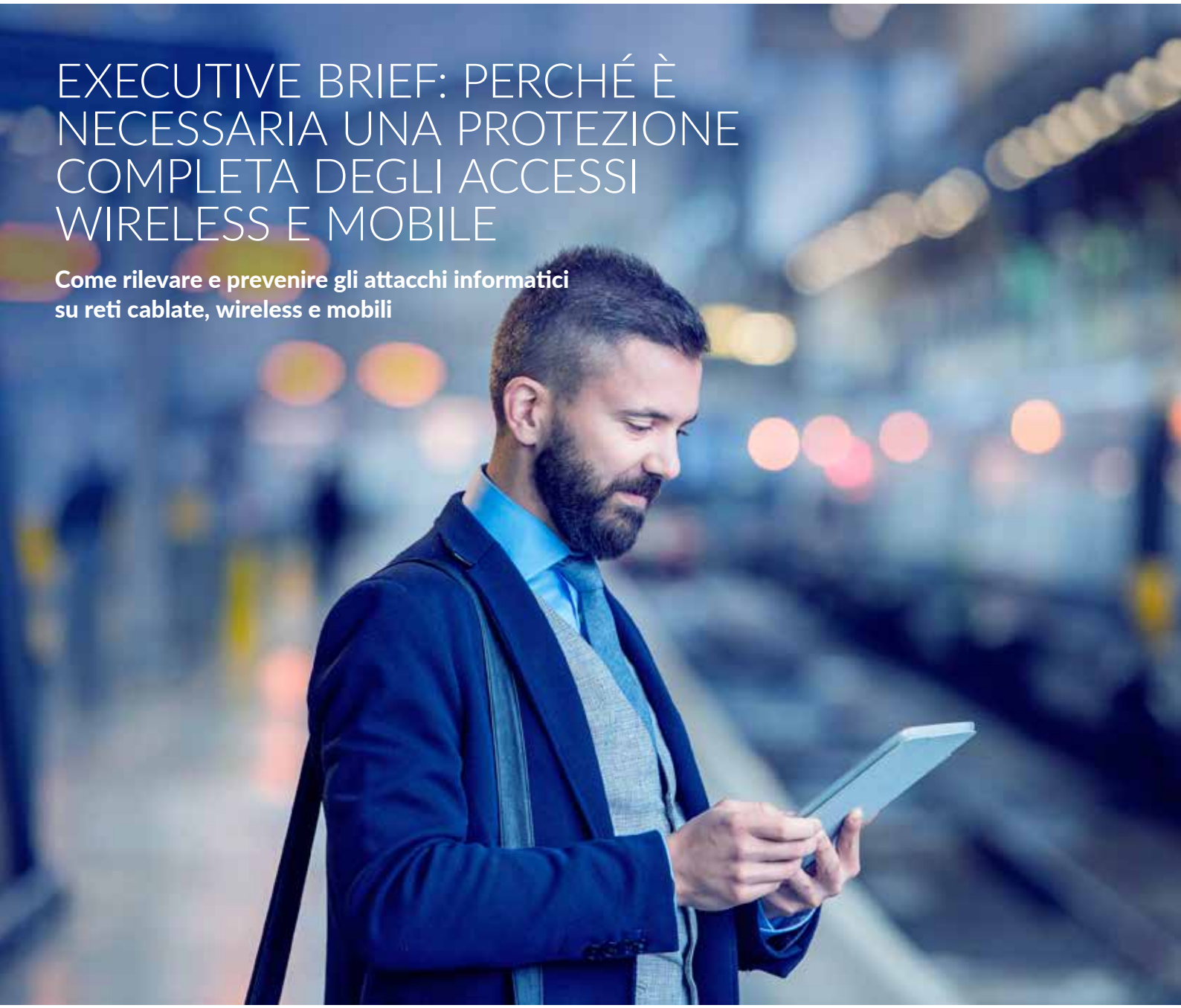
SONICWALL

EXECUTIVE BRIEF: PERCHÉ È NECESSARIA UNA PROTEZIONE COMPLETA DEGLI ACCESSI WIRELESS E MOBILE

Come rilevare e prevenire gli attacchi informatici su reti cablate, wireless e mobili



