FORTINET

Herkömmliche Netzwerk-Segmentierung: Kein Schutz vor einer wachsenden Angriffsfläche

Warum Netzwerk-Verantwortliche handeln müssen

Inhaltsverzeichnis

FORTINET

Zusammenfassung

Immer mehr Unternehmen führen Mobility- und Multi-Cloud-Lösungen ein. Diese Innovationen bringen nicht nur Vorteile, sondern auch neue Risiken mit sich: Die Angriffsfläche des Unternehmens wächst und wird zugleich fragmentierter. Netzwerk-Verantwortliche haben zunehmend damit zu kämpfen, die Leistung, Security, Ausfallsicherheit und Verfügbarkeit von Netzwerken aufrechtzuerhalten. Eine herkömmliche netzwerkbasierte Segmentierung erweist sich – neben neueren Mikro-Segmentierungstechniken – als unzureichend, da sich hiermit weder Bedrohungen erkennen noch verhindern lassen. Da diese Arten von Segmentierungen durch die Netzwerk-Architektur eingeschränkt werden, sind sie eher taktischer als strategischer Natur, allein auf die Geschäftslogik ausgerichtet und verfolgen ein statisches Sicherheitskonzept: Benutzer, Geräte und Anwendungen werden „ein für allemal“ als vertrauenswürdig erklärt und können dann in den für sie zugelassenen Segmenten frei „schalten und walten“. Dazu kommt, dass es keine umfassende Security-Transparenz über das gesamte Netzwerk und verschlüsselten Datenverkehr gibt – die jedoch für ein effektives Risikomanagement zwingend notwendig ist.

Einleitung: Schwierigkeiten beim Management unterschiedlicher Netzwerke – Ist Segmentierung die Lösung?

In einem durchschnittlichen Unternehmensnetzwerk geht der Trend hin zur Dezentralisierung: Benutzer, Geräte und Anwendungen, die auf die IT-Ressourcen des Unternehmens zugreifen, sind zunehmend geografisch verteilt. Durch den Einsatz von IoT-Technologien (Internet der Dinge) und SaaS-Anwendungen (Software-as-a-Service) in mehreren Public Clouds wird es selbst bei einer starken Security am Netzwerkrand immer schwieriger, alle Angriffsflächen zu schützen.

Ein Problem bei diesen expandierenden, zunehmend fragmentierten Angriffsflächen ist, dass sie zahlreiche neue Einstiegspfade für Kriminelle schaffen. Hinzu kommt, dass Bedrohungen immer komplexer werden, automatisch nach Schwachstellen suchen und diese gezielt ausnutzen können. Noch komplizierter wird die Situation nach Fusionen und Übernahmen, wenn Infrastrukturen zusammengelegt werden, aber die Koordination und Transparenz aller Bereiche des neuen Unternehmens nur eingeschränkt möglich ist. In vielen Firmen führt das dazu, dass Security-Teams nur noch auf Sicherheitsprobleme reagieren können. Insbesondere seitliche Bewegungen von Angreifern im Netzwerk über verbundene Geräte und den Anwendungs-Traffic kann das IT-Team so nicht verhindern.

Seit Jahren reagieren Netzwerk-Verantwortliche auf diese Herausforderungen mit der Segmentierung von Netzwerken. Herkömmliche Segmentierungstechniken nach IP-Adressen werden durch eine VLAN- und VMware NSX-Segmentierung für virtualisierte Workloads erweitert. Netzwerke mit Cisco-Hardware verwenden die Cisco ACI-Segmentierung, die mit physischen Switches und VXLANs funktioniert. Mit diesen Mikro-Segmentierungstechniken lassen sich Richtlinien für die Zugriffskontrolle basierend auf Workload-, Anwendungs- oder Architektur-Attributen definieren, z. B. anhand der virtuellen Maschinen (VMs), auf denen sich Anwendungen, Daten und Betriebssysteme befinden.

Bei diesen Segmentierungsansätzen trennen Firewalls die Netzwerk-Ressourcen jeder Gruppe, damit kein unautorisierter Datenverkehr zwischen den Segmenten stattfindet. Wird ein Bereich kompromittiert, soll so verhindert werden, dass sich der Angriff seitlich auf andere Netzwerk-Bereiche ausbreiten kann. Soweit die Theorie.

