IL FATTORE FIDUCIA

Il ruolo della sicurezza informatica nel sostenere l'andamento degli affari

Executive Summary

Nel 2018, il rischio di attacchi cibernetici è stato più alto che mai. Importanti incidenti a carico della sicurezza dei dati hanno continuato a fare notizia, tra i quali il maggiore attacco diffuso di tipo "denial of service" mai registrato a 1,7 Tbps[1]. Nell'Unione Europea, il 25 maggio 2018 è entrato in vigore il Regolamento Generale sulla Protezione dei Dati (GDPR) che ha imposto nuove regole più rigide su come le informazioni a carattere personale (PII) debbano essere raccolte, elaborate e controllate. Inoltre, cryptominer si sono infiltrati nei network alla ricerca di un risultato più rapido.

Siamo entrati in una «post-trust» era, nella quale organizzazioni e individui diffidano sempre di più delle promesse di sicurezza al valore nominale. Ogni volta che i consumatori interagiscono con un brand, essi valutano se possono fidarsi della società abbastanza da condividere con la stessa le loro informazioni a carattere personale. Ogni tentativo di attacco informatico andato a buon fine contribuisce purtroppo a diminuire la fiducia che le società hanno tanto faticato a costruire tra brand e consumatori. Le implicazioni non sono più di esclusiva responsabilità dei professionisti della sicurezza, ma anche degli alti dirigenti aziendali.

Per fornire indicazioni utili sulle sfide complesse che le organizzazioni si ritrovano ad affrontare lottando per proteggere i loro brand, Radware redige un rapporto annuale "Global Application & Network Security Report". L'ottava edizione annuale del rapporto combina la ricerca organica di Radware, i dati da attacchi reali e l'analisi delle tendenze e tecnologie in sviluppo con i risultati di un'indagine globale condotta a livello di settore.

Il rapporto evidenzia gli impatti della cybersicurezza sulle società e la tecnologia, tra i quali:

- Quanto appreso dagli attacchi più recenti
- I costi reali degli attacchi informatici, tanto quantitativi quanto qualitativi
- Una panoramica delle minacce a livello di rete e di applicazioni
- Informazioni sulle vulnerabilità delle tecnologie emergenti
- Previsioni per il 2019.

RISULTATI CHIAVE

Valutare il costo rispetto al calcolo dei rischi

Proteggersi dagli attacchi informartici richiede significativi investimenti che rientrano tra le spese operative del bilancio. Per loro natura, le organizzazioni cercano costantemente dei modi per risparmiare. Ma quanto si può risparmiare se si considera il rischio di attacchi informatici che superano le difese e impattano sulle società?

Considerate le più significative informazioni emerse dall'indagine globale di settore Radware 2018-2019:

- In un solo anno, i costi iniziali attribuibili agli attacchi informatici sono aumentati del 52% arrivando a $1,1 milioni
- Le organizzazioni che hanno adattato i costi generali degli attacchi informatici alle loro aziende hanno stimato un importo quasi doppio rispetto alle società che non lo hanno fatto
- Due società su cinque hanno riportato una customer experience negativa e perdita di reputazione a seguito di un attacco andato a buon fine
- Il 93% degli intervistati ha sperimentato un attacco informatico negli ultimi 12 mesi; soltanto il 7% ha dichiarato di non aver subito alcun attacco
- Gli attacchi informatici hanno avuto una frequenza settimanale per un terzo delle organizzazioni
- L'impatto principale degli attacchi informatici è stata l'interruzione del servizio, riportata da quasi metà degli intervistati. Gli attacchi con conseguente interruzione totale o parziale del servizio sono cresciuti del 15% e hanno inciso sulla produttività
- Il cyber-ransom si è confermata la principale motivazione degli hackers ed è stato il motivo alla base del 51% degli attacchi

[1]https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/memcache-ddos-as-a-service/

Vettori di attacco emergenti

Gli attaccanti impiegano tecniche efficaci per causare denial of service quali burst, amplification/reflection, encryption o internet of things (IoT) botnets e colpiscono a livello applicativo per creare danni maggiori.

