

La sicurezza informatica in azienda

Qual è l'impatto del cyber crime sui costi aziendali,
e come proteggere i propri dati

Contenuti

03 | Introduzione

05 | Sfatiamo i miti sulla sicurezza informatica

13 | L'impatto della criminalità informatica sulle aziende

24 | Il futuro della sicurezza informatica aziendale

28 | Glossario e approfondimenti

Introduzione

“Molti dirigenti affermano che saranno i rischi informatici a caratterizzare la nostra generazione.”

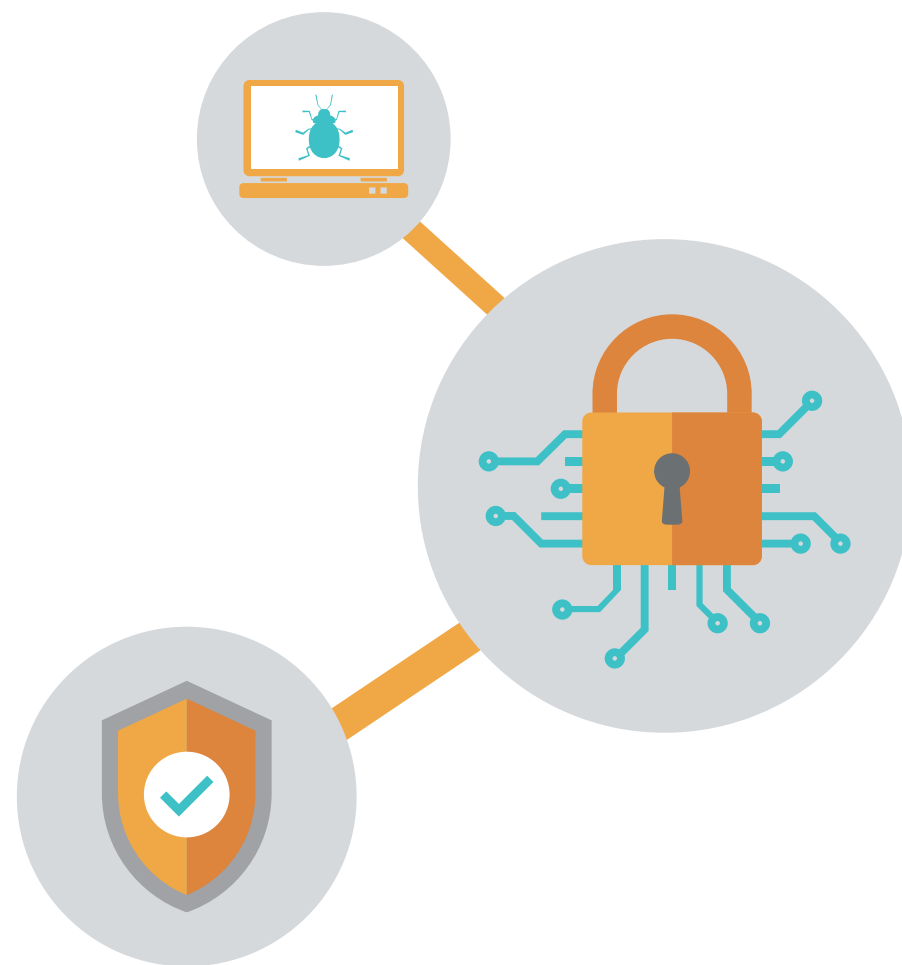
– Dennis Chesley, Global Risk Consulting Leading, PwC¹

La sicurezza informatica non è una sfida nuova. Tuttavia cresce di giorno in giorno. Gli hacker stanno affinando le loro tecniche e sono oggi in grado di violare una rete da più punti. L'Internet of Things sta moltiplicando il numero di dispositivi endpoint, che spesso sono il punto d'ingresso più vulnerabile per le violazioni dei sistemi. La quantità di bersagli aumenta così come aumentano i danni potenziali.

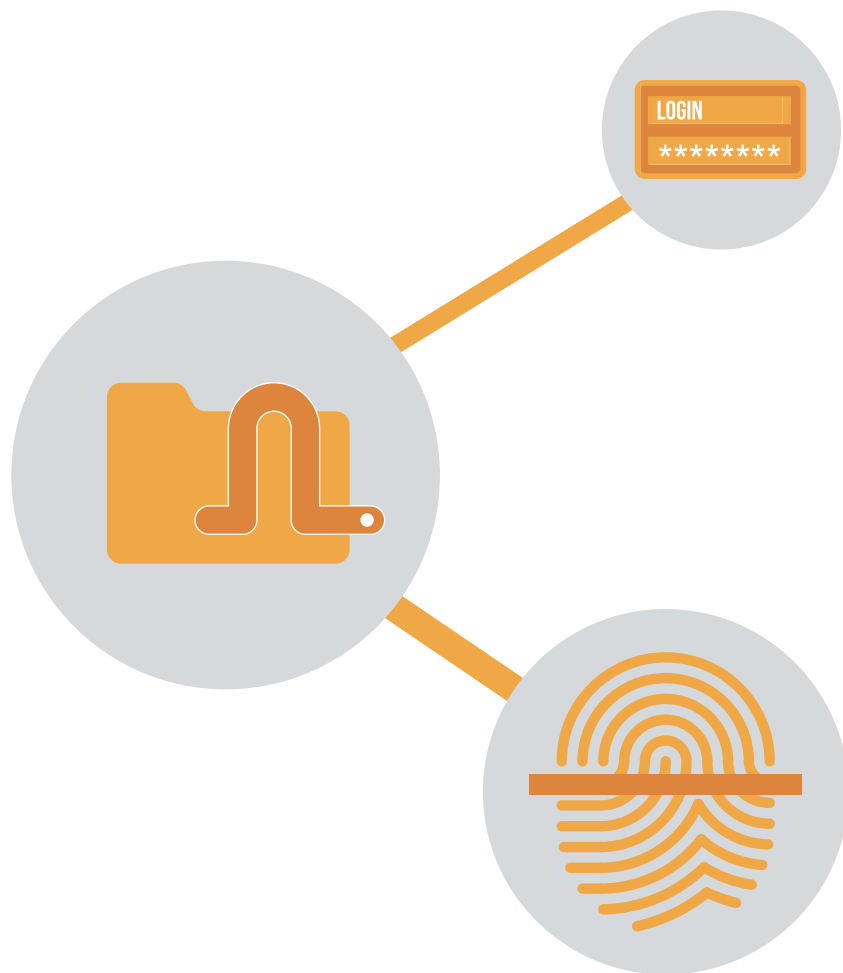
Il 21 ottobre 2016, Dyn, provider DNS con sede negli Stati Uniti, ha subito un attacco di tipo DDoS

(Distributed Denial of Service) tra i più estesi di sempre. Alcuni dei maggiori siti al mondo, tra cui Netflix, Amazon e Twitter, sono rimasti offline per ore.²

A gennaio 2017, i clienti della Lloyds Bank non sono riusciti a controllare gli account né ad effettuare pagamenti attraverso il portale della banca. Non era nemmeno possibile accedere alle applicazioni mobili. Nonostante Lloyds non abbia mai confermato nulla al riguardo, ci sono forti sospetti che si sia trattato di un attacco DDoS.³



Introduzione



Violazioni di questo livello sono più dannose di una cattiva pubblicità. E si traducono in costi concreti.

Nel sondaggio sulla sicurezza delle stampanti del 2016 di Spiceworks, il 34% delle aziende afferma che una violazione comporta un aumento delle chiamate all'help desk e dei tempi di assistenza, il 29% sostiene che le violazioni riducono produttività ed efficienza e il 26% riporta l'aumento dei tempi di inattività del sistema come un problema.⁴

Quasi il 60% dei leader in fatto di sicurezza, intervistati per un rapporto CSO Assessment di IBM, afferma che la complessità degli attacchi supera quella delle difese aziendali.⁵ Per oltre un decennio i CIO hanno collocato

la sicurezza informatica tra le prime 10 preoccupazioni aziendali, mentre ora, secondo lo studio annuale dei trend di SIM (Security Information Management), si trova in seconda posizione.⁶

Molti di questi danni si possono prevenire. A seguire, tratteremo i pregiudizi comuni sulla sicurezza informatica, esaminando più nel dettaglio l'impatto della criminalità informatica sulle imprese e le soluzioni per difendersi al meglio dagli attacchi. Infine, proiettandoci nel futuro, discuteremo di cosa ci attende e di come prepararsi.

Sfatiamo i miti sulla sicurezza informatica

Cinque pregiudizi comuni che possono esporre le aziende al rischio della criminalità informatica

Solamente alcune aziende note finiscono sui giornali per violazioni di dati, ma tutte possono considerarsi a rischio. Ecco i sei miti sulla sicurezza informatica che rendono le aziende vulnerabili agli attacchi degli hacker.



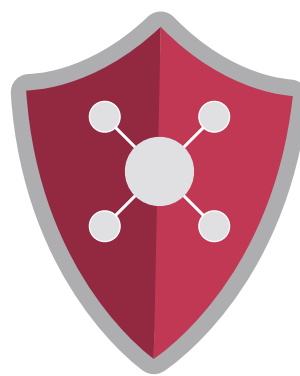
**Violazioni della
sicurezza**



**Fughe di
dati**



**Pratiche di
sicurezza**



**Software
antivirus**



**Attacco
informatico**

1 Le aziende si riprendono in fretta dopo qualsiasi violazione



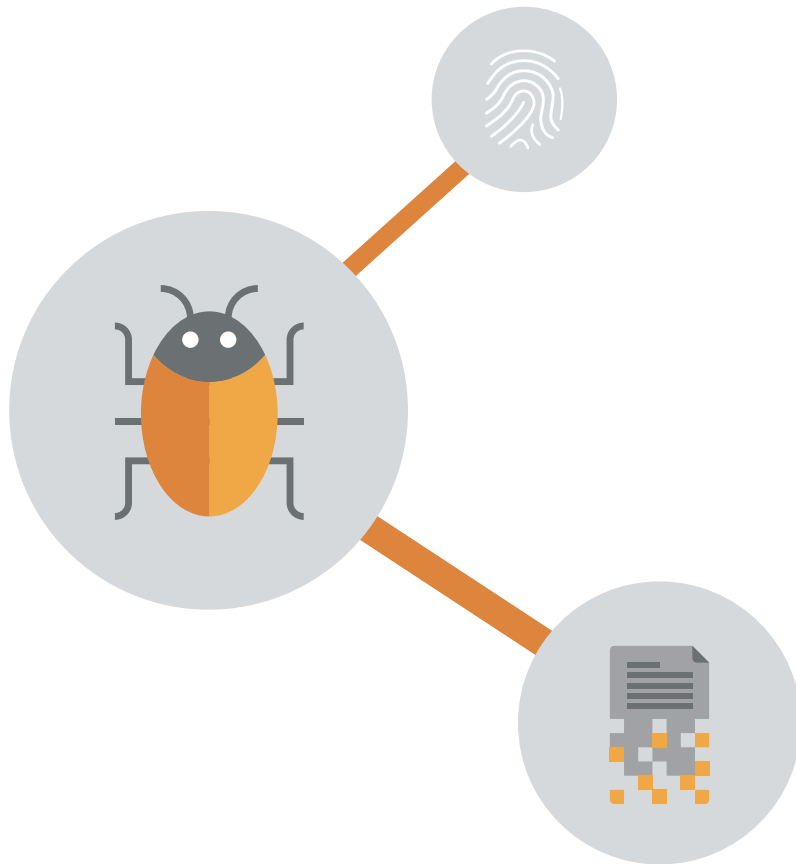
È ancora molto difficile stimare i costi legati alle violazioni della sicurezza informatica per una azienda. Si pensava comunemente che l'impatto di una violazione fosse riscontrabile nelle svalutazioni sul mercato azionario.

Ma le azioni quotate sono solo un piccolo aspetto della questione. Anche se le azioni potrebbero riprendersi in poche settimane, i costi a lungo termine sono ingenti: nuovi programmi di sicurezza, personale sostitutivo, spese legali, sono solo alcuni esempi di quali e quanti siano i fattori che possono compromettere notevolmente le attività di un'azienda, in seguito a una violazione.

Senza contare l'aumento dei costi. Uno studio recente di Ponemon ha rivelato che il costo medio annuo di una violazione quest'anno è passato, rispetto all'anno scorso, da **7,7 milioni** di dollari a **9,5 milioni**.⁷



2 Raramente si verificano criticità nei sistemi di sicurezza, quindi non è necessario tutelarsi



IDC ha riscontrato⁸ che la percentuale delle aziende vittima di violazioni è stata del 99% nel 2016. Mentre la percentuale delle aziende che dichiarano di aver subito da 6 a 10 violazioni in un anno è passata dal 9% nel 2014 al 18,9% nel 2016.⁹

Questi valori potrebbero essere più bassi di quelli reali. Spesso infatti viene dichiarata solo una parte delle violazioni subite, in quanto le aziende cercano di evitare la cattiva pubblicità che ne deriverebbe.

L'altro fattore che non viene considerato in questo mito è l'impatto debilitante di una potenziale fuga di informazioni. Se anche si trattasse di un caso isolato, un singolo episodio è sufficiente a causare danni ingenti.

3

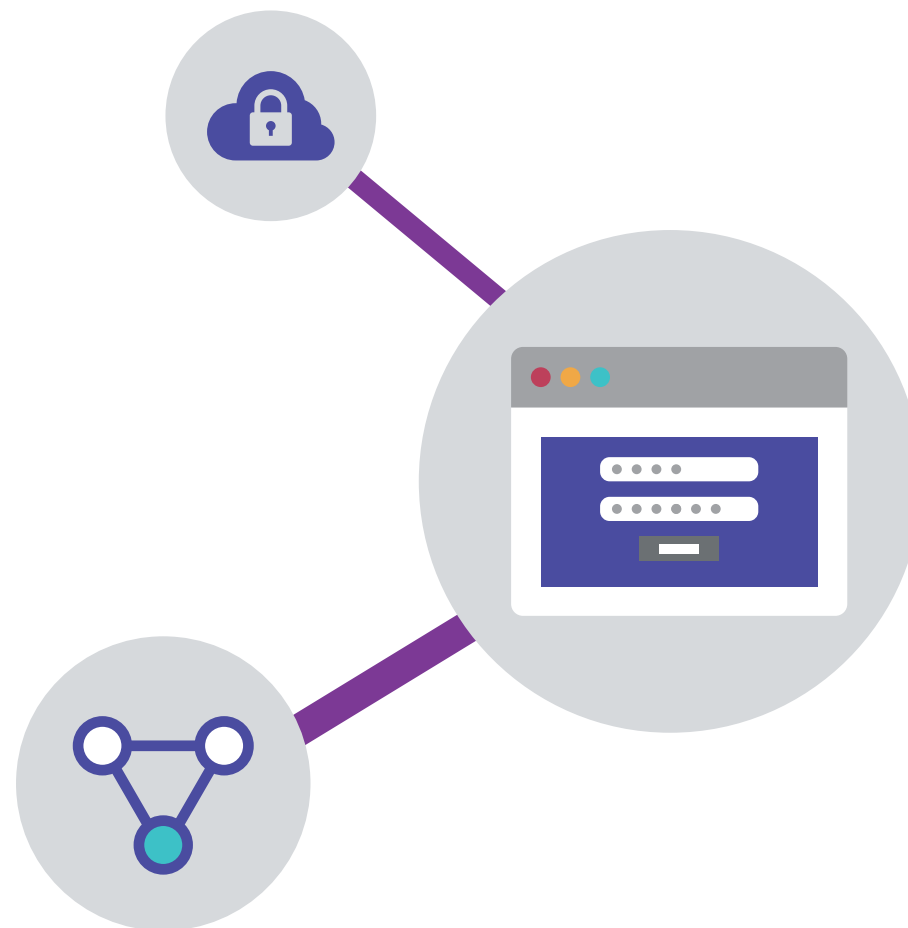
Abbiamo assunto un esperto informatico che si occuperà della sicurezza, quindi non ci serve sapere altro



Nonostante assumere un esperto informatico sia un'ottima idea, ogni dipendente in azienda dovrebbe partecipare a corsi di formazione in materia di sicurezza informatica.

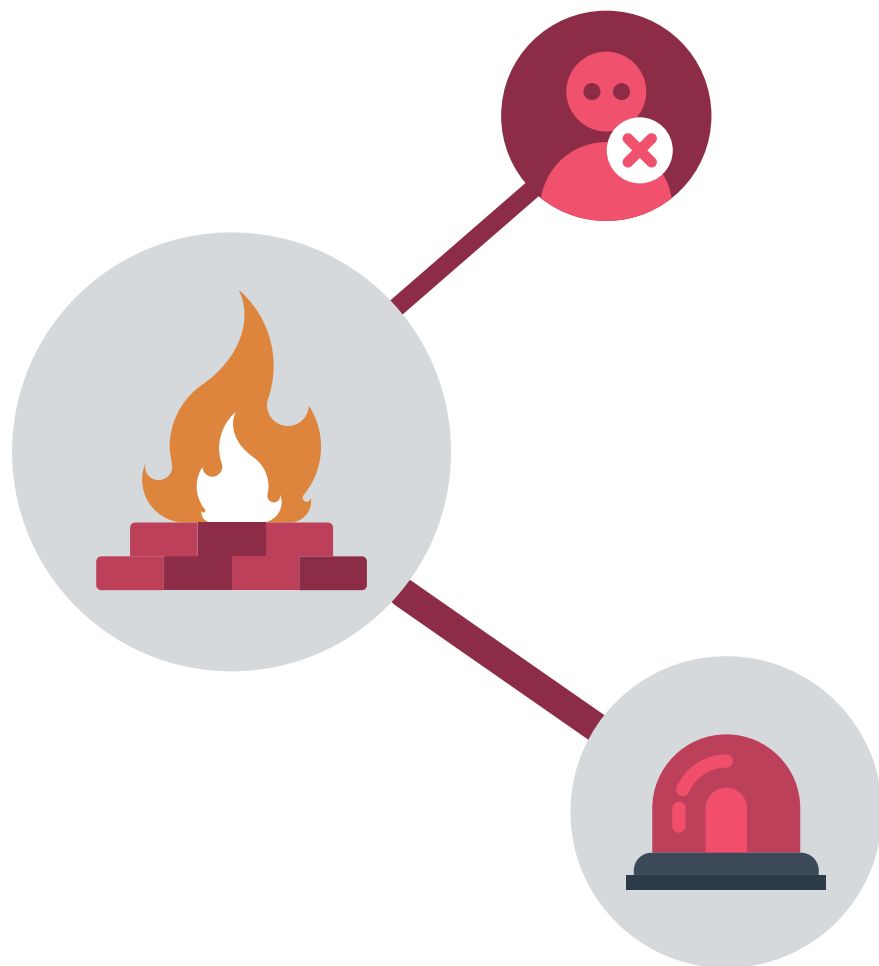
Si pensi al collega che inconsapevolmente scarica l'allegato dannoso di un'e-mail o che visita un sito pericoloso, infettando la rete aziendale con un malware che rallenta i computer o che invia dati sensibili a un criminale informatico.

Secondo il Report sulle minacce informatiche 2016 di CyberEdge, le aziende hanno valutato la "scarsa conoscenza dei sistemi di sicurezza da parte dei dipendenti" come il problema principale nella difesa dalle minacce alla sicurezza. Nella classifica, tale ragione precedeva la "mancanza di budget" e la "mancanza di personale qualificato".¹⁰



4

I nostri sistemi sono dotati di un efficientissimo software antivirus, quindi siamo protetti



Il software antivirus esegue una scansione dei sistemi per cercare eventuali malware scaricati dai siti Web e dalle e-mail. Tuttavia, gli hacker dispongono di altri mezzi per aggirare questo sistema di difesa.

Tra gli attacchi informatici che non possono essere bloccati dall'antivirus vi sono: attacchi DDoS (Distributed Denial of Service), nei quali un sito Web è invaso da traffico spazzatura che rallenta o blocca l'antivirus; attacchi basati sul Web, dove gli hacker inseriscono codici dannosi per appropriarsi di informazioni o per spiare da remoto; infine, l'accesso degli hacker tramite dispositivi rubati.

5 Se c'è un intruso, ce ne accorgiamo subito



Non è facile individuare un attacco informatico. I malware che entrano in un sistema potrebbero non essere in grado di bloccare immediatamente le operazioni, ma potrebbero spiare il sistema fornendo all'hacker informazioni per pianificare attacchi più mirati.

Attacchi di questo tipo a sistemi specifici vengono classificati come minacce mirate e persistenti (APT, Advanced Persistent Threats). Gli attacchi APT sono caratterizzati da un monitoraggio continuo e dall'ottenimento di informazioni da un sistema di elaborazione dati specifico. Questo tipo di attacco è molto difficile da individuare.

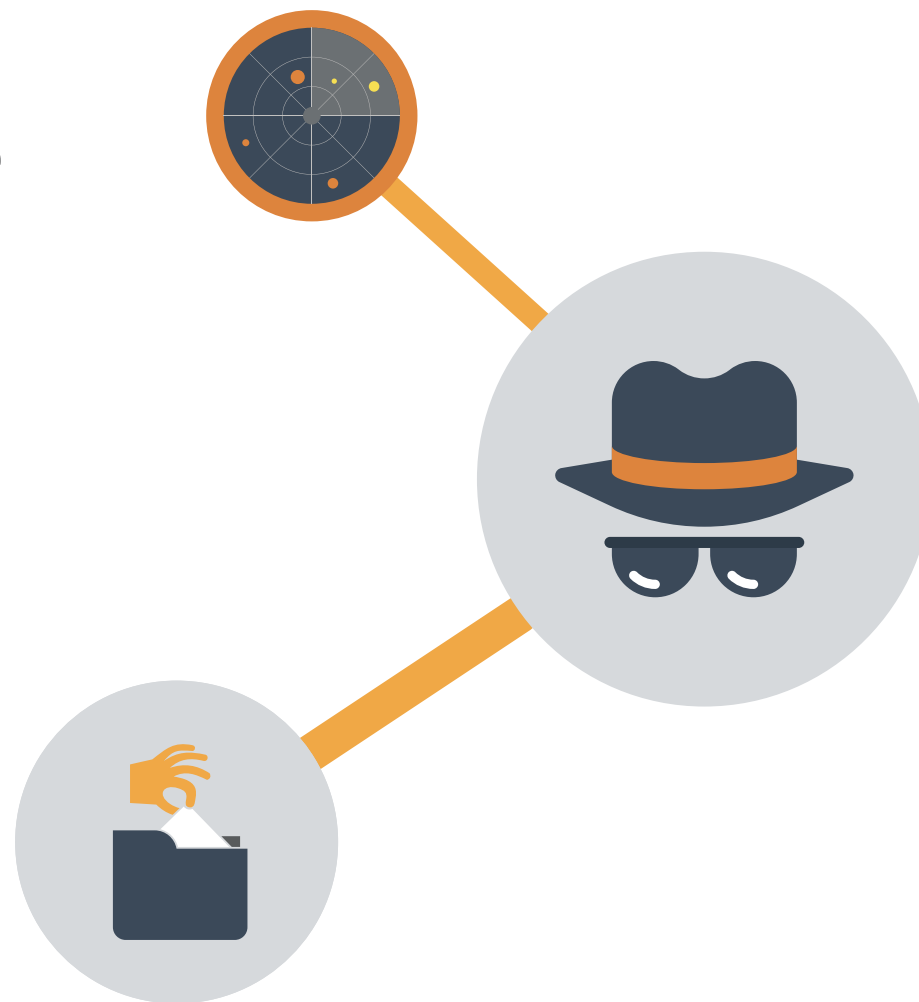
Daisy Group, che si occupa di consulenza informatica, ha stimato che metà delle imprese britanniche potrebbe essere violata in meno di un'ora.

