LÖSUNGSPROFIL

Herausforderungen für Network Security Management

Eine Untersuchung der Hürden bei der Handhabung von Risiken, Vorgängen und Ressourcen

Zusammenfassung

Die Notwendigkeit einer schnellen Einbindung von Firewalls und anderen Sicherheitsdiensten über hyperverteilte Netzwerke hinweg und die unabdingbare Mobilität in der „neuen Normalität" unterstreichen die Wichtigkeit eines einheitlichen Sicherheitsmanagements in Unternehmen jeder Größe. In diesem Lösungsprofil werden aufkommende Trends untersucht und Herausforderungen im Bereich Netzwerksicherheit in den Bereichen Risikomanagement, Sicherheitsvorgänge und Ressourcenzuweisung untersucht.

Einführung

Angesichts der neuen Normalität mit Remote-Arbeit, verteilten Netzwerken, Migration in die Cloud und Proliferation von Apps und Geräten stehen wir einer explosionsartigen Vermehrung von Schwachstellen gegenüber. Heute ist die Geschäftstätigkeit jederzeit und allerorts möglich, weshalb für kleine Unternehmen bis hin zu großen verteilten Konzernen der Schutz von Netzwerken eine zunehmend wichtigere Rolle einnimmt.

Gleichzeitig werden Bedrohungen zunehmend raffinierter. Bei einem Anstieg der Zahl unentdeckter Bedrohungen um 145 % gegenüber dem Vorjahr[1] sind sich Unternehmen wahrscheinlich nicht bewusst, was alles unentdeckt geblieben ist.

Darüber hinaus stehen IT-Organisationen vor steigenden Kosten, schrumpfenden Budgets und einem eingeschränkten Pool qualifizierter Fachkräfte.

Gemeinsam bringen diese Auswirkungen erhebliche Herausforderungen für die IT in Bezug auf Netzwerksicherheit, Risikoeindämmung, Verwaltungsaufgaben und Zuweisung von Ressourcen.

Unterschiedliche Bedürfnisse

Alle Organisationen müssen die sich entwickelnden Bedrohungen verstehen und erkennen. Sie alle brauchen Einblick in Netzaktivitäten, Nutzung und Risiken. Sie alle müssen auch die in Bezug auf Sicherheit und Betrieb entstehenden Herausforderungen überwachen und bewältigen. Und sie alle müssen strenge interne Sicherheitsrichtlinien einhalten.

Kleine Unternehmen werden jedoch nur über begrenzte interne technische Ressourcen verfügen. Die Wahrung der Sicherheit und Optimierung der Leistung kann überwältigend sein. Größere Unternehmen und Dienstleister verfügen zwar meistens über eigene SecOps-Mitarbeiter, stehen aber auch vor noch größeren und schwierigeren Problemen. Implementierung und Verwaltung von Sicherheitseinrichtungen müssen oft über komplexe verteilte Netzwerke hinweg skaliert werden. Es entstehen oft Bedenken bezüglich Sicherheitsautomatisierung und Change Management, Audit Reporting und Policy Continuity.

Risikomanagement

Organisationen wissen nur zu gut, wie die an einem Tag normale Lage in wenigen Sekunden zum Chaos werden kann. Das Risiko, Opfer von gezielten Angriffen zu werden, besteht für viele Organisationen weiter und Nachrichten über Netzwerkeinbrüche und massive Datenklaus machen weiterhin Schlagzeilen.

Wie erkennen Sie, in welchem Maße Ihre Organisation gefährdet ist? Gibt es Sicherheitslücken in Ihrem internen Betrieb? Wie sieht es bei Ihren Netzwerkbenutzern sowie den Assets, Websites und von Ihnen verwendeten SaaS-Anwendungen aus? Wie entscheiden Sie, welche Prioritäten und Lösungen auf diese Risiken angewandt werden sollten?

Anwendungs- und Datenverkehr durchläuft das Internet, dezentrale Campus-Anlagen, Zweigstellen und vielleicht sogar die Netze von Drittanbietern. Organisationen verfügen meist über ungenügende Transparenz und Kontrolle für die Handhabung von riskanten Netzwerkaktivitäten, Verkehrsunregelmäßigkeiten, ungewöhnlichen Datenzugriffen und -bewegungen, nicht gepatchter Firmware, Sicherheitsvorfällen und Systemzuständen.

Risiken, die nicht beseitigt werden, können noch schlimmere Folgen nach sich ziehen. Bedrohungen und Angriffe bremsen die Dynamik und das Wachstum eines Unternehmens ab. Betriebsabläufe werden gestört, da Mitarbeiter von

gewinnbringenden geschäftlichen Prioritäten abgelenkt werden. Führungskräfte sind gezwungen, ihre ganze Zeit für Schadensbegrenzung und Öffentlichkeitsarbeit einzusetzen. Die Unfähigkeit, Sicherheitsrisiken zu erkennen, hemmt die Fähigkeit zur effektiven Sicherheitsplanung, Entscheidungsfindung und entschlossenen Handlung.

Sicherheitsvorkehrungen

Selbst Firewalls können Schwachstellen sein. Untersuchungen von Gartner[2] legen nahe, dass 99 % der Firewall-Einbrüche durch eine falsche Konfiguration der Firewall verursacht werden. Da Firewall-Regeln erstellt, kopiert und wieder geändert werden, können sie auch gegeneinander wirken und unerwünschte Sicherheits- und Performance-Folgen verursachen. Fehlkonfigurationen und widersprüchliche Regeln können das Netzwerk anfällig für komplexe Bedrohungen, unbefugten Zugriff oder Eindringversuche machen.

Anstatt Sicherheitslücken und Schwachstellen aufzuspüren, sollte mehr Zeit für die Prüfung von Firewall-Konfigurationen aufgebracht werden, um sicherzustellen, dass diese nicht übermäßig freizügig sind und Hintertüren zu ihren Infrastrukturen öffnen. Organisationen müssen Richtlinien und Konfigurationen vor ihrer Einführung validieren und prüfen und diese bei Bedarf schnell rückgängig machen.

Der neue digitale Arbeitsplatz von heute geht mit der Entwicklung von größeren, komplexeren Multi-Cloud-Netzwerken einher, die mehr Anwendungen und Nutzer unterstützen. Mit der kontinuierlichen Ausbreitung von Netzwerken werden Verwaltung von Sicherheitsvorkehrungen, Leistungssteigerungen, Lösung betrieblicher Probleme, Gewährleistung von Sicherheitsmaßnahmen und die Kontrolle des Zugangs für Benutzer, Geräte und Anwendungen immer mehr zu komplexen Herausforderungen.

Organisationen haben Schwierigkeiten, angemessene interne Sicherheitsvorkehrungen zu implementieren, die für eine Einhaltung interner Servicelevel-Richtlinien notwendig wären. Diese Richtlinien sollen Unternehmen und ihre Mitarbeiter schützen, Sicherheitsrisiken verringern und auch die finanzielle und rechtliche Haftung beschränken.

Bei der individuellen und manuellen Verwaltung ungleicher Firewall-Geräte haben Unternehmen häufig mit uneinheitlichen Richtlinien und Verfahren zu kämpfen. Es gibt oft nur wenige oder gar keine Analyse-, Test-, Audit- und Genehmigungsprozesse für die Sicherstellung, dass das Unternehmen die richtigen Firewall-Regeln zur richtigen Zeit und in Übereinstimmung mit internen Compliance-Anforderungen durchsetzt.

Ressourcenzuweisung

Ein Mangel an ausgebildeten Fachkräften in der Sicherheitsbranche hat die Personalausstattung zu einem ernsthaften Problem gemacht. Viele Organisationen, insbesondere KMU, verfügen nicht über ausreichende Sicherheitsfachkräfte und Fähigkeiten, um Firewalls kompetent zu pflegen und ernsthafte Sicherheitsprobleme zu lösen, wenn sie auftreten.

Jede einzelne Firewall erfordert regelmäßige Wartung, tägliche Überwachung, Richtlinienüberprüfungen und Verwaltung sowie Firmware-Upgrades. Da Netzwerke über verteilte Unternehmen und Multi-Tenant-Provider-Netzwerke hinweg skaliert werden und wachsen, vervielfacht sich die Belastung des Sicherheitspersonals exponentiell.

Erschwerend kommt hinzu, dass das Sicherheitspersonal mit der Verwaltung und dem Betrieb komplexer und fragmentierter Firewall-Silos belastet wird. Die Verwaltung ist oft komplex, umständlich und arbeitsintensiv. Aufgaben und Prozesse werden im Allgemeinen nicht geprüft, nicht bestätigt und sind nicht konform. Dies führt dazu, dass sich in kleinen Netzwerken über viele Jahre hinweg Dutzende – und in größeren Netzwerken sogar Tausende – von Firewall-Regeln anhäufen können.

Fazit

Wir brauchen eine bessere Lösung. Intelligentere Management-Tools sind erforderlich, damit Sicherheitsteams ihre Arbeit effektiv erledigen können.

SonicWall Network Security Manager (NSM) bietet Ihnen alles, was Sie für ein umfassendes Firewall-Management benötigen. Sie erhalten umfassende Transparenz, granulare Kontrolle und die Fähigkeit, den gesamten SonicWall Network Security-Betrieb mit größerer Klarheit, Präzision und Geschwindigkeit zu leiten. All das wird über eine funktionsreiche zentrale Benutzeroberfläche abgewickelt, die von jedem Ort aus über ein browserfähiges Endgerät zugänglich ist.

Erfahren Sie mehr. Wenden Sie sich noch heute an Ihren SonicWall-Vertreter oder besuchen Sie www.sonicwall.com/nsm.

Über SonicWall

SonicWall bietet Boundless Cybersecurity für das hyperverteilte Umfeld einer neuen Arbeitsrealität, in der jeder remote, mobil und ungeschützt ist. Indem SonicWall das Unbekannte kennt, Echtzeit-Transparenz und skalierbare Ökonomien ermöglicht, werden Cybersicherheitslücken bei Unternehmen, Regierungen und KMU weltweit geschlossen. Weitere Informationen finden Sie auf www.sonicwall.com.

[1] 2020 SonicWall Cyber Threat Report
[2] Info Security

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035, USA
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

ExecutiveBrief-TheChallengeOfNSM-US-VG-1965