- Gli attacchi di tipo "application-layer" hanno causato la maggior parte dei danni. Due terzi degli intervistati hanno subito attacchi di questo tipo. Un terzo prevede che le vulnerabilità a livello di applicazione saranno il maggior problema nel 2019, specialmente in ambienti cloud. Più della metà ha apportato cambiamenti e aggiornato le applicazioni mensilmente, mentre il resto ha effettuato gli aggiornamenti con una maggiore frequenza, stimolando l'esigenza di una sicurezza automatizzata.
- Gli attacchi informatici con conseguente inattività o interruzione del servizio sono aumentati del 15% e un'organizzazione su sei ha dichiarato di aver subito un attacco da 1 Tbps.
- Gli hackers hanno trovato nuove tattiche per mettere in ginocchio network e data centre: Gli attacchi di tipo HTTPS Flood sono aumentati del 20%, quelli di tipo DNS e Burst del 15% e quelli di tipo bot del 10%.
- Un terzo delle società ha dichiarato di aver subito attacchi per i quali non ha potuto identificare il motivo.

Prepararsi per il futuro

Le aziende dichiarano di comprendere la serietà dei cambiamenti nel panorama delle minacce e di prendere misure per proteggere i propri asset digitali, ma la gravità delle minacce alla sicurezza è molto pesante.

- Quasi metà di esse si è sentita poco preparata a difendersi da tutti i tipi di attacchi informatici, nonostante le soluzioni di sicurezza adottate.
- L'86% delle aziende ha sperimentato soluzioni di machine-learning e intelligenza artificiale (IA) negli ultimi 12 mesi. Quasi la metà di esse ha dichiarato che la motivazione alla base di tale scelta erano i tempi di risposta più rapidi agli attacchi informatici. Radware ha rilevato una crescita del 44% in quelle che svolgono attività su blockchain.
- Le società hanno continuato a diversificare le operazioni di rete tra diversi cloud provider. Due organizzazioni su cinque usano soluzioni di cybersicurezza che combinano protezione on-premise e cloud-based.
- Il 49% delle organizzazioni in EMEA ha dichiarato di non essere preparata per il GDPR.

L'unica opzione è il successo

Il costo degli attacchi informatici è semplicemente troppo alto per non riuscire ad attenuare la minaccia ogni volta. Bastano pochi istanti per annullare la fiducia del cliente e l'impatto sulla reputazione del brand e sui costi per recuperare il cliente è significativo. Il GDPR e altri regolamenti di legge possono mandare in rovina le aziende che non vi si attengono.

Per le organizzazioni è essenziale integrare la sicurezza informatica nei loro piani di crescita a lungo termine. Mettere al sicuro gli asset digitali non può più essere delegato esclusivamente al reparto IT. Piuttosto, la pianificazione della sicurezza deve essere infusa nell'offerta di nuovi prodotti e servizi, nella sicurezza, nei piani di sviluppo e nelle nuove iniziative aziendali. I CEO ed i gruppi dirigenziali dovranno esercitare un ruolo di primo piano nell'investire nella garanzia della customer experience.

Prospettiva C-Suite

I CEO sono i nuovi responsabili della fiducia

La sicurezza informatica sta diventando un argomento molto personale per i dirigenti a livello più elevato. Per costruire e mantenere un rapporto solido con i clienti, i CEO devono svolgere il ruolo aggiuntivo di "chief trust officer". In un periodo in cui una strategia di brand accurata può essere spazzata via da un solo attacco informatico, affidare la strategia di sicurezza al chief information security officer (CISO) non è più sufficiente. La posta in gioco è troppo alta.

Si veda il destino dei CEO di società che hanno subito violazioni di alto profilo quali Equifax, Yahoo, Moller-Maersk e Anthem Healthcare. Tutto il lavoro svolto da queste organizzazioni per costruire il valore del loro brand è stato spazzato via nel momento in cui i clienti hanno perso fiducia in conseguenza degli attacchi subiti. Prima di ciò, i CEO della maggior parte di queste società "perseguivano altri interessi".

Garantire la sicurezza informatica è parte integrante dei modelli di business societari e i CEO devono verificare gli sforzi e finanziare le misure protettive. I CEO che delegano la strategia di sicurezza senza sovrintendere alla stessa lo fanno a loro rischio e pericolo.

Download the Free Report

2018–2019 Global Application & Network Security Report