DIE ENTWICKLUNG DER NETZZUGANGSKONTROLLE (NAC)

Wie IoT und BYOD-Geräte die NAC-Lösungen verändert haben

ZUSAMMENFASSUNG

Die Zunahme von BYOD-(Bring Your Own Device-)Richtlinien und des Internet der Dinge (IoT) hat das Aussehen von Netzwerken verändert und nachfolgend auch die Art und Weise, wie sie geschützt werden müssen. Was den Schutz von Endgeräten betrifft, sind Netzwerksicherheitsstrategien wie die Lösungen zur Netzzugangskontrolle (NAC) der vorherigen Generation veraltet. Ihnen fehlen die umfassende Transparenz, die Kontrolle und die automatisierten Reaktionen, die notwendig sind, um sichere Unternehmensimplementierungen sowohl des IoT als auch von BYOD-Geräten zu gewährleisten. Dieses Abwehrdefizit bringt nicht nur die Daten, Benutzer und regelmäßigen Geschäftsvorgänge in Gefahr, sondern setzt das Unternehmen potenziellen behördlichen Bußgeldern und anderen möglichen Schadensersatzansprüchen aus.

Als Teil der digitalen Transformation prognostiziert IDC, dass die weltweiten Ausgaben für den Bereich **IoT im Jahr 2018 772,5 Milliarden US-Dollar** erreichen und bis 2021 die Marke von **1 Billion US-Dollar** übertreffen werden.[1]

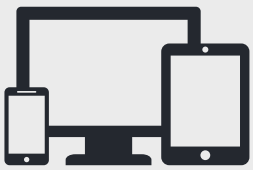
VON MOBILEN ENDGERÄTEN BIS ZU IOT-GERÄTEN

WHITEPAPER

Unternehmen kämpfen weiterhin mit der Sicherung mobiler Endgeräte. Gäste, Auftragnehmer, Servicemitarbeiter und andere „Außenstehende“ benötigen häufig einen Netzwerkzugang. EMM-(Enterprise Mobility Management -)Technologien und Firewalls können zwar helfen, bieten aber keine ausreichende Sichtbarkeit des Geräte- und Benutzerstatus, um festzustellen, ob sie die Berechtigung zur Verbindung mit dem Netzwerk erhalten oder den granularen Kontrollen zur Festlegung von Zugriffsgrenzen unterzogen werden sollten.

Gleichzeitig zielen Cyber-Kriminelle auch häufig auf IoT-Geräte ab, weil sie zu den Schwachstellen im Netzwerk gehören. Beispielsweise sind viele IoT-Produkte „kopflos“, also nicht in der Lage, selbst einfache Patches durchzuführen, und bieten wenig bis gar keine eingebaute Sicherheit.

Während sich die Branchenvorschriften für IoT-Geräte in der Entwicklung befinden, ist die IoT-Sicherheit bereits ein wichtiger Faktor für die Einhaltung bestehender Standards und Anforderungen. Die meisten Unternehmen müssen Vorschriften einhalten, die eine strenge Netzzugangskontrolle und strengen Datenschutz erfordern – wie die Datenschutz-Grundverordnung (DSGVO), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), den Payment Card Industry Data Security Standard (PCI DSS) und Vorschriften der US-amerikanischen Börsenaufsichtsbehörde (U.S. Securities and Exchange Commission, SEC). Um die Vorschriften einzuhalten, müssen Unternehmen alle Endgeräte schützen oder mit Geldstrafen rechnen, die pro Datenschutzverletzung Millionen von US-Dollar betragen können.



BYOD wächst ebenfalls weiter – die Zahl der mobilen Mitarbeiter hat 1,76 Milliarden überschritten und macht damit ca. 59,4 % der gesamten globalen Beschäftigung aus.[2]

Einer Studie zufolge sind 63 % der Unternehmen nicht in der Lage, mobile Geräte zu überwachen, wenn sie das Unternehmensnetzwerk verlassen. 53 % geben an, dass die Zahl der mit Malware infizierten Endgeräte in den letzten 12 Monaten gestiegen ist.[3]

Mit virtuellen/Cloud-Diensten, Switches, Routern und Zweigstellen, die weltweit vernetzt sind und Informationen austauschen, kann die Aufgabe, Endgeräte zu identifizieren und zu schützen, überwältigend erscheinen. Individuelle Security-Lösungen können zwar einige Angriffsvektoren abdecken, ihnen fehlen jedoch im Allgemeinen eine integrierte und umfassende Verlaufsverfolgung sowie forensische Informationen, die Vorfallsreaktions- und Compliance-Teams für die Prävention, Erkennung und Behebung von Datenschutzverletzung benötigen.

