PROTEZIONE DEI DATI

per le piccole e medie imprese

- Comprendere l'attuale panorama delle minacce
- Panoramica delle soluzioni per proteggere la vostra piccola/media impresa
- Minimizzare l'impatto di una violazione dei dati

CYBERSECURITY
EXPERTS ON YOUR SIDE

Le violazioni dei dati e gli attacchi informatici non sono una novità, ma lo sono le tecniche e le tattiche utilizzate dai moderni cyber-criminali - e sono in costante evoluzione. Uno dei bersagli preferiti sono le piccole e medie imprese che rappresentano la stragrande maggioranza delle operazioni commerciali in tutto il mondo. I vostri dati aziendali sono più preziosi di quanto crediate.

Protezione dei Dati per le Piccole e Medie Imprese è progettato per aiutare aziende come la vostra a gestire le complesse necessità di protezione dei dati con un approccio logico, completo ed efficace.

All'interno, troverete:

- Cyberattacchi, il panorama normativo e possibili conseguenze di una violazione dei dati
- Come valutare le tecnologie di protezione dei dati e le opzioni di implementazione
- Valutazione del rischio: identificare le risorse, le minacce e le vulnerabilità
- Diversi approcci: crittografia, protezione degli endpoint, firewall e altro
- Implementazione di controlli organizzativi e di gestione fondamentali

PROTEZIONE DEI DATI

per le piccole e medie imprese

CYBERSECURITY
EXPERTS ON YOUR SIDE

Ringraziamo con gratitudine Lawrence Miller per la preparazione dei contenuti di questo libro.

CONTENUTI

INTRODUZIONE

"Questa azienda è troppo piccola, non ne vale la pena" - nessun hacker ha mai pronunciato queste parole, mai!! I criminali informatici sono predatori opportunisti, quindi anche se non prenderanno specificamente di mira la vostra piccola o media impresa, basta una connessione internet per essere trovati e sfruttati, qualsiasi sia il loro scopo. Se la rete aziendale, i server, le applicazioni, i dati, i desktop, i portatili e i dispositivi mobili non sono adeguatamente protetti, possono essere violati. Anche se molto probabilmente una violazione non vi regalerà "15 minuti di vergogna" al TG nazionale, avrà certamente un impatto serio - potenzialmente sufficiente a far fallire la vostra azienda. La sicurezza sta diventando sempre più un aspetto imprescindibile. Questo libro è il punto di partenza per migliorare il proprio business digitale.

Anche se le violazioni dei dati e gli attacchi informatici non sono una novità, lo sono molte delle tecniche e delle tattiche utilizzate dai moderni criminali informatici - e sono particolarmente adatte a un ambiente allettante come quello delle piccole e medie imprese (PMI) che comprendono più del 95% delle aziende in tutto il mondo, impiegano più della metà della forza lavoro globale e contribuiscono a più della metà del prodotto interno lordo dell'economia globale (PIL). I metodi di attacco più recenti includono:

- Tecniche avanzate di malware (come il polimorfismo e il metamorfismo), ransomware e trojan ad accesso remoto (RAT).
- Attacchi directory harvest (DHA) e campagne e-mail mirate di spam e phishing (spearphishing).
- Attecchi massivi con botnet automatizzate
- Domain Name System (DNS) hijacking e DNS cache poisoning
- Port hopping e occultamento del secure sockets layer (SSL).
- Attacchi DDoS (Distributed denial-of-service).

Le minacce alla sicurezza sono un problema più serio e frequente che mai, e le PMI, che spesso gestiscono attività IT snelle con budget e personale limitati, sono spesso facili bersagli per i criminali informatici. Allo stesso tempo,

il fatto che le PMI sono, per definizione, più piccole delle grandi imprese e generalmente hanno meno dispositivi connessi significa che possono essere più flessibili e agili quando definiscono e implementano una strategia di protezione dei dati. Con le mosse giuste, le PMI possono rendersi molto meno attraenti per i potenziali criminali.

In questo libro imparerete a conoscere le tecnologie, gli strumenti e i processi di sicurezza di cui avete bisogno per migliorare la capacità della vostra azienda di proteggere i dati e le risorse IT, e minimizzare efficacemente l'impatto di una violazione dei dati.

Struttura del libro

Protezione dei Dati per Piccole e Medie Imprese consiste in sei brevi capitoli:

1. Cyberattacchi e nuove tendenze, il panorama normativo e l'impatto aziendale di una violazione
2. Come valutare le diverse tecnologie per la protezione dei dati e opzioni di implementazione
3. Il processo di valutazione del rischio: identificare le risorse, analizzare le minacce e valutare le vulnerabilità
4. Varie tecnologie per la protezione dei dati, come la crittografia, la protezione degli endpoint, i firewall e altro ancora
5. Importanti controlli organizzativi e di gestione necessari per assicurare un'efficace protezione dei dati
6. Dieci punti chiave per un'efficace protezione dei dati per le piccole e medie imprese

Alla fine del libro è presente un glossario per aiutarvi a interpretare rapidamente qualsiasi acronimo o termini poco familiari.

Presupposti

Questo libro si rivolge a professionisti IT che lavorano per piccole o medie imprese. Che siate i responsabili di un piccolo team IT "tuttofare" - o che siate voi stessi l'intero team IT! Voi e il vostro team siete responsabili di tutto, dal cambio delle cartucce di toner all'impostazione degli endpoint degli

utenti, dalla gestione della rete aziendale, ai problemi di sicurezza. Come tale, il vostro lavoro richiede una vasta gamma di conoscenze ed esperienze IT, ma ci sono forse alcune aree - come la sicurezza e la protezione dei dati - dove la conoscenza e l'esperienza non sono così profonde come vorreste.

Icone utilizzate nel libro

In tutto il libro, vengono usate icone speciali per identificare informazioni importanti.

RICORDA

Questa icona identifica un'informazione da memorizzare, perché potrà servire in futuro

SUGGERIMENTO

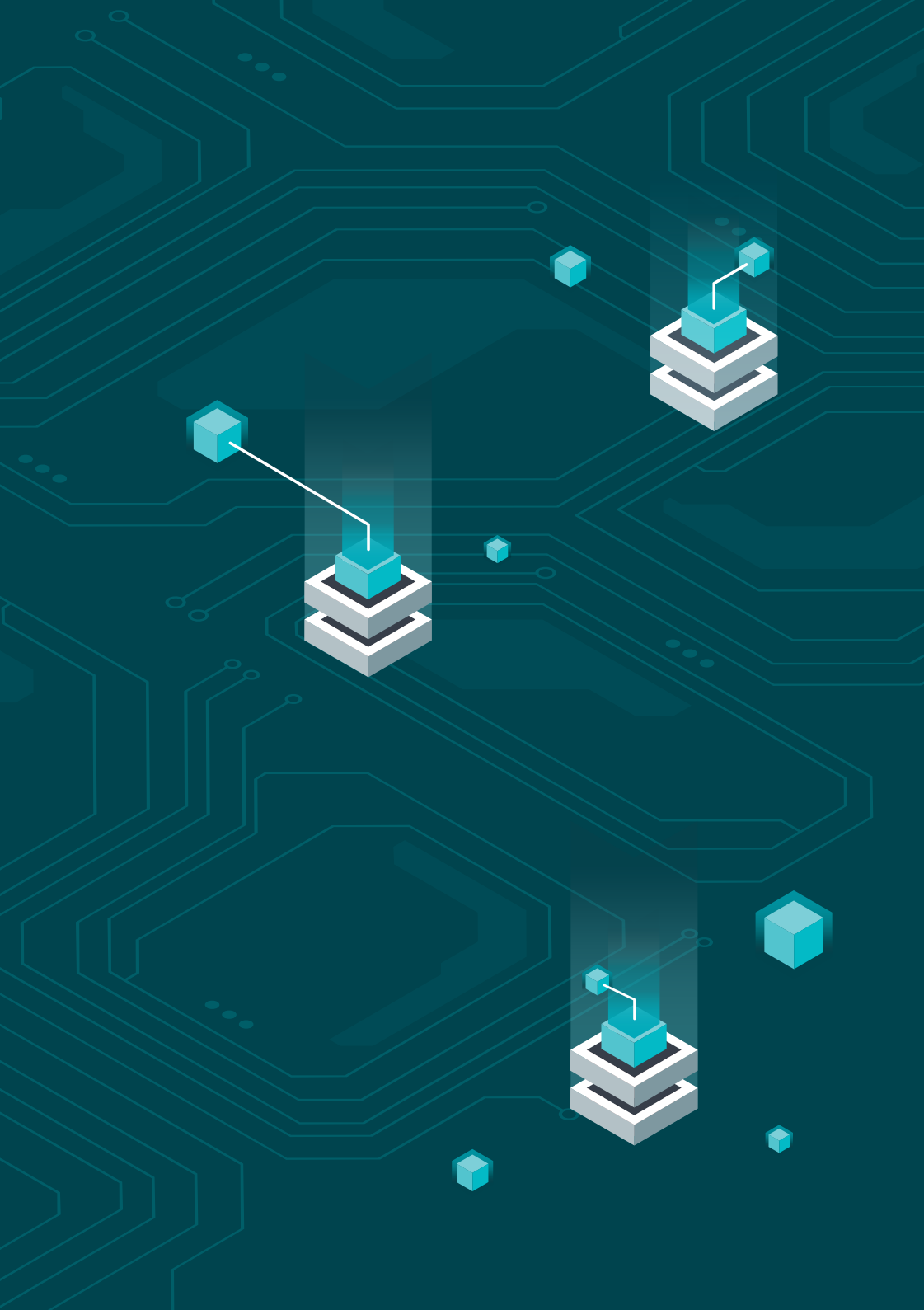
Questa icona indica informazioni e consigli particolarmente utili

ATTENZIONE

Con questi simboli vengono segnalati consigli pratici per aiutarvi a evitare insidie potenzialmente costose o frustranti

Oltre il libro

Le informazioni che si possono racchiudere in un breve libro sono limitate, quindi se sentite l'esigenza di saperne di più, andate su www.eset.com/it/



In questo capitolo

- Misurare il vero costo di una violazione dei dati
- Uno sguardo al moderno panorama delle minacce
- Imparare dal passato
- Comprendere i mandati di conformità

Capitolo 1

PROTEZIONE DEI DATI: UN IMPERATIVO DI CUI PRENDERE ATTO

In questo capitolo, imparerete come una violazione dei dati può avere delle conseguenze sulla vostra azienda, come si è evoluto il panorama delle minacce moderne, come le recenti violazioni dei dati hanno avuto un impatto su altre piccole e medie imprese (PMI) e cosa comportano per la vostra azienda i cambiamenti dei requisiti legali e normativi.

Comprendere l'impatto aziendale di una violazione

Le piccole e medie imprese (PMI) rappresentano il 99 per cento di tutte le imprese nell'UE e più del 95 per cento delle imprese in tutto il mondo, quindi non dovrebbe sorprendere che le PMI siano vittime di più del 70 per cento delle violazioni della sicurezza, come riportato dall'International Data Corporation (IDC). Eppure molte aziende credono di non essere esposte ai cyberattacchi per via delle loro piccole dimensioni e dei loro beni limitati. Sfortunatamente, non è così.

RICORDA

Secondo il Verizon 2017 Data Breach Investigations Report (DBIR), il principale obiettivo degli attacchi (in particolare, POS Intrusion) si è spostato sui ristoranti e sulle piccole imprese. Inoltre, tre quarti delle vittime delle prime sei tipologie di minaccia - credenziali rubate, backdoor, spyware, phishing, esfiltrazione di dati e malware command-and-control (C2) - sono piccole imprese di commercio all'ingrosso web-based.

Nel Regno Unito, la compagnia assicurativa Zurich riferisce che l'anno scorso più di 875.000 piccole e medie imprese sono state colpite da un attacco informatico, con una spesa superiore ai 13.000 dollari per oltre un quinto di queste imprese, e superiore a 69.000 dollari per un'azienda su dieci. In confronto, il Ponemon Institute's 2017 Cost of a Data Breach Study ha scoperto che il costo totale medio di una violazione dei dati per le grandi imprese è di circa 3,62 milioni di dollari.

Da uno studio sul costo globale delle violazioni dei dati, è emerso che questo è più che raddoppiato tra il 2014 e il 2015, mentre il costo medio per ogni dato perso o rubato è aumentato leggermente a quasi 150 euro. Questo suggerisce che il costo complessivo di una violazione dei dati non ha subito fluttuazione significative nel corso degli anni; è quindi un costo permanente che le organizzazioni devono essere preparate ad affrontare e incorporare nelle loro strategie di protezione dei dati.

Mentre il costo per le PMI è significativamente inferiore al quello per le grandi imprese, le PMI in genere non hanno le risorse finanziarie o altri mezzi per rispondere e risollevarsi da una grave violazione dei dati. Con regolamenti come il General Data Protection Regulation (GDPR) dell'UE che richiedono alle aziende - indipendentemente dalle dimensioni - di essere in grado di spiegare esattamente cosa è successo in caso di violazione l'impatto di un attacco per le PMI probabilmente in futuro sarà maggiore.

L'assicurazione informatica è un ottimo modo per le PMI di mitigare il costo di un attacco informatico o di una violazione dei dati. Tuttavia, l'assicurazione informatica non vi proteggerà da un attacco o da una violazione e NON è un'alternativa all'implementazione delle migliori pratiche, politiche, controlli e tecnologie di sicurezza.

Il costo di una violazione della sicurezza include:

- Interruzione dell'attività (compresa la perdita di tempo e di produttività)
- Costi diretti (come notifiche, assistenza clienti, servizi di monitoraggio del credito, incentivi per il mantenimento del cliente, restituzione e sostituzione della carta)
- Perdita di clienti (churn rate), danni al marchio e perdita di reputazione
- Contenziosi da parte di consumatori, partner commerciali e investitori.
- Multe e sanzioni regolamentari

- Costi di recupero e spese legali (questi possono rappresentare la maggior parte dei costi)
- Perdita di beni (come la proprietà intellettuale)

Secondo la National Cyber Security Alliance, il 60% delle piccole imprese fallisce entro sei mesi da un attacco informatico.

Indagine sull'attuale panorama delle minacce

Per il prossimo futuro, il numero, la vastità e il costo delle violazioni di dati proseguiranno le loro traiettorie ascendenti Questi attacchi saranno sostenuti da diverse tendenze che continueranno a incombere sulle aziende di tutte le dimensioni:

Gli attacchi automatizzati su larga scala stanno diventando il modus operandi dei criminali informatici che sfruttano malware sofisticati e botnet per violare qualsiasi organizzazione o rete vulnerabile, piuttosto che prendere di mira aziende specifiche. Se sei connesso a internet, prima o poi ti troveranno. Nessuno è un bersaglio, ma tutti possono essere vittime.

Il ransomware continuerà ad essere una minaccia crescente. Secondo una ricerca di Datto, lo scorso anno circa il 5 per cento di tutte le PMI del mondo sono state vittime di attacchi ransomware. Il trentacinque per cento degli MSP (Managed Service Providers) ha riferito che le vittime di piccole imprese pagano il riscatto, il 15 per cento di questi non recupera i propri dati.

Il Crime-as-a-service (CaaS) si espanderà man mano che le organizzazioni criminali renderanno le loro pericolose merci sempre più sofisticate. I gruppi criminali stanno facendo incursioni in nuovi mercati e mercificando le loro attività a livello globale, il che porterà a episodi di cybersecurity più persistenti e dannosi che mai. Le porte d'ingresso di questo pericolose settore sono rese ancora più accessibili con armi informatiche come il ransomware-as-a-service e siti maligni (come nulled. to) che offrono la possibilità di agire anche ad aspiranti criminali informatici poco qualificati.

L'internet delle cose (IoT) aggiungerà rischi non gestiti in quanto le organizzazioni abbracciano i dispositivi IoT ma, nella corsa al mercato, perdono di vista il fatto che questi dispositivi sono spesso poco sicuri per impostazione, offrendo così ampie opportunità di attacco, Non bisogna inoltre dimenticare quanti dati sono raccolti nei dispositivi mobili.

Il cloud computing permette alle PMI di competere con i "grandi", offrendo alle piccole imprese la possibilità d avere accesso alle stesse potenti risorse informatiche delle grandi imprese, senza tuttavia sostenere ingenti spese di capitale e di supporto informatico. Secondo la società di consulenza e soluzioni cloud BCSG, con sede nel Regno Unito, circa due terzi delle PMI stanno già utilizzando una media di tre applicazioni software-as-a-service (SaaS) basate sul cloud. Le applicazioni SaaS tipiche per le PMI includono la gestione delle relazioni con i clienti (CRM), la collaborazione online, l'archiviazione dei dati, il marketing online, la gestione dei contratti e software per la catena di approvvigionamento. Mentre questi tipi di soluzioni sono di solito intrinsecamente più sicuri di soluzioni simili on-premises, le aziende devono comunque assicurarsi che i loro fornitori di servizi cloud - in particolare nei mercati più piccoli o nel caso di applicazioni SaaS- seguano le migliori pratiche di sicurezza, siano conformi alle normative pertinenti (come il GDPR), e soddisfino accettabili accordi di livello di servizio (SLA). Per quanto riguarda le PMI, il cloud non elimina la responsabilità finale per la sicurezza e la privacy dei dati sensibili e la conformità normativa. Le PMI devono garantire una solida gestione delle identità e degli accessi, un'autenticazione sicura ai servizi cloud e corretta configurazione, funzionamento e manutenzione dei server basati sul cloud (nel caso di infrastructure-as-a-service, o IaaS).

La catena di approvvigionamento continuerà ad essere presa di mira come backdoor nelle aziende sfruttando le vulnerabilità dei partner della catena di approvvigionamento a monte e a valle che condividono informazioni preziose e sensibili. Ricordate che anche voi siete parte di una catena di approvvigionamento per i vostri clienti.

La regolamentazione costituisce un'ulteriore complessità, e le aziende rischiano di distogliere attenzione e investimenti da altre importanti iniziative di sicurezza a causa delle risorse aggiuntive richieste per affrontare i requisiti di conformità (discussi più avanti in questo capitolo).

Per le PMI, questi nuovi trend e il loro mancato coordinamento, prefigurano uno scenario particolarmente negativo. Poiché tipicamente prive delle risorse finanziarie e delle tecnologie per la sicurezza delle informazioni che hanno le grandi imprese, le PMI rappresentano un "sweet spot" per i criminali informatici (Figura 1-1). Ma non sono loro a portare scompiglio: vale la pena menzionare anche le violazioni involontarie da parte degli insider.

ATTENZIONE

L'Information Security Forum (ISF) fa notare che l'aumento della pervasività delle violazioni di dati e il maggior volume di dati colpiti potrebbero portare a costi molto più elevati per le organizzazioni di tutte le dimensioni.

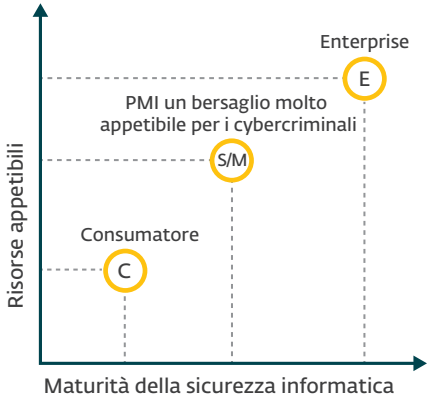


Figura 1-1: Le PMI sono in genere un obiettivo più appetibile dei consumatori e più vulnerabile rispetto alle grandi imprese.

Uno sguardo alle recenti violazioni e fughe di dati

Anche se le grandi violazioni della sicurezza informatica che coinvolgono le grandi imprese e i dati sensibili sembrano ottenere una sensazionalistica copertura mediatica, i cyberattacchi e le violazioni che coinvolgono le PMI non sono meno frequenti e dannosi. Infatti, dato il grande numero di PMI e le loro limitate risorse finanziarie e di sicurezza rispetto alle grandi imprese, l'impatto di un cyberattacco o di una violazione dei dati sui clienti di una PMI - così come per la sopravvivenza della PMI stessa - può essere molto più dannoso.

RICORDA

Le piccole imprese (meno di 50 dipendenti) e le piccole imprese office-home office (SOHO) hanno una diffusione mediatica meno sensazionalistica delle grandi imprese, ma non sono meno vulnerabili ai cyberattacchi e alle violazioni.

Alcuni esempi recenti di violazioni dei dati delle PMI e di cyberattacchi includono:

Obike

Nel dicembre 2017, è stato riferito che già nel giugno 2017, Obike, una società con sede a Singapore che offre servizi di bike sharing in diverse città in tutta l'Asia Pacifica, Europa e Regno Unito, è stata vittima di una violazione dei dati che ha coinvolto le informazioni sensibili dei clienti tra cui nomi, contatti, foto del profilo e posizione.

TIO Networks USA

Nel dicembre 2017, è stato riferito che TIO Networks USA, un servizio canadese di elaborazione dei pagamenti recentemente acquistato da PayPal Holding of California, è stato vittima di una violazione dei dati che coinvolgeva le informazioni personali e finanziarie di circa 8.000 clienti della città di Tallahassee (Florida).

Longs Peak Family Practice

Nel novembre 2017, la Longs Peak Family Practice, una clinica medica con sede in Colorado, ha scoperto una violazione dei dati che ha compromesso i nomi dei pazienti, le date di nascita, i numeri di telefono, gli indirizzi e-mail, i numeri di previdenza sociale, i numeri di patente, le assicurazioni e altre informazioni sensibili.

Royal National Institute of Blind People (RNIB)

Nel novembre 2017, la società britannica RNIB è stata vittima di una violazione dei dati che ha coinvolto i dettagli delle carte di credito e di debito di 817 clienti nel suo negozio di beneficenza online.

Chilton Medical Center

Nell'ottobre 2017, il Chilton Medical Center, con sede nel New Jersey, ha scoperto che un ex dipendente aveva venduto un disco rigido rubato contenente informazioni sanitarie protette (PHI) su 4.600 pazienti.

Secondo il Verizon 2017 Data Breach Investigations Report (DBIR), il 60% dei casi di violazione dei dati coinvolge il furto di dati da parte di insider.

London Bridge Plastic Surgery and Aesthetic Centre (LBPS)

Nell'ottobre 2017, è stato riferito che LBPS era stato vittima di una violazione dei dati che coinvolgeva dati sensibili e fotografie dei pazienti.

Colorado Center for Reproductive Medicine (CCRM)

Nell'ottobre 2017, CCRM Minneapolis (Minnesota) è stato vittima di un attacco ransomware che ha colpito le informazioni sanitarie protette (PHI) su quasi 3.300 pazienti.

Heritage Valley Health Systems

Nel giugno 2017, la Heritage Valley Health Systems, una rete sanitaria che gestisce due ospedali e numerosi servizi di assistenza di lungodegenza, ambulatoriale e ausiliaria in tutta la Pennsylvania occidentale, è stata vittima di un attacco ransomware globale che ha colpito i servizi dei pazienti.

Affrontare il cambiamento del quadro legale e normativo

Con centinaia di regolamenti in tutto il mondo che impongono requisiti di sicurezza delle informazioni e di protezione dei dati, le aziende di tutte le dimensioni stanno lottando per raggiungere e mantenere la conformità. Alcuni esempi di questi regolamenti e standard includono:

Regolamento generale sulla protezione dei dati dell'UE (GDPR)

Applicabile a qualsiasi organizzazione che fa affari con i cittadini dell'UE. Questo regolamento rafforza la protezione dei dati per i cittadini dell'UE e affronta l'esportazione di dati personali al di fuori dell'UE.

Legge federale svizzera sulla protezione dei dati ("LPD")

La Svizzera ha recentemente aggiornato la sua legge federale del 1992 sulla protezione dei dati (FADP) per mantenere la parità con i requisiti del GDPR. Questi aggiornamenti modernizzano le leggi svizzere sulla protezione dei dati per mantenere lo status di adeguatezza della Svizzera concesso dalla Commissione europea e garantire il libero flusso di dati dall'UE in Svizzera e viceversa. Altri paesi dell'UE stanno analogamente aggiornando le loro leggi sulla protezione dei dati sulla scia del GDPR.

South Africa Protection of Personal Information (PoPI) Act

Assicura che le istituzioni sudafricane raccolgano, elaborino, conservino e condividano le informazioni personali di un'altra entità in modo responsabile, e conferisce alcuni diritti di protezione e controllo agli individui come proprietari delle loro informazioni personali.

US Health Insurance Portability and Accountability Act (HIPAA)

Applicabile a qualsiasi organizzazione che tratta o conserva informazioni sanitarie protette (PHI). Protegge la riservatezza del paziente e la privacy dei dati.

Canada Personal Information Protection and Electronic Documents Act (PIPEDA)

Applicabile alle organizzazioni che fanno affari con cittadini canadesi. Questo regolamento protegge la privacy delle informazioni personali dei cittadini canadesi.

International Organisation for Standardisation/ International Electrotechnical Commission (ISO/IEC) 27000 family of standards

Standard sulla sicurezza delle informazioni adottati a livello internazionale, tra cui: Tecnologia dell'informazione - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti (ISO/IEC 27001), Tecnologia dell'informazione - Tecniche di sicurezza - Codice di condotta per i controlli di sicurezza delle informazioni (ISO/IEC 27002), Tecnologia dell'informazione - Tecniche di sicurezza - Codice di condotta per i controlli di sicurezza delle informazioni basati su ISO/IEC 27002 per i servizi cloud (ISO/IEC 27017), e Tecnologia dell'informazione - Tecniche di sicurezza - Codice di condotta per la protezione delle informazioni di identificazione personale (PII) su piattaforme cloud pubbliche che agiscono come elaboratori di PII (ISO/IEC 27018).

Payment Card Industry (PCI) Data Security Standards (DSS)

Applicabile a qualsiasi azienda che accetta, elabora o memorizza transazioni con carte di pagamento (come carte di credito, di debito e prepagate).
Sebbene questi e altri regolamenti siano stati emanati per garantire che la sicurezza appropriata e le migliori pratiche di protezione dei dati siano implementate all'interno delle organizzazioni che gestiscono dati sensibili, sono spesso complessi, ambigui e costosi da affrontare. Purtroppo, questo conduce alla conseguenza involontaria di portare molte organizzazioni a concentrare i loro sforzi sulla conformità normativa piuttosto che sulla sicurezza delle informazioni e la protezione dei dati.

Conformità e sicurezza non sono la stessa cosa. Un'organizzazione può essere conforme, ma non sicura. Al contrario, un'organizzazione può essere sicura, ma non conforme.

Il GDPR è progettato per proteggere la privacy degli individui dell'UE dando loro un maggiore controllo e diritti sui loro dati personali. Gli individui possono, per esempio:

- Richiedere che le imprese forniscano una copia dei loro dati in un formato strutturato, comunemente usato e machine-readable
- Far trasmettere i propri dati a un altro titolare (il "diritto alla portabilità dei dati")
- Far cancellare le loro informazioni (il "diritto all'oblio")

Il GDPR implementa regole molto più severe per quanto riguarda il consenso, la notifica delle violazioni dei dati, le valutazioni d'impatto sulla privacy obbligatorie e il requisito della "privacy by design e by default"

Il mancato rispetto del GDPR può comportare multe fino al 4% delle entrate annuali di un'azienda in tutto il mondo, o 20 milioni di euro (più di 24 milioni di dollari) - qualunque sia il maggiore.

Il GDPR suggerisce anche una serie di misure tecniche di sicurezza che possono essere utilizzate per ottenere la protezione dei dati, tra cui:

- La pseudonimizzazione e la crittografia dei dati personali
- La capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali
- La capacità di ripristinare la disponibilità e l'accesso ai dati personali in modo tempestivo in caso di incidente fisico o tecnico
- Un procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative per garantire la sicurezza del trattamento dei dati personali

Per saperne di più sul GDPR e sulle misure di sicurezza che la vostra azienda può prendere per ottenere la conformità al GDPR, vai su https://encryption.eset.com/

CINQUE PASSI VERSO LA CONFORMITÀ AL GDPR PER LE PICCOLE E MEDIE IMPRESE

1 Stabilire e valutare come vengono trattati i dati

Una comprensione approfondita di come la vostra organizzazione tratta i dati è fondamentale. Con i regolamenti precedenti, solo i titolari dei dati erano responsabili della conformità, ma gli obblighi del GDPR ricadono anche sui gestori dei dati. Serve stabilire se la vostra organizzazione è un elaboratore di dati o un controllore di dati, tenendo presente che potrebbe essere entrambi. Sapere dove sono immagazzinati i dati e la sicurezza di quel luogo, così come determinare se quei dati vengono condivisi, è fondamentale.

2 Imparare dal passato

Per verificare le vostre capacità in termini di reazione a un eventuale attacco futuro, esaminate ciò che è successo durante le violazioni passate e chiedetevi se le misure adottate possono soddisfare i nuovi requisiti stabiliti dal GDPR. Secondo le nuove regole, le violazioni devono essere segnalate entro 72 ore, insieme alle informazioni sulla gravità dell'attacco. Se la vostra azienda non è in grado di farlo, questa mancanza può comportare una multa molto salata. Aggiornare (o creare) il proprio piano di azione agli incidenti e testare regolarmente ala propria capacità ed efficacia di risposta agli incidenti è un passo fondamentale per garantire la conformità al GDPR.

3 Nominare un responsabile della protezione dei dati o qualcuno con relativa responsabilità formale.

Questo può essere un consiglio semplice per un'azienda con un sacco di soldi, ma la spesa aggiuntiva rende la cosa scoraggiante per le

aziende più piccole. Tuttavia, non è così sconvolgente come essere multati del 4% delle proprie entrate e potrebbe non essere un impegno a tempo pieno. Il responsabile della protezione dei dati agisce in modo indipendente e, facendo riferimento al più alto livello di gestione, dovrebbe aiutare ad attuare i requisiti. Allocare ulteriori risorse prima piuttosto che dopo assicurerà che la vostra azienda non solo sia conforme, ma anche attrezzata per affrontare qualsiasi violazione dei dati e mitigare la possibilità di essere multata.

4 Educare lo staff, e se stessi, alle regole

Uno degli obiettivi principali del GDPR è quello di rafforzare la capacità delle persone di essere dimenticate e di poter cancellare i propri dati. Le aziende dovranno anche ottenere un consenso esplicito dagli individui prima di trattare i loro dati. Le regole rendono anche più difficile per i bambini fornire i loro dati. Sapere come le regole cambiano la gestione del consenso della vostra organizzazione e i diritti degli individui è imperativo.

5 Conoscere la propria autorità di vigilanza principale

L'autorità che gestisce qualsiasi reclamo contro l'azienda dipende da dove questa ha sede, non dalla posizione dell'individuo che solleva il reclamo. Questo può essere difficile per le aziende che operano a livello internazionale, o che hanno più sedi in diverse regioni. Ci sono anche altre direttive in diversi paesi che possono andare oltre il GDPR e che devono essere considerate.

In questo capitolo

- I fondamenti della protezione dei dati
- Distribuzione on-premises e nel cloud
- La scelta degli MSP e l'outsourcing

Capitolo 2

PRIMI PASSI NELLA PROTEZIONE DEI DATI

In questo capitolo, imparerete le basi della tecnologia di protezione dei dati, confronterete diverse opzioni di implementazione on-premises e nel cloud ed esplorerete i fornitori di servizi di sicurezza gestiti (MSP) e le opzioni di outsourcing.

Capire le basi della protezione dei dati

Proteggere la sicurezza e la privacy delle informazioni sensibili dei clienti è un obbligo fondamentale per tutte le aziende, comprese le PMI.

La protezione dei dati (e più in generale la sicurezza delle informazioni) comprende tutti i controlli amministrativi, logici e tecnici necessari per proteggere le informazioni. La triade C-I-A (Figura 2-1) è comunemente usata per guidare lo sviluppo e l'implementazione di una struttura per gestire la sicurezza delle informazioni all'interno di un'organizzazione. Consiste in tre concetti fondamentali di sicurezza delle informazioni:

Confidenzialità (e privacy)

Impedisce l'accesso non autorizzato, l'uso, la divulgazione, lo sfruttamento, l'ispezione o la registrazione dei dati.

Integrità

Impedisce la modifica non autorizzata o impropria dei dati.

Disponibilità

Assicura che gli utenti autorizzati abbiano un accesso affidabile e tempestivo ai dati e previene la distruzione o l'interruzione non autorizzata dei dati.

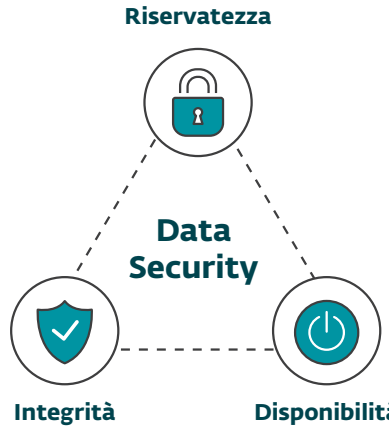


Figura 2-1: La triade C-I-A.

Per esempio, per proteggere la riservatezza dei dati sensibili, varie politiche occupazionali, di sicurezza e privacy solitamente definiscono chi ha accesso a certi dati all'interno di un'organizzazione, per quali scopi e cosa sono autorizzati a fare con quei dati. I controlli tecnici per garantire la riservatezza potrebbero includere la gestione dell'identità e dell'accesso (IAM), la crittografia e le soluzioni di prevenzione della perdita di dati.

Per proteggere l'integrità dei dati, possono essere implementate varie soluzioni tecniche come i checksum e la convalida dei dati inseriti nei moduli e nei database. Le firme digitali e l'hashing utilizzano tecnologie di crittografia per provare l'autenticità dei dati o per verificare che i dati non siano stati alterati. Infine, le soluzioni anti-malware proteggono l'integrità dei dati (e potenzialmente la riservatezza e la disponibilità di questi).

Per proteggere la disponibilità dei dati dalla distruzione accidentale (per esempio, la cancellazione) o intenzionale (per esempio, un attacco ransomware), vengono implementati sistemi di backup e recupero, così come politiche di backup e conservazione. Le tecnologie di protezione dei dati sono ulteriormente affrontate nel capitolo 4.

Un'efficace sicurezza delle informazioni richiede che un'azienda si occupi della riservatezza, dell'integrità e della disponibilità di tutti i suoi dati sensibili, compresi i sistemi e le applicazioni che elaborano e conservano quei dati.

Utilizzando un approccio basato sul rischio, le organizzazioni possono implementare controlli appropriati per affrontare le vulnerabilità e raggiungere un livello accettabile di rischio per i dati contro minacce specifiche. Più alto è il rischio per i dati, maggiori sono le misure di protezione che dovrebbero essere implementate. La gestione del rischio di sicurezza consiste in quattro fasi chiave (Figura 2-2)

Figura 2-2: Un processo di base per la gestione del rischio.

Valutazione dei rischi

Ci sono molte metodologie di valutazione del rischio con vari livelli di costo e complessità. Il processo di base consiste in:

- **Identificazione degli asset**
  Identificare tutti gli asset dell'organizzazione (sia tangibili che intangibili) che richiedono protezione, includendo il valore quantitativo (come il costo o il contributo alle entrate) e/o qualitativo (come l'importanza relativa) dell'asset.
- **Analisi delle minacce**
  Definire possibili circostanze o eventi avversi naturali e/o causati dall'uomo, il potenziale impatto o le conseguenze, la probabilità e la frequenza del loro verificarsi.
- **Valutazione della vulnerabilità**
  Determinare quali salvaguardie e/o controlli sono assenti o deboli in un asset, rendendo così una minaccia potenzialmente più dannosa, costosa, probabile o frequente.

Trattamento del rischio

La valutazione del rischio fornisce la base per le decisioni di gestione riguardo a rischi specifici. Le opzioni includono:

- **Mitigazione del rischio**
  Implementare politiche, controlli e/o altre misure per ridurre l'impatto o la probabilità di una specifica minaccia contro una specifica risorsa.
- **Assegnazione del rischio (o trasferimento)**
  Trasferire il rischio potenziale a una terza parte, come un assicuratore, un fornitore di servizi o un altro agente che accetta esplicitamente di accettare il rischio.

- **Evitare il rischio**
  Eliminare del tutto il rischio, per esempio migliorando o eliminando l'asset, o cessando l'attività che introduce il rischio.

Accettazione del rischio

Si tratta dell'approvazione formale da parte della direzione delle misure di trattamento del rischio che vengono attuate, e dell'accettazione di qualsiasi rischio residuo (o rimanente) che non può essere ulteriormente o praticamente mitigato, assegnato o evitato.

Comunicazione del rischio

Le parti interessate di competenza devono essere messe al corrente di qualsiasi decisione di trattamento del rischio e/o di accettazione del rischio che sia stata presa, inclusi i loro ruoli e responsabilità individuali riguardo a rischi specifici.

Confronto tra opzioni di distribuzione on-premises, cloud e ibride

Le aziende oggi hanno molte opzioni per la distribuzione della tecnologia, tra cui on-premises, nel cloud, e una distribuzione ibrida con alcune risorse situate on-premises e altre situate nel cloud.

In un passato non troppo lontano, l'unica opzione di implementazione per le aziende era on-premises. Anche le aziende più piccole si sono spesso trovate a dover acquistare diversi server costosi, spesso installati in modo precario in un armadio buio e affollato da qualche parte nell'edificio (magari con uno sprinkler antincendio nel soffitto - giusto nel caso in cui un incendio non distruggesse i vostri costosi investimenti IT). Questi server richiedevano un'amministrazione e una manutenzione continua, che spesso significava personale IT aggiuntivo o imprese terze. Non solo i server, ma anche le apparecchiature di rete come i router, gli switch e il cablaggio di rete dovevano essere installati e gestiti. Come minimo, un firewall proteggeva la rete interna "affidabile" da internet "non affidabile".

Gestire una sala server on-premises o un centro dati è ancora un'opzione valida per molte aziende. Ma poiché la virtualizzazione, la connettività di rete e le tecnologie di cloud computing sono diventate più solide e stabili nell'ultimo decennio, molte aziende stanno spostando alcune o tutte le loro risorse IT nel cloud.

Ma cos'è esattamente il cloud? Praticamente ogni fornitore di prodotti tecnologici sul mercato ha un'offerta "cloud" di qualche tipo e, purtroppo, la definizione di cloud può essere a volte un po', beh, torbida. Quindi, per fare chiarezza, definiamo alcuni elementi importanti del cloud usando le definizioni del National Institute of Standards and Technology (NIST) degli Stati Uniti, neutrali rispetto ai fornitori. Secondo il NIST, i tre modelli di servizio di cloud computing sono i seguenti:

Software as a Service (SaaS)

Ai clienti viene fornito l'accesso a un'applicazione in esecuzione su un'infrastruttura cloud. L'applicazione è accessibile da vari dispositivi e interfacce client, ma il cliente non ha conoscenza e non gestisce o controlla l'infrastruttura cloud sottostante. Il cliente può avere accesso a impostazioni limitate delle applicazioni specifiche dell'utente, e la sicurezza dei dati del cliente è ancora responsabilità del cliente.

Platform as a Service (PaaS)

I clienti possono distribuire le applicazioni supportate sull'infrastruttura cloud del fornitore, ma il cliente non ha alcuna conoscenza e non gestisce o controlla l'infrastruttura cloud sottostante. Il cliente ha il controllo sulle applicazioni distribuite e sulle impostazioni di configurazione limitate per l'ambiente di hosting delle applicazioni. L'azienda possiede le applicazioni e i dati distribuiti ed è quindi responsabile della sicurezza di tali applicazioni e dati.

Infrastructure as a Service (IaaS)

I clienti possono fornire l'elaborazione, lo stoccaggio, le reti e altre risorse di calcolo e distribuire ed eseguire sistemi operativi e applicazioni, ma il cliente non ha alcuna conoscenza e non gestisce o controlla l'infrastruttura cloud sottostante. Il cliente ha il controllo sui sistemi operativi, lo storage e le applicazioni distribuite, così come alcuni componenti di rete. L'azienda possiede le applicazioni e i dati distribuiti ed è quindi responsabile della sicurezza di tali applicazioni e dati.

SUGGERIMENTO

I diversi modelli di servizi cloud (SaaS, PaaS e IaaS) hanno diverse implicazioni di sicurezza per i clienti. Per esempio, le offerte SaaS come Microsoft 365 e Salesforce forniscono la sicurezza dell'infrastruttura attraverso il fornitore di cloud, ma la sicurezza dei dati e l'autenticazione sono responsabilità del cliente. Le responsabilità di sicurezza del cliente aumentano progressivamente nelle offerte PaaS e IaaS. Molte soluzioni cloud spostano l'attenzione dalla sicurezza delle applicazioni o delle infrastrutture alla sicurezza dell'autenticazione e dell'integrità dei dati.

Il NIST definisce anche quattro modelli di distribuzione del cloud computing:

Pubblico

Un'infrastruttura cloud aperta all'uso da parte di un'utenza pubblica. È di proprietà, gestito e operato da una terza parte (o più parti) ed esiste nei locali del fornitore di cloud.

Privato

Un'infrastruttura cloud utilizzata esclusivamente da una singola organizzazione. Può essere posseduto, gestito e operato dall'organizzazione o da una terza parte (o una combinazione di entrambi), e può esistere in sede o fuori sede.

Ibrido

Un'infrastruttura cloud composta da caratteristiche di due o più degli altri modelli di implementazione, legati insieme da una tecnologia standardizzata o proprietaria che permette la portabilità dei dati e delle applicazioni.

Comunità (non comune)

Un'infrastruttura cloud utilizzata esclusivamente da un gruppo specifico di organizzazioni.

Il passaggio verso il cloud spesso inizia come molte nuove iniziative, con applicazioni e sistemi non rivolti alla produzione o non critici, come un ambiente di sviluppo o sistemi di backup. Mentre il viaggio continua, molte aziende iniziano a "sollevare e spostare" le applicazioni esistenti e a distribuirne di nuove direttamente nel cloud. Infine, le organizzazioni "cloud first" puntano a distribuire la maggior parte possibile del loro ambiente IT nel cloud e sviluppare applicazioni "cloud native" per i loro clienti.

Fra i molti vantaggi del cloud per le aziende ricordiamo:

Maggiore agilità e reattività

È possibile accedere ad applicazioni e dati nel cloud da qualsiasi luogo, in qualsiasi momento e su qualsiasi dispositivo.

Time-to-market più veloce

È possibile sviluppare e fornire nuovi prodotti e servizi più rapidamente nel cloud con PaaS o risorse IaaS facilmente disponibili.

Scalabilità on-demand

Ulteriori licenze software e/o infrastrutture possono essere fornite e rimosse a seconda delle necessità, il che supporta le esigenze di aziende in rapida crescita e cicliche che potrebbero non essere in grado di prevedere accuratamente i cambiamenti del mercato e la crescita del business.

Maggiore stabilità

L'infrastruttura cloud è tipicamente installata in solidi data center costruiti in un'ottica di performance, stabilità e affidabilità, e gestiti da grandi team di personale IT specializzato.

Investimenti di capitale ridotti

È possibile implementare l'intera infrastruttura IT nel cloud e rinunciare a costosi investimenti di capitale. Il cloud offre servizi pianificabili con abbonamento "pay as you go" che vi permettono di preventivare le vostre esigenze IT come una spesa operativa continua e di pagare solo per quello che usate.

ATTENZIONE

Spostare le applicazioni e i dati nel cloud non elimina o trasferisce la vostra responsabilità per la sicurezza delle vostre applicazioni e dei vostri dati. Anche se il fornitore di servizi cloud è responsabile di alcuni aspetti dell'ambiente, siete sempre voi i responsabili in ultima analisi della protezione e della sicurezza delle vostre applicazioni e dei vostri dati. I fornitori di servizi cloud fanno comunemente riferimento a un "modello di responsabilità condivisa" che mostra chiaramente di cosa sono responsabili nel cloud e di cosa siete responsabili voi - e da nessuna parte il modello di responsabilità condivisa mostra che il fornitore di servizi cloud è responsabile della sicurezza dei vostri dati!

Prendere in considerazione gli MSP (Managed Security Service Providers) e l'outsourcing

Mantenere i sistemi e le applicazioni IT sicuri, riparati, protetti e conformi di fronte a rischi sempre crescenti e minacce sempre più sofisticate è un onere impegnativo per le aziende di tutte le dimensioni. Questo è particolarmente vero per le PMI con personale IT e risorse di sicurezza limitate. Ed è per questo motivo che molte PMI si stanno rivolgendo ai Managed Security Service Providers (MSP) I benefici e il valore di un MSP per le PMI includono:

Migliore controllo del budget IT

Gli MSP possono offrire un portafoglio completo di prodotti e servizi rispetto alle risorse interne relativamente limitate delle PMI. Optare per i servizi di un MSP porta anche a una maggiore flessibilità finanziaria e a costi più prevedibili, e con piani di fatturazione regolabili, le PMI hanno anche un migliore controllo sul loro budget IT e di sicurezza.

Consulente di fiducia con conoscenza ed esperienza

Le PMI possono sfruttare la profonda conoscenza e la vasta esperienza del personale IT e di sicurezza impiegato dagli MSP.

Conoscenza e attenzione al mercato

Gli MSP che si concentrano sulla sicurezza hanno una migliore conoscenza delle soluzioni disponibili sul mercato e possono fornire offerte di sicurezza personalizzate per i loro clienti.

Innovazione

I team specializzati in sicurezza degli MSP possono facilitare l'adozione e l'implementazione di soluzioni innovative e aiutare i clienti a stare al passo con gli attuali sviluppi del mercato.

Pronti al cambiamento

Gli MSP permettono ai loro clienti di aggiungere o rimuovere qualsiasi software o hardware in base alle loro esigenze attuali senza dover passare attraverso il processo minuzioso di acquisizione, implementazione e manutenzione di nuove risorse hardware e software.

SHEFFIELD WEDNESDAY CHAMPIONS ESET I.T. SECURITY

Lo Sheffield Wednesday Football Club (SWFC) è uno dei più antichi club di calcio professionali del mondo. Lo stadio Hillsborough ha ospitato sia la Coppa del Mondo che i Campionati Europei e le semifinali della FA Cup. Il club ha un forte programma comunitario che incoraggia le persone a partecipare alle attività sportive e a sfruttare al massimo le strutture comunitarie di SWFC. Una parte fondamentale del programma è lo sviluppo delle life skills (competenze per la vita), e SWFC ha investito in attrezzature informatiche per avere la possibilità di gestire aule portatili, accanto a strutture più permanenti.

Sfide

Il software antivirus di SWFC era diventato ingombrante e consumava troppa potenza di elaborazione. SWFC voleva anche una console di amministrazione centralizzata e aggiornamenti automatici per garantire che le sue 310 macchine fossero protette dalle ultime minacce per assicurare la continuità del business.

Soluzione

Da quando è passato a ESET Endpoint Antivirus, Richard Ford, responsabile IT, non si è più voltato indietro. "ESET era proprio quello che stavamo cercando: potenza di elaborazione, protezione affidabile e costi scalabili, facile da implementare e gestire a livello centrale. Non distoglie l'attenzione degli utenti con problemi come rallentamenti o falsi positivi e funziona esattamente come tutti gli antivirus dovrebbero fare, tranquillamente in background"

Risultati

- Una soluzione di sicurezza facilmente integrabile, non invasiva, con un ingombro ridotto che non ostacola il traffico di rete
- Facile installazione e bassa manutenzione
- Una console di amministrazione centralizzata fornisce una protezione affidabile contro le minacce per server e workstation, offrendo una panoramica centralizzata e analisi dettagliate in tempo reale
- La soluzione si aggiorna regolarmente una volta configurata

In questo capitolo

- Uno sguardo al processo di valutazione del rischio
- Identificazione delle operazioni di trattamento dei dati
- Determinare l'impatto di una violazione dei dati
- Identificare le minacce relative alla sicurezza dei dati
- Implementare controlli appropriati sulla protezione dei dati

Capitolo 3

VALUTARE I RISCHI PER LA SICUREZZA DEI DATI

In questo capitolo imparerete come applicare il processo di gestione del rischio (discusso nel capitolo 2) alla sicurezza dei dati.

Comprendere il processo di valutazione del rischio

La valutazione del rischio è la prima fase del processo di gestione del rischio (discussa nel capitolo 2). Una valutazione del rischio consiste in:

- Identificare i propri beni (sia tangibili che intangibili)
- Analizzare le minacce (compreso l'impatto e la probabilità)
- Valutare le vulnerabilità (cioè, quali salvaguardie o controlli sono assenti o insufficienti in un dato asset)

Allo stesso modo, la valutazione dei rischi per la sicurezza dei dati comporta:

- Identificare i propri processi relativi al trattamento dei dati (per determinare come e dove le risorse di dati sono utilizzate dall'azienda)
- Determinare il potenziale impatto aziendale (se i dati vengono compromessi)
- Identificare le possibili minacce e valutare la loro probabilità di verificarsi, inclusa la frequenza
- Valutazione del rischio (per valutare quali azioni preventive o controlli dovrebbero essere implementati per proteggere i dati)

Passo 1
Identificare le operazioni di trattamento dei dati messe in atto dall'azienda

I dati all'interno di un'organizzazione hanno diversi profili di rischio, non solo in base al contenuto dei dati, ma anche a causa del modo in cui i dati vengono utilizzati all'interno dell'organizzazione. Quindi, nel processo di valutazione del rischio è importante capire come i questi vengono elaborati all'interno della vostra azienda. Per esempio, una tipica PMI potrebbe utilizzare alcuni o tutti i seguenti tipi di operazioni di elaborazione dei dati:

Risorse umane come la gestione del libro paga dei dipendenti, il reclutamento e la conservazione, i registri di formazione, le azioni disciplinari e le valutazioni delle prestazioni.

Gestione dei clienti, marketing e fornitori come informazioni sui clienti, ordini di acquisto e vendita, fatture, liste di e-mail, dati di marketing e pubblicità e contratti con i fornitori.

Sicurezza del personale e sicurezza fisica come i registri di accesso dei dipendenti, i registri dei visitatori e il monitoraggio video.

Per ogni operazione di trattamento dei dati, considerate quanto segue:

- Quali dati personali vengono trattati?
- Qual è lo scopo del processo?
- Dove avviene l'elaborazione?
- Chi è responsabile del processo?
- Chi ha accesso ai dati?

Il principio del minimo privilegio è una buona pratica di sicurezza delle informazioni in cui agli utenti finali è concesso solo il livello minimo di accesso richiesto per eseguire una specifica funzione lavorativa.

Passo 2
Determinare il potenziale impatto sul business

Successivamente, è necessario determinare l'impatto potenziale di una violazione o compromissione dei dati. Una violazione o una compromissione può colpire la riservatezza dei dati (per esempio, un accesso non autorizzato), l'integrità dei dati (per esempio, una modifica non autorizzata), o la disponibilità dei dati (per esempio, un attacco ransomware).

RICORDA

Le organizzazioni devono proteggere la riservatezza, l'integrità e la disponibilità dei dati. Nell'ambito della sicurezza informatica, questo è noto come la triade C-I-A (vedi pagina 14-15).

In una tipica valutazione del rischio, l'impatto potenziale di un dato rischio è tipicamente espresso in termini di danno all'organizzazione, come la perdita o la distruzione di un asset fisico (per esempio, un server, una macchina fotocopiatrice o un veicolo).

L'impatto di un rischio per la sicurezza dei dati sul business è simile agli altri impatti del rischio, ma può essere indiretto. Nel caso di dati personali sensibili, l'individuo i cui dati sono violati o compromessi è la vittima diretta. In questi casi, l'identità o i beni finanziari di un individuo possono essere rubati e/o la loro privacy può essere violata. L'impatto sul business è meno diretto ma comunque molto costoso e può includere (tra gli altri):

- Perdita di clienti e di entrate
- Danni al marchio e alla reputazione
- Multe regolamentari e contenziosi
- Notifiche di violazione e servizi di monitoraggio del credito
- Analisi forense e ripristino

SUGGERIMENTO

L'impatto aziendale può essere classificato come basso, medio o alto. Tuttavia, la definizione effettiva di ciascuno di questi livelli di impatto sarà unica per ogni azienda e dovrebbe coinvolgere sia misure oggettive (quantitative) che soggettive (qualitative).

Passo 3
Identificare le possibili minacce e valutarne la probabilità

Una minaccia può essere qualsiasi evento o circostanza, naturale o artificiale, che ha il potenziale di influenzare negativamente la riservatezza, l'integrità o la disponibilità dei dati personali o sensibili. Questo può includere attacchi di cybersecurity, perdita o divulgazione accidentale, minacce interne, incendi e inondazioni, terremoti e tsunami, condizioni meteorologiche gravi (come un uragano o un tornado), disordini civili, controversie di lavoro e altro. Le aziende devono identificare le possibili minacce alle loro operazioni di trattamento dei dati e valutare la probabilità (inclusa la frequenza) di ogni possibile minaccia. Assicuratevi di prendere in considerazione le minacce in aree ben definite, comprese quelle provenienti dalla rete e dalle risorse tecniche (software/hardware) che sono usate per l'elaborazione dei dati, dai processi e dalle procedure correlate, dalle risorse umane coinvolte e dalla scala di elaborazione.

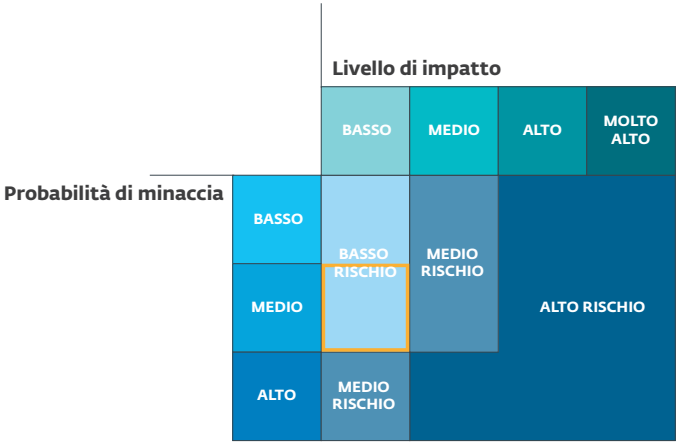
SUGGERIMENTO

Per ogni minaccia identificata, la probabilità può essere classificata in modo simile all'impatto aziendale: Basso, Medio o Alto. Quando si valuta la probabilità che una minaccia si verifichi, si considera sia la probabilità che la minaccia si verifichi, sia la frequenza con cui potrebbe presentarsi in un dato periodo (per esempio, in un periodo di un anno).

Passo 4
Valutare il rischio

Una volta identificate tutte le operazioni di elaborazione dei dati (e i dati elaborati), determinato il potenziale impatto aziendale di una violazione o compromissione dei dati e identificato le possibili minacce e la probabilità e la frequenza di accadimento, è possibile valutare il rischio associato a ciascuna operazione e determinare appropriati controlli in ambito di protezione dei dati sia a livello tecnologico che organizzativo/procedurale. Secondo la valutazione dei rischi, i controlli organizzativi e di processo (discussi nel Capitolo 5) dovrebbero essere implementati per proteggere adeguatamente i dati e le operazioni di elaborazione dei dati utilizzando un approccio basato sul rischio.

La Figura 3-1 mostra un modello di valutazione dei dati e un esempio di valutazione di un'operazione di trattamento dei dati.



Probabilità di minaccia

Per una particolare operazione di elaborazione dei dati, esaminate la lista delle possibili minacce e analizzate/valutate la probabilità di incidenza. La probabilità finale dovrebbe essere basata sulla somma del punteggio di tutte le minacce della relativa lista.

- **Basso** – è improbabile che la minaccia si materializzi
- **Medio** – c'è una ragionevole possibilità che la minaccia si materializzi
- **Alto** – è probabile che la minaccia si materializzi

Livello di impatto

Per una particolare operazione di trattamento dei dati, valutate il possibile impatto sulla riservatezza, integrità e disponibilità dei dati (triade C-I-A). L'impatto più alto dei tre è il livello di impatto finale.

- **Basso** – inconvenienti minori, che potrebbero essere superati senza problemi
- **Medio** – inconvenienti significativi, che potrebbero essere superati nonostante alcune difficoltà
- **Alto** – conseguenze significative, che potrebbero essere superate ma con serie difficoltà
- **Molto alto** – conseguenze significative, o addirittura irreversibili, potrebbero non essere superate

L'operazione di elaborazione dei dati prevede

- **Rischio basso**
- **Rischio medio**
- **Rischio alto**

Esempio

Operazione di elaborazione dei dati: Marketing/Pubblicità
Dati elaborati: Informazioni di contatto (ad esempio, nome, indirizzo postale, numero di telefono, e-mail)
Classificazione dei dati: Dati personali
Scopo del trattamento: Promozione di beni e offerte speciali a possibili clienti
Proprietari dei dati: Clienti e lead

Probabilità di minaccia

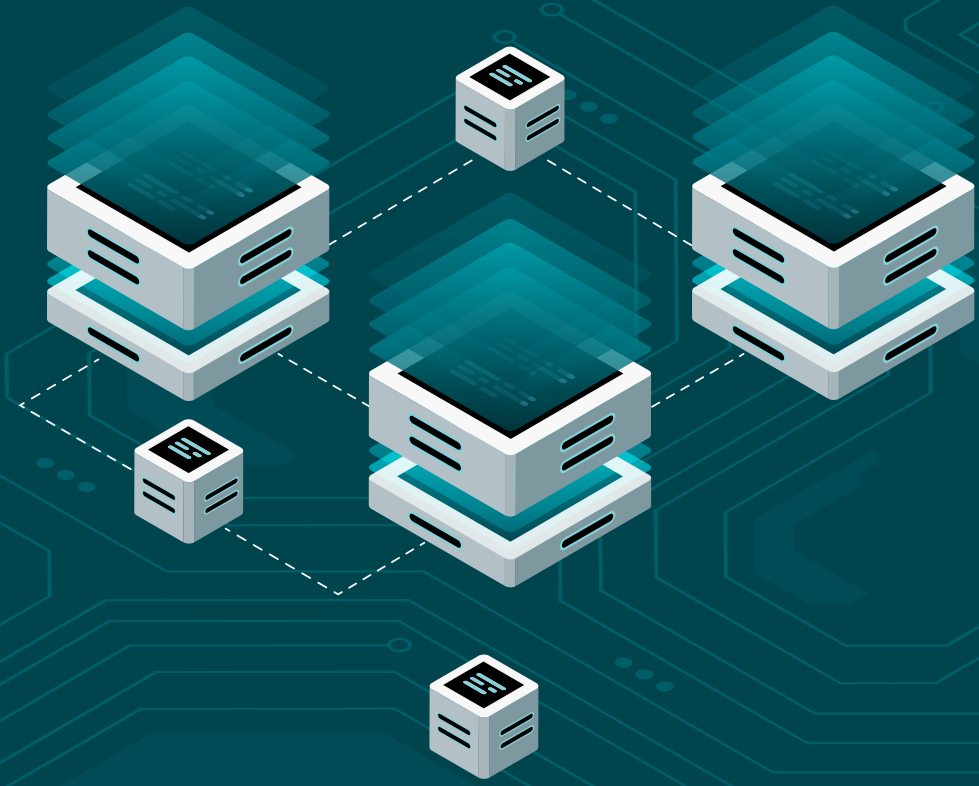
Minacce alla rete e alle risorse tecniche (HW, SW): Medio
minacce ai processi e alle procedure: Basso
minacce alle risorse umane coinvolte: Medio
Settore di attività e portata delle minacce: Medio
Probabilità finale: Medio

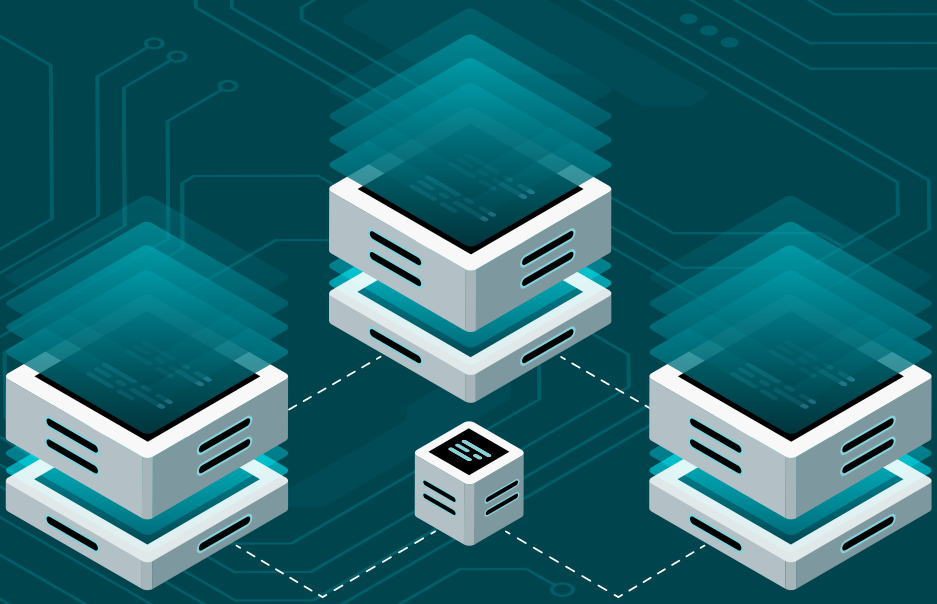
Livello di impatto

Valutazione del livello di impatto confidenza: bassa, integrità: bassa, disponibilità: bassa
Livello di impatto finale: Basso

Operazione di elaborazione dati pos

- **Rischio basso** – l'elaborazione dei dati di marketing/pubblicità pone un rischio basso - devono essere implementate misure tecniche e organizzative adeguate a questo rischio.





In questo capitolo

- Valutare le soluzioni di protezione dei dati
- Proteggere la rete
- Ridurre gli errori e migliorare l'efficienza con un sitema di orchestrazione

Capitolo 4

COMPRENDERE LA TECNOLOGIA RELATIVA ALLA PROTEZIONE DEI DATI

In questo capitolo, verranno presentate le diverse tecnologie di sicurezza informatica e di protezione dei dati che potete considerare di implementare in tutta la vostra azienda - dall'endpoint alla rete e oltre.

Proteggere i dati ovunque

I dati sono una risorsa fondamentale, ma possono rappresentare un rischio enorme per il vostro business. Ci sono molte tecnologie di sicurezza che si possono usare per proteggere i dati negli spazi di lavoro (come computer e dispositivi mobili), in rete e nel backend (come una sala server in sede o un datacenter basato sul cloud). La Figura 4-1 mostra vari sistemi di sicurezza (discussi di seguito) da considerare per la vostra azienda, in considerazione del vostro livello di rischio e le risorse disponibili.

Oltre al software anti-virus (A/V), le PMI dovrebbero considerare l'implementazione:

Protezione degli endpoint

Andando oltre il software antivirus, la protezione degli endpoint è una tecnologia a più livelli che previene le infezioni da malware (inclusi virus, worm, ransomware, spyware, trojan e trojan di accesso remoto, e rootkit/bootkit), gli exploit di vulnerabilità, gli attacchi di rete, l'infiltrazione di botnet e altro ancora (vedi "Sscegliere la protezione degli endpoint" qui sotto).

Autenticazione a più fattori (MFA)

L'MFA migliora ulteriormente l'autenticazione di base (per esempio, username e password) richiedendo un fattore aggiuntivo per accedere a un sistema o un'applicazione. Tipicamente, questo consiste in un codice una tantum inviato a un indirizzo e-mail separato precedentemente configurato o tramite messaggio di testo a uno smartphone. L'utente deve prima fornire il suo nome utente e la sua password. Il codice può essere usato solo per autenticare una singola sessione utente entro un periodo di tempo limitato (per esempio, 60 secondi), il che mitiga l'efficacia degli attacchi replay in cui un aggressore intercetta il codice, per poi usarlo in una sessione separata per autenticarsi. L'ultima forma di MFA challenge-response (supportata da ESET Secure Authentication) permette all'utente di confermare semplicemente l'autenticazione su uno smartphone accoppiato, eliminando così la necessità di ridigitare il codice monouso.

Firewall

(discusso più avanti in questo capitolo).

Crittografia

La crittografia rende i dati inintelligibili senza la chiave di decrittazione appropriata. La crittografia e la decrittografia possono essere eseguite sia in hardware (più veloce) che in software (meno costoso). La crittografia dell'intero disco e dei supporti rimovibili protegge i dati su server, computer desktop e portatili e dispositivi mobili nel caso in cui un endpoint venga perso o rubato, o si verifichi una violazione dei dati. La crittografia di file, cartelle ed e-mail permette una collaborazione in tutta sicurezza attraverso diversi gruppi di lavoro e limitazioni per team, con criteri di sicurezza applicati a tutti gli endpoint tramite una gestione centrale remota.

Backup e recupero

I sistemi di backup e di recupero includono il software di backup e i supporti di backup, come il nastro o il disco, sia in sede (e conservati fuori sede), sia in remoto o nel cloud. I backup dovrebbero essere testati regolarmente per garantire che possano essere recuperati, e che tutti i sistemi e i dati necessari siano correttamente sottoposti a backup abbastanza frequentemente per soddisfare le esigenze aziendali. I backup proteggono le aziende dalla distruzione, cancellazione o modifica accidentale o dolosa dei dati (compresi gli attacchi ransomware), e aiutano a garantire la continuità delle attività in caso di incidente.

MDM - Online Device Management (Gestione dei dispositivi online)

Molte organizzazioni, in particolare le PMI, permettono ai dipendenti di utilizzare i loro dispositivi mobili personali per scopi lavorativi. Questa tendenza

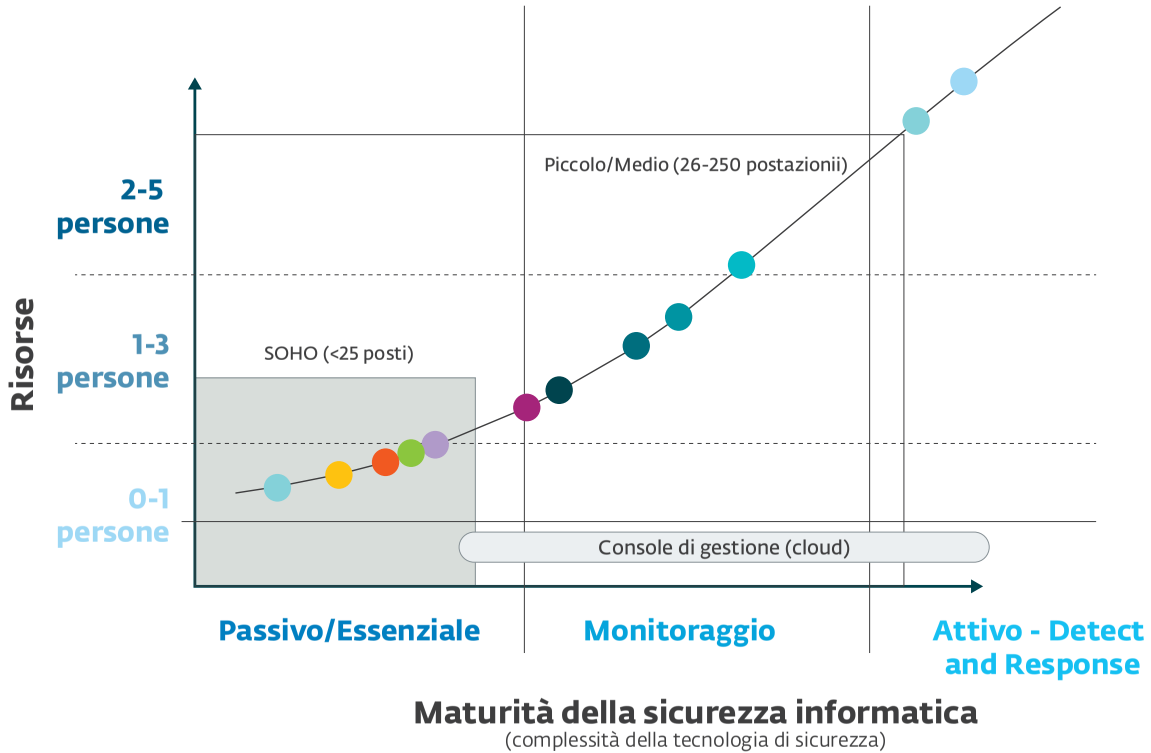
popolare è conosciuta con l'acronimo BYOD - *bring your own device* (in italiano: porta il tuo dispositivo) Tuttavia, le aziende devono assicurarsi che questi dispositivi siano gestiti in modo sicuro per garantire che le informazioni aziendali sensibili o i dati dei clienti non siano compromessi se il dispositivo viene perso, rubato o altrimenti violato. Il software MDM offre funzionalità come il rispetto delle normative (per esempio, richiedendo un codice di accesso), la crittografia, la containerizzazione (per isolare le app/dati aziendali dalle app/dati personali) e la cancellazione/il blocco a distanza.

Prevenzione della perdita di dati (DLP)

Il software DLP impedisce la divulgazione accidentale (o intenzionale) non autorizzata di certi dati, come i numeri di previdenza sociale, le informazioni sanitarie protette (PHI) e i dati finanziari, scansionando e-mail e documenti per certe parole chiave e modelli di corrispondenza dei dati.

ATTENZIONE

Per essere efficace, la DLP richiede risorse aggiuntive per modificare le politiche, valutare gli incidenti (sia interni che esterni) e applicare azioni correttive. Se la DLP viene implementata senza questo sforzo aggiuntivo, la sua efficacia sarà limitata.


Risorse
2-5 persone
1-3 persone
0-1 persone
Piccolo/Medio (26-250 postazionii)
SOHO (<25 posti)
Console di gestione (cloud)
Passivo/Essenziale
Monitoraggio
Attivo - Detect and Response
Maturità della sicurezza informatica
(complessità della tecnologia di sicurezza)

Tecnologie per la sicurezza

- AV
- Protezione degli endpoint
- Autenticazione a più fattori
- Firewall
- Crittografia
- Backup e recupero
- MDM - Online Device Management (Gestione dei dispositivi online)
- NAC (Controllo dell'accesso alla rete)
- SIEM
- Gestione delle patch
- DLP
- EDR/EDTR

Maturità della sicurezza informatica

- **Passivo/Essenziale** - Azioni automatizzate, reazioni ad-hoc sui rischi identificati
- **Monitoraggio** - Azioni automatizzate, monitoraggio attivo dello stato attuale con azioni che reagiscono agli avvisi su attacchi o rischi potenziali
- **Active-Detect and Response** - Analisi interna dei dati e monitoraggio dello stato al fine di rilevare attacchi mirati, azioni secondo le politiche atte a rispondere agli attacchi e ai possibili attacchi

Risorse

- Squadra formale: Specialista a tempo pieno **2-5 persone**
- Dedicato: Specialista part-time **1-3 persone**
- In base alle necessità: "installa e dimentica" **0-1 persone**

Figura 4-1: Tecnologie per la sicurezza.

SCELTA DELLA PROTEZIONE DEGLI ENDPOINT

La protezione degli endpoint su computer desktop, dispositivi mobili e server è la prima linea di difesa contro i cyberattacchi, perché gli aggressori in genere sfruttano "l'anello più debole" nel tentativo di violare la vostra rete. Pertanto, affidare la sicurezza dei vostri endpoint a un software anti-malware "gratuito" può essere un invito al disastro sotto forma di infezione da malware e violazione dei dati.

La protezione avanzata degli endpoint incorpora varie e sofisticate tecnologie come l'apprendimento automatico, il rilevamento pre-esecuzione, il sandboxing e altro ancora in una soluzione multi-dimensionale. Molti prodotti di protezione degli endpoint "di nuova generazione" presenti oggi sul mercato hanno la pretesa di essere la "prossima grande risorsa" nella lotta contro i malware, ma per essere etichettati come "di nuova generazione", questi prodotti tecnicamente devono solo - e spesso lo fanno - implementare un singolo aspetto della protezione degli endpoint, come l'apprendimento automatico. Quando valutate la protezione degli endpoint per la vostra azienda, cercate una soluzione che includa TUTTO quanto segue: apprendimento automatico, rilevamento pre-esecuzione, sandboxing e altre tecnologie all'avanguardia, oltre al tradizionale rilevamento delle minacce informatiche basato sulla firma e aggiornato in tempo reale con le informazioni sulle minacce basate sul cloud.

Per essere efficace, la protezione degli endpoint deve avere:

Un ingombro di installazione contenuto

Un software anti-malware che richiede un significativo spazio su disco, elevate risorse di memoria e un massiccio utilizzo del processore può causare problemi di prestazioni e finire per essere spesso aggirato (cioè, disabilitato) dagli utenti finali.

Solide funzionalità di aggiornamento

Il software anti-malware deve essere in grado di ottenere informazioni sulle minacce in tempo reale senza singoli punti di fallimento o colli di bottiglia (come un server di aggiornamento sulla vostra rete). Il cloud viene sempre più sfruttato per fornire aggiornamenti e informazioni sulle minacce agli endpoint.

Resilienza

Il software anti-malware deve essere efficace anche quando è disconnesso dalla rete e deve essere resistente al malware che mira specificamente all'anti-malware.

Stabilità del prodotto

I prodotti rilasciati dovrebbero avere una comprovata esperienza di sicurezza, stabilità e assenza di bug.

Gestione centrale

Oltre a distribuire la protezione degli endpoint, le aziende devono essere in grado di verificare che il software sia correttamente installato, che funzioni correttamente e che riceva aggiornamenti regolari. Dovete essere in grado di affrontare i problemi di protezione degli endpoint da remoto, e riuscire a dimostrare che la vostra protezione degli endpoint sta funzionando (per esempio, con la registrazione e l'auditing per verificare la conformità).

Proteggere la rete

Proteggere la rete aziendale è diventato molto più impegnativo negli ultimi anni con la proliferazione dei dispositivi mobili e l'aumento del cloud computing, ma non è meno importante per la sicurezza informaticai e la protezione dei dati. Alcuni esempi di tecnologie di protezione dei dati per la rete includono:

Firewall

I firewall di rete rimangono la pietra miliare della sicurezza della rete e sono forse l'investimento più importante che un'azienda può fare per la sicurezza della rete. I firewall di base forniscono funzionalità di packet filtering e l'ispezione statica del traffico di rete. Un firewall di nuova generazione (NGFW) fornisce funzionalità avanzate di sicurezza della rete, compresa la protezione anti-malware, il filtraggio dei contenuti, il rilevamento e la prevenzione delle intrusioni e la cosiddetta threat intelligence. Un web application firewall (WAF) è un tipo di firewall specificamente progettato per proteggere i siti web aziendali e le applicazioni rivolte a Internet.

Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS)

IDS e IPS rilevano il traffico di rete dannoso sulla base di firme e regole preconfigurate. Un IDS è un sistema passivo che avvisa solo il team IT di una possibile intrusione. Un IPS è un sistema attivo che può intraprendere azioni specifiche, come l'abbandono o il blocco del traffico dannoso.

Software as a Service (SaaS)

Le applicazioni SaaS sono diventate onnipresenti poiché gli utenti trovano e installano facilmente un software facile da usare per aiutarli a svolgere le loro funzioni aziendali quotidiane. Esempi di applicazioni SaaS popolari includono Box, Dropbox, Google Docs, OneDrive e altri. Le aziende devono identificare attivamente le applicazioni SaaS che vengono utilizzate sulla loro rete e sanzionare (ed educare) l'uso di specifiche applicazioni SaaS, o bloccarle esplicitamente.

Segmentazione VLAN

La segmentazione della rete locale virtuale (VLAN) segmenta logicamente una rete, per esempio, per dipartimenti (come la contabilità, le risorse umane e l'operatività) per impedire l'accesso non autorizzato a certi dati e per prevenire un traffico di rete eccessivo (per esempio, broadcast storm) che può causare il rallentamento delle prestazioni.

Rete privata virtuale (VPN)

Un apparecchio o un software VPN permette agli utenti remoti di connettersi alla rete aziendale su Internet utilizzando un tunnel criptato. Una VPN può anche essere utilizzata per collegare reti di partner e/o collaboratori esterni, come un fornitore, nella vostra catena di approvvigionamento o un cloud service provider.

Controllo dell'accesso alla rete (NAC)

NAC è una soluzione di gestione della sicurezza unificata che applica le politiche di sicurezza basate sull'autenticazione dell'utente o del sistema, permettendo l'accesso a certe parti della rete a seconda della conformità del sistema o dell'utente con le politiche di sicurezza (per esempio, le patch di sicurezza e le firme antivirus sono attuali, la connessione di rete è criptata utilizzando una VPN, e così via).

Gestione delle informazioni e degli eventi di sicurezza (SIEM)

Le soluzioni SIEM aggregano e analizzano le informazioni di log da numerose fonti di dati come firewall, IDS/IPS, WAF, server ed endpoint.

Gestione delle patch

Patchare le vulnerabilità di sicurezza conosciute su server ed endpoint è una funzione fondamentale per tutte le organizzazioni. Man mano che le dimensioni della vostra organizzazione crescono, installare manualmente le patch del software su centinaia di server ed endpoint che possono essere sparsi in più sedi remote diventa sempre più difficile. Le soluzioni di gestione delle patch aiutano le organizzazioni ad automatizzare e gestire molte funzioni di gestione delle patch.

Gestori di password

Semplice ma potente - implementare dei gestori di password in tutta l'azienda è molto utile.

Protezione del DNS (Domain Name System)

Il DNS è nuovamente tornato in voga come popolare vettore di attacco, in particolare per gli attacchi denial-of-service (DoS). Per questo motivo è fondamentale implementare miglioramenti della sicurezza del protocollo DNS - come le estensioni di sicurezza DNS (DNSSEC) così come una configurazione ottimale del server DNS (come la disabilitazione dei recursive lookup). Altre opzioni di sicurezza DNS includono l'installazione di apparecchi DNS dedicati (e protetti) o l'uso di un servizio di gestione DNS.

Filtraggio dei contenuti web

Il filtraggio dei contenuti impedisce agli utenti di visitare siti web non autorizzati e potenzialmente dannosi o maligni in base all'indirizzo del sito web (indirizzo IP o URL) o al contenuto effettivo.

Comprendere l'importanza dell'orchestrazione

Man mano che il vostro business cresce, la necessità di automazione e orchestrazione nei vostri processi IT diventa sempre più importante, soprattutto se avete un piccolo staff IT con risorse limitate. Installare e configurare manualmente gli endpoint - PC desktop, dispositivi mobili e server - è insostenibile in un'azienda in crescita, soprattutto in più sedi remote.

Oltre alle inefficienze associate al "mettere mano" ad ogni endpoint, i processi manuali introducono opportunità di errori come impostazioni inconsapevoli o mal configurate.

L'automazione e l'orchestrazione migliorano l'efficienza del vostro team IT, aumentano la produttività dei vostri utenti finali (riducendo i tempi di inattività) e riducono gli errori di configurazione potenzialmente costosi. Le piattaforme di gestione possono aiutare ad automatizzare i processi manuali e a stabilire politiche standard.

Per le PMI che non hanno le risorse per implementare una piattaforma di gestione on-premises, una soluzione basata sul cloud o un fornitore MSP possono fornire i servizi di automazione e orchestrazione necessari per supportare la rapida crescita e un ambiente IT sempre più complesso.

ESET DELIVERS PROTEZIONE PER ENDPOINT ON-PREMISES, REMOTI E MOBILI

Mercury Engineering è la più grande società di ingegneria d'Irlanda, con circa 4.000 dipendenti, compresa una grande forza lavoro mobile che spesso lavora in remoto in oltre 30 paesi e in ambienti operativi vari e complessi. Molti impiegati si collegano a reti non sicure come il Wi-Fi pubblico e le reti cellulari.

Sfide

Il principale obiettivo IT di Mercury è garantire la sicurezza dei dati in questi ambienti potenzialmente pericolosi. Le informazioni commerciali dell'azienda sono essenziali per la sua crescita - i dati delle gare e delle stime sono fondamentali per acquisire e mantenere i clienti. La sicurezza di queste informazioni è vitale per l'azienda. Anche la salute delle singole macchine è estremamente importante per Mercury. La maggior parte dello staff lavora a scadenze molto strette e utilizzano PC con configurazioni software/hardware personalizzate che non possono essere sostituite rapidamente se compromesse.

I precedenti prodotti anti-malware di Mercury non sono riusciti a fermare diverse infezioni di malware e gravi epidemie di virus. Il personale era spesso bloccato fuori dai propri computer e l'helpdesk di Mercury spendeva molto tempo per trattare diverse infezioni da malware, spesso ricorrendo a vari prodotti freeware anti-malware che non avevano la gestione, la scalabilità e le capacità di reporting di una soluzione di livello aziendale. Il backend era molto complesso, difficile da gestire, pesante per la manutenzione e costoso - erano necessari servizi professionali quando erano necessarie modifiche o aggiornamenti. La soluzione di monitoraggio e gestione era molto limitata nelle sue funzionalità, specialmente sugli endpoint remoti fuori dalla rete. C'era una mancanza di consapevolezza in tempo reale di ciò che stava accadendo sugli endpoint di Mercury - scoprire un'epidemia alla fine della giornata era spesso troppo tardi per prevenire l'ulteriore diffusione del danno. I loro vecchi prodotti anti-malware hanno fatto gli straordinari per compensare le carenze del software.

Soluzione

Quando Mercury è passato a ESET, il processo è stato veloce. È stato "dispiegato in poche ore piuttosto che in giorni". Anche l'implementazione è stata semplice: la nuova rete è stata implementata interamente da un amministratore di siste-

ma Mercury (con un po' di supporto tecnico da ESET Ireland). L'intera rete ESET è ora amministrata da una piccola macchina con un solo processore e 4 gigabyte (GB) di memoria che supporta la gestione di oltre 1.000 computer e 200 server in vari paesi, oltre alle reti pubbliche di tutto il mondo. Assicura anche che la sicurezza di Mercury sia conforme agli standard e ai mandati internazionali, come ISO 27001.

"Per l'utente finale, non c'è impatto, non sanno che cosa sta accadendo - agisce silenziosamente ed efficientemente in background. Le attività quotidiane proseguono come al solito e noi continuiamo ad essere protetti senza che l'utente finale ne sia condizionato in alcuna forma. La migliore testimonianza? Le statistiche del nostro helpdesk: da quando ci siamo affidati a ESET, i nostri ragazzi del supporto non registrano alcuna chiamata, non devono occuparsi di problemi relativi all'antivirus o ai malware!" ha dichiarato il responsabile dell'infrastruttura IT di Maercury.

Risultati

- Oltre quattro anni completamente liberi da malware e virus
- Profilo discreto e ingombro ridotto per questa soluzione ESET
- Monitoraggio in tempo reale per la mitigazione e il trattamento immediato delle minacce
- Gestisce gli endpoint remoti e mobili al di fuori della rete aziendale
- Aiuta a proteggere le informazioni riservate come le offerte e i dati di stima

Molte PMI utilizzano ESET Security Management Center (ESMC) ed ESET Cloud Administrator (ECA) per gestire in modo semplice e sicuro le loro risorse remote e cloud, rispettivamente, senza richiedere costose e complesse implementazioni hardware in loco.

ESET SECURITY MANAGEMENT CENTER

ESET CLOUD ADMINISTRATOR

In questo capitolo

- Integrare i controlli tecnici con i controlli organizzativi
- Riconoscere la necessità di controlli di processo

Capitolo 5

PANORAMICA DEI CONTROLLI ORGANIZZATIVI E DI GESTIONE FONDAMENTALI

In questo capitolo imparerai come i controlli organizzativi e di gestione si integrano ai controlli tecnici per aiutare la vostra azienda a proteggere i propri dati.

Stabilire i controlli organizzativi

Una protezione efficace dei dati richiede più che mere soluzioni tecniche. È necessario stabilire controlli amministrativi e organizzativi per garantire che i controlli tecnici siano adeguatamente distribuiti, configurati e gestiti a sostegno di una strategia coesiva di gestione della sicurezza. Alcuni esempi di controlli organizzativi includono:

Dati personali privati e sensibili

I controlli tecnici, come la crittografia e il software per la prevenzione della perdita di dati (DLP), devono essere usati con discrezione a causa dei loro costi (sia finanziari che di performance). La crittografia richiede un'elaborazione aggiuntiva per crittografare e decrittografare i dati, e le soluzioni DLP devono eseguire la scansione di parole chiave e modelli per identificare i dati privati o sensibili come i numeri delle carte di credito, le informazioni sanitarie e i numeri di previdenza sociale. Stabilire uno schema di classificazione dei dati può aiutare i vostri utenti a capire quali di questi devono essere protetti, perché e come.

Documentazione e controllo dei dati

Le aziende che raccolgono, elaborano e/o conservano dati sensibili devono documentare perché raccolgono quei dati, come vengono raccolti (quali sono le fonti), come vengono usati e come vengono protetti. Documentare le proprie politiche di sicurezza e privacy dei dati può aiutarvi ad affrontare queste domande e a soddisfare i requisiti di audit, in particolare per quanto riguarda i regolamenti come l'Health Insurance Portability and Accountability Act (HIPAA) statunitense e il General Data Protection Regulation (GDPR) dell'UE.

Politiche di sicurezza

Le politiche non hanno bisogno di essere dei tomi infiniti. In molti casi, pochi paragrafi possono essere tutto ciò che serve. Le politiche di sicurezza dovrebbero definire chiaramente i ruoli e le responsabilità individuali in relazione alla protezione dei dati personali. Esempi di importanti politiche di sicurezza che ogni azienda dovrebbe creare includono:

- Politica per un utilizzo accettabile di Internet e della posta elettronica
- Politica per l''utilizzo del proprio dispositivo privato
- Politica per l'accesso remoto
- Politica sui software autorizzati

Risorse umane

Questo prevede politiche e procedure per garantire che i dati personali (come le domande di assunzione, i dati del libro paga, la formazione e i registri disciplinari) che vengono raccolti, mantenuti e trattati dalle risorse umane siano adeguatamente protetti. Questo include anche processi come lo screening pre-assunzione, i test antidroga e le rotazioni di lavoro.

Utilizzare un security maturity model (modello per la valutazione della maturità in materia di sicurezza)

Un modello di maturità della sicurezza può aiutarvi a determinare le vostre capacità di sicurezza in aree specifiche e a identificare eventuali lacune tra dove siete e dove dovreste essere. Dove dovreste essere, ovviamente, dipenderà da una serie di fattori come:

- Cosa state proteggendo - come dati sensibili, informazioni finanziarie, proprietà intellettuale, attrezzature mediche o infrastrutture critiche.
- Il proprio settore di competenza - come quello medico, finanziario, della vendita al dettaglio, degli appalti della difesa o dei servizi pubblici.

- I vostri requisiti di conformità normativa - per esempio, siete soggetti all'Health Insurance Portability and Accountability Act (HIPAA) degli Stati Uniti, al General Data Protection Regulation (GDPR) dell'UE, al Personal Information Protection and Electronic Documents Act (PIPEDA) del Canada, al Payment Card Industry Data Security Standards (PCI DSS), o altri?
- Il proprio threat profile (profilo delle minacce) - siete geograficamente situati in una regione ostile o instabile, in una città ad alta criminalità o in una zona pericolosa o industriale?

Formazione e test dei dipendenti

La formazione sulla consapevolezza della sicurezza per tutti i vostri dipendenti è necessaria per garantire che questi non siano l'anello più debole inmateria di protezione dei dati nella vostra organizzazione. È necessario coprire argomenti come la sicurezza delle password, lo spam e il phishing, la protezione da malware, i requisiti di conformità e la protezione dei dati (come la classificazione dei dati, i tipi di dati sensibili e le tecnologie per la protezione dei dati). I test possono assumere molte forme per assicurare che la formazione sia coinvolgente e rinforzata durante l'anno.

Esecuzione dell'analisi d'impatto sulla protezione dei dati (DPIA)

La DPIA è richiesta dal GDPR per tutte le operazioni di trattamento dei dati che "possono comportare un rischio elevato per i diritti e le libertà delle persone" Una DPIA è simile al processo di gestione del rischio di base (discusso nel Capitolo 2), ma definisce ulteriormente i parametri aggiuntivi che sono legati al trattamento dei dati personali.

Implementare la protezione dei dati per progettazione e per impostazione predefinita

Il GDPR richiede "la protezione dei dati per progettazione e per impostazione predefinita", il che significa che le organizzazioni dovrebbero implementare misure tecniche e organizzative per ridurre al minimo i dati personali che vengono raccolti, elaborati e memorizzati da un'organizzazione.

PROTEZIONE DEI DATI PUNTO PER PUNTO

Il seguente approccio sistematico alla sicurezza informatica può aiutarvi a proteggere i dati preziosi della vostra azienda. Una guida step by step.

VALUTATE i vostri beni, rischi e risorse

Fare un elenco di tutti i sistemi e servizi informatici che utilizza la vostra azienda. Dopo tutto, se non sai cosa hai, non puoi proteggerlo. Assicuratevi di includere i dispositivi mobili come smartphone e tablet che possono essere utilizzati per accedere alle informazioni aziendali o dei clienti. Questo è particolarmente importante perché, secondo il Ponemon Institute, si stima che il 60 per cento dei dipendenti elude le funzioni di sicurezza sui loro dispositivi mobili, e il 48 per cento dei dipendenti disattiva le impostazioni di sicurezza richieste dal datore di lavoro. E non dimenticare i servizi cloud, come Box, Dropbox, iCloud, Google Docs, Office365, OneDrive e SalesForce.

In seguito, rileggete la vostra lista e considerate i rischi associati ad ogni elemento e se avete ancora bisogno o meno di un determinato sistema, software o servizio. Chi o cosa rappresenta una minaccia? Un'altra buona domanda da fare è: "Cosa potrebbe mai andare storto?" Alcuni rischi sono più probabili di altri, ma è bene elencarli tutti e poi classificarli in base a quanto danno potrebbero causare e alla probabilità che si verifichino.

Potreste aver bisogno di un aiuto esterno in questo processo, ed è per questo che avete bisogno di un'altra lista: le risorse da sfruttare sfruttare per i problemi di cybersecurity. Questo potrebbe essere qualcuno dello staff che sia esperto e che conosca la sicurezza, oppure un partner o un fornitore. Anche le rappresentanze commerciali nazionali e le associazioni locali hanno risorse e possono fornire consigli utili. La National Cyber Security Alliance fornisce materiali educativi gratuiti, consigli e suggerimenti per la formazione dei dipendenti. Inoltre, raccogliete informazioni sulle forze dell'ordine locali (dovreste almeno avere a disposizione nomi e numeri di contatto da chiamare nel caso cadiate vittime di un crimine informatico).

CREARSI le proprie politiche

Un buon programma di sicurezza inizia con politiche di sicurezza che hanno l'approvazione dei dirigenti. Se siete voi i responsabili, dovere far sapere a tutti che

prendete sul serio la sicurezza e che la vostra azienda si impegna a proteggere la privacy e la sicurezza di tutti i dati che gestisce. Successivamente, è necessario specificare le politiche che si desidera applicare, ad esempio, non ci deve essere alcun accesso non autorizzato ai sistemi e ai dati aziendali, e i dipendenti non saranno autorizzati a disattivare le impostazioni di sicurezza sui loro dispositivi mobili.

DEFINIRE i controlli

Ricorrete ai controlli per far applicare le politiche. Per esempio, per far rispettare la politica di nessun accesso non autorizzato ai sistemi e ai dati aziendali, si può scegliere di controllare tutti gli accessi ai sistemi aziendali con un unico nome utente, password e token.

Per controllare quali programmi possono essere eseguiti sui computer aziendali, si può decidere di non dare ai dipendenti diritti amministrativi. Per prevenire le violazioni causate da dispositivi mobili persi o rubati, si potrebbe richiedere ai dipendenti di segnalare tali incidenti il giorno stesso e specificare che tali dispositivi saranno bloccati e cancellati in remoto immediatamente.

Come minimo, avete bisogno di tre tecnologie di sicurezza di base:

- **Software anti-malware** che impedisce al codice maligno (come virus e ransomware) di essere scaricato sui vostri dispositivi.
- **Crittografia** che rende inaccessibili i dati sui dispositivi persi o rubati.
- **Autenticazione a più fattori** in modo che più di un nome utente e una password (come un codice di accesso unico inviato a un telefono cellulare registrato) sia richiesto per accedere ai vostri sistemi e dati.

IMPLEMENTARE i controlli

Quando implementate i controlli, assicuratevi che funzionino. Per esempio, si può avere una politica che proibisce l'utilizzo di un software non autorizzato sui sistemi aziendali; uno dei controlli sarà un software anti-malware che ricerca eventuali codici dannosi. È necessario installarlo e testare che non interferisca con le normali operazioni aziendali, e documentare le procedure da seguire quando viene rilevato un malware.

EDUCARE dipendenti, partner e fornitori

I vostri dipendenti hanno bisogno di andare oltre alle sole conoscenze delle politiche e le procedure di sicurezza dell'azienda. Devono anche capire perché sono necessarie Questo significa investire nella consapevolezza e nell'educazione alla sicurezza, che spesso rappresenta l'azione più efficace che si possa implementare.

Lavorando con lo staff, è possibile aumentare la consapevolezza su varie problematiche, i come le email di phishing. Un recente Data Breach Investigations Report (DBIR) di Verizon ha mostrato che il 23 per cento delle e-mail di phishing inviate ai dipendenti sono state aperte e l'11 per cento dei destinatari ha aperto un allegato, entrambi i quali aumentano notevolmente le possibilità di violazione dei dati e furto di informazioni.

Educare tutti coloro che usano i vostri sistemi, compresi i dirigenti, i fornitori e i partner. E fate presente che violazioni delle politiche di sicurezza avranno delle conseguenze. La mancata applicazione delle politiche mina l'intero sforzo volto alla sicurezza.

Valutare, controllare e testare ulteriormente

La sicurezza informatica per qualsiasi azienda, grande o piccola, è un processo continuo, non un progetto una tantum. Pianificate di rivalutare la vostra sicurezza su base periodica, almeno una volta all'anno. Rimanete aggiornati sulle minacce emergenti esaminando regolarmente le notizie sulla sicurezza tramite siti web come WeLiveSecurity.com, KrebsOnSecurity.com e DarkReading.com.

Potrebbe essere necessario aggiornare le politiche e i controlli di sicurezza più di una volta all'anno, a seconda dei cambiamenti nell'azienda, come collaborazioni con nuovi fornitori, nuovi progetti, nuove assunzioni o dipendenti che se ne vanno (compreso assicurarsi che tutti gli accessi al sistema siano revocati quando qualcuno lascia l'azienda). Considerate l'assunzione di un consulente esterno per eseguire un test di penetrazione e un audit di sicurezza per individuare i punti deboli e per poi affrontarli.

Uno sguardo ai Controlli di Processo

I controlli di processo aiutano le aziende a minimizzare l'impatto di una violazione o perdita di dati. Per esempio, un recente studio del Ponemon Institute ha scoperto che le aziende possono ridurre il costo medio per record di una violazione dei dati da una media che va dai 122$ ai 141$ dollari se viene implementato un efficace processo di risposta agli incidenticosì da ridurre il tempo necessario per identificare e contenere una violazione dei dati. Il team incaricato alla gestione degli incidenti può essere in-house, un partner esterno di terze parti, o una combinazione di entrambi. Per una violazione di soli 10.000 record, potrebbe significare un risparmio medio di circa 190.000 dollari - un investimento che vale la pena.

Nello stabilire i controlli dei processi, le aziende devono:

Coinvolgere il personale

Questa non dovrebbe essere un'attività gestita dall'alto verso il basso. Coinvolgere le persone che effettivamente lavorano con i vari processi e la tecnologia aiuterà a garantire che i controlli abbiano senso e possano essere implementati efficacemente.

Definire le responsabilità

Le responsabilità individuali devono essere chiaramente definite e comprese: ognuno deve conoscere il proprio ruolo.

Spiegare perché sono necessari i controlli di processo

Le misure di sicurezza sono spesso viste come un peso o un ostacolo. Alla fine rischiano di essere ignorate o aggirate se gli impiegati non capiscono perché i controlli sono necessari e perché sono importanti per il business.

Secondo il Ponemon Institute, il tempo medio necessario per identificare una violazione di dati è di 191 giorni, e il tempo medio per contenerla è di 66 giorni. La quantità di tempo necessaria per identificare e contenere una violazione dei dati ha un impatto diretto sulla dimensione della violazione e sul suo costo totale.

Le aziende che creano processi per il trasferimento sicuro dei dati possono anche ridurre il costo di una violazione o perdita di dati. Per esempio, la crittografia riduce il costo medio per record di 16 dollari, secondo il Ponemon Institute. In molti casi, criptare i dati (ed essere in grado di dimostrare che sono crittografati correttamente) può far scattare le disposizioni "safe harbor" per molti regolamenti sulla privacy, Facendo questo, le aziende possono evitare notifiche di violazione, il che riduce significativamente il costo - sia in termini di costi diretti (come le notifiche, i servizi di monitoraggio del credito e le controversie) che di costi indiretti (come danni al marchio e perdita di clienti). Nel caso di una violazione di 10.000 record, la crittografia può ridurre il costo totale della violazione di circa 160.000 dollari.

Importanti controlli di processo includono:

Politiche di controllo dell'accesso

Definisce chi ha accesso a quali sistemi, applicazioni e dati e per quali scopi.

Gestione delle risorse/attività

È importante sapere cosa state proteggendo e perché (il suo valore o rischio per l'organizzazione). Oltre a mantenere un inventario accurato delle risorse informatiche e dei dati, le organizzazioni devono garantire un'adeguata igiene di sicurezza, mantenendo i sistemi e le applicazioni aggiornati con le ultime patch di sicurezza e cancellando o distruggendo prontamente i dati sensibili che non sono più necessari, in conformità con le politiche di conservazione, archiviazione e distruzione dei dati stabilite.

Gestione del cambiamento

Assicura che le modifiche ai sistemi e alle applicazioni siano documentate, testate e approvate, in modo che l'impatto di una modifica si integri alla struttura di sicurezza complessiva dell'organizzazione.

Risposta agli incidenti

Quando si verifica un incidente di sicurezza (come una violazione dei dati o un attacco), le aziende devono avere un piano di azione chiaramente definito e ben compreso. Questo aiuta a garantire una risposta rapida ed efficace, compreso il contenimento dei danni, il recupero, la conservazione delle prove, le comunicazioni interne ed esterne e l'analisi delle cause principali.

Continuità del business

Un piano di continuità aziendale riduce al minimo l'impatto aziendale di un'interruzione o di un attacco, aiutando le aziende a proseguire le attività fino a quando le operazioni di routine saranno completamente ripristinate.

Infine, le aziende possono sfruttare i servizi di sicurezza professionali per integrare le capacità interne. Questo include il monitoraggio quotidiano e l'intelligence delle minacce, così come il rilevamento, l'escalation e la risposta agli incidenti. Questo è particolarmente importante nelle attività forensi e investigative, nei servizi di valutazione e audit, nelle comunicazioni e nella gestione dei team addetti al contenimento della crisi.

I controlli organizzativi e di processo che vengono implementati dovrebbero essere appropriati al livello di rischio.

In questo capitolo

- Iniziare con i controlli amministrativi
- Sapere cosa state proteggendo e come farlo
- Implementare i controlli tecnici
- Garantire il backup e il ripristino, la risposta agli incidenti e il disaster recovery
- Collaborare con i propri utenti e altri esperti di sicurezza

Capitolo 6

DIECI PUNTI CHIAVE PER UN'EFFICACE PROTEZIONE DEI DATI

In questo capitolo, proponiamo dieci buone pratiche di sicurezza per aiutarvi a garantire un'efficace protezione dei dati per la vostra azienda.

1. Creare politiche di sicurezza

Molte aziende ignorano l'importanza delle politiche di sicurezza scritte e passano direttamente ai controlli tecnici. I controlli tecnici (come i firewall, la protezione degli endpoint e così via) applicati senza i controlli amministrativi (cioè le politiche e le procedure) sono quasi sempre implementati in modo reattivo senza una strategia di sicurezza ponderata, coesa e completa, e un quadro di gestione della sicurezza (che le politiche, insieme all'analisi della sicurezza delle informazioni, aiutano a definire). Questo significa inevitabilmente che si spenderà troppo per soluzioni tecniche che non sono efficacemente (o correttamente) implementate e che forniscono una protezione incompleta o inadeguata.

2. Identificare i propri asset

Dovete sapere cosa state proteggendo, quindi è importante mantenere un inventario accurato di tutto l'apparato hardware e software IT. Senza un inventario completo, potreste non essere consapevole dei sistemi vulnerabili nella rete che potrebbero aumentare l'esposizione agli attacchi. Per esempio, nella violazione dei dati di Target del 2013, gli aggressori sono entrati da remoto in un sistema di manutenzione di riscaldamento, ventilazione e aria condizionata (HVAC) per violare infine le carte di credito/debito e/o le informazioni personali di 110 milioni di clienti. Per iniziare ci sono molti strumenti disponibili gratuita-

mente da usare per scansionare la propria rete e gli endpoint. Le soluzioni commerciali possono aiutarvi a mantenere accuratamente l'inventario delle vostre risorse su base continua, e molte forniscono anche capacità di gestione remota per aiutarvi a installare, rimuovere e aggiornare il software. È necessario ridurre la superficie di attacco per tutte le vostre risorse collegate a Internet (compresi i dispositivi mobili personali), installando e mantenendo una protezione di sicurezza adeguata.

3. Conoscere il proprio livello di sicurezza

Questo è semplice come creare una roadmap o un modello di maturità per mostrare dove siete oggi (il vostro stato attuale) e usare un approccio basato sul rischio per identificare le minacce rilevanti contro le risorse nel vostro ambiente (vedere il suggerimento precedente) e le misure appropriate di cybersecurity e protezione dei dati. Potete quindi eseguire un'analisi delle lacune e determinare i passi da fare e dove investire le vostre risorse. Fate riferimento al capitolo 3 per saperne di più sulla valutazione dei rischi per la sicurezza dei dati.

4. Classificare tutti i dati

Per molte aziende, i dati sensibili dei clienti e altre informazioni proprietarie rappresentano i "gioielli della corona" del business, ma fornire protezione e controlli uguali per tutti i dati durante il loro ciclo di vita non è né pratico né auspicabile. Pensate invece a quali dati vi terrebbero svegli di notte se venissero persi o rubati. Che impatto avrebbe una violazione dei dati sull'immagine del marchio, sulla fedeltà dei clienti o anche sulla redditività continua del business? Create (e documentate) una politica di classificazione dei dati intuitiva per la vostra organizzazione che includa etichette di classificazione (come "Solo per uso interno", "Dati sensibili" e "Approvato per il rilascio pubblico") e che specifichi i requisiti di protezione dei dati (come crittografia, backup, approvazione del rilascio e distruzione) per diversi livelli di informazioni.

Il regolamento generale sulla protezione dei dati (GDPR) richiede alle organizzazioni di cancellare i dati personali se richiesto da un soggetto (come un individuo). Per aiutarvi a rispettare i requisiti del GDPR, progettate la vostra strategia di classificazione dei dati per aiutarvi a identificare o segnalare i dati personali (compresi i backup) che potrebbero dover essere cancellati o altrimenti modificati in futuro.

5. Crittografia dei dati sensibili

La crittografia dei dati converte i dati in chiaro in una forma illeggibile (nota come "testo cifrato"), rendendoli inutili alle parti non autorizzate che non possiedono le chiavi di cifratura/decifratura. Quindi, la base per una crittografia efficace è proteggere adeguatamente le chiavi. Come minimo, dovreste criptare i dati "a riposo" (in memoria). È possibile utilizzare una crittografia aggiuntiva sui dati "in movimento" (o "in transito"), per esempio, utilizzando la crittografia Secure Sockets Layer (SSL). Infine, per i dati "in uso", si dovrebbe approfittare della crittografia all'interno dell'applicazione, se disponibile. La crittografia può essere hardware o software.

Molti regolamenti sulla violazione dei dati includono disposizioni di approdo sicuro per i dati che sono criptati, che possono ridurre significativamente il costo e l'impatto di una violazione.

6. Backup e (test di) recupero dei dati preziosi

Garantire backup regolari e affidabili dei vostri sistemi e dati è una best practice di sicurezza di base, ma essenziale. Un buon backup assicura la possibilità di recuperare un file cancellato accidentalmente o un disco rigido danneggiato. Con i costi di backup basati su disco che continuano a scendere e le soluzioni di basate sul cloud che sono convenienti e facili da usare, non ci sono semplicemente scuse per non avere backup. Con il rapido aumento dei ransomware negli ultimi anni, i backup sono l'unico modo per avere la garanzia di riavere i propri dati se si è vittima di un attacco. Come bonus, non sarà necessario pagare il riscatto.

Dovete testare regolarmente la vostra capacità di recuperare i vostri sistemi e i dati critici dai backup, non solo per assicurarvi che i backup non siano corrotti, ma anche per verificare che voi e il vostro staff conosciate il processo di recupero.

7. Investire nella protezione degli endpoint

"Investire" non significa scaricare qualche software antivirus gratuito da internet, ma significa proteggere tutti gli endpoint - PC desktop, dispositivi mobili e server - con una solida soluzione commerciale. Oggi l'informazione è ovunque e ora più che mai l'endpoint è il luogo in cui tutto si riunisce. Quindi è sicuramente un'area in cui vale la pena investire.

8. Pianificare e preparare

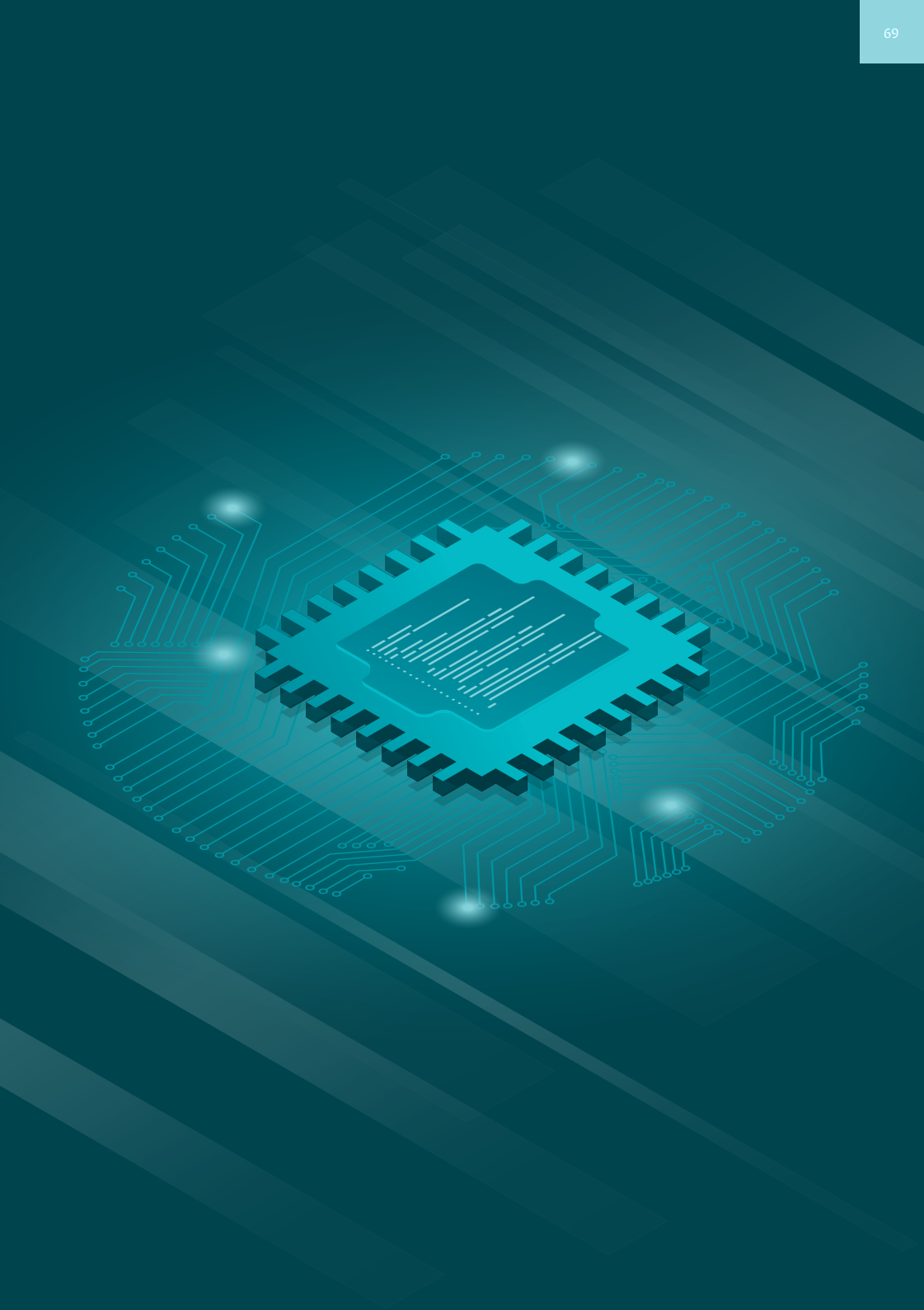
Ogni azienda deve avere un piano di risposta agli incidenti, piani di continuità aziendale e di disaster recovery. Il vostro team di risposta agli incidenti deve essere addestrato nelle procedure forensi di base per garantire che ogni incidente di sicurezza sia trattato come un potenziale caso legale e assicurare che la catena di custodia sia mantenuta per qualsiasi prova potenziale. I piani di continuità aziendale e di disaster recovery aiutano la vostra azienda a riprendere le normali operazioni commerciali il più rapidamente possibile dopo un evento importante o grave. Comunicazioni accurate e tempestive, sia interne che esterne, sono una componente fondamentale di qualsiasi piano di continuità aziendale e di disaster recovery.

9. Formare gli utenti

L'anello più debole della sicurezza di qualsiasi organizzazione è sempre stato l'utente finale, ma non è necessariamente colpa loro. È improbabile che tutti quelli che lavorano per la vostra azienda siano stati assunti perché esperti di sicurezza. Gli aggressori lo sanno e usano varie tecniche di ingegneria sociale per attirare gli utenti ignari a cliccare su link dannosi nelle e-mail di spam o di phishing, a rivelare le loro password (vedi "Come si crea una password forte?" qui sotto) e a visitare siti web dannosi. Organizzate regolarmente incontri di formazione sulla consapevolezza della sicurezza, coinvolgenti, pertinenti e brevi, per aiutare i vostri utenti ad aiutare se stessi - e quindi ad aiutare voi!

