SONICWALL

SICUREZZA E-MAIL DI NUOVA GENERAZIONE PER BLOCCARE LE MINACCE AVANZATE

Abstract

Le attuali minacce avanzate richiedono l'uso di nuove funzionalità, oltre a quelle tradizionali, per la protezione della posta elettronica. Un approccio alla sicurezza su più livelli garantisce una protezione adeguata per le comunicazioni aziendali. Le aziende hanno bisogno di una soluzione di sicurezza e-mail di nuova generazione con capacità di prevenzione completa delle minacce.

La crescente importanza della sicurezza e-mail di nuova generazione

La posta elettronica è ormai divenuta il mezzo di diffusione più importante per una grande varietà di minacce informatiche, sia in entrata che in uscita, che si stanno rapidamente evolvendo da attacchi spam di massa ad aggressioni mirate estremamente sofisticate. La maggior parte di questi attacchi predilige l'e-mail come veicolo di trasmissione del payload. Secondo il Rapporto annuale sulle minacce redatto da SonicWall, l'uso di ransomware - che risulta il payload più utilizzato per le campagne di attacchi tramite e-mail - è cresciuto di 167 volte di anno in anno. Le soluzioni di sicurezza e-mail tradizionali non sono però equipaggiate per gestire minacce sofisticate come ransomware e attacchi zero-day. Oggi serve una soluzione di sicurezza e-mail di nuova generazione.

Funzionalità essenziali per la sicurezza e-mail di nuova generazione

Per garantire una prevenzione efficace delle violazioni, una soluzione di sicurezza e-mail di nuova generazione deve offrire le funzionalità seguenti:

Protezione contro le minacce avanzate

La maggior parte delle soluzioni antivirus è basata sulle firme e perciò risulta inefficace contro le minacce avanzate quali ransomware e malware ignoti. Questi tipi di malware sono mascherati in modo univoco e non sono rilevabili con le tecniche tradizionali. Per rilevare e prevenire i ransomware e gli attacchi zero-day ancora prima che raggiungano una rete è quindi necessario un ambiente sandbox.

Le soluzioni di sicurezza e-mail di nuova generazione devono offrire le funzionalità seguenti:

- Protezione multilivello completa delle comunicazioni e-mail
- Sandboxing e quarantena per i file sconosciuti
- Blacklist dinamiche basate sulle reputazioni
- Analisi avanzata dei contenuti e riconoscimento di pattern
- Crittografia avanzata e DLP per rispettare le politiche aziendali e le normative vigenti

Protezione contro le minacce conosciute

I criminali informatici realizzano una grande varietà di attacchi utilizzando malware noti. I database di firme antivirus rappresentano un modo semplice ed efficace per scansionare le e-mail dannose in arrivo ed evitare che i dipendenti trasmettano virus con i messaggi e-mail in uscita. Per aumentare l'efficacia consigliamo di utilizzare più motori di rilevamento antivirus per ispezionare i messaggi e gli allegati in cerca di virus, trojan, worm e altri contenuti dannosi.

Protezione contro il phishing

Le campagne di phishing sono diventate uno degli strumenti più diffusi per veicolare payload per gli attacchi ransomware. Una soluzione di sicurezza e-mail deve offrire funzioni di analisi avanzata dei contenuti in grado di esaminare qualsiasi oggetto, corpo e allegato delle e-mail e disporre di un ambiente sandbox per verificare gli allegati sospetti. Inoltre, deve conservare una blacklist dinamica di indirizzi IP aggiornata in tempo reale per filtrare le e-mail contenenti link dannosi.

Protezione contro le frodi

Gli hacker usano tattiche avanzate come lo spear phishing, il whaling e la cosiddetta "truffa del CEO" per richiedere informazioni d'identificazione personale o per attuare raggiri spacciandosi per un altro mittente e inviando e-mail che sembrano autentiche. Per impedire che questi messaggi illeciti raggiungano la rete aziendale è necessaria una configurazione granulare delle impostazioni e-mail. Le configurazioni di posta elettronica come SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) e DMARC (Domain-based Message Authentication, Reporting and Conformance), assieme al riconoscimento di pattern e all'analisi dei contenuti, consentono una convalida efficace di tutti i messaggi in arrivo.

Protezione antispam

I messaggi di spam possono intasare le caselle della posta in arrivo e impegnare inutilmente le risorse di rete, causando notevoli perdite di tempo e un aumento dei costi operativi per le aziende. Una soluzione di protezione della posta elettronica dovrebbe utilizzare diversi metodi per rilevare lo spam e altri messaggi indesiderati, come ad esempio elenchi di blocco/autorizzazione per persone, mailing list e domini specifici, oppure modelli creati analizzando ciò che altri utenti contrassegnano come posta indesiderata, con la possibilità di abilitare elenchi di blocco di terzi.