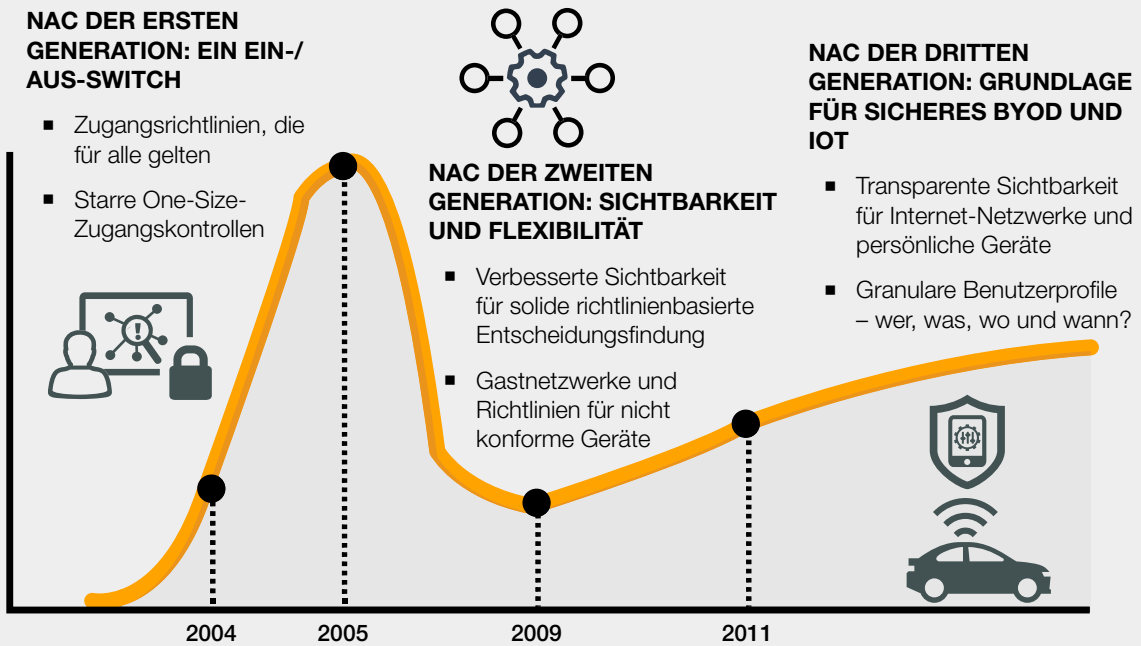
Das Hauptproblem dabei ist, dass veraltete Zugangskontrollen Netzwerke angriffsfähig machen (z. B. Kontamination durch Malware-infizierte Geräte oder unbefugter Zugriff über gestohlene Zugangsdaten).
NAC-Produkte der ersten Generation dienten zur Authentifizierung und Autorisierung von Endgeräten (vor allem verwaltete PCs) und verwendeten dafür eine einfache Scan-and-Block-Technologie. Die Entwicklung hin zu NAC-Lösungen der zweiten Generation befasste sich mit der sich abzeichnenden Nachfrage nach der Verwaltung des Gastzugangs zu Unternehmensnetzen. Diese Zugangskontrollen der zweiten Generation ermöglichten externen Benutzern, wie Besuchern, externen Mitarbeitern und Geschäftspartnern, einen begrenzten Internet-Zugang.

Veränderungen sowohl in der Netzwerkinfrastruktur (digitale Transformation) als auch in der Entwicklung anspruchsvoller, gezielter Angriffe haben jedoch eine Reihe neuer Schwachstellen im Bereich des Netzwerkzugangs offenbart, die beseitigt werden müssen.

1. Mangelnde Sichtbarkeit und Sensibilisierung. Sie können nicht schützen, was Sie nicht sehen können – der derzeitige Mangel an umfassender und zentralisierter Gerätesichtbarkeit (sowohl bei BYOD- als auch bei IoT-Produkten) macht Unternehmen anfällig. Sicherheitsteams müssen in der Lage sein, alle Geräte der Netzwerkinfrastruktur über die vielen verschiedenen Standorte hinweg, einschließlich jener an den extremen Netzwerkrändern, zu sehen. Da Endgerätesicherheit und Netzwerksicherheit gewöhnlich separat voneinander verfolgt werden, können sie auch kaum aussagekräftige Informationen in Echtzeit austauschen. Wenn ein einzelnes Gerät angegriffen wird, sollten alle anderen verbundenen Geräte (und der Rest der Netzwerksicherheitsarchitektur) sofort über die Bedrohung informiert werden, um koordinierte Abwehrmaßnahmen über das gesamte Unternehmen hinweg durchzuführen – was bei vielen herkömmlichen Security-Ansätzen nicht möglich ist.

2. Fehlende automatisierte Reaktionen auf Bedrohungen. Angesichts Tausender Security-Warnungen täglich, können IT-Teams nicht bei jeder potenziellen Netzwerkbedrohung manuell

NAC-LÖSUNGEN DER ERSTEN UND ZWEITEN GENERATION



eingreifen. Wenn die Firewall, das Intrusion Detection System (IDS), das Intrusion Prävention-System (IPS) oder ein ähnliches Tