FORTINET

Risiken durch die digitale Transformation

Warum eine herkömmliche Netzwerk-Segmentierung die wachsende Angriffsfläche nicht sichern kann

Inhaltsverzeichnis

FORTINET

Zusammenfassung

Bei der digitalen Transformation (DX) von Netzwerken werden Anwendungen und Dienste in die Cloud migriert sowie zunehmend benutzereigene Technologien (BYOD) und IoT-Geräte (Internet der Dinge) eingebunden. All diese Änderungen haben den herkömmlichen Netzwerk-Rand in zahlreiche „Mikro-Perimeter“ aufgelöst – und so die Angriffsfläche von Unternehmen gewaltig vergrößert.

Diese breitere Angriffsfläche hat fatale Konsequenzen: Neue Bedrohungen, die sich immer schneller entwickeln, können leichter bisherige Sicherheitsmaßnahmen am Netzwerk-Rand aushebeln und sich quer durch das interne Netzwerk bewegen. Das interne Netzwerk ist dem schutzlos ausgeliefert, weil die herkömmliche Bedrohungserkennung und -abwehr nicht im Inneren des Netzwerks greift. Network-Operations-Teams bemühen sich nach Kräften, diese Sicherheitslücken mit verschiedenen Segmentierungstechniken zu schließen. Doch die Sicherheitseffektivität und Kosteneffizienz leiden unter dem Mangel an umfassender Transparenz über den Datenverkehr und der Unfähigkeit, aus geschäftlicher Sicht sinnvolle Zugangsrichtlinien zu definieren. CIOs sind zudem ständig bemüht, einen Kompromiss zwischen der Notwendigkeit einer strengen Traffic-Inspektion zur Risikominimierung und den Implementierungskosten einer erstklassigen Security zu finden.

Kann die Cyber-Security eines Unternehmens nicht mit seinen digitalen Transformationsinitiativen mithalten, drohen durch Cyber-Angriffe Verluste von 1 Million US-Dollar oder mehr.[1]

Einleitung: Erweiterung der Angriffsfläche und Zunahme von lateralen Bedrohungen

Als das Netzwerk auf Unternehmensstandorte begrenzt war und Benutzer nur mit Firmengeräten auf Unternehmensnetzwerke oder virtuelle private Netzwerke (VPN) zugriffen, war eine starke Security am Netzwerk-Rand ein sinnvoller Ansatz. Doch infolge der digitalen Transformation (DX) zeigt dieses Modell zunehmende Schwachstellen.

DX – über die Grenzen klassischer Netzwerke hinaus

Dank der digitalen Transformation (DX) können Unternehmen ihre Netzwerke modernisieren, um profitablere Serviceleistungen, eine bessere Nutzererfahrung und überall einen flexiblen Zugang zum Netzwerk anzubieten. Auch ermöglicht DX die Einführung unterschiedlichster Cloud-Dienste und -Anwendungen mit Hochverfügbarkeit und On-Demand-Skalierung und schafft die Voraussetzungen, um eine höhere Netzwerk-Effizienz und Geschäftsziele zu erreichen. Damit das erfolgreich gelingt, müssen nicht nur IoT-Geräte und private Geräte von Mitarbeitern (BYOD) ins Netzwerk eingebunden werden. Auch müssen Netzwerke ein höheres Verkehrsaufkommen bewältigen und schnellere Verbindungen bereitstellen, die sich aus der Zunahme der Geschäftsanwendungen und einem wachsenden DevOps-Bereich ergeben.

Durch die Einführung und das Wachstum dieser verschiedenen Dienste und Geräte – von Mobilgeräten, IoT-Geräten und Multi-Cloud-Diensten bis hin zu DevOps-Initiativen – wird der bisherige Netzwerk-Perimeter in viele kleine Mikro-Perimeter aufgesplittert, die einzelnen Benutzergeräten zugeordnet sind. Diese erweiterte Angriffsfläche erschwert CIOs den Schutz des Unternehmens vor einer sich ständig weiterentwickelnden, komplexen Bedrohungslandschaft.

Interne Netzwerke werden immer anfälliger

Trotz Verteidigungsmechanismen an jedem Perimeter können Angreifer ins Netzwerk eindringen und sich dann relativ problemlos quer durch das interne Netzwerk bewegen, Angriffe starten und Firmendaten abgreifen – alles ohne entdeckt zu werden. Schuld daran ist die „flache“ Architektur vieler Netzwerke, in der es nur minimale Sicherheitskontrollen und praktisch keine Netzwerk-Geräte gibt, die den Durchsatz und die Anwendungsleistung beeinträchtigen könnten.