CONSIGLIO:

monitorare i dati in uscita in caso di un traffico più elevato del solito può aiutare a rilevare furti di informazioni, in quanto potrebbe trattarsi di un attacco APT.

COSA FARE:

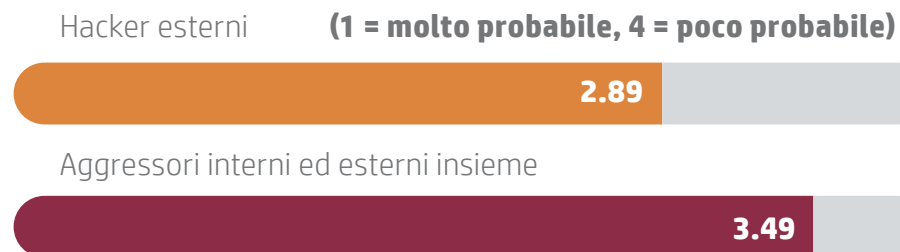
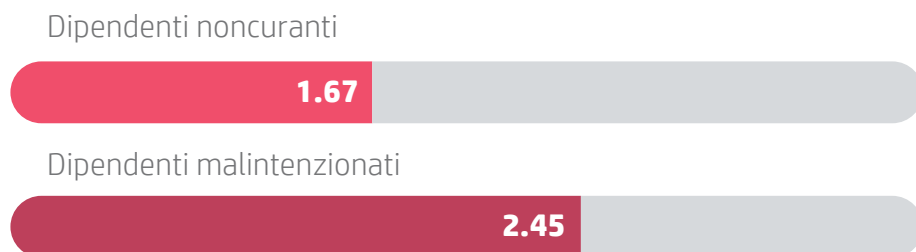
scegliere un software per la sicurezza dotato di un sistema di protezione dei dati, come HP SureStart, che ripristina automaticamente il BIOS del computer quando viene rilevato un attacco malware, bloccando le violazioni prima che i dati vengano compromessi.



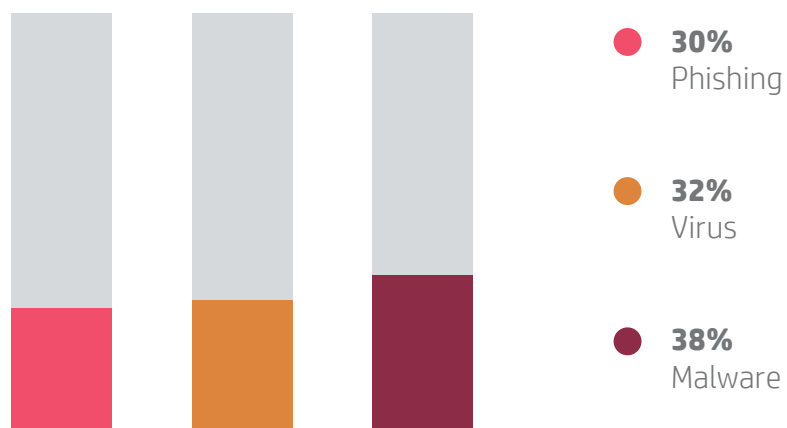
Da dove arrivano le minacce?

Per proteggere la rete è necessario conoscerne i punti deboli.

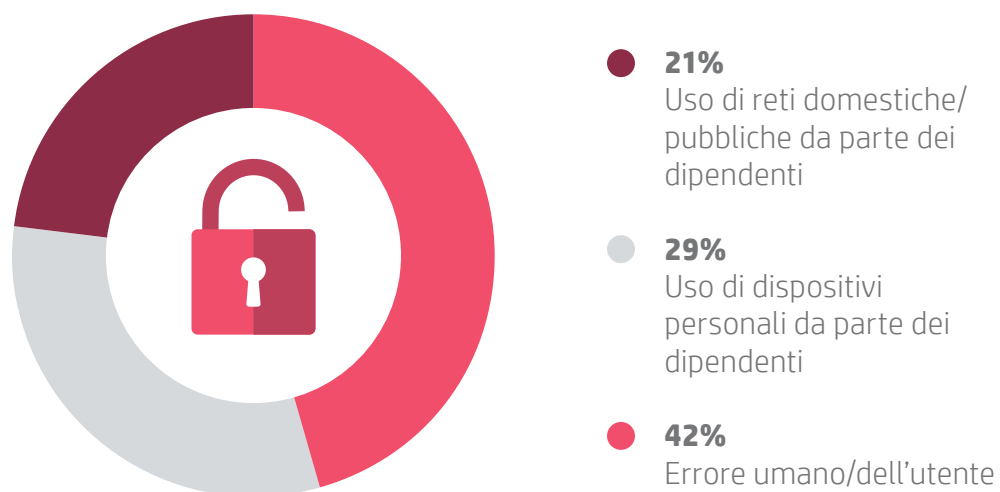
Le cause più frequenti delle violazioni di dati sono:¹¹



I tipi più comuni di minacce esterne:¹²



Cause delle violazioni interne:¹²



Quanto costa riprendersi dai crimini informatici?

I tipi di attacchi informatici più costosi:¹³

25%

1.140.000€

Codice dannoso e malware

Software che danneggia il sistema creando criticità nella sicurezza, compromettendo file o rubando informazioni (script, virus e worm inclusi)

24%

1.000.000€

Distributed Denial of Service

Gli attacchi "DDoS" consistono in una valanga di traffico web che debilita il sito di un'azienda e i suoi server

16%

760.000€

Attacchi basati sul Web

Attacchi che puntano ai visitatori del tuo sito, come codici che reindirizzano i browser a pagine piene di malware

13%

620.000€

Dispositivi rubati

Lo smarrimento di dispositivi dei dipendenti con accesso alle password aziendali può comportare il furto dei dati e atti fraudolenti

9%

420.000€

Phishing e ingegneria sociale

E-mail o pop-up che sembrano richieste legittime di login

9%

420.000€

Malintenzionati all'interno dell'organizzazione

Dipendenti che diffondono informazioni sensibili

4%

190.000€

Botnet

Reti di computer infetti che sono controllati per eseguire attività fraudolente, come l'invio di spam

L'impatto della criminalità informatica sulle aziende

Il costo reale della criminalità informatica va oltre la riparazione dei danni di un attacco

Le violazioni dei sistemi di sicurezza sono incredibilmente costose. In genere, una violazione può colpire le risorse finanziarie aziendali in tre modi.



Risorse aziendali

Naturalmente a seguito di un attacco è necessario fare ordine. Cosa che comporta un dispendio notevole in termini di tempo e denaro. Inoltre, significa dover sospendere momentaneamente altri progetti per concentrare le risorse nel ripristinare i corretti livelli di sicurezza aziendali.



Sanzioni/penali

Si potrebbe ricevere una sanzione per inadempienza (ad esempio, l'HIPAA). Il prossimo anno, dopo la ratifica del regolamento generale sulla protezione dei dati dell'Unione europea, le aziende inadempienti potrebbero incorrere in una sanzione del 4% sul fatturato globale. Si potrebbe anche rischiare di incorrere in azioni legali se la fuga di informazioni desse origine a una violazione dei termini sulla riservatezza dei clienti.



Danno di immagine

Questo può rivelarsi l'effetto più negativo di una violazione. I clienti, la stampa e il pubblico in generale hanno la memoria lunga quando si tratta di violazioni della sicurezza. Potrebbe volerci molto tempo per riconquistare la loro fiducia.

Anatomia di un attacco inaspettato

Quando Sony Pictures fu attaccata nel 2014, gli hacker entrarono semplicemente dall'ingresso principale.¹⁴

Secondo “Lena” del gruppo di hacker Guardiani della Pace (GOP), che ha rivendicato l'attacco, Sony “non dispone più di un servizio di sicurezza fisico”. Ottennero infatti l'accesso alla rete di Sony entrando fisicamente nell'edificio e rubando le credenziali di un amministratore di sistema.

