SONICWALL®

OTTO MODI PER PROTEGGERE LA TUA RETE DAL RANSOMWARE

Gli interventi per evitare attacchi ransomware e risparmiare denaro

A volte il passato torna di moda. È il caso degli attacchi ransomware, che sono nuovamente popolari. Uscito per la prima volta nel 1989, il ransomware infetta un sistema e «chiude fuori» l'utente impedendogli di accedere al dispositivo o ai file su di esso. Solo se la vittima accetta di pagare un riscatto, solitamente sotto forma di bitcoin, è possibile sbloccare il sistema e accedervi nuovamente.

Il seguente e-book propone otto modi per proteggere la vostra rete dagli attacchi ransomware ed evitare di dare denaro ai criminali informatici.

L'ammontare del riscatto può variare, ma spesso è compreso fra $200 e $400.[1]

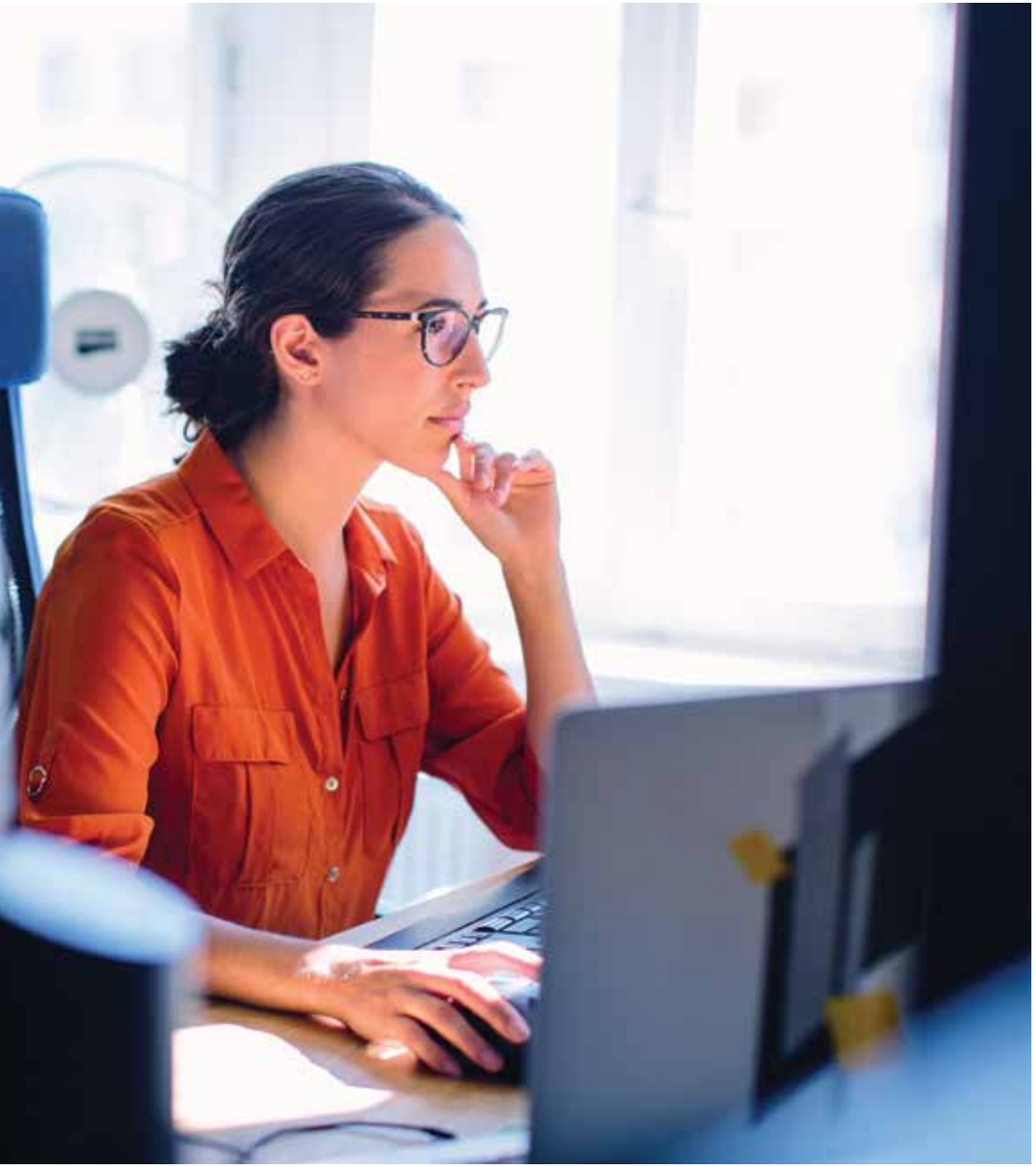
1. Educate i vostri dipendenti

L'educazione e la consapevolezza dell'utente sono fondamentali quando si tratta di sconfiggere il ransomware. Trattate le e-mail sospette con attenzione. Controllate il nome di dominio che ha inviato l'e-mail. Cercate eventuali errori di ortografia, verificate la firma e la legittimità della richiesta. Passate il puntatore del mouse sui link per verificare la loro destinazione.

