I 7 pericolosi miti da sfatare sulla Cybersecurity

DIGIWAY

Il pericolo dei 7 falsi miti

Nonostante la crescita della consapevolezza riguardo alla cyber security, resistono ancora molti falsi miti; queste certezze fallaci possono rappresentare un ostacolo rilevante nella implementazione di una sicurezza efficace.

In collaborazione con il nostro Partner TAG Distribuzione, cyber security specialist, abbiamo realizzato questo breve ebook in cui evidenziamo 7 diversi aspetti di questo problema.

Dimostreremo che i miti e le idee negative sulla cyber security rappresentano un ostacolo, una minaccia reale per le strutture, piccole o grandi, dedicate alla sicurezza delle organizzazioni che ogni giorno sono esposte a varie minacce informatiche. La disinformazione può aprire molte porte che si rivelano opportunità offerte agli hacker, ormai parte di una vera e propria filiera del crimine informatico, di infiltrarsi nella rete.

È quindi bene scegliere e incaricare aziende competenti, esperte e aggiornate per adottare soluzioni moderne che applichino metodologie attuali e che mantengano alta la guardia come zero trust oltre che tenersi informati sulle migliori e più recenti pratiche di cyber security.

MITO UNO

Troppi vincoli, la sicurezza riduce la produttività

C'è un'idea comune e diffusa secondo cui una maggiore sicurezza rende più lungo e più difficile anche, e soprattutto, alle persone autorizzate, l'accesso alle informazioni di cui hanno bisogno, non solo agli hacker. Si sostiene che rigorose politiche di sicurezza come il monitoraggio regolare e il controllo degli accessi ostacolino la produttività sul lavoro, rallentino le attività e dilatino la reattività nell'operatività quotidiana. È vero in parte soprattutto se la cybersecurity è progettata in modo inadeguato.

Tuttavia, rinunciare alla sicurezza potrebbe avere conseguenze di vasta portata per un'azienda. Un attacco riuscito come un ransomware DDoS può portare l'azienda a un blocco completo di tutta

l'operatività: dall'amministrazione alla logistica, dalla produzione alle attività commerciali e di marketing. Il personale potrebbe non essere in grado di accedere a file, reti e informazioni importanti dopo un attacco. Il recupero richiede giorni e talvolta anche settimane. Spesso il ripristino risulta solo temporaneo se non si sradicano le cause profonde dell'attacco che, spesso è stato perpetrato mesi prima della propria evidenza.

Verità: una maggiore sicurezza informatica può aumentare la produttività.

Un moderno approccio alla cyber security utilizza strumenti e metodologie che tramite le proprie caratteristiche di sicurezza avanzata si integra perfettamente nel sistema. Sfrutta anche l'intelligence tecnologica evoluta e l'analisi per il rilevamento e la mitigazione delle minacce in tempo reale. Ciò consente agli specialisti e agli utenti di concentrarsi sul miglioramento della produttività e migliorarla poiché non devono più preoccuparsi costantemente dei problemi di sicurezza.

MITO DUE

Gli attacchi informatici sono causati solo da minacce esterne

In passato si riteneva che gli attacchi provenissero dall'esterno in modo esclusivo o al massimo con l'aiuto del famoso "dipendente infedele". Le statistiche più recenti confermano che le minacce interne sono in aumento e stanno rapidamente diventando motivo di forte preoccupazione per le aziende. Le minacce interne possono includere dipendenti, fornitori, consulenti, appaltatori, partner commerciali oltre ad intrusi esterni che cercano di impersonare un utente autorizzato. Un recente sondaggio ha rivelato che le minacce interne sono responsabili del 60% delle violazioni dei dati.

Inoltre, non si può mai essere completamente certi della provenienza di questi attacchi e le soluzioni di sicurezza tradizionali sono in gran parte inefficaci quando si tratta di queste minacce. Ciò rende questo

tipo di attacco molto più difficile da rilevare e contenere rispetto alle minacce esterne.

Verità: Gli attacchi informatici possono benissimo iniziare, anche inconsapevolmente, da qualcuno di cui ti fidi.

È necessario utilizzare una combinazione di analisi comportamentale e gestione dei privilegi e degli accessi per ridurre al minimo le minacce interne o che appaiono tali. Inoltre, si consiglia di condurre sessioni di formazione del personale che elevi la consapevolezza circa l'importanza e le basi della sicurezza per istruire i collaboratori sui pericoli delle minacce interne e su come fare attenzione per rilevarle. L'errore umano e, talvolta, la volontà di una risorsa interna di creare un danno è un rischio che si può mitigare notevolmente con gli opportuni strumenti e un'adeguata formazione.

MITO TRE

I criminali informatici attaccano solo le grandi aziende

Le piccole e medie imprese hanno spesso coltivato una falsa sensazione di sicurezza pensando che fosse scarso l'interesse per i loro dati da parte degli hacker. Oggi sappiamo che le piccole e medie imprese sono tra i principali obiettivi degli hacker.

Uno studio recente ha rivelato che gli hacker hanno preso di mira le piccole imprese quasi la metà delle volte. E, ciò che è impressionante, solo il 14% di queste imprese era pronto a difendersi in una situazione del genere.

Verità: nessuna azienda, non importa quanto sia grande o piccola, è immune da tentativi di hacking e attacchi dannosi.