Una volta entrati, inserirono un malware in grado di appropriarsi di file privati, codice sorgente e password dei database Oracle e SQL. Da lì, rubarono i programmi, le e-mail, i documenti finanziari inerenti alla produzione cinematografica e molto altro. Infine, pubblicarono gran parte di quelle informazioni online.

Gli hacker minacciarono di pubblicare altre informazioni top secret se la compagnia non avesse ritirato il film “The Interview” dalle sale. Sony alla fine si arrese, registrando incalcolabili perdite al botteghino nonché subendo enormi danni di immagine.

Sony commise due errori. Ignorare la possibilità di accesso fisico ai dati della compagnia da parte di intrusi e non investire in un piano di sicurezza a più livelli, che avrebbe potuto prevenire l'accesso alle informazioni sensibili dopo l'intrusione iniziale.

Dopo l'attacco, l'esperto in sicurezza Bruce Schneier scrisse: “Qualsiasi rete è vulnerabile di fronte a un aggressore sufficientemente abile, determinato e motivato”. Il trucco sta nel riconoscere i punti vulnerabili della propria rete. Uno di questi potrebbe essere l'ingresso principale.

COSA FARE:

creare un piano di difesa contro le violazioni per ogni reparto, dall'ufficio tecnico all'assistenza clienti, per minimizzare i tempi di recupero.

CONSIGLIO:

molte tipologie di malware vengono trasmesse attraverso gli allegati delle e-mail. Raccomandiamo di formare il personale affinché possa riconoscere anche quei file sospetti progettati per non sembrare tali.

- Costi stimati della criminalità informatica per le imprese britanniche: 21 miliardi di sterline¹⁵
- Costo medio della criminalità informatica per ogni impresa britannica nel 2016: 5,7 milioni di sterline¹⁶
- Imprese britanniche vittime di violazioni informatiche o attacchi 2015-2016: 66%¹⁷

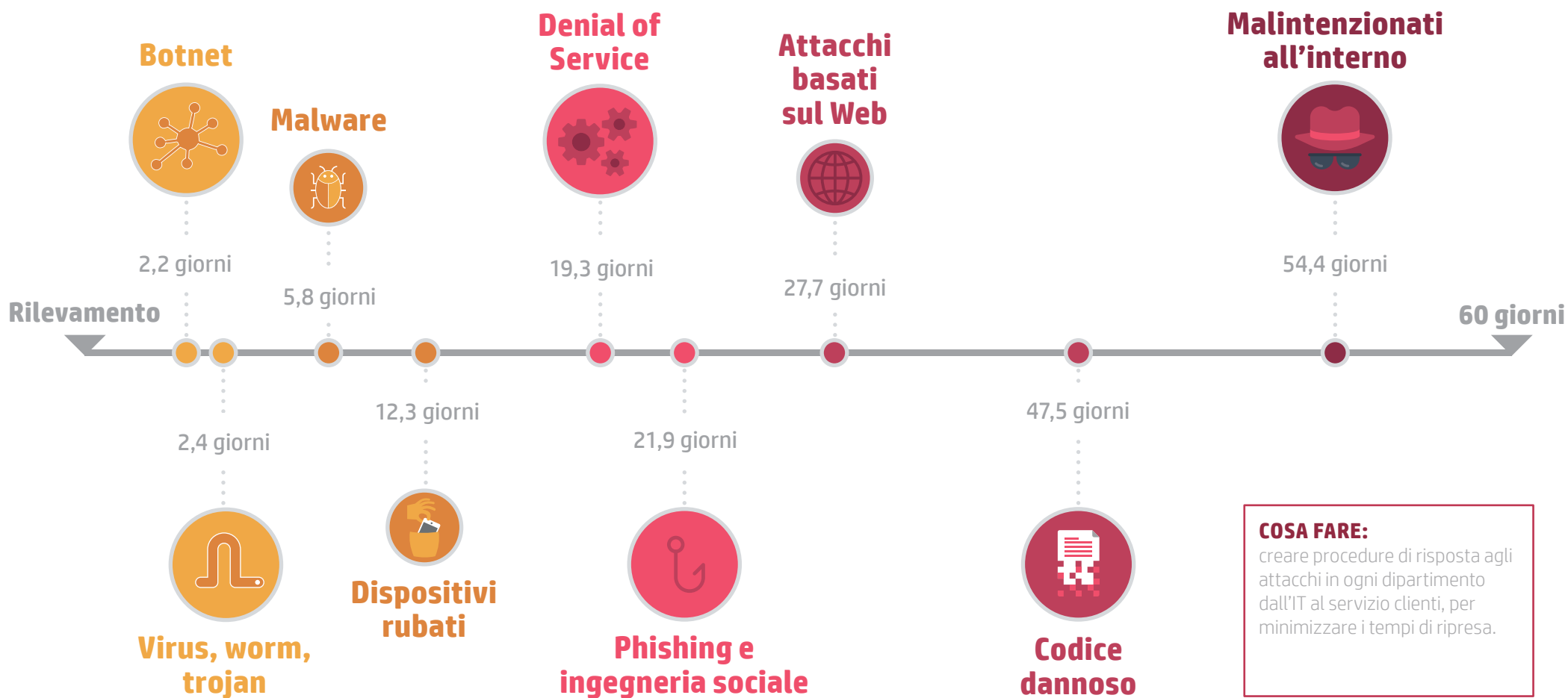
Fonti: ¹⁴ <http://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12?IR=T> ¹⁵ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

¹⁶ <https://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/> Stat is \$7.21m – have converted to £

¹⁷ <https://www.gov.uk/government/news/two-thirds-of-large-uk-businesses-hit-by-cyber-breach-or-attack-in-past-year>

Cyber crime: quanto tempo è necessario per ripristinare il sistema

Quanto tempo occorre per riparare danni di un attacco al sistema?
L'Istituto Ponemon considera una media di 46 giorni, affermazione alquanto preoccupante per piccole e medie imprese che contano su cicli di operatività senza interruzioni.



COSA FARE:
creare procedure di risposta agli attacchi in ogni dipartimento dall'IT al servizio clienti, per minimizzare i tempi di ripresa.

Come proteggere la tua azienda dalla criminalità informatica

Consigli fondamentali e strategie per la sicurezza informatica aziendale

Qui riportiamo i sei bersagli comuni per gli hacker che violano i sistemi aziendali e i consigli per affrontarli.



Database di clienti



Servizi cloud



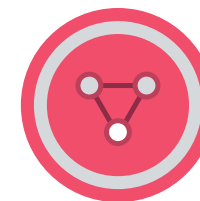
Smartphone e tablet dei dipendenti



Errori dei dipendenti



Internet of Things



Gateway di rete

I criminali informatici sono costantemente alla ricerca di informazioni ed essendoci più dispositivi connessi nell'ambiente di

lavoro (da smartphone e tablet alle stampanti Wi-Fi) i potenziali punti di accesso sono sempre più numerosi.

1 Database di clienti



I dati finanziari non sono gli unici bersagli degli hacker; le informazioni come nomi e indirizzi e-mail possono essere usate per furti di identità, spam o per aggredire altri account.

La soddisfazione più grande per i veri hacker è quella di danneggiare le aziende che servono una vasta rete di imprese. Si pensi a tutto ciò come all'equivalente digitale dell'introdursi in una ferramenta solo per raggiungere la parete del seminterrato condivisa con il caveau della banca nazionale adiacente. Dopo essersi introdotti nel sistema più piccolo, gli aggressori sono in una posizione migliore per ottenere l'accesso ai dati dei clienti custoditi da grandi imprese.

Come potrebbe essere compromesso il database dei vostri clienti? Virus, worm e trojan, scaricati da siti dannosi o e-mail, possono rilasciare i codici necessari ad un hacker per accedervi e rubare il loro contenuto.