Eindringlinge sind heutzutage auch schwerer zu entdecken, da über 72 % des Netzwerk-Traffics über sichere Verschlüsselungsprotokolle wie SSL (Secure Sockets Layer) oder TLS (Transport Layer Security) laufen.[2] Es überrascht kaum, dass rund 50 % der Malware – wie Zeus, Dridex oder TrickBot – mittlerweile in SSL- oder TLS-verschlüsselten Paketen versteckt sind. Sofern bei der Firewall keine SSL/TLS-Inspektion aktiviert ist, bleiben diese Angriffe unentdeckt.[3]

Über 72 % des Netzwerk-Traffics läuft über sichere Verschlüsselungsprotokolle wie SSL oder TLS.[4] 50 % aller Angriffe nutzt daher die SSL/TLS-Verschlüsselung aus, um Schadsoftware ins Unternehmen zu schleusen.

Reaktive Sicherheit fördert die Netzwerk-Segmentierung

Um fragmentierte, anfällige Netzwerk-Perimeter zu schützen, setzen viele Unternehmen zunehmend auf die Netzwerk-Segmentierung. Eine klassische Netzwerk-Segmentierung erweist sich jedoch als ineffektiv, da hierbei immer Lücken entstehen, die Angreifern den Zugriff auf geschäftskritische Informationen ermöglichen.

Netzwerkbasierte Segmentierung führt zu Sicherheitslücken

Eine herkömmliche Netzwerk-Segmentierung bietet heutigen dynamischen Unternehmensnetzwerken keinen ausreichenden Schutz vor einer sich weiterentwickelnden Bedrohungslandschaft. In typischen Segmentierungsszenarien werden Gruppen von IP-Adressen oder Segmenten von virtuellen lokalen Netzwerken (VLANs) definiert – mit jeweils einem Segment pro Ressourcen- oder Benutzergruppe. Andere Techniken wie VXLAN segmentieren nach Workloads und virtualisierten Anwendungen.

Diese Ansätze können höchst problematisch sein. Denn die Geschäftsprozesse, Compliance-Vorgaben und Netzwerk-Zugangsanforderungen eines Unternehmens sind erheblich komplexer als die Struktur seines Netzwerks. Aus diesem Grund lassen sich nur schwer sichere netzwerkbasierte Segmente definieren, auf die ausschließlich autorisierte Benutzer und Anwendungen gleichzeitig und vollständig zugreifen können.

Beispielsweise enthalten die Datenschutz-Grundverordnung der Europäischen Union (DSGVO) und der Zahlungsstandard PCI DSS (Payment Card Industry Data Security Standard) Bestimmungen, die eine effektive Isolierung sensibler Daten erfordern. Das Problem ist, dass die meisten vertraulichen Daten überall im Unternehmensnetzwerk verteilt sind und berechtigte Benutzer mit Zugriffsrechten auf diese Daten sich im selben Netzwerk-Segment wie unautorisierte Benutzer befinden können. Dient nun die Netzwerk-Architektur als Grundlage zur Definition von Segmenten, wird es äußerst schwierig, ein Segment zu finden, das alle autorisierten Benutzer und keinen der unautorisierten Benutzer umfasst bzw. das alle Daten enthält, die unter die Compliance-Regel fallen, aber alle anderen Daten ausschließt. Das Endergebnis ist eine begrenzte Transparenz.

Selbst die beste Segmentierung führt so unweigerlich zu Sicherheitslücken, die Angreifer ausnutzen können. Dabei handelt es sich oft um Zugangsszenarien, die Netzwerk-Architekten nicht vorgesehen haben.

Keine verlässliche Vertrauenswürdigkeit

Auch wenn es möglich ist, Benutzer-, Anwendungs- und Datensegmente zu erstellen, die gesetzlichen Vorschriften und den Geschäftsanforderungen entsprechen, bleibt ein Unternehmen dennoch anfällig für Angriffe, wenn Zugriffsberechtigungen auf dem angenommenen Vertrauen in ursprünglich überprüfte Benutzer, Geräte und Anwendungen basieren.
Die tatsächliche Vertrauenswürdigkeit von Netzwerk-Ressourcen kann sich unerwartet ändern. Viele Unternehmen wurden von Angriffen vermeintlich vertrauenswürdiger Mitarbeiter und Auftragnehmer überrascht. Auch können externe Angreifer mit Phishing-Techniken an vertrauenswürdige Anmeldedaten von Benutzern gelangen.

Einige Unternehmen blockieren den gesamten Zugang, bis der Vertrauensstatus überprüft wurde. Zwar kann dieser Ansatz das Risiko deutlich minimieren, ist jedoch wegen des immensen Zeit- und Ressourcenaufwands und der hochkomplexen Implementierung und Wartung praktisch nicht machbar.

Über ein Drittel der gemeldeten Sicherheitsverletzungen betreffen interne Benutzer, während 29 % auf gestohlene Anmeldedaten zurückgehen.[5]

Schwer zu rechtfertigende Kosten für eine leistungsstarke Security

Bis zum Jahr 2022 werden die weltweiten Ausgaben für Security-Produkte und -Serviceleistungen voraussichtlich um 45 % gegenüber dem heutigen Aufwand steigen. Zu diesem Anstieg dürften Datenschutzbestimmungen und Compliance-Bedenken maßgeblich beitragen.[6] Dieser Aufwand ist gerechtfertigt, wenn CIOs nachweisen können, dass durch Investitionen in die Security die Zahl der Sicherheitsverletzungen zurückgeht. Tatsächlich erhöhen Unternehmen, die im vergangenen Jahr keine Verstöße verzeichneten, mit einer viermal höheren Wahrscheinlichkeit ihre Cyber-Security-Budgets als Firmen, die im gleichen Jahr mehr als sechs Sicherheitsverletzungen hinnehmen mussten.[7]

Die Herausforderung für CIOs besteht darin zu ermitteln, welche Investitionen in den Bedrohungsschutz die Sicherheit tatsächlich verbessern – ohne Produktivität, Kundenerfahrung oder andere wichtige Geschäftskennzahlen zu beeinträchtigen. Der Kompromiss scheint zwischen der Genauigkeit der Traffic-Inspektion und der Schnelligkeit dieser Überprüfung zu liegen, um keine spürbare Verlangsamung der Anwendungsleistung zu verursachen.

Kompromiss bei der SSL/TLS-Inspektion

Wenn eine Firewall Datenpakete überprüft, verzögert sie zwangsläufig deren Übertragung im Netzwerk. Das Ausmaß der Verlangsamung – und damit die Folgen für Benutzer und Anwendungen – hängt allerdings von der Verarbeitungsleistung der Firewall und der Konfiguration der Firewalls im Netzwerk ab.

Next-Generation-Firewalls (NGFWs) führen eine Vielzahl von Überprüfungen durch. Dabei ist die SSL/TLS-Inspektion oft die größte „Durchsatz-Bremse“. Bei genauerem Blick in die Datenblätter der meisten Firewalls zeigt sich, dass für grundlegende Firewall-Funktionen eine höhere Leistung als bei aktivierter SSL/TLS-Inspektion angegeben wird. Dies ist ein Beweis für die zusätzliche Belastung, die die Verschlüsselung und Überprüfung von Paketen für Firewall-Prozessoren darstellt. Viele Unternehmen verdoppeln oder verdreifachen daher die Anzahl der Firewalls, um eine funktionierende SSL/TLS-Inspektion zu erhalten – eine gewaltige Investition, die zudem höhere Betriebskosten verursacht. Eine Alternative ist die Anschaffung dedizierter Appliances für die SSL/TLS-Inspektion, was jedoch zusätzliche Kosten und Komplexität bedeutet.

Wegen des Leistungsabfalls bei der SSL/TLS-Inspektion deaktivieren einige Unternehmen diese Überprüfung für durchsatzkritische Netzwerk-Segmente. Da jedoch der Anteil des verschlüsselten Traffics zunimmt und immer mehr Hacker Malware in verschlüsselten Paketen verstecken, steigt das Risiko für das Unternehmen dadurch dramatisch. Denn bei einer deaktivierten SSL/TLS-Inspektion werden fast drei Viertel des Netzwerk-Traffics nicht mehr überprüft.[8]

Durchsatz – ein wichtiger Aspekt bei den Gesamtbetriebskosten (TCO)

Eine kosteneffiziente Sicherheit maximiert den Bedrohungsschutz und minimiert die Gesamtbetriebskosten (TCO). Der Vergleich verschiedener Sicherheitslösungen wäre einfacher, könnte man Security-Produkte anhand von Kriterien wie Sicherheitseffektivität, Gesamtbetriebskosten sowie weiteren Funktionalitäten beurteilen.

Da dies nahezu unmöglich ist, arbeitet das unabhängige Testinstitut NSS Labs mit der Kennzahl „TCO pro geschütztem Mbit/s“, die sich auf die Kosten für den Netzwerk-Durchsatz bezieht.[9] Bei den von den NSS Labs getesteten NGFWs betragen die TCO pro geschütztem Mbit/s 2–57 US-Dollar (durchschnittlich 20,86 US-Dollar). In großen Netzwerken mit hohen Datenvolumina kann die Auswahl der NGFWs und die Anzahl der erforderlichen NGFWs einen großen Unterschied bei der Gesamtbetriebskosten machen.

„Bis zum Jahr 2022 werden die weltweiten Ausgaben für Security-Produkte und -Services voraussichtlich um 45 % gegenüber dem Aufwand in 2018 steigen.“[10]

Security und Datenschutz sind für viele Unternehmen nach wie vor Betriebsausgaben – nur die Hälfte betrachtet diese Bereiche als strategisches Kapital.[11]

Isolierte Sicherheitsaktivitäten beeinträchtigen das Risiko-Management

Zu viele Firewalls bedeuten mehr als eine Kostenbelastung: Sie stellen auch ein Sicherheitsrisiko dar, wenn sie isoliert voneinander arbeiten. Komplexe Bedrohungen können sich über Netzwerk-Segmente verbreiten und gleichzeitig mehrere Punkte auf der Angriffsfläche attackieren. Wenn aber sämtliche Firewalls – On-Premise sowie in Public und Private Clouds – nicht automatisch Bedrohungsinformationen austauschen und neuste globale Threat-Intelligence-Daten anwenden können, verzögert sich die Bedrohungserkennung und -abwehr unnötigerweise. Derzeit dauert es im Durchschnitt 197 Tage, bis eine Sicherheitsverletzung erkannt wird – eine Zahl, die Unternehmen einem hohen Risiko aussetzt.[12]

Ein wesentlicher Teil des Problems, mit dem CIOs konfrontiert sind, ist die mangelnde Integration von Sicherheitslösungen. Dadurch kann nicht automatisch auf Bedrohungen, unbefugte Zugriffe und Sicherheitsverletzungen reagiert werden. Jedoch geht dies nicht auf den Mangel an Tools oder Beratungsangeboten zur Security-Bewertung zurück, sondern auf die Schwierigkeit, Daten aus unterschiedlichen Quellen zeitnah zu sammeln und zu organisieren. Erfolgen Datensammlung und -abgleich zudem manuell, ist dies ein massiver – und vergeblicher – Mehraufwand, der CIOs mit schlanken IT-Teams enorm belastet.

Mangelnde Integration und Automatisierung zählen zu den Hauptgründen, warum es 197 Tage braucht, um eine Sicherheitsverletzung überhaupt zu erkennen.[13]

Fazit: Richtige Idee, aber der Ansatz muss sich ändern

Fest steht, dass Cyber-Angriffe früher oder später die Netzwerk-Security am Perimeter aushebeln werden. Ist das Netzwerk intern ungeschützt und nicht segmentiert, wird nichts die Angreifer aufhalten können.

Eine interne Netzwerk-Segmentierung ist daher ein Muss, aber mit herkömmlichen Methoden nicht zu erreichen – einerseits aufgrund der mangelnden Sicherheitseffizienz, andererseits wegen nicht zu rechtfertigender Gesamtbetriebskosten (TCO). Sollten CIOs weiterhin für den Schutz der unternehmenseigenen Datenbestände verantwortlich sein, müssen sie einen stärker geschäftsorientierten Ansatz verfolgen, der die digitale Transformation (DX) unterstützt.

[1] „The Cybersecurity Imperative“. Von securityindustry.org, abgerufen am 28. Mai 2019.

[2] „Q3 2018 Threat Landscape Report“. Fortinet, November 2018.

[3] „Study Reveals Hackers Increasingly Use Encryption to Hide Criminal Activity“. Lifeline Data Centers, abgerufen am 21. März 2019.

[4] „Q3 2018 Threat Landscape Report“. Fortinet, November 2018.

[5] „2019 Data Breach Investigations Report“. Verizon, Mai 2019.

[6] „New IDC Spending Guide Forecasts Worldwide Spending on Security Solutions Will Reach $133.7 Billion in 2022“. IDC, 4. Oktober 2018.

[7] „CISOs und Cyber-Security: Ein Bericht über aktuelle Prioritäten und Herausforderungen“. Fortinet, 26. April 2019.

[8] „Q3 2018 Threat Landscape Report“. Fortinet, November 2018.

[9] Thomas Skybakmoen: „Next Generation Firewall Comparative Report Security Value Map™ (SVM)“. NSS Labs, 17. Juli 2018.

[10] „New IDC Spending Guide Forecasts Worldwide Spending on Security Solutions Will Reach $133.7 Billion in 2022“. IDC, 4. Oktober 2018.

[11] Bill Briggs, et al.: „Manifesting legacy: Looking beyond the digital era: 2018 global CIO survey“. Deloitte, 2018.

[12] „2018 Cost of a Data Breach Study“. Ponemon Institute, Juli 2018.

[13] Ebd.

www.fortinet.com/de

339188-0-0-DE

4. Dezember, 2019

eb-risk-that-arise-from-digital-transformation_DE