Leider ist die Mikro-Segmentierung nicht die Patentlösung, als die sie manchmal angepriesen wird. Das Konzept ist zwar prinzipiell sinnvoll, aber wenn die zugrunde liegende Netzwerk-Infrastruktur schlecht gestaltet ist, gefährdet die Mikro-Segmentierung u. U. sogar die Sicherheit: Wird ein komplexes Unternehmensnetzwerk in eine große Anzahl kleiner Segmente aufgeteilt, kann dies die Transparenz über Bedrohungen und Aktivitäten zur Abwehr von Angriffen im gesamten Netzwerk einschränken.[1]

Wird ein komplexes Unternehmensnetzwerk in eine große Anzahl kleiner Segmente aufgeteilt, kann dies die Transparenz über Bedrohungen und Aktivitäten zur Abwehr von Angriffen im gesamten Netzwerk einschränken.[2]

3 Gründe, warum heutige Segmentierungspraktiken das Risiko erhöhen

Bei den aktuellen Segmentierungstechniken gibt es drei Hauptprobleme:

1. Die Zugriffskontrolle für interne Netzwerk-Segmente richtet sich nach der Architektur – ein taktischer Ansatz, der sich nicht einfach an wechselnde Geschäftsanforderungen anpassen lässt.
2. Die Vertrauensbewertungen, auf denen Zugriffsrichtlinien basieren, sind in der Regel statisch und schnell veraltet.
3. Richtlinien für die Zugriffskontrolle lassen sich nicht effektiv durchsetzen, wenn vom Rechenzentrum bis zum Netzwerk-Rand und anderen Bereichen moderne Security-Komponenten (für Layer 7) fehlen und diese Komponenten nicht effizient angezeigt und gesteuert werden können.

Diese Probleme gehen oft darauf zurück, dass Netzwerk-Verantwortliche die Security bei der Planung der Segmentierungsarchitektur nicht angemessen berücksichtigen. Werden diese Probleme und ihre weitreichenden Folgen jedoch bedacht, lassen sich die Risiken bei der Segmentierung deutlich verringern.

„Allzu oft wird das Netzwerk ohne Berücksichtigung der Security und ihrer Funktionsweise geplant. IT-Teams vernachlässigen die Sicherheit beim Netzwerk-Design – dabei greifen Security und Netzwerk untrennbar ineinander. Das Netzwerk wird der Sicherheit übergeordnet, statt beide Bereiche gleichberechtigt zu behandeln. Dieses Fehlkonzept potenziert sich dann in Form von stark segmentierten, komplexen Netzwerk-Umgebungen.“[3]

Ein taktischer Bottom-up-Ansatz für die Zugriffskontrolle

In vielen Fällen richtet sich das Design des Unternehmensnetzwerks nach dynamischen Geschäftsanforderungen. Die Regeln, wer und was auf welche Netzwerk-Ressourcen zugreifen darf, werden durch Geschäftsrichtlinien, Industriestandards und behördliche Vorschriften vorgegeben. Nach diesen Regeln konfiguriert das Netzwerk-Team die Einstellungen für die Zugriffssteuerung in den Routern und Switches, über die Benutzer, Geräte oder Anwendungen auf bestimmte Netzwerk-Ressourcen zugreifen können.

Netzwerk-Verantwortliche werden sofort zwei Nachteile dieses Ansatzes erkennen. Erstens sind die Geschäftsprozesse, Compliance-Vorgaben und Netzwerk-Zugangsanforderungen eines Unternehmens erheblich komplexer als die Struktur seines Netzwerks. Folglich lassen sich nur schwer sichere Segmente für Netzwerk-Ressourcen definieren, auf die allein autorisierte Benutzer und Anwendungen gleichzeitig und vollständig zugreifen können. In der Praxis wird es Sicherheitslücken geben, die Angreifer ausnutzen können: Zugriffsszenarien, an die die Netzwerk-Architekten nicht gedacht haben. Mit fortschrittlicher, hochentwickelter Malware ist das heute schon machbar.

Zweitens kann sich jeder Prozess, jede Vorschrift und jede Organisationsstruktur ändern. Selbst ein unter Sicherheitsaspekten optimales Netzwerk-Design muss irgendwann angepasst werden. Auch hier gibt es zahlreiche Möglichkeiten für Sicherheitslücken, ganz zu schweigen von der Zeit und dem Aufwand für die Neukonfiguration – etwas, was sich kaum ein Netzwerk-Team leisten kann.

Die Netzwerk-Architektur ist zum Definieren sicherer Segmente denkbar ungeeignet. In der Praxis wird es Sicherheitslücken geben, die Angreifer ausnutzen können: Zugriffsszenarien, an die die Netzwerk-Architekten nicht gedacht haben.