Come proteggere i dati dei tuoi clienti

- Usare software per la sicurezza ideati per le aziende, che proteggano la rete, le caselle di posta e gli endpoint.
- Aggiornare sempre i software per la sicurezza bloccando così i malware in evoluzione.
- Scaricare gli aggiornamenti software per i programmi del sistema, poiché le versioni precedenti potrebbero celare vulnerabilità a vantaggio degli hacker.

2 Servizi cloud



Come proteggere le informazioni nel cloud

- Criptare le informazioni più importanti usando strumenti come la tecnologia Smartcrypt di PKWARE, che si basa sulle politiche di accesso per determinare la complessità della crittografia. In questo modo gli utenti autorizzati visualizzeranno i dati cui hanno accesso, mentre gli utenti non autorizzati non li potranno visualizzare.
- Creare una password efficace per l'account del cloud.
- Richiedere un'autenticazione a due fattori, come un codice smartphone combinato alla password, per effettuare modifiche ai dati del cloud, come il download, l'eliminazione o lo spostamento di file.

Il cloud computing è diventato fondamentale per le infrastrutture aziendali.

Il sondaggio sul cloud computing 2016 di IDG rivela che il¹⁹ 70% delle aziende ha almeno alcune infrastrutture nel cloud, mentre Tripwire ha evidenziato che il 90% usa il cloud per le infrastrutture e/o per l'archiviazione dei dati, tra cui quelli mission-critical.²⁰

La sicurezza è decisamente una preoccupazione, ma in realtà i dati sono più sicuri nel cloud, custoditi in server fuori sede da imprese specializzate in sicurezza dei dati. Ecco perché il 64% delle aziende intervistate da Tripwire considera il cloud più sicuro dei sistemi legacy.

Fortunatamente, questa fiducia non è mal riposta. Secondo l'indagine del 2015 del BIS,²¹ solo il 7% delle aziende (piccole e medie) ha subito serie violazioni dei servizi cloud, generalmente causate da permessi di accesso o da password insufficienti. Un cloud sicuro infatti ha ancora bisogno di una forte governance sulla sicurezza interna. Basta pensare alla porta di ingresso di Sony.

Fonti:

¹⁹ <https://www.scribd.com/document/329518100/IDG-Enterprise-2016-Cloud-Computing-Survey>

²⁰ <https://www.tripwire.com/state-of-security/security-data-protection/enterprise-impressions-of-cloud-security-in-2016/>

²¹ 2015 Small Business Survey. Department for Business, Innovation & Skills

3 Smartphone e tablet dei dipendenti



Molti usano i dispositivi personali a scopo professionale.

Le politiche Bring-Your-Own-Device (BYOD) per le aziende sono un modo efficace di sfruttare gli smartphone già in possesso dei dipendenti. Questo trend è in crescita, con il 53,2% delle aziende che implementerà una politica BYOD entro i prossimi due anni.²² Sfortunatamente, questi dispositivi rappresentano un bersaglio facile per gli hacker.

Si stima che un'app Android su cinque contenga un qualche tipo di malware invasivo, che potrebbe essere trasmesso a file e sistemi aziendali al fine di monitorare le attività o sottrarre informazioni.²³

Anche i dipendenti a cui è stato rubato lo smartphone possono inconsapevolmente favorire l'accesso degli hacker. Un ladro di cellulari potrebbe vendere il dispositivo a un acquirente del mercato nero, che può usare le informazioni per violare l'azienda dello sfortunato o per penetrare nei sistemi di un cliente più grande.²⁴

Come proteggere i dispositivi dei dipendenti

- Installare uno strumento di rilevazione delle minacce come X-Ray di Duo per i dispositivi Android per tracciare più facilmente le app pericolose e i codici sospetti.
- Chiedere ai dipendenti di attivare la cancellazione remota (disponibile gratuitamente per Android, iPhone e Windows Phone; su abbonamento per BlackBerry), così in caso di smarrimento, sia i dati sensibili personali che aziendali potranno essere cancellati. Inoltre, chiedere ai dipendenti di attivare la crittografia sui loro smartphone per proteggere i dati (opzione attiva di default sui nuovi telefoni iOS e Android).

4 Errori dei dipendenti



Come fornire supporto ai dipendenti

- Formare i dipendenti sulle pratiche migliori per la sicurezza informatica e organizzare sessioni di training periodiche per mantenersi in linea con le ultime minacce.
- Sviluppare un protocollo di sicurezza su misura per l'azienda e per il tipo di dati che vengono elaborati.
- Creare un team per comunicare la politica sulla sicurezza informatica ai dipendenti nonché a clienti e partner.

La corretta gestione delle password rientra nei principi basilari della sicurezza informatica. Eppure, il 31% delle peggiori violazioni informatiche del 2015 è ancora imputabile a errori del personale in questo campo.

Dalla violazione di password deboli al furto di documenti inviati per e-mail da una connessione non sicura, oppure una email di phishing ai danni di un dipendente specifico: gli aggressori spesso traggono vantaggio dall'errore umano.

5 Prepararsi per l'Internet of Things



Il centro di ricerca IDC prevede che il numero di dispositivi connessi a Internet raggiungerà i 30 miliardi nel 2020, partendo da una stima di 13 miliardi.²⁵

Anche se i computer in ufficio sono sicuri grazie alle password e idealmente anche grazie a un software per la sicurezza, le code e i lavori di stampa spesso non sono protetti da protocolli di sicurezza simili e con l'aumento del numero di dispositivi mobili e del lavoro remoto nemmeno tutti i dispositivi personali sono sicuri come dovrebbero.

Queste stampanti non protette e altri hardware connessi alla rete potrebbero diventare il bersaglio di "programmi di sniffing" in grado di registrare lavori di stampa e informazioni sul traffico di rete, nomi utente e password, tutti in seguito reinviati a un server del cyber crime.

Vale la pena sottolineare che la violazione ampiamente resa pubblica da Dyn era legata ad una rete di telecamere a circuito chiuso abilitate dal Web e prodotte da un'unica compagnia, la XiongMai Technologies, secondo l'azienda di servizi per la sicurezza Flashpoint.

Questo dimostra che ogni dispositivo connesso alla rete è un endpoint e la rete è tanto forte quanto il dispositivo meno sicuro che vi è connesso. Il 97% delle aziende dispone di procedure sulla sicurezza per desktop e laptop, il 77% per i dispositivi mobili, ma solo il 57% dispone di procedure per le stampanti.²⁶

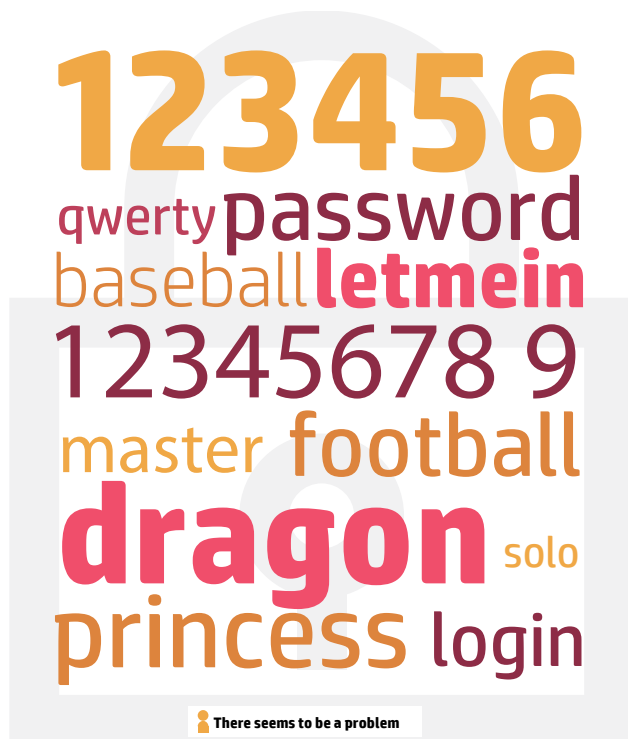
Come prepararsi all'Internet of Things

- Rimuovere o disabilitare le funzioni non necessarie dell'hardware, poiché più queste sono numerose più si possono creare gateway potenzialmente sfruttabili per l'accesso.

Password e ransomware

Le password più diffuse

All'inizio del 2013, un reporter di Ars Technica, che non si era mai interessato alla criminalità informatica e tanto meno aveva sperimentato la violazione di sistemi protetti da password, ottenne 8.000 password crittografate su un totale di oltre 16.000 in un solo giorno. Quindi, quanto è probabile che queste password d'uso estremamente comune resistano all'attacco di un criminale informatico professionista?



* Splashdata

Cos'è un ransomware

I criminali informatici ricorrono sempre più frequentemente al ransomware, un tipo di malware che prende il controllo dei sistemi e consente di sbloccarli solo tramite il pagamento di un riscatto in bitcoin. Nel 2013, migliaia di sistemi furono infettati da un trojan chiamato Cryptolocker, che catturò l'attenzione della National Crime Agency nel Regno Unito e della sua Unità nazionale anti-crimine informatico. Ecco un prospetto più dettagliato che spiega come si verificano gli attacchi di questo tipo.

	1. Installazione	Un codice dannoso viene introdotto nel computer dopo un download accidentale tramite e-mail o siti corrotti.
	2. Notifica alla sede	Il ransomware si connette al server principale per stabilire una chiave di crittografia.
	3. Crittografia i tuoi file	Il ransomware esegue una scansione dei file presenti in rete e li crittografa, rendendoli inaccessibili.
	4. Estorsione	Sul computer dell'utente generalmente appare un messaggio che mostra un limite di tempo e un importo da pagare per decrittografare i file prima che vengano eliminati.
	5. Pagamento	Le aziende coinvolte possono acquistare una valuta digitale come i bitcoin da versare all'aggressore, che quindi dovrebbe decrittografare i file.

6 Gateway di rete



Quando un hacker vuole entrare in una rete, potrebbe sferrare un attacco DDoS: milioni di macchine infettate da malware vengono collegate per generare un'ingente quantità di traffico fasullo che manda in tilt la rete.

Spesso, gli aggressori DDoS vogliono distrarre gli amministratori del sito con un blocco del sistema, mentre rubano dati o installano malware per pianificare successivi furti digitali. Alcuni attacchi DDoS sono anche frutto di “script kiddies”, ossia hacker principianti che vogliono danneggiare un sito solo per il gusto di farlo. Anche poche ore di inattività di un sito Web possono essere devastanti per il bilancio e per la reputazione di un'azienda.

CONSIGLIO:

investire su hardware che offra protezione integrata, come strumenti di autenticazione avanzata per la crittografia

Come proteggere la tua rete

- Costruire un sistema che controlli il traffico in entrata e in uscita della rete. Un piccolo improvviso può essere indice di un attacco, mentre un'attività costante ma inspiegabile può indicare che un trojan sta trasmettendo i dati alla sua base.
- Filtrare tutto il traffico affinché solo quello necessario a sostenere l'azienda finisca nella rete.
- Rendere sicuro ogni router, switch e qualsiasi altro dispositivo di rete che opera con lo stesso software di base e con le stesse funzioni, e scaricare sempre gli aggiornamenti del software.

Il futuro della sicurezza informatica aziendale

Ora che le aziende dipendono così tanto da Internet, è sempre più essenziale costruire sistemi di difesa solidi per la sicurezza informatica

Oggi i dipendenti portano i dispositivi personali al lavoro. Le aziende utilizzano piattaforme di cloud computing ed esternalizzano i servizi tecnici principali. Inoltre, più di quattro milioni di britannici ora lavorano da casa. La sicurezza informatica diventa più difficile se non si controllano né i dispositivi, né le infrastrutture, né lo spazio di lavoro.

Allo stesso tempo, gli smartphone ci hanno insegnato che si può fare business ovunque e in qualsiasi momento. Un bar è un luogo perfetto per lavorare quanto un ufficio. Usiamo le reti Wi-Fi pubbliche per elaborare grandi quantità di dati aziendali e

personali, spesso su smartphone che sono decisamente poco sicuri.

Nei prossimi anni, sicurezza vorrà dire molto di più che installare un software antivirus sui dispositivi o aggiornare le password ogni sei mesi. Le aziende dovranno ricorrere a misure di sicurezza che funzionino con la stessa efficacia sia in remoto che in un ufficio gestito da un esperto informatico.

Per le aziende distribuite di domani, la sicurezza informatica dipenderà da analisi complesse in grado di isolare i comportamenti insoliti e da un sistema di sicurezza su diversi livelli in grado di proteggere tutti i punti di accesso.

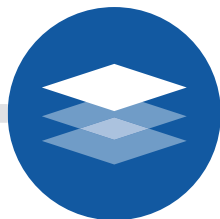


Il futuro della sicurezza informatica aziendale



Analisi: il detective della sicurezza informatica

Anche se un sito non ha molto traffico, presenta comunque dei trend. L'uso di strumenti di analisi che ne misurano e registrano l'attività può semplificare la diagnostica quando qualcosa non va. Questi strumenti tracciano e registrano prima i comportamenti normali per poi riuscire a individuare le anomalie. Dopo l'intercettazione di un'anomalia, gli amministratori possono contrattaccare ed eliminare gli attacchi prima che scatenino il caos informatico.



Stratificazione: tiene a distanza gli aggressori

A volte detta "difesa in profondità", la sicurezza su diversi livelli protegge ogni punto di accesso in vari modi. L'approccio comune include dei certificati SSL di validazione estesa che complicano la falsificazione delle credenziali necessarie per accedere a una rete sicura. Può essere utile anche ricorrere a un'autenticazione a più fattori, che costringe gli aggressori a dover violare più di una sola password.

Indipendentemente dalla tecnologia specifica in ufficio, il principio della stratificazione è di blindare ogni area sensibile di una rete aziendale in qualche modo. Gli utenti e i partner potrebbero impiegare più tempo ad accedere a dati fondamentali, ma i benefici di questo sistema sono impagabili.



Reazione immediata

Investire in un software per la sicurezza informatica e nella formazione è la miglior difesa. Si può iniziare con un audit dei sistemi e delle infrastrutture a disposizione. Stai facendo abbastanza? Cosa potresti fare meglio?

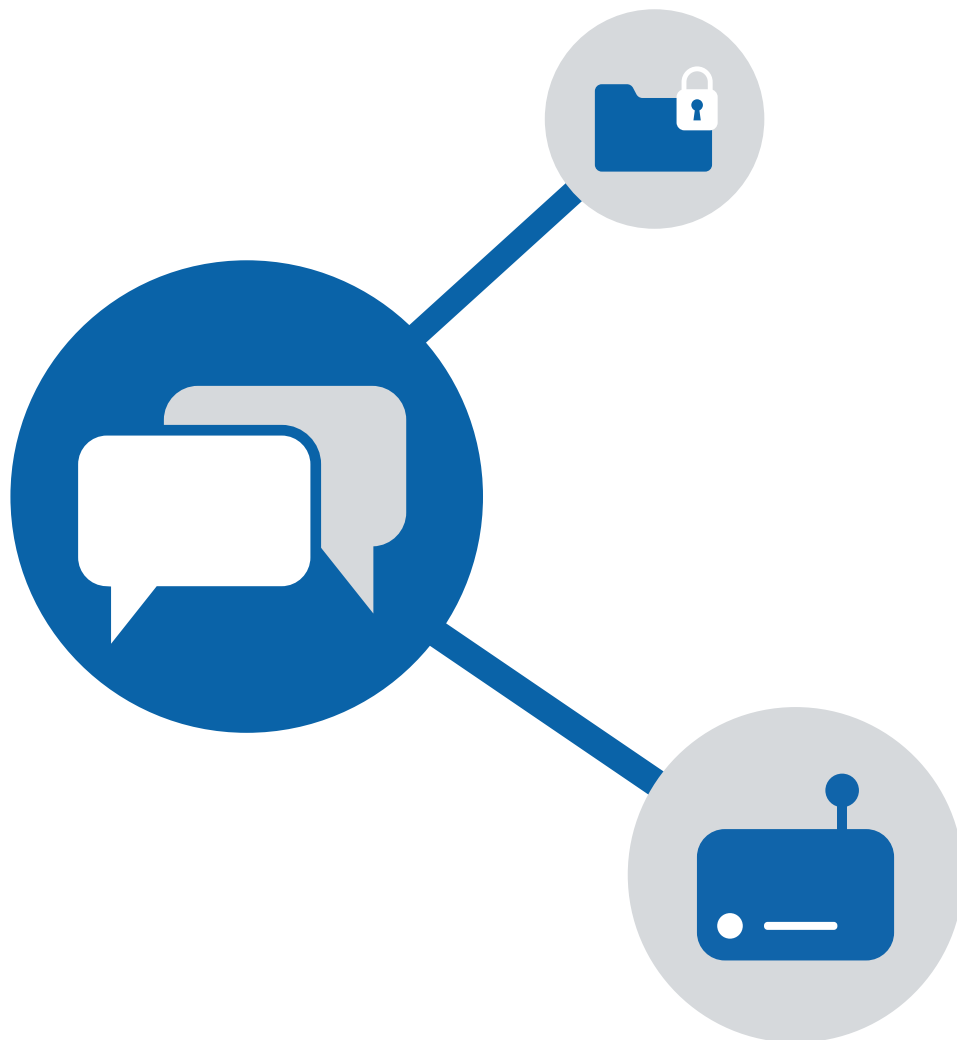
Per finire, puoi contattare i nostri esperti di HP. La nostra knowledge base collettiva si concentra sulla prevenzione delle minacce, non solo nella difesa. Per saperne di più, visita il sito HP.com.

CONSIGLIO:

tracciare e registrare prima i comportamenti normali per poi riuscire a rilevare le anomalie.

Considerazioni sulla sicurezza dei dispositivi endpoint

Proteggere ogni singolo dispositivo nella tua rete



Una ricerca sulla sicurezza eseguita da Spiceworks²⁷ rivela che le principali fonti di minacce per la sicurezza aziendale sono:

- Laptop e desktop: 81% esterne e 80% interne
- Dispositivi mobili: 36% esterne e 38% interne
- Stampanti: 16% esterne e 16% interne

Quali tra queste sono le minacce che devono essere messe al sicuro con più urgenza? La risposta è molto semplice: tutte.

Una logica intuitiva potrebbe suggerire che rendere sicura una stampante connessa non ha la stessa importanza di rendere sicura la tua flotta di laptop. Ma il rischio è lo stesso. È risaputo che gli hacker puntano a bersagli come le stampanti o a qualsiasi

dispositivo intelligente che si connetta alla rete. Questo perché sanno che quei dispositivi non sono generalmente sicuri e offrono lo stesso livello di accesso.

HP: tracciamo la strada in un mondo in evoluzione

La sicurezza informatica sta cambiando. Abbiamo gli strumenti giusti per aiutarti a difenderti.

Non ci sono soluzioni rapide per la sicurezza informatica. Un sistema di difesa solido ha bisogno di un approccio variegato che comprenda reti, dispositivi e persone. Scegliere la tecnologia giusta è il punto di partenza.

In HP, la sicurezza è al primo posto. La nostra gamma HP Elite Premium include funzionalità per la sicurezza leader nel mercato, come HP SureView e HP SureStart.

Molti dispositivi HP hanno in dotazione:

- **Blocco Bluetooth:** usando il Bluetooth, la macchina si blocca automaticamente quando ci si allontana e si sblocca quando ci si avvicina.
- **Sicurezza biometrica:** il riconoscimento facciale e delle impronte digitali autorizza l'accesso solo agli utenti autenticati biometricamente.
- **Display HP SureView*:** il monitor oscurato previene gli sguardi indiscreti proteggendo il materiale confidenziale mentre si lavora in viaggio.
- **BIOS con riparazione automatica HP SureStart:** HP Elite Premium monitora il proprio BIOS ogni 15 minuti. Se viene rilevata un'anomalia, riporta il PC al suo stato originale, respingendo qualsiasi intruso.

Gli HP Elite non potranno proteggere la tua azienda da soli, ma contribuiranno alla costruzione di una prima linea solida.

Visita www8.hp.com saperne di più sulla gamma completa HP Elite.

Glossario

Per approfondire i concetti chiave

Attacchi basati sul Web:

spesso un attacco basato sul Web comporta il reindirizzamento del browser verso siti dannosi.

Botnet:

generalmente si riferisce a un tipo di programmi automatici creati per accedere e controllare computer connessi a Internet senza che il proprietario se ne accorga. Spesso i computer vengono infettati da malware. Gli hacker usano i botnet per sferrare attacchi **Denial of Service** su un sito Web.

Controlli perimetrici:

categoria generale che descrive una difesa informatica nel punto in cui l'Internet pubblico o altre reti pubbliche entrano in contatto con una rete privata, gestita internamente. Generalmente vengono coinvolti diversi livelli e tipi di dispositivi differenti.

Ingegneria sociale:

garantisce l'accesso agli aggressori che riescono a ottenere informazioni da parte di un utente autorizzato.

Malware:

vasta categoria di software in grado di danneggiare o perfino di disabilitare altri sistemi. Virus, worm e trojan sono tutti esempi di malware.

Phishing:

generalmente veicolato tramite e-mail in cui un aggressore chiede delle informazioni personali in una finestra di dialogo apparentemente normale.

Strumenti per la gestione delle policy:

in genere, gli strumenti per la gestione delle policy stabiliscono uno standard di ciò che è visibile o nascosto agli utenti. Inoltre, rafforzano tale pratica in tutta la rete. La coerenza (almeno in teoria) garantisce la sicurezza.

Strumenti GRC:

pensati per iniziative vaste e coordinate all'interno di un'azienda con l'obiettivo di gestire e governare le operazioni in modo conforme alle norme.

Strumenti per la prevenzione della perdita di dati:

vasta categoria di software con l'obiettivo di monitorare i dati sensibili e di bloccare eventuali tentativi di accesso e copia da parte di personale non autorizzato. Diversi approcci consentono di proteggere i punti di accesso (come gli endpoint) mentre si estendono attraverso una rete o un sistema di file. Questo mercato della Gartner è **creciuto del 25%** dal 2013.

Sistemi di security intelligence:

una grande varietà di servizi di sicurezza può aiutare a raccogliere e sintetizzare informazioni relative alle minacce. I sistemi variano dalla registrazione delle attività dei responsabili a sistemi per rilevare anomalie della rete.

Glossario

Tecnologie Firewall:

un altro termine ampio che descrive un tipo di dispositivo che usa algoritmi e altre tecniche per bloccare l'accesso alla rete di traffico e utenti non autorizzati. **Le versioni della prossima generazione** di questi dispositivi saranno più potenti grazie all'abilità di combinare funzioni che in precedenza venivano gestite da dispositivi diversi.

Tecnologie per la crittografia:

strumenti che **rendono i dati illeggibili** senza un relativo decodificatore. Negli anni passati, l'Information Commissioner britannico si è pronunciato **assolutamente a favore** rispetto a vari tipi di crittografia. Più recentemente, il governo è stato costretto a **rivedere la sua posizione in merito alla tecnologia per la crittografia** a causa di severe critiche.

Trojan:

con un impatto simile a quello di virus e worm, il trojan deve essere installato dall'utente e quindi viene generalmente mascherato. I suoi effetti spaziano da impostazioni del computer modificate alla cancellazione di file al fine di creare delle "backdoor" che l'hacker può sfruttare in un secondo momento

Virus:

codice dannoso in grado di replicarsi e di diffondersi in una rete.

Worm:

a differenza dei virus che si diffondono con la condivisione di un file ospite, i worm si possono replicare indipendentemente dal file ospite come un documento di Word o un foglio di lavoro di Excel e quindi non necessitano di alcuna interazione umana per provocare danni.