Prevenzione della perdita dei dati

Le comunicazioni più sensibili e delicate di un'organizzazione richiedono la massima protezione. Il sistema migliore consiste nel crittografare le e-mail e gli allegati sensibili. Un servizio di crittografia deve operare all'unisono con la soluzione di sicurezza e-mail per proteggere tutti i messaggi di posta elettronica.

Conclusioni

Le soluzioni di sicurezza e-mail tradizionali utilizzano meccanismi di rilevamento statici basati sulle firme e sulla reputazione IP, che non sono in grado di proteggere efficacemente dai sofisticati malware evasivi di oggi. Il semplice rilevamento non è sufficiente, in quanto le notifiche non permettono di prevenire un attacco in corso. Le soluzioni per la sicurezza della posta elettronica devono evolversi da un approccio di semplice rilevamento alla prevenzione vera e propria, con la capacità di bloccare gli attacchi ancora prima che raggiungano la propria rete.

Le soluzioni di sicurezza e-mail di nuova generazione di SonicWall adottano un approccio di difesa su più livelli con la premiata tecnologia di sandboxing Capture ATP. Le eccellenti funzioni di prevenzione delle violazioni di Capture ATP proteggono dalle minacce avanzate provenienti dalle e-mail. Capture ATP offre inoltre funzionalità anti-phishing, anti-spoofing e anti-spam di livello superiore, un antivirus multi-engine e la prevenzione della perdita dei dati (DLP), garantendo una protezione completa.

Per saperne di più, visita www.sonicwall.com/products/email-security-appliance.

© 2017 SonicWall Inc. TUTTI I DIRITTI RISERVATI.

SonicWall è un marchio o marchio registrato di SonicWall Inc. e/o delle sue affiliate negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi e marchi registrati appartengono ai rispettivi proprietari.

Le informazioni contenute nel presente documento si riferiscono ai prodotti di SonicWall Inc. e/o delle sue affiliate. Né il presente documento né la vendita di prodotti SonicWall costituiscono alcuna licenza, espressa o implicita, di estoppel o di altro tipo, né garantiscono diritti di proprietà intellettuale. SALVO QUANTO SPECIFICATO NEI TERMINI E NELLE CONDIZIONI STABILITI NEL CONTRATTO DI LICENZA DI QUESTO PRODOTTO, SONICWALL E/O LE SUE AFFILIATE NON SI ASSUMONO ALCUNA RESPONSABILITÀ ED ESCLUDONO GARANZIE DI QUALSIASI TIPO, ESPLICITE, IMPLICITE O LEGALI, IN RELAZIONE AI PROPRI PRODOTTI, INCLUSE, IN VIA ESEMPLIFICATIVA, QUALSIASI GARANZIA IMPLICITA DI COMMERCIABILITÀ, IDONEITÀ A SCOPI SPECIFICI O VIOLAZIONE DI DIRITTI ALTRUI. SONICWALL E/O LE SUE AFFILIATE DECLINANO OGNI RESPONSABILITÀ PER DANNI DI QUALUNQUE TIPO, SIANO ESSI DIRETTI, INDIRETTI, CONSEQUENZIALI, PUNITIVI, SPECIALI O INCIDENTALI (INCLUSI, SENZA LIMITAZIONI, DANNI PER MANCATO GUADAGNO, INTERRUZIONI DELL'ATTIVITÀ O PERDITE DI DATI) DERIVANTI DALL'UTILIZZO O DALL'IMPOSSIBILITÀ DI UTILIZZARE IL PRESENTE DOCUMENTO, ANCHE NEL CASO IN CUI SONICWALL E/O LE SUE AFFILIATE SIANO STATE AVVERTITE DELL'EVENTUALITÀ DI TALI DANNI. SonicWall e/o le sue affiliate non rilasciano alcuna garanzia o dichiarazione relativamente alla precisione o completezza dei contenuti del presente documento e si riserva il diritto di apportare modifiche, in qualsiasi momento e senza preavviso, alle specifiche e alle descrizioni dei prodotti. SonicWall Inc. e/o le sue affiliate non si assumono alcun impegno di aggiornare le informazioni contenute in questo documento.

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 internazionali in più di 150 paesi, per consentire loro di fare più affari con maggior sicurezza.

Per qualsiasi domanda sul possibile utilizzo di questo materiale, contattare:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com