Abstract

Oggi le organizzazioni devono fornire al proprio personale un accesso ad alta velocità alle risorse su reti cablate, wireless e mobili.
Tuttavia, i criminali informatici sfruttano ciascuno di questi vettori per dare il via ad attacchi avanzati, con minacce crittografate e attacchi zero-day. Inoltre, le organizzazioni possono perdere il controllo dei dati in ambienti per team in remoto che utilizzano reti wireless e mobili in connessione con servizi sul cloud.
L'interruzione dell'accesso porta a una perdita di produttività, alla crescita dello Shadow IT e alla creazione di lacune nell'approccio alla sicurezza di un'organizzazione.

Accesso alle risorse da ogni luogo

I lavoratori di oggi sono sempre in movimento e hanno bisogno di poter accedere 24 su 24 e ogni giorno della settimana alle risorse aziendali utilizzando il dispositivo da loro scelto ovunque si trovino. Inoltre, le organizzazioni stanno adottando iniziative per BYOD, IoT, mobilità e cloud. Per rimanere competitive, le organizzazioni devono fornire accesso alle risorse in modo trasparente su reti cablate, reti wireless e reti mobili. Le reti cablate si stanno evolvendo verso 2.5G, 5G e 10G, ma non sono soltanto i dispositivi cablati a connettersi alla rete: gli endpoint sono variegati e includono desktop e laptop, nonché tablet e smartphone. Inoltre, con il crescente numero di endpoint

> L'accesso non deve essere soltanto disponibile in qualunque luogo, in qualunque momento e su qualunque dispositivo, ma deve anche essere veloce e sicuro.

BYOD e Internet of Things (IoT), sempre più dispositivi si connettono alla rete aziendale.

Le organizzazioni si affidano sempre più spesso alla connettività wireless ad alta velocità all'interno dei loro ambienti e il personale mobile e operante in remoto si collega tramite VPN da abitazioni, sedi distaccate, uffici in work-sharing, aeroporti, hotel o bar. Ne deriva che i dipendenti iniziano ad aspettarsi di ottenere la stessa esperienza utente e lo stesso accesso ad alte prestazioni non soltanto su reti cablate, ma anche su tutte le connessioni wireless e mobili che utilizzano. Quando i dipendenti sono in trasferta, essi richiedono la possibilità di accedere alle stesse applicazioni aziendali di cui dispongono quando sono connessi alle reti cablate in ufficio.

Gli attacchi informatici sfruttano reti cablate, wireless e mobili

Sebbene accesso e connettività ad alta velocità da qualunque luogo siano importanti tanto per gli utenti quanto per le organizzazioni, stesso vale per la sicurezza dei dati che viaggiano sulla rete. In definitiva, le organizzazioni devono estendere funzionalità complete di sicurezza per il rilevamento e la prevenzione delle violazioni in modo trasparente su reti cablate, wireless e mobili.

Su qualsiasi piattaforma di rete, una delle principali sfide da affrontare nel combattere gli attacchi informatici è il fatto che ora la maggior parte del minacce sono crittografate. La tendenza verso la crittografia TLS/SSL è in crescita già da diversi anni. Con l'aumentare del traffico sul Web, lo stesso ha fatto la crittografia, passando da 5,3 bilioni di connessioni Web nel 2015 a 7,3 bilioni nel 2016, secondo la SonicWall Capture Threat Network. La maggior parte delle sessioni Web rilevate dalla Capture Threat Network nel corso dell'anno era crittografata in TLS/SSL, totalizzando il 62% del traffico Web. Questo numero continuerà ad aumentare con il crescente utilizzo della crittografia da parte dei siti Web per proteggere le connessioni al loro sito.