Vertrauensbewertungen sind in der Regel statisch

Um Risiken effektiv zu managen, müssen Netzwerk-Verantwortliche über aktuelle, korrekte Informationen zur Vertrauenswürdigkeit von Benutzern, Anwendungen und Netzwerk-Ressourcen verfügen. Interne Firewalls oder andere Zugriffskontrollmechanismen, die den Verkehrsfluss zwischen Netzwerk-Segmenten zulassen oder untersagen, müssen jederzeit mit aktuellen Vertrauensdaten arbeiten. Sind Vertrauensbewertungen nicht mehr auf dem neuesten Stand, werden Segmentierungstechnologien unbrauchbar und können die Verbreitung potenzieller Bedrohungen quer im Netzwerk nicht mehr verhindern.

Die Qualität von Vertrauensdaten wird zu einem dringenden Problem bei der Sicherheit der Netzwerk-Segmentierung, da sich die tatsächliche Vertrauenswürdigkeit von Netzwerk-Ressourcen unerwartet ändern kann. Tatsächlich wurden zahlreiche Unternehmen von Angriffen aus den Reihen vertrauenswürdiger Mitarbeiter und Auftragnehmer überrascht: Über ein Drittel der gemeldeten Verstöße betreffen interne Benutzer und 29 % der Sicherheitsverletzungen gehen auf gestohlene Anmeldedaten zurück.[4]

Einige Unternehmen haben auf diese Gefahren rigoros reagiert: Netzwerke wurden praktisch gesperrt, keinem Benutzer bzw. keiner Anwendung mehr vertraut und mehrstufige Zugriffskontrollen implementiert. Natürlich müssen Netzwerk-Verantwortliche wichtiges Unternehmenskapital schützen. Das darf aber nicht zu Lasten berechtigter Anwender gehen, die für ihre Arbeit auf diese Ressourcen zugreifen müssen.

„Vertrauen ist nicht absolut, binär oder statisch, sondern reflektiert die angenommene, relative Zuverlässigkeit. Zudem ist der Grad des Vertrauens dynamisch und ändert sich mit der Zeit. Daher sollte der Zugriff an die Funktionalität angepasst werden.“[5]

Zugriffskontrollen ohne Durchsetzung bringen wenig

Richtlinien für die Zugriffskontrolle können nicht wie erwartet funktionieren, wenn im Netzwerk die Kernelemente einer effektiven Security-Infrastruktur fehlen. Herkömmliche Segmentierungsansätze setzen voraus, dass alle erforderlichen Netzwerk-Security-Komponenten vorhanden sind, um die vom IT-Team definierten Richtlinien für die Zugriffskontrolle umzusetzen. Diese Annahme kann jedoch aus mehreren Gründen nicht zutreffen.

Die Gesamtbetriebskosten (TCO) können ein Hauptgrund dafür sein, dass Unternehmen auf eine allgegenwärtige fortschrittliche Sicherheit verzichten. Beispielsweise kann das für die Segmentierung zuständige Netzwerk-Team entscheiden, dass einige Netzwerk-Segmente mit kleineren Angriffsflächen keine erweiterte Sicherheitsstufe 7 brauchen. Aus Budgetgründen – oder einfach, weil die Implementierung und das Management zu viele Ressourcen erfordern – werden Next-Generation-Firewalls (NGFWs) und ein moderner Bedrohungsschutz nicht überall dort eingesetzt, wo sie benötigt werden: innerhalb des Unternehmens, in jeder genutzten Cloud und bei jedem Endpunkt und IoT-Gerät.

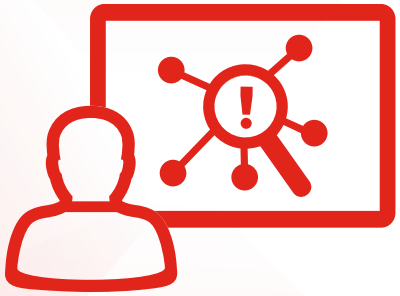
Vorhandene Security-Komponenten arbeiten mit eingeschränkter Funktionalität. Einige Netzwerk-Teams deaktivieren womöglich absichtlich bei NGFWs die SSL/TLS-Inspektion (Secure Sockets Layer/Transport Layer Security), um die Netzwerk-Performance zu verbessern. Eine solche Beschränkung von Sicherheitsfunktionen kann zwar die Übertragung von legitimem Traffic zwischen Netzwerk-Segmenten beschleunigen, ermöglich jedoch gleichzeitig auch unzulässigen Datenverkehr. Da 72 % des Netzwerk-Verkehrs mittlerweile verschlüsselt sind und Cyber-Kriminelle hierüber Netzwerke infiltrieren und Daten abgreifen, ist dies ein ernstes Problem.[6]

Security-Komponenten sind insgesamt weniger effektiv, wenn sie nicht eng integriert sind. Eine mangelnde Integration hat mehrere Auswirkungen. Erstens wäre da der Zeitfaktor: Erkennt eine Firewall ein verdächtiges Paket, kann es Stunden oder noch länger dauern, bis die Informationen vom Security-Administrator gesichtet und an das restliche Netzwerk weitergeleitet werden.