10. Non fatelo da soli

I criminali informatici non lavorano da soli. Collaborano con altri personaggi dubbi per raggiungere i loro obiettivi di attacco, riutilizzare il codice maligno sul dark web e arruolare vittime ignare i cui endpoint violati sono diventati bot in un esercito di botnet che prendono di mira altre vittime. Ma anche i buoni non sono soli. Sfrutta l'ampia comunità di esperti di sicurezza, dalle forze dell'ordine locali alle associazioni professionali, ai servizi di sicurezza in outsourcing e gestiti, all'intelligence sulle minacce basata sul cloud in tempo reale e altro ancora.



COME CREARE UNA PASSWORD FORTE?

Quasi tutto quello che facciamo online richiede un login, e ogni login richiede un qualche tipo di autenticazione per verificare che siamo chi diciamo di essere. Come tale, la tua password dovrebbe essere unica (e complessa) come te! Ecco alcuni consigli:

Utilizzare password e passphrase lunghe

Le password dovrebbero essere lunghe almeno 8 caratteri, ma non così lunghe da non poterle ricordare (vedi il consiglio qui sotto). Controlla che la tua password non sia stata esposta a una violazione dei dati su https://haveibeenpwned.com/Passwords.

Utilizzare frasi uniche e caratteri speciali

Una breve frase composta da 30 o più caratteri (forse con alcuni numeri, maiuscole e punteggiatura) che puoi ricordare è molto meglio di una parola di 8 caratteri con sostituzioni comuni (come un '3' per la lettera 'e').

Utilizzare un programma di gestione delle password (gratuito o a pagamento)

Un gestore di password può essere utile per creare, memorizzare, gestire e ricordare password uniche e forti per i vari dispositivi, sistemi e accessi alle applicazioni. Può anche aiutare a eliminare la pratica comune di scrivere le password in documenti o post-it.

Usare password che si possono ricordare

Password troppo complesse, completamente casuali e difficili da ricordare possono in realtà essere controproducenti e rendere il tuo account meno sicuro, perché tendono a portare a cattive pratiche come scrivere le password e utilizzare le stesse password su diversi account personali e di lavoro.

Utilizzare l'autenticazione a più fattori (MFA)

Quando possibile, l'MFA dovrebbe essere abilitato sui tuoi account al posto delle password o in aggiunta ad esse. L'MFA incorpora due o più fattori di autenticazione ("qualcosa che conosci", come il tuo nome utente e/o password, e "qualcosa

che hai", come un token hardware o software, o uno smartphone). Quando accedi a un account MFA, un codice unico viene generato sul tuo token o inviato via SMS al tuo smartphone. Il codice può essere usato solo una volta e solo in un periodo di tempo limitato (in genere da uno a cinque minuti). Questo rende estremamente difficile per un aggressore intercettare il tuo codice e usarlo per accedere al tuo account a tua insaputa e prima che il codice scada.

NON usare la stessa password due volte, indipendentemente da quanto sia forte

Se la vostra password viene compromessa in un posto (ad esempio, il vostro account personale di posta elettronica Yahoo!), i criminali informatici cercheranno di utilizzare quelle stesse credenziali in altri posti (come il vostro conto bancario online).

NON condividere le propria password con nessuno - mai!

Trattate le vostre password come più sacre del vostro spazzolino da denti (che potreste occasionalmente condividere con la vostra dolce metà - o il vostro cane).

NON usare semplici parole comuni

Per i programmi di cracking automatico delle password è semplice individuarle con i dizionari - comprese le lingue straniere e i termini medici, legali o ingegneristici. Evitate anche caratteri ripetitivi (per esempio, 'aaaa'), caratteri sequenziali (per esempio, '1234'), e schemi riconoscibili (per esempio, 'qwerty').

NON utilizzare password che contengono informazioni personali

I social media rendono più facile che mai per i criminali informatici apprendere dettagli personali - come il secondo nome, la data di nascita, l'indirizzo, la scuola, il nome del coniuge o del figlio e quello che avete fatto la scorsa estate!

GLOSSARIO

adware
Programmi di pubblicità pop-up che vengono comunemente installati con freeware o shareware, e talvolta considerati una forma di malware. Vedi anche malware.

backdoor
Malware che permette a un criminale di bypassare la normale autenticazione per ottenere l'accesso a un sistema compromesso. Vedi anche malware.

bootkit
Una variante di malware in modalità kernel di un rootkit, comunemente usato per attaccare i computer che sono protetti da una crittografia completa del disco.
Vedi anche malware e rootkit.

bot
Un computer bersaglio che è infettato da malware e fa parte di una botnet. Vedi anche botnet e malware.

botnet
Un'ampia rete di bot infettati da malware che lavorano insieme e controllati da un aggressore attraverso server di comando e controllo (C2). Vedi anche bot e malware.

bring your own device (BYOD)
Una politica sui dispositivi mobili che permette ai dipendenti di utilizzare i loro dispositivi personali, come smartphone e tablet, sul posto di lavoro sia per uso lavorativo che personale.

Cavallo di Troia
Un programma malware che si propone di eseguire una data funzione, ma invece esegue un'altra (di solito malevola). Vedi anche malware.

ciphertext
Un messaggio in chiaro criptato incomprensibile senza la chiave di decrittazione appropriata. Vedi anche decrittazione, crittografia e testo in chiaro.

criptovaluta
Un bene digitale che usa la crittografia per proteggere le transazioni, controllare la creazione di unità aggiuntive e verificare il trasferimento di beni. Bitcoin è un esempio popolare di criptovaluta.

crittografia
Il processo di trasformazione del testo cifrato in testo in chiaro. Vedi anche ciphertext e plaintext.

decrittazione
Il processo di trasformazione del testo cifrato in testo in chiaro. Vedi anche ciphertext e plaintext.

directory harvest attack (DHA)
Una tecnica di forza bruta usata dagli spammer nel tentativo di trovare indirizzi e-mail validi in un dominio.

distributed denial-of-service (DDoS)
Un attacco su larga scala che tipicamente utilizza bot in una botnet per bloccare una rete o un server mirato. Vedi anche bot e botnet.

DNS cache poisoning
Un tipo di attacco, noto anche come DNS spoofing , che sfrutta le vulnerabilità del DNS per deviare il traffico internet dai legittimi server di destinazione a server fasulli. Vedi anche Domain Name System (DNS).

DNS hijacking
Una tecnica di attacco utilizzata per reindirizzare le query DNS lontano dai server DNS legittimi. Vedi anche Domain Name System (DNS).

Domain Name System (DNS)
Un database gerarchico decentralizzato per computer, servizi e altre risorse collegate a una rete o a internet che fornisce la mappatura degli indirizzi IP numerici ai nomi di dominio, così come altre informazioni. Vedi anche Protocollo Internet (IP).

drive-by download
Software, spesso malware, scaricato su un computer da internet senza che l'utente lo sappia o lo autorizzi. Vedi anche malware.

endpoint
Un dispositivo informatico dell'utente finale, come un computer desktop o portatile, un tablet o uno smartphone.

exploit
Software o codice che approfitta di una vulnerabilità in un sistema operativo (OS) o in un'applicazione, e provoca un comportamento non previsto nell'OS o nell'applicazione, come l'escalation dei privilegi, il controllo remoto o un denial-of-service.

firewall di nuova generazione (NGFW)
Una piattaforma di sicurezza di rete che integra completamente il firewall tradizionale e le capacità di prevenzione delle intrusioni di rete con altre funzioni di sicurezza avanzate che forniscono l'ispezione profonda dei pacchetti (DPI) per una visibilità completa, un'accurata identificazione di applicazioni, contenuti e utenti e un controllo granulare basato su criteri definiti. Vedi anche intrusion prevention system (IPS).

Health Insurance Portability and Accountability Act (HIPAA)
Applicabile a qualsiasi organizzazione che tratta o conserva informazioni sanitarie protette (PHI). Protegge la riservatezza del paziente e la privacy dei dati.

informazioni sanitarie protette (PHI)
Qualsiasi informazione sulla salute, sulla fornitura di assistenza sanitaria o sul pagamento dell'assistenza sanitaria di uno specifico individuo che viene creata o raccolta da un'organizzazione, come un fornitore di assistenza sanitaria, un assicuratore o un'altra entità simile.

Ingegneria sociale
Un metodo di attacco low-tech che impiega tecniche come il shoulder surfing e il dumpster diving per ottenere informazioni sensibili, come le password, da un utente.

internet protocol (IP)
Il principale protocollo di comunicazione nella suite di comunicazione TCP/IP per l'instradamento attraverso i confini della rete (router) e Internet. Vedi anche Transmission Control Protocol (TCP).

intrusion detection system (IDS)
Un'applicazione hardware o software che rileva sospette intrusioni nella rete o negli host.

intrusion prevention system (IPS)
Un'applicazione hardware o software che rileva sospette intrusioni nella rete o negli host.

logic bomb
Un programma malware, o parte di esso, progettato per eseguire qualche funzione dannosa quando si verifica una circostanza predeterminata. Vedi anche malware.

Malware
Software o codice maligno che tipicamente danneggia o disabilita, prende il controllo o ruba informazioni da un sistema informatico. Il malware include ampiamente virus, worm, cavalli di Troia, logic bomb, ransomware, rootkit, bootkit, backdoor, spyware e adware.

Metamorfismo
Una tecnica utilizzata per riscrivere il codice del malware ad ogni iterazione in modo che ogni nuova versione sia diversa da quella precedente. Vedi anche malware e polimorfismo.

Organizzazione internazionale per la normazione (ISO)
Un organismo internazionale per la definizione di standard. ISO deriva dalla parola greca 'isos', che significa uguale.

Payment Card Industry (PCI) Data Security Standards (DSS)
Applicabile a qualsiasi azienda che accetta, elabora o memorizza transazioni con carte di pagamento (come carte di credito, di debito e prepagate).

Personal Information Protection and Electronic Documents Act (PIPEDA)
Applicabile alle organizzazioni che fanno affari con cittadini canadesi. Protegge la privacy delle informazioni personali dei cittadini canadesi.

phishing
Una tecnica di ingegneria sociale in cui un'email che sembra provenire da un'azienda legittima (come un'istituzione finanziaria) cerca di ingannare il destinatario a cliccare su un link incorporato nell'email o ad aprire un allegato contenente malware o un exploit. Il link incorporato reindirizza il browser

del destinatario a un sito web dannoso che richiede di inserire informazioni personali sensibili (come le informazioni dell'account). In alternativa, il sito web maligno può fornire malware o un exploit all'endpoint della vittima in background attraverso il browser. Vedi anche drive-by download, endpoint, exploit e malware.

polimorfismo
Una tecnica utilizzata per riscrivere una porzione del codice del malware ad ogni iterazione in modo che ogni nuova versione sia legegrmente diversa da quella precedente. Vedi anche malware e metamorfismo.

port hopping
Una tecnica utilizzata dalle applicazioni per migliorare l'accessibilità, ma anche usata nei cyberattacchi per cambiare dinamicamente le porte TCP per eludere il rilevamento. Vedi anche Transmission Control Protocol (TCP).

ransomware
Software maligno che cripta i dati di una vittima e la induce a pagare un riscatto specificato (di solito in criptovaluta) per decriptare i dati (anche se il pagamento di un riscatto non garantisce che i dati della vittima vengano decriptati). Vedi anche criptovalute e malware.

Regolamento generale sulla protezione dei dati (GDPR)
Applicabile a qualsiasi organizzazione che fa affari con i cittadini dell'UE. Rafforza la protezione dei dati per i cittadini dell'UE e disciplina l'esportazione di dati personali al di fuori dell'UE.

remote access Trojan (RAT)
Un programma malware che include una backdoor per fornire il controllo amministrativo di un computer di destinazione.

rete locale virtuale (VLAN)
Un dominio di trasmissione che è partizionato e isolato in una rete locale.

rete privata virtuale (VPN)
Una rete privata utilizzata per comunicare privatamente su reti pubbliche. Le VPN utilizzano la crittografia e l'incapsulamento per proteggere e semplificare la connettività.

rootkit
Malware che fornisce un accesso privilegiato (livello root) a un computer. Vedi anche malware.

Secure Sockets Layer (SSL)
Un protocollo di livello di trasporto che fornisce una crittografia session-based per la comunicazione sicura tra client e server su Internet.

spam
E-mail massive non richieste che sono comunemente usate per diffondere malware attraverso link o allegati dannosi. Vedi anche malware.

spearphishing
Un tentativo di phishing mirato che sembra più credibile per le sue vittime e quindi ha una maggiore probabilità di successo. Per esempio, un'email di spearphishing può spacciarsi per un'organizzazione o un individuo che il destinatario conosce. Vedi anche phishing.

spyware
Malware che raccoglie informazioni su una persona o un'organizzazione senza che ne siano a conoscenza o che ne abbiano dato consenso. Vedi anche malware.

SSL hiding
Una tecnica che utilizza la crittografia SSL (Secure Sockets Layer) per nascondere il contenuto del traffico di rete, ad esempio, per eludere il rilevamento da parte delle difese di rete mentre si rubano dati sensibili (noto come data exfiltration).

testo in chiaro
Un messaggio nel suo formato leggibile originale o un messaggio cifrato che è stato decifrato correttamente per produrre il messaggio leggibile originale. Vedi anche ciphertext e decrittazione.

Transmission Control Protocol (TCP)
Uno dei protocolli centrali della suite del protocollo internet, il TCP è uno dei due componenti originali della suite, complementare al protocollo internet (IP), e quindi l'intera suite è comunemente chiamata TCP/IP. Il TCP fornisce una consegna affidabile e ordinata di un flusso di byte da un programma su un computer a un altro programma su un altro computer. TCP è il protocollo

su cui si basano le principali applicazioni internet come il World Wide Web, la posta elettronica, l'amministrazione remota e il trasferimento di file. Vedi anche Internet Protocol (IP).

unified threat management (UTM)
Un'appliance di sicurezza che integra varie funzionalità come firewall, anti-malware e prevenzione delle intrusioni in una singola piattaforma.

Uniform Resource Locator (URL)
Un indirizzo web.

virus
Un insieme di istruzioni del computer il cui scopo è quello di incorporarsi in un altro programma per replicarsi. Vedi anche malware.

vulnerabilità
Un bug o un difetto nel software che crea un rischio per la sicurezza che può essere sfruttato da un criminale. Vedi anche exploit.

web application firewall (WAF)
Un firewall progettato per proteggere le applicazioni basate su web e server web.

worm
Malware che solitamente ha la capacità di replicarsi da computer a computer senza bisogno di interazione umana. Vedi anche malware.

I VOSTRI DATI
SONO IL VOSTRO BUSINESS

ASSICURATEVI CHE LA VOSTRA AZIENDA SIA AL SICURO DA VIOLAZIONI O FUGHE DI DATI. AFFIDATEVI A ESET ENDPOINT ENCRYPTION, POTENTE E FACILE DA IMPLEMENTARE

- Dischi rigidi, supporti rimovibili, file ed e-mail crittografati in modo sicuro
- Maggiore sicurezza delle informazioni e conformità al GDPR
- Integrabile con ESET Secure Authentication per un ulteriore livello di sicurezza

VISITA IL SITO WEB DI ESET PER SCOPRIRE TUTTE LE NOSTRE SOLUZIONI.

eset CYBERSECURITY EXPERTS ON YOUR SIDE

WWW.ESET.COM

COME CREARE UNA PASSWORD FORTE?

COSA FARE

- Utilizzare password e passphrase lunghe
- Utilizzare frasi uniche e caratteri speciali
- Utilizzare un programma di gestione delle password (gratuito o a pagamento)
- Usare password che si possono ricordare
- Utilizzare l'autenticazione a più fattori (MFA)

COSA EVITARE

- NON usare la stessa password due volte, indipendentemente da quanto sia forte
- NON condividere le propria password con nessuno - mai!
- NON usare semplici parole comuni
- NON utilizzare password che contengono informazioni personali

ESET
CYBERSECURITY
EXPERTS ON YOUR SIDE