Inoltre, sono in aumento anche minacce avanzate come gli exploit zero-day e il malware personalizzato. Organizzazioni di ogni dimensione sono l'obiettivo dei criminali informatici che cercano, trovano e sfruttano continuamente le falle nei software vulnerabili. Il loro obiettivo è ottenere l'accesso a reti, sistemi e dati, spesso causando gravi danni nel giro di pochi minuti. Per migliorare il rilevamento di queste minacce sconosciute, i professionisti della sicurezza implementano attualmente tecnologie di rilevamento delle minacce avanzate come le sandbox virtuali, che analizzano il comportamento dei file sospetti e portano allo scoperto il malware nascosto. Tuttavia, anche le minacce si stanno facendo più intelligenti. Oggi il malware è progettato per rilevare la presenza di sandbox virtuali e riuscire a eluderle. Gli odierni ambienti di sandbox devono essere completi e dinamici al pari delle minacce che tentano di prevenire. Oggi è indispensabile essere in grado di decodificare, scansionare e chiudere in sandbox i file sospetti in tutto il traffico nel suo complesso, a prescindere che sia su reti cablate, wireless o mobili.

Collaborazione con i team in remoto

Inoltre, le organizzazioni possono perdere il controllo dei dati in ambienti per team in remoto che utilizzano reti wireless e mobili in connessione con servizi sul cloud. Molte organizzazioni dispongono di team operanti in remoto che necessitano di utilizzare strumenti collaborativi come SharePoint o Dropbox per condividere file e lavorare insieme. Anche le collaborazioni a progetto coinvolgono solitamente degli interessati esterni, come contratti con terze parti o partner. Ad esempio, gli istituti di istruzione elementare, inferiore e superiore forniscono a studenti e personale docente l'accesso a Internet wireless per connettersi e collaborare con altre persone in locale e in tutto il mondo.

Ne deriva che sulle reti mobili e wireless vengono continuamente caricati o condivisi file utilizzando laptop e smartphone personali (non gestiti). Ogni volta che si offre la possibilità di condividere dei file, esiste il rischio che venga caricato del malware. Tuttavia, quando i reparti informatici intervengono con policy di condivisione file restrittive per motivi di sicurezza, gli utenti finali iniziano a utilizzare account di condivisione file personali, come Google Drive, per trasferire i file e collaborare. Questi file bypassano i firewall di rete quando gli utenti accedono alla rete aziendale utilizzando un accesso completo tramite VPN. Inoltre, le organizzazioni perdono il controllo dei dati quando questi escono dal perimetro di sicurezza attraverso servizi di cloud pubblici come Google Drive, tramite e-mail o USB. Si tratta di un elevato rischio per la sicurezza e la conformità per le organizzazioni.

Prestazioni di rete e produttività del personale

L'accesso non deve essere soltanto disponibile in qualunque luogo, in qualunque momento e su qualunque dispositivo, ma deve anche essere veloce e sicuro. La sicurezza necessaria per proteggere dalle moderne minacce informatiche può avere potenzialmente un impatto sulla produttività del personale, aumentare le spese generali per l'IT e, in definitiva, aumentare il costo totale di proprietà per un'organizzazione.

Il crescente volume di traffico incide esso stesso sulla larghezza di banda disponibile e sulle prestazioni di rete. Il numero di dispositivi con abilitazione Wi-Fi, sia di tipo personale sia forniti

dall'IT, continua ad aumentare al crescere dell'uso e dell'importanza della mobilità. Secondo Gartner, quasi 1,5 miliardi di soli smartphone sono stati consegnati nel 2016.[1] Entro la fine dello stesso anno, la Wi-Fi Alliance aveva previsto che le consegne di dispositivi Wi-Fi superassero i 15 miliardi di dispositivi.[2] Abbinato all'aumento dei dispositivi Wi-Fi è l'utilizzo di applicazioni a elevato consumo di larghezza di banda come la multimedialità in HD e le app su cloud e dispositivi mobili.

La crescita dell'IoT ha alimentato un aumento nel numero di dispositivi wireless in grado di far girare applicazioni ad elevato consumo di larghezza di banda. L'utilizzo di applicazioni video e collaborative, come Microsoft Lync, SharePoint e WebEx, richiede grandi quantità di larghezza di banda disponibile per funzionare in modo ottimale. Inoltre, il cloud computing può comportare il trasferimento di grandi file di dati sulla rete wireless, occupando completamente la preziosa larghezza di banda.

