SONICWALL

LE MINACCE SOFISTICATE RICHIEDONO UNA PROTEZIONE E-MAIL AVANZATA

Con la diffusione del ransomware e di altre minacce sconosciute, è più che mai indispensabile proteggere la posta elettronica

Abstract

Nella moderna era dell'iperconnessione, le comunicazioni di posta elettronica sono diventate non solo la normalità, ma anche un elemento imprescindibile per fare business con successo. Il volume complessivo di e-mail inviate ogni giorno in tutto il mondo continuerà ad aumentare di almeno il 5% ogni anno. Vista la capillare diffusione, la posta elettronica è un mezzo di comunicazione critico che le aziende devono proteggere.

L'uso della posta elettronica è in continuo aumento

Nonostante la proliferazione di soluzioni di messaggistica e dei social media, le comunicazioni tramite e-mail sono ancora in forte crescita. Secondo un recente studio condotto dal gruppo Radicati, il numero totale di e-mail inviate e ricevute nel mondo ha raggiunto i 205 miliardi al giorno e se ne prevede un aumento di almeno il 5% all'anno.[1] Uno sviluppo che di certo non sfugge ai criminali informatici, alla costante ricerca di opportunità di sfruttamento delle organizzazioni.

1 The Radicati Group, Inc., Email Statistics Report, 2015-2019

Analisi di un attacco e-mail:

- Un direttore amministrativo riceve un'e-mail dal CEO con cui viene autorizzato un trasferimento di fondi in emergenza, ma l'e-mail in realtà proviene da un criminale informatico.
- Un dipendente con diritti amministrativi per i sistemi chiave riceve un'e-mail urgente dal responsabile IT in cui gli si chiede di aggiornare la password di rete. Così facendo rivela la password ai pirati informatici.
- Un dipendente riceve un'e-mail in cui gli viene chiesto di leggere un allegato importante che riguarda un ente convenzionato. Aprendo l'allegato, attiva inconsapevolmente un trojan.

Le minacce e-mail per le aziende

Le e-mail rappresentano per gli hacker un veicolo con cui insidiare in vari modi le aziende. Tra le minacce più comuni veicolate via e-mail troviamo:

- **Ransomware** – Il ransomware è una variante di malware particolarmente dannosa. Appena l'allegato e-mail viene attivato, il codice si infiltra nella rete e il ransomware cripta o blocca file e sistemi di importanza cruciale. Gli hacker richiedono poi all'azienda il pagamento di un riscatto per decrittografare o sbloccare i file compromessi. L'e-mail è il mezzo preferito per distribuire ransomware attraverso allegati infettati o URL dannosi.
- **Spear Phishing / Whaling** – Questa variante di phishing, indirizzata a responsabili IT/di rete o altre figure chiave aziendali, sfrutta e-mail contenenti malware che apparentemente provengono da una fonte affidabile per ottenere l'accesso a dati e sistemi interni. Oltre il 90% degli attacchi informatici ha inizio con una campagna di phishing.[1]
- **Business Email Compromise / Truffa del CEO / E-mail fasulle** – Secondo le ultime cifre dell'FBI[2], negli ultimi anni le truffe perpetrate con le cosiddette Business Email Compromise (BEC) hanno causato perdite complessive per almeno 5,3 miliardi di dollari in circa 22 mila imprese in tutto il mondo. L'FBI definisce le truffe BEC come sofisticati raggiri messi in atto tramite messaggi e-mail, a danno di imprese che lavorano con partner esteri e che effettuano pagamenti periodici con bonifico bancario.
- **Phishing** – Questo sistema molto comune utilizza e-mail con link che rimandano a siti pirata. Quando gli utenti cliccano ingenuamente sui link o visitano questi siti, viene chiesto loro di inserire informazioni d'identificazione personale che vengono poi utilizzate per rubare identità, compromettere dati aziendali o accedere ad altri sistemi critici.
- **Malware** – L'e-mail è uno dei meccanismi più utilizzati per diffondere malware noti e ignoti, che generalmente vengono nascosti negli allegati nella speranza che questi ultimi vengano aperti o scaricati in un computer o una rete, consentendo così agli hacker di accedere a risorse, rubare dati o causare il blocco del sistema.
- **Spam** – La posta elettronica viene usata per recapitare spam, ossia messaggi indesiderati che possono intasare le caselle di posta in arrivo e le risorse di rete, riducendo la produttività aziendale e aumentando i costi operativi.
- **Hijacking / dirottamento di e-mail in uscita** – Le grandi aziende devono rispettare politiche aziendali e normative che addossano all'impresa stessa la responsabilità delle proprie e-mail in uscita e la protezione delle informazioni personali dei propri clienti. Gli attacchi zombie e il dirottamento IP possono causare la divulgazione incontrollata dei dati personali dei clienti, con gravi danni per la reputazione aziendale.

Conclusioni

Oggi le comunicazioni e-mail sono fondamentali per le aziende, e gli hacker lo sanno bene. Considerato il grado di sofisticazione degli attacchi mirati attuali, è indispensabile che le aziende adottino una soluzione di sicurezza multilivello che includa una protezione dedicata contro le minacce avanzate per i messaggi e-mail. Per contrastare efficacemente le minacce emergenti, le aziende dovrebbero implementare una soluzione di gestione della sicurezza e-mail di nuova generazione con funzioni di prevenzione delle violazioni in tempo reale.

Per scoprire come proteggere le e-mail della tua azienda, leggi il nostro documento Sicurezza e-mail di nuova generazione per bloccare le minacce avanzate.

1 www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
2 www.ic3.gov/media/2016/160614.aspx

Informazioni su SonicWall

Da oltre 25 anni SonicWall combatte il crimine informatico, proteggendo piccole, medie e grandi imprese in ogni parte del mondo. La nostra combinazione di prodotti e partner ha permesso di realizzare una soluzione di difesa informatica in tempo reale ottimizzata per le specifiche esigenze di oltre 500.000 aziende in più di 150 paesi, per consentire loro di fare più affari con maggior sicurezza.

Per eventuali domande in merito all'utilizzo potenziale del presente materiale, si prega di contattare:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Per maggiori informazioni, visitare il nostro sito web.
www.sonicwall.com