa contro gli attacchi più avanzati. Previene le violazioni e blocca il malware nel punto di ingresso, quindi rileva, contiene e pone rimedio rapidamente alle minacce avanzate che eludono le difese di prima linea e riescono a infiltrarsi nella rete.

Previeni: rafforza le difese utilizzando la miglior intelligence globale sulle minacce e blocca in tempo reale il malware basato o meno su file.

Rileva: monitora e registra continuamente tutte le attività dei file per rilevare rapidamente il malware nascosto.

Intervieni: velocizza le indagini e poni rimedio automaticamente al malware su PC, Mac, Linux, server e dispositivi mobili (Android e iOS).

Può utilizzare il cloud pubblico o essere implementato come cloud privato. AMP monitora e analizza continuamente tutta l'attività di file e processi all'interno della rete per scoprire quell'1 per cento di minacce che altre soluzioni non rilevano. AMP tiene sempre d'occhio dove va un file o cosa fa. Se un file che sembrava pulito dopo l'ispezione iniziale dovesse mostrare un comportamento malevolo, AMP conserva una cronologia completa del comportamento della minaccia per intercettarlo, contenerlo e porvi rimedio.

Rileva le minacce sconosciute

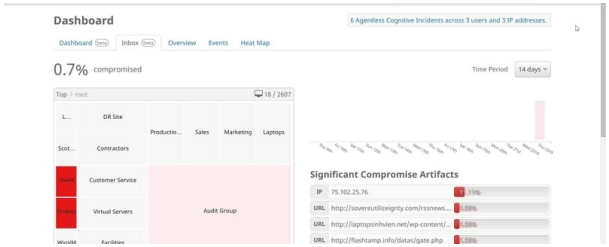
La tecnologia di sandboxing integrata di AMP analizza il comportamento dei file sospetti e lo associa ad altre fonti di informazione. L'analisi dei file produce informazioni dettagliate per permetterti di capire meglio come contenere l'infezione e bloccare gli attacchi futuri.

Quando un file viene ritenuto dannoso, AMP riduce drasticamente la quantità di tempo e le risorse necessarie per analizzarlo. Fornisce automaticamente risposte alle domande più urgenti, tra cui:

- Cosa è successo?
- Da dove è venuto il malware?
- Dove è stato il malware?
- Cosa sta facendo il malware ora?
- Come lo blocchiamo?

Con alcuni clic sulla console di gestione basata su browser di AMP, si può bloccare l'esecuzione del file su tutti gli endpoint. Cisco AMP conosce tutti gli altri endpoint raggiunti dal file, quindi lo può mettere in quarantena per tutti gli utenti. AMP elimina il malware con precisione chirurgica senza danneggiare i sistemi IT né l'attività aziendale.

Come bloccare e mettere in quarantena un file con Cisco AMP:



Cisco Meraki

Sicurezza gestita tramite cloud e SD-WAN

Gestione tramite cloud centralizzata al 100% per garantire sicurezza, networking e controllo delle applicazioni.

Cisco Meraki Security Appliances può essere implementata da remoto in pochi minuti utilizzando il provisioning zero-touch del cloud. La impostazioni di sicurezza sono facili da sincronizzare su migliaia di siti utilizzando dei modelli. La tecnologia di VPN automatica connette in modo sicuro le filiali in 3 clic, attraverso un dashboard intuitivo e basato sul Web.

Sicurezza completa in un'unica soluzione

Ogni appliance di sicurezza Meraki supporta diverse funzionalità, come un firewall stateful e un motore IPS integrato Sourcefire per proteggere le reti. Le definizioni delle minacce e gli elenchi dei filtri sono aggiornati di continuo, garantendo che ogni sito abbia una protezione all'avanguardia dalle ultime vulnerabilità e dai siti Web problematici.

Proteggi un sito in pochi minuti

1. Aggiungi Meraki Security Appliance al dashboard.
2. Abilita la prevenzione delle intrusioni.
3. Seleziona il livello di protezione dalle minacce desiderato.

Scopri di più

Per le ultime informazioni e innovazioni, visita: Cisco Tech Connection for SMB o esplora altre risorse Cisco per le PMI e Cisco Security per proteggere l'azienda.

Grazie per l'attenzione

I fondamenti della sicurezza per PMI