SONICWALL

KURZDARSTELLUNG: WARUM EINE UMFASSENDE SICHERHEIT BEIM DRAHTLOSEN UND MOBILEN ZUGRIFF ESSENZIELL IST

Erkennen und verhindern Sie Cyberangriffe auf kabelgebundene, drahtlose und mobile Netzwerke

Zusammenfassung

Heutzutage müssen Organisationen ihren Mitarbeitern einen ultraschnellen Zugriff auf Ressourcen über kabelgebundene, drahtlose und mobile Netzwerke hinweg zur Verfügung stellen. Das Problem dabei: Cyberkriminelle nutzen diese unterschiedlichen Vektoren, um ausgeklügelte Angriffe – z. B. verschlüsselte und Zero-Day-Angriffe – zu starten. Auch in Umgebungen mit geografisch verteilten Mitarbeitern, die drahtlose und mobile Netzwerke für Cloud-Services nutzen, können Organisationen schnell die Kontrolle über die Daten verlieren. Unterbrechungen beim Zugriff führen zu Produktivitätsverlusten und Lücken im Sicherheitskonzept der Organisation und begünstigen darüber hinaus die Schatten-IT.

Zugriff auf Ressourcen von jedem beliebigen Ort aus

Mitarbeiter sind heute ständig unterwegs. Sie benötigen rund um die Uhr einen Zugriff auf Unternehmensressourcen über das Gerät ihrer Wahl und von jedem beliebigen Standort aus. Immer mehr Organisationen setzen außerdem auf BYOD-, IoT-, Mobility- und Cloud-Initiativen. Um wettbewerbsfähig zu bleiben, müssen sie ihren Mitarbeitern einen nahtlosen Zugriff auf Ressourcen über kabelgebundene, drahtlose und mobile Netzwerke ermöglichen. Kabelgebundene Netzwerke sind gerade dabei, sich zu 2,5G-, 5G- und 10G-Netze weiterzuentwickeln. Aber nicht nur kabelgebundene Geräte sind an das Netzwerk angeschlossen. Es gibt verschiedene Endpunkte, angefangen bei Desktop-PCs und Laptops bis hin zu Tablets und Smartphones.

> Der Zugriff muss nicht nur überall, jederzeit und auf jedem beliebigen Gerät funktionieren – er muss darüber hinaus auch schnell und sicher sein.

Und mit der wachsenden Zahl der BYOD- und Internet-of-Things(IoT)-Endpunkte sind mehr Geräte als je zuvor mit dem Unternehmensnetzwerk verbunden.

Viele Organisationen setzen zunehmend auf eine drahtlose Highspeed-Verbindung für Ihre Standorte. Mobile und Remote-Mitarbeiter stellen über VPNs von zu Hause, Zweigniederlassungen, Bürogemeinschaften, Flughäfen, Hotels oder Cafés aus eine Verbindung zum Unternehmensnetz her. Mittlerweile erwarten Mitarbeiter denselben effizienten Zugriff und dieselbe Benutzererfahrung, die kabelgebundene Netzwerke bieten, auch bei ihren drahtlosen und mobilen Verbindungen. Wenn Mitarbeiter unterwegs sind, müssen sie auf dieselben Geschäftsapplikationen zugreifen können, die sie auch im Büro über kabelgebundene Netzwerke verwenden.

Cyberangriffe nutzen kabelgebundene, drahtlose und mobile Netzwerke

Der Zugriff auf Highspeed-Verbindungen von jedem beliebigen Ort aus ist für User und Organisationen gleichermaßen wichtig. Genauso entscheidend ist jedoch die Sicherheit der Daten, die im Netzwerk übertragen werden. Organisationen müssen umfassende Sicherheitsfunktionen zur Erkennung und Prävention von Sicherheitslücken nahtlos über kabelgebundene, drahtlose und mobile Netzwerke hinweg bereitstellen.

Egal um welche Netzwerkplattform es sich handelt – eine der größten Herausforderungen im Kampf gegen Cyberangriffe liegt darin, dass die meisten Bedrohungen mittlerweile verschlüsselt sind. Die TLS-/SSL-Verschlüsselung gewinnt schon seit mehreren Jahren zunehmend an Bedeutung. Nicht nur der Webverkehr hat zugenommen, sondern auch die Verschlüsselung: laut dem SonicWall Capture Threat Network von 5,3 Billionen Webverbindungen im Jahr 2015 auf 7,3 Billionen im Jahr 2016. Der Großteil der Websitzungen, die das Capture Threat Network im Laufe des Jahres identifizierte, war TLS-/SSL-verschlüsselt, darunter 62 Prozent des Webverkehrs. Diese Zahl wird noch weiter wachsen, da immer mehr Websites Verschlüsselungstechnologien nutzen, um ihre Verbindungen zu schützen.

Hinzu kommt, dass hoch entwickelte Bedrohungen wie Zero-Day-Exploits und maßgeschneiderte Malware weiterhin auf dem Vormarsch sind. Cyberkriminelle suchen kontinuierlich nach anfälliger Software, um Schwachstellen in großen und kleinen Organisationen auszunutzen. Auf diese Weise verschaffen sie sich Zugriff auf Netzwerke, Systeme und Daten und können innerhalb weniger Minuten großen Schaden anrichten. Um diese unbekannten Bedrohungen besser zu identifizieren, nutzen Sicherheitsexperten hoch entwickelte Threat-Detection-Technologien wie z. B. virtuelle Sandboxen, die das Verhalten verdächtiger Dateien analysieren und versteckte Malware aufdecken. Doch auch Bedrohungen werden immer intelligenter. Malware wird mittlerweile so konzipiert, dass sie virtuelle Sandboxen aufspüren und umgehen kann. Daher müssen moderne Sandbox-Umgebungen so hoch entwickelt und dynamisch sein wie die Bedrohungen selbst, die sie stoppen sollen. Heute ist es unglaublich wichtig, verdächtige Dateien im gesamten Datenverkehr – egal ob über kabelgebundene, drahtlose oder mobile Netzwerke – zu entschlüsseln, zu durchleuchten und in einer Sandbox zu analysieren.

Zusammenarbeit bei geografisch verteilten Mitarbeitern

Auch in Umgebungen mit geografisch verteilten Mitarbeitern, die drahtlose und mobile Netzwerke für Cloud-Services nutzen, können Organisationen schnell die Kontrolle über die Daten verlieren. In vielen Organisationen gibt es Remote-Mitarbeiter, die auf Kollaborationstools wie SharePoint oder Dropbox angewiesen sind, um Dateien auszutauschen und mit anderen zusammenzuarbeiten. Bei gemeinsamen Projekten sind in der Regel auch externe Stakeholder wie Lieferanten oder Partner beteiligt. Beispielsweise bieten sowohl Schulen als auch Hochschuleinrichtungen ihren Schülern und Studenten sowie Lehrern und Professoren einen drahtlosen Internetzugang, um mit anderen Usern lokal oder weltweit zusammenzuarbeiten.

Folglich werden Dateien ständig mittels privater (unverwalteter) Laptops und Smartphones über mobile und drahtlose Netzwerke hochgeladen oder ausgetauscht. Wo auch immer Sie die Möglichkeit zum Datenaustausch bieten, besteht das Risiko, dass Malware hochgeladen wird. Wenn die IT aber aus Sicherheitsgründen mit restriktiven Filesharing-Regeln durchgreift, verwenden die Endbenutzer einfach private Filesharing-Accounts wie Google Drive, um Dateien zu übertragen und mit anderen Usern zusammenzuarbeiten. Diese Dateien umgehen die Netzwerkfirewalls, wenn Remote-Nutzer über einen vollständigen VPN-Zugang auf das Unternehmensnetzwerk zugreifen. Organisationen verlieren die Kontrolle über ihre Daten auch, wenn diese die Sicherheitsgrenze über Public-Cloud-Services wie Google Drive, E-Mails oder USB-Sticks verlassen – ein hohes Risiko im Hinblick auf Sicherheit und Compliance.

Netzwerkperformance und Mitarbeiterproduktivität

Der Zugriff muss nicht nur überall, jederzeit und auf jedem beliebigen Gerät funktionieren – er muss darüber hinaus auch schnell und sicher sein. Viele Sicherheitsfunktionen zur Bekämpfung moderner Cyberbedrohungen können die Mitarbeiterproduktivität beeinträchtigen, den Aufwand für die IT steigern und letzten Endes die Total Cost of Ownership für die Organisation erhöhen.

Schon allein die wachsende Menge des Datenverkehrs beeinträchtigt die Bandbreite und die Netzwerkleistung. Mit der zunehmenden Bedeutung und Verbreitung von Mobilitätslösungen steigt auch die Zahl WLAN-fähiger Geräte – ob privat oder von der IT betreut – kontinuierlich an. Gartner zufolge wurden allein 2016 knapp 1,5 Milliarden Smartphones verkauft.[1] Die Wi-Fi Alliance sagte voraus, dass der Verkauf WLAN-fähiger Geräte bis Ende desselben Jahres die 15-Milliarden-Marke übersteigen werde.[2] Mit der wachsenden Zahl der WLAN-Geräte steigt auch die Nutzung bandbreitenintensiver Anwendungen wie HD-Multimedia- sowie Cloud- und mobiler Apps.

Mit dem Vormarsch des IoT stieg auch die Zahl drahtloser Geräte, auf denen bandbreitenintensive Anwendungen laufen können. Video- und Kollaborationsanwendungen wie Microsoft Lync, SharePoint und WebEx brauchen enorm viel Bandbreite, um optimal zu laufen. Hinzu kommt, dass beim Cloud-Computing auch große Datendateien im Drahtlosnetzwerk übertragen werden, was zusätzlich wertvolle Bandbreite verbraucht.

