ZEBRA

Zebra Security Platform

Proteggete il vostro margine prestazionale

La connettività pervasiva che accelera la vostra attività può anche esporla a potenziali rischi per la sicurezza. Un firewall può essere certamente un buon inizio, ma non è certo una soluzione definitiva in presenza di minacce emergenti e altamente sofisticate. Scoprite le best practice e le soluzioni aziendali per difendere meglio la vostra azienda e i vostri dati.

Come impedire alle minacce informatiche di fermare la vostra attività

La sicurezza prima di tutto

Numeri di carte di credito. Cartelle cliniche. Codici fiscali. Password. Sia che le vostre controparti siano clienti, pazienti o cittadini, avete il compito – e spesso l'obbligo – di mantenere riservate le informazioni personali.

Rischi in aumento

In futuro, questa esigenza diventerà sempre più pressante e complicata. Innanzi tutto, l'Internet delle cose e la tecnologia cloud oggi connettono persone e informazioni come mai prima, dando alla vostra azienda un livello di controllo operativo e di visibilità senza precedenti. Si tratta di una prospettiva entusiasmante, ma non priva di rischi.

I 50 miliardi[1] di dispositivi interconnessi previsti per il 2022 potrebbero aprire innumerevoli punti di vulnerabilità nelle aziende e nei dati riservati. Motivati da profitti allettanti e da una bassa probabilità di ripercussioni (solo il 5% degli hacker viene perseguito[2]), i criminali informatici sono più agguerriti che mai.

Qual è la posta in gioco?

Anche una sola violazione può costare cara in termini di calo della produttività e di perdite finanziarie, oltre a mettere a repentaglio la vostra reputazione.

Cosa potete fare? Per cominciare, mettete al primo posto la sicurezza. Anche se la vostra azienda ha un programma per la sicurezza, è probabile che un'errata percezione del problema ne possa compromettere l'integrità e stia creando vulnerabilità indesiderate.

3,9 milioni di dollari:
costo medio di una violazione dei dati[3]

25.575 record:
dimensione media di una violazione dei dati[3]

12 ore:
tempo medio necessario all'88% degli hacker per neutralizzare le difese di sicurezza digitali[4]

197 giorni:
tempo medio necessario a un'azienda per scoprire una violazione.[3]

Obiettivi

Retail:
l'80% del traffico di login nei siti dei retailer online è riferibile ad hacker che usano dati rubati[5]

Pubblica amministrazione/ settore pubblico:
target numero uno, con moventi quali spionaggio e ricerca di profitti[6]

Sanità:
secondo settore più preso di mira, con il 15% degli attacchi informatici[6]

Produzione:
ha registrato negli ultimi anni un maggiore livello di violazioni dovute a tentativi di spionaggio rispetto ad altri mercati verticali[6]

Non lasciate che un'errata percezione della sicurezza metta a rischio la vostra attività

Nonostante l'ampia risonanza mediatica avuta da numerose violazioni di sistemi informatici, molte aziende rimangono troppo indifferenti in tema di sicurezza. Non fatevi cullare da un falso senso di sicurezza. Potreste pentirvene amaramente quando sarà troppo tardi.

"La mia azienda non è abbastanza grande per essere presa di mira."

Il 43% degli attacchi digitali colpisce aziende di piccole dimensioni.[6] Gli hacker sfruttano la mancanza di risorse e conoscenze delle piccole imprese. Possono addirittura usare la vostra azienda per accedere ai contatti con organizzazioni più grandi.

"Siamo protetti dalla nostra rete."

Un sistema di sicurezza efficace deve essere di tipo stratificato e in costante evoluzione. Potete chiudere a chiave la porta d'ingresso, ma se lasciate aperta una finestra il ladro entrerà comunque. In effetti, uno studio ha rivelato che le contromisure tradizionali, come i firewall e gli antivirus, non sono riuscite quasi mai a rallentare gli aggressori, mentre le tecnologie di sicurezza degli endpoint si sono rivelate più efficaci nel bloccare gli attacchi.[4]

"Non abbiamo subito una violazione, quindi la nostra sicurezza funziona bene."

È possibile che abbiate subito una violazione ma non ve ne siate ancora accorti. Le ricerche mostrano che possono essere necessari fino a 197 giorni prima che un'azienda scopra di essere stata attaccata.[3]

"Abbiamo già un formale programma di sicurezza."

Bene. Lo aggiornate costantemente per stare al passo con la costante evoluzione delle minacce? Copre tutte le vostre tecnologie? Un approccio "una tantum" non è sufficiente per contrastare i sofisticati attacchi digitali degli hacker moderni.

"La sicurezza è una cosa troppo complicata."

Una sicurezza ben congegnata è intuitiva e facile da implementare. Funziona in modo trasparente per i vostri dipendenti ed è semplice da gestire per il personale IT.

"La sicurezza ha un impatto negativo sulla produttività."

I dipendenti si lamentano spesso di sistemi di sicurezza troppo "ingombranti", difficili da integrare o persino capaci di mandare in blocco i processi. Tuttavia, una violazione può mettere in ginocchio l'intera attività aziendale. La soluzione è scegliere una tecnologia nella quale la sicurezza è integrata fin dal progetto iniziale. È così che la sicurezza può supportare anziché intralciare la produttività.