Zweitens können unterschiedliche Sicherheitslösungen Bedrohungsinformationen nicht einfach gemeinsam nutzen – weder erhaltene allgemeine Informationen zu bekannten und neuen Bedrohungen noch Zero-Day-Bedrohungsdaten zu neu entdeckten Gefahren. Dies kann ein Grund sein, warum es im Durchschnitt ganze 197 Tage dauert, bis eine Sicherheitsverletzung erkannt wird.[7]

Drittens können Unternehmen nicht effektiv reagieren, um die Folgen erkannter Verstöße einzudämmen: Ohne eine integrierte Sandbox-Technologie zur automatischen Quarantäne und zum Testen aller verdächtigen Pakete kann erheblicher Schaden entstehen, wenn das Security-Team eine Bedrohung manuell bekämpfen muss.

Unter diesen Umständen kann es vorkommen, dass sich Netzwerk-Verantwortliche in falscher Sicherheit wiegen und das segmentierte Netzwerk für gut geschützt halten. Eine unablässige, lückenlose Bewertung der Sicherheit könnte ihnen genau zeigen, wie ihre Security-Plattform funktioniert und ob die Zugriffsrichtlinien im Sinne der Geschäftsanforderungen greifen. Leider ist eine zuverlässige Bewertung ohne umfassende Security und Transparenz nicht möglich. Die Folge ist, dass viele Netzwerk-Verantwortliche das Sicherheitsprofil des Unternehmens falsch einschätzen.



Unterschiedliche Sicherheitslösungen können Bedrohungsdaten zu bekannten oder neu entdeckten Bedrohungen nicht gemeinsam nutzen. Dies kann ein Grund sein, warum es im Durchschnitt ganze 197 Tage dauert, bis eine Sicherheitsverletzung erkannt wird.[8]

Fazit: Wichtige Aspekte für Ihr Segmentierungskonzept

Obwohl eine Netzwerk-Segmentierung unverzichtbar ist, wird sie in der Praxis nur selten sinnvoll umgesetzt. Unternehmen, die auf dynamische Vertrauensbewertungen bei der Zugriffskontrolle zwischen Segmenten verzichten, schaffen unnötige Risiken für Benutzer und Ressourcen. Auch unterstützen Netzwerke, in denen die Segmentierungsarchitektur die Geschäftsabsicht beschränkt, nicht die unternehmerischen Ziele. Hat die Performance auf Kosten der Sicherheit Priorität, kann die Segmentierung zu einer passiven, wirkungslosen Bedrohungsabwehr führen. Und mangelt es im Netzwerk an Transparenz, um das Sicherheitsprofil richtig einzuschätzen, wird womöglich keine Layer-7-Security implementiert, die aber für die Abwehr komplexer Bedrohungen notwendig ist.

Die Festlegung angemessener Zugriffsrichtlinien für interne Netzwerk-Segmente angesichts ständig wachsender, fragmentierter Angriffsflächen liegt ganz in der Hand von Netzwerk-Verantwortlichen. Nur mit einem sorgfältig geplantem Segmentierungskonzept haben Unternehmen gute Chancen, sich quer im Netzwerk verbreitende Angriffe erfolgreich zu bekämpfen.

[1] Keith Townsend: „Get a Quick Primer on How Microsegmentation Can Improve Network Security“. BizTech, 26. Mai 2017.

[2] Ebd.

[3] „Friction in the IT Helix: How to Create Harmony between Network Design and Security“. Masergy, 8. August 2018.

[4] „2019 Data Breach Investigations Report“. Verizon, abgerufen am 8. Juli 2019.

[5] Neil MacDonald: „Zero Trust Is an Initial Step on the Roadmap to CARTA“. Gartner, 10. Dezember 2018.

[6] John Maddison: „More Encrypted Traffic Than Ever“. Fortinet, 10. Dezember 2018.

[7] „2018 Cost of a Data Breach Study“. Ponemon, Juli 2018.

[8] Ebd.

www.fortinet.com/de

361475-0-0-DE

31. August 2020, 8:38 Uhr