Mit der wachsenden Anzahl an Geräten kommt es außerdem häufig zu einer gegenseitigen Störung von Funksignalen, weil so viele Geräte sich dasselbe Netzwerk teilen, angefangen bei Laptops, Smartphones, Tablets und Access-Points bis hin zu Mikrowellen, Bluetooth-Geräten usw. Mit der daraus resultierenden schlechten Performance haben Organisationen aus unterschiedlichen Bereichen zu kämpfen, z. B. Healthcare-Firmen, Bildungseinrichtungen, Flughäfen oder Einkaufszentren. WLAN im Freien ist mittlerweile auch in Stadien, (Hoch-)Schulgeländen, Baustellen, Gewerbegebieten und anderen Freigeländen üblich – alles Umgebungen, in denen das Signal durch die physischen Gegebenheiten beeinträchtigt werden kann (z. B. durch Bäume und andere Gebäude).

Auch die Sicherheitsdienste selbst können die Netzwerkperformance beeinträchtigen. Es ist wichtig, dass bei der Entschlüsselung von verschlüsseltem Datenverkehr und der Prüfung auf Bedrohungen geringe bzw. gar keine Latenzzeiten entstehen, da Verzögerungen den Datenfluss im Netzwerk verlangsamen. Die Entschlüsselung und gleichzeitige Prüfung Tausender verschlüsselter Webverbindungen auf Bedrohungen kann sehr rechenintensiv sein. Ältere Firewalls sind vielleicht in der Lage, den Verkehr zu entschlüsseln und einige Bedrohungen zu erkennen, doch sie können diese nicht abwehren. Oder sie bieten alles, was nötig wäre, sind dabei aber zu langsam, weil die Leistung nicht stimmt. Viele Unternehmen schalten sogar wichtige Firewalldienste aus, um keine Performance zu verlieren.

Organisationen müssen also einen Weg finden, Kunden, Mitarbeitern sowie Schülern und Studenten eine optimale Benutzererfahrung über alle Plattformen hinweg zu bieten. Die neueste Highspeed-Wireless-Technologie 802.11ac Wave 2 sorgt für einen sicheren Wireless-Multi-Gigabit-Durchsatz. Um dieses Leistungspotenzial zu realisieren, müssen allerdings sowohl der Access-Point als auch die verbundenen Geräte den 802.11ac-Wave-2-Wireless-Standard unterstützen. Um den erforderlichen Wireless-Durchsatz zu ermöglichen, brauchen die meisten Firewalls zudem einen überdimensionierten abwärtskompatiblen 5-GbE- oder 10-GbE-Port, der schlicht zu viel Kapazität als nötig bietet, oder es müssen Switches hinzugefügt werden, die zusätzliche Kosten verursachen.

Die meisten Organisationen setzen auf eine Mischung aus lokalen und Cloud-basierten Anwendungen in einer hybriden IT-Umgebung – und machen es noch komplizierter, die gewünschte Performance und Sicherheit aufrechtzuerhalten. IT-Abteilungen müssen mehrere Benutzerverzeichnisse für Anwendungen in ihren lokalen Datencentern sowie für Drittanbieter-SaaS-Cloud-Anwendungen verwalten. Dies ist mit viel Aufwand verbunden: Die Verzeichnisse müssen kontinuierlich aktualisiert werden, um sicherzustellen, dass die richtigen User einen entsprechenden Zugriff auf die richtigen Anwendungen zur richtigen Zeit haben. Die Nutzer sind gezwungen, mehrere URLs und Passwörter zu pflegen und sich diese zu merken, was zu schlechten Sicherheitspraktiken führen kann. Unterbrechungen beim Zugriff führen zu Produktivitätsverlusten und Lücken im Sicherheitskonzept der Organisation und begünstigen darüber hinaus die Schatten-IT.

Fazit

Erfahren Sie mehr. Finden Sie heraus, wie Sie über Ihre kabelgebundenen, drahtlosen und mobilen Netzwerke hinweg Sicherheitslücken identifizieren und verhindern können. Lesen Sie unsere Lösungsübersicht „Best Practices für eine umfassende Sicherheit beim kabelgebundenen, drahtlosen und mobilen Zugriff“ und besuchen Sie unsere Webseite „Wireless & Mobile Access“.

[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*

Über uns

Seit über 25 Jahren gehört SonicWall zu den weltweit führenden Anbietern effizienter Sicherheitslösungen. Angefangen bei Access-Security über Netzwerksicherheit bis hin zu E-Mail-Security: Wir entwickeln unser Produktportfolio kontinuierlich weiter, damit unsere Kunden Innovationen realisieren, Prozesse beschleunigen und wachsen können. Mit über einer Million Sicherheitsgeräte in nahezu 200 Ländern und Regionen weltweit bietet SonicWall seinen Kunden alles, was sie brauchen, um für die Zukunft gerüstet zu sein.

Wenn Sie Fragen zur Nutzung dieser Unterlagen haben, wenden Sie sich an:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, Kalifornien 95054, USA

Weitere Informationen finden Sie auf unserer Website.
www.sonicwall.com

ExecBrief-NS-WhyYouNeed-US-IMAG-29144

SONICWALL®