Costruite attorno alla vostra organizzazione uno scudo protettivo fatto di difese multistratificate

Non tutte le misure di sicurezza sono su misura per le vostre esigenze. Quando valutate una tecnologia, considerate queste caratteristiche di sicurezza integrate nelle soluzioni Zebra Technologies.

Protezione e prestazioni integrate:
scegliete il marchio che integra sicurezza e produttività nella tecnologia fin dall'inizio. Scoprirete che le nostre soluzioni sono progettate con il chiaro obiettivo di innalzare le prestazioni e di implementare nel contempo, in modo assolutamente trasparente per gli utenti, un'intera gamma di protocolli e funzionalità di sicurezza altamente efficaci.

Funzioni di sicurezza automatiche:
le certificazioni Wi-Fi® che una volta richiedevano settimane di lavoro per essere completate dal reparto IT, ora possono essere eseguite automaticamente, accelerando la creazione di un ambiente connesso protetto per voi e il vostro team.

Personalizzabile in base alle vostre esigenze:
preferite impostare autonomamente le vostre soglie di tolleranza per la sicurezza? Zebra vi viene incontro con soluzioni configurabili che permettono di regolare i livelli di sicurezza in base alle esigenze dell'azienda o di particolari reparti.

Semplicità di manutenzione e assistenza:
potete stare certi che le nostre soluzioni di sicurezza – funzionalità, software e hardware – sono state sviluppate e testate per funzionare con una manutenzione minima e un'operatività massima. Inoltre, il nostro team di supporto e assistenza è disponibile 24 ore al giorno, qualora ne aveste necessità.

Integrazione semplificata:
con Zebra potete contare su un'integrazione fluida e rapida. Grazie alla nostra profonda conoscenza del vostro settore e delle vostre applicazioni, abbiamo già progettato le nostre soluzioni per prevedere e soddisfare le vostre esigenze in fatto di integrazione.

Vigilanza e supporto continui:
aggiornamenti della sicurezza del sistema operativo e del firmware garantiti per anni, abbinati ad assistenza nella risoluzione dei problemi, verifiche della vulnerabilità e collaborazione con la sicurezza interna.

Conformità con best practice riconosciute a livello globale:
potete contare sul fatto che Zebra segue le best practice e le linee guida definite da esperti di sicurezza internazionale, ad esempio enti quali l'ISO, il NIST (National Institute of Standards and Technology) e i controlli di benchmark del CIS (Center for Internet Security). I nostri prodotti e le nostre soluzioni sono utilizzati in applicazioni che aiutano le aziende a garantire la conformità con le norme HIPAA, PCI-DSS e GDPR.

Leader nella tecnologia di protezione per le aziende:
entrate in partnership con il brand che ha rafforzato il sistema operativo Android™ di Google per le aziende e offre fino a dieci anni di supporto per la sua sicurezza. Dai nostri mobile computer rinforzati per uso aziendale alle nostre stampanti protette con tecnologia rivoluzionaria, scoprirete che produttività e sicurezza sono alla base di tutto quello che facciamo.

Prodotti, soluzioni e servizi Zebra
Supporto in ogni fase del NIST Cybersecurity Framework

IDENTIFICARE	Monitoraggio della gestione dei rischi Printer Security Assessment Wizard Servizi professionali	Gestione dei rischi della supply chain Comitato di sicurezza
PROTEGGERE	LifeGuard™ for Android Protected Mode per stampanti Controllo dispositivi	Aggiornamenti di PrintSecure Gestione automatica dei certificati Wi-Fi Framework di gestione dei rischi
RILEVARE	Printer Profile Manager Enterprise Monitoraggio della sicurezza	Rilevamento in tempo reale
INTERVENIRE	Gestione dispositivi Contromisure di rilevamento delle minacce	Risposta agli incidenti Avvisi ai clienti
RIPRISTINARE	Servizi professionali Ottimizzazioni	Ripristino dell'ultimo stato noto

Proteggete il vostro margine prestazionale

La sicurezza è vitale per la vostra azienda e i suoi flussi di lavoro. È per questo che Zebra difende in modo proattivo le vulnerabilità della sicurezza integrando più strati di protezione nelle proprie soluzioni. I dispositivi, le tecnologie e i servizi Zebra sono progettati per garantire la sicurezza, senza intralciare la produttività. Scoprirete che la nostra sicurezza è facile da implementare e trasparente per il personale di prima linea. Con le nostre tecnologie intelligenti e configurabili, troverete il giusto equilibrio tra obiettivi operativi e sicurezza, in tempo reale, nel mondo reale. Affidatevi a Zebra per implementare le vostre strategie di business e tecnologiche d'avanguardia in totale sicurezza.

ZEBRA

Scoprite come i nostri standard di sicurezza migliorano la vostra sicurezza

Visitate **www.zebra.com/product-security**

Fonti:
1. Juniper Research, 2018 **2.** Carbon Black Incident Response Threat Report, Nov. 2018 **3.** Ponemon Institute, 2018 and 2019 Cost of Data Breach **4.** Black Report, Nuix 2017 **5.** Shape Credential Spill Report 2018 **6.** Verizon 2019 Data Breach Investigations Report