2. Utilizzate un approccio multi-livello alla sicurezza di rete

La protezione dal ransomware e da altre forme di malware non si limita al livello del gateway. È fondamentale estendere la sicurezza attraverso l'uso di antivirus, anti-spyware, prevenzione delle intrusioni e altre tecnologie su dispositivi sul perimetro della rete. Adottate un approccio a strati per fermare il ransomware evitando un singolo «point of failure» nella vostra architettura di sicurezza.

1 US Computer Emergency Readiness Team Alert (TA16-091A)



3. Eseguite backup regolari dei vostri file

Un'altra protezione per evitare di dover pagare un riscatto è un'affidabile strategia di backup e ripristino. A seconda della velocità di rilevamento della compromissione, dell'ampiezza di diffusione e del livello di perdita di dati accettabile, il ripristino da un backup potrebbe essere un'opzione valida. Tuttavia, questa soluzione richiede una strategia di backup più intelligente, che sia allineata al livello di criticità dei dati e dei bisogni della vostra attività in termini di Recovery point objective (RPO) e Recovery time objective (RTO).

4. Assicuratevi che i vostri endpoint siano protetti

Poiché la maggior parte degli utenti interagisce principalmente con dispositivi personali e aziendali, gli endpoint sono particolarmente esposti al rischio, nel caso in cui non siano gestiti o non dispongano della giusta protezione anti-malware. La maggior parte delle soluzioni antivirus si basano su firme e si dimostrano inefficaci se non aggiornate regolarmente. Le più recenti varianti di ransomware presentano hashing di tipo esclusivo e, pertanto, non sono rilevabili utilizzando tecniche basate su firme. Molti utenti, inoltre, disattivano le scansioni antivirus per non rallentare il loro sistema.

Implementate una strategia di sicurezza a strati per una maggiore protezione della rete.

5. Applicate le patch a sistemi e applicazioni

Molti attacchi si basano su vulnerabilità note presenti nei browser, tra cui Internet Explorer, e in comuni app e plug-in. Pertanto è fondamentale applicare gli aggiornamenti e le patch in modo rapido e affidabile. Scegliere una soluzione in grado di automatizzare l'applicazione di patch e upgrade delle versioni in un ambiente eterogeneo in termini di dispositivi, SO e applicazioni contribuisce in maniera determinante ad affrontare una vasta gamma di minacce informatiche, incluso il ransomware.

6. Segmentate la vostra rete per arrestare la diffusione

La maggior parte dei ransomware tenta di diffondersi dall'endpoint al server/storage, dove risiedono tutti i dati e tutte le applicazioni fondamentali per l'azienda. La segmentazione della rete e l'isolamento di applicazioni e dispositivi critici su una rete separata o su una LAN virtuale possono limitare la diffusione.

7. Mettete in quarantena e analizzate i file sospetti

Tecnologie come il sandboxing offrono la possibilità di spostare i file sospetti in quarantena per analizzarli prima che possano entrare nella rete. I file vengono trattenuti al gateway fino all'emissione di un verdetto. Se un file viene riconosciuto come maligno, è possibile prevenire attacchi successivi implementando misure protettive come policy che blocchino gli indirizzi IP o i domini associati oppure consegnando firme alle appliance di sicurezza su tutta la rete.

Segmentate la vostra LAN wireless per separare gli utenti interni dagli ospiti per un ulteriore livello di sicurezza.

8. Proteggete i vostri dispositivi Android

I dispositivi con sistema operativo Google Android sono diventati le vittime predilette per gli attacchi ransomware. Adottate i seguenti interventi per proteggere il vostro smartphone Android:

- Non eseguite il rooting del dispositivo, in quanto espone i file di sistema a modifiche
- Installate sempre le app da Google Play; le app da siti/negozi sconosciuti possono essere fasulle o maligne
- Disabilitare l'installazione di app provenienti da fonti sconosciute
- Consentire a Google di eseguire la scansione del dispositivo per rilevare eventuali minacce
- Fate attenzione quando aprite link sconosciuti ricevuti tramite SMS o e-mail
- Installare applicazioni di sicurezza di terzi che effettuano la scansione periodica del dispositivo alla ricerca di contenuti dannosi
- Tenete sotto controllo le app registrate come Amministratori dispositivo
- Per i dispositivi aziendali create una blacklist di app non consentite

Il malware per gli ecosistemi Android ha continuato a crescere nel 2015, mettendo a rischio quasi l'85 percento degli smartphone.

Conclusione

Gli attacchi ransomware sono sempre più popolari tra i criminali informatici. Assicuratevi che la vostra rete sia protetta. SonicWall può migliorare la protezione in tutta la vostra azienda attraverso l'ispezione di ogni pacchetto e mediante il controllo di ogni identità. Il risultato è la protezione dei vostri dati ovunque si trovino, condividendo informazioni utili per la difesa da una gran varietà di minacce, incluso il ransomware.

Visita la pagina web con i prodotti per la sicurezza della rete di SonicWall.

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

Ebook-8waysRansomware-EU-IMAG-29271-D1

SONICWALL®