L'aumento del numero di dispositivi ha creato inoltre un ambiente in cui i segnali wireless interferiscono spesso fra loro a causa del gran numero di dispositivi che condividono la stessa rete. Questa situazione riguarda ogni tipo di dispositivo: laptop, smartphone, tablet e access point, ma anche microonde, dispositivi Bluetooth e molto altro ancora. Le conseguenti scarse prestazioni si riscontrano nei settori verticali tra cui l'assistenza sanitaria, l'istruzione, gli aeroporti e i centri commerciali. Un'altra funzionalità che gli utenti si attendono è il wireless in ambienti esterni, come stadi, campus, cantieri, parchi industriali e altri spazi aperti, dove il segnale può subire l'influsso dell'ambiente fisico, come gli alberi e altri edifici.

Gli stessi servizi di sicurezza incidono sulle prestazioni della rete. La capacità di decodificare e scansionare il traffico crittografato alla ricerca di minacce con una latenza ridotta o assente è fondamentale, in quanto qualunque ritardo rallenta il flusso dei dati attraverso la rete. Decodificare e scansionare potenzialmente migliaia di connessioni Web crittografate simultaneamente alla ricerca di minacce può richiedere un'elevata potenza di calcolo. I firewall tradizionali potrebbero decodificare il traffico ed eseguire un certo grado di rilevamento delle minacce, ma non prevenirle. In alternativa, potrebbero svolgere tutte le funzioni richieste, ma molto lentamente a causa di scarse prestazioni. Alcune organizzazioni hanno addirittura scelto di disattivare dei servizi firewall fondamentali per mantenere le prestazioni.

Tutti questi fattori sono alla base dell'esigenza delle organizzazioni di fornire a clienti, dipendenti e studenti un'esperienza potenziata su diverse piattaforme. L'ultima arrivata fra le tecnologie wireless ad alta velocità, la 802.11ac Wave 2, offre un throughput wireless multi-gigabit. Tuttavia, per mettere in pratica questo potenziale prestazionale, sia l'access point sia i dispositivi che si connettono devono supportare lo standard wireless 802.11ac Wave 2. Inoltre, per abilitare il livello richiesto di throughput wireless, la maggior parte dei firewall deve utilizzare una porta 5 GbE o 10 GbE retrocompatibile, la cui capacità è di gran lunga superiore a quella richiesta, oppure aggiungere uno switch che fa aumentare i costi.

A complicare ulteriormente il discorso delle prestazioni e della sicurezza, la maggior parte delle organizzazioni dispone di una miscela di applicazioni sul posto e sul cloud, andando a creare un ambiente IT ibrido. Il reparto IT viene sovraccaricaricato dalla gestione di più directory utente per applicazioni distribuite nei data center locali e per applicazioni cloud SaaS di terze parti. Queste directory devono essere aggiornate costantemente per assicurarsi che le persone giuste abbiano l'accesso giusto alle applicazioni giuste al momento giusto. Gli utenti sono quindi obbligati a conservare e ricordare più URL e password con la conseguenza di cattive pratiche di sicurezza. Qualsiasi interruzione dell'accesso porta a una perdita di produttività, alla crescita dello Shadow IT e alla creazione di lacune nell'approccio alla sicurezza di un'organizzazione.

Conclusione

Per saperne di più. Scoprite come fornire rilevamento e prevenzione delle violazioni sulle vostre reti cablate, wireless e mobili. Leggete il nostro Brief sulle soluzioni Best practice per proteggere l'accesso a reti cablate, wireless e mobili e visitate il nostro sito Wireless e Mobilità.

[1] *http://www.gartner.com/newsroom/id/3609817*
[2] *http://www.wi-fi.org/news-events/newsroom/wi-fi-device-shipments-to-surpass-15-billion-by-end-of-2016*

Informazioni su SonicWall

Da oltre 25 anni, SonicWall è un fidato partner per la sicurezza nel settore. Dalla sicurezza di rete alla sicurezza degli accessi, fino alla protezione e-mail, SonicWall ha sviluppato continuamente la sua gamma di prodotti, consentendo alle organizzazioni di innovare, accelerare e crescere. Con oltre un milione di dispositivi di sicurezza in quasi 200 paesi e territori in tutto il mondo, SonicWall permette ai suoi clienti di guardare positivamente al futuro.

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

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

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

ExecBrief-NS-WhyYouNeed-US-IMAG-29144