Gli hacker attuali non discriminano più le loro vittime. A ciascuna vittima compete un ruolo sul mercato degli indirizzi violati: i piccoli saranno prevalentemente riusati come ponti per altri attacchi mentre i grandi saranno propriamente attaccati come obbiettivo finale per il valore dei loro dati. L'abbattimento delle barriere di ingresso al mercato degli strumenti di attacco consente oggi a persone con pochissima o anche nessuna cultura informatica di diventare hacker con la promessa di facili e sostanziosi guadagni in quello che orai è un business strutturato. Pertanto, non possiamo considerare che le dimensioni dell'attività determinino la probabilità di attacco: siamo tutti un potenziale bersaglio!.

MITO QUATTRO

Il software antivirus o antimalware è sufficiente per proteggere la mia attività

Il software antivirus è una parte importantissima del piano di cyber security. Tuttavia, protegge solo uno dei punti di ingresso nel sistema. Gli hacker hanno molti modi e strumenti per aggirare il software antivirus e infiltrarsi nelle reti con attacchi come quelli di phishing e ransomware.

Quindi, anche con il software anti-malware in azione, gli hacker hanno molte altre opzioni di ingresso tramite le quali lanciare un attacco.

Verità: il software antivirus può proteggerti solo da un insieme unico di minacce informatiche riconosciute, non da altre minacce informatiche emergenti.

Nella protezione di un'azienda, l'antivirus non basta, bisogna fare molto di più per proteggere i dati dagli accessi non autorizzati. Utilizzare soluzioni più evolute che, seguendo i principi dello zero trust, siano in grado di prevenire e di proteggere proattivamente le aziende dalle minacce informatiche emergenti, soprattutto nel periodo di tempo (più o meno lungo) in cui le minacce rimangono sconosciute agli antivirus e le porte di elezione rimangono aperte per le minacce come ad esempio le vulnerabilità zero day.

MITO CINQUE

La sicurezza informatica è troppo costosa

Anche se gli attacchi informatici dannosi continuano a fare notizia e costano milioni alle aziende, molti manager si chiedono ancora se valga la pena investire nella cyber security. La sicurezza dei dati è spesso trascurata ed è solo un "nice to have" per molte aziende. Il costo medio di una violazione dei dati nel 2021 è di 4,24 milioni di dollari, il più alto degli ultimi 17 anni. E questa cifra non include il danno che deriva dalle perdite di reputazione e dalle perdite dei clienti conseguenti ad una violazione.

Verità: il costo di una buona soluzione di cyber security è molto conveniente in confronto al costo di un attacco riuscito.

Troppo spesso, ci si rende conto di questo fatto a posteriori come capita a chi monta l'antifurto dopo la prima effrazione. Il costo di investire in cyber security è conveniente rispetto a tutto quello che c'è da spendere e da fare per gestire le conseguenze di un attacco riuscito. Come sempre il detto "meglio prevenire che curare" è valido a tutti gli effetti anche da un punto di vista economico, ma come si diceva, si deve considerare anche la perdita di credibilità che in molti settori è una parte meno tangibile ma molto importante dell'avviamento di un business.

MITO SEI

Non hai bisogno di cyber security perché non sei mai stato attaccato

Chi non ha mai subito un attacco informatico o una violazione dei dati, è probabile che non sappia quanti danni possano causare. Si può anche presumere che l'attuale sistema di sicurezza sia abbastanza forte da tenere lontani i cattivi attori poiché non si ha notizia di essere stati attaccati.

Va tenuto presente che molte aziende usate come "ponte" sono utilizzate a loro insaputa per colpirne altre. Questo può essere anche causa di problemi giudiziari ove scoperto e accertata la mancata protezione.

Verità: potresti facilmente essere il prossimo obiettivo.

Le minacce informatiche e gli strumenti di hacking sono in continua evoluzione per diventare ogni giorno più sofisticati e non rilevabili, qualsiasi dato sensibile è un potenziale bersaglio per una violazione e qualsiasi sistema in rete "acceso" è appetibile come trampolino per proseguire nella diffusione di attacchi.

Sviluppare una solida strategia di sicurezza che aiuti a identificare i punti deboli esistenti e a mitigare i tentativi di attacco prima che si verifichino danni significativi è dunque una responsabilità connessa all'esercizio di una rete informatica che va difesa per proteggere sé stessa e per non divenire inconsapevolmente strumento di reato.

MITO SETTE

Hai raggiunto una sicurezza informatica totale

“

“Lo scorso anno abbiamo installato un sistema di sicurezza, quindi siamo a posto.”

Verità: non esiste una cyber security totale o perfetta contro gli attacchi informatici.

La sicurezza informatica è un processo continuo che deve essere aggiornato con i cambiamenti nel panorama delle minacce e delle caratteristiche delle piattaforme impiegate. Pertanto, non si può assolutamente mai smettere di lavorare per proteggere le risorse IT. Qualsiasi organizzazione sarà sempre sottoposta al rischio di nuove minacce emergenti.

È quindi bene rivedere, periodicamente, le politiche di sicurezza, condurre audit di sicurezza, monitorare continuamente le risorse critiche e investire nei prossimi aggiornamenti nelle misure e delle tecnologie di sicurezza.

HAI TROVATO QUESTO ARGOMENTO INTERESSANTE ?

Puoi inviarci le tue esperienze e i tuoi commenti all'indirizzo info@digiway.it . I casi più interessanti li pubblicheremo sul nostro blog. Se invece vuoi approfondire l'argomento Cybersecurity o valutare con i nostri specialisti il livello delle protezioni attuali nella tua azienda, siamo a tua disposizione. Scrivici un'email o chiamaci direttamente:

DIGIWAY SRL

Via Caldera, 21
Edificio Easypoint, 1° piano
+39 02 8715 8030

info@digiway.it

www.digiway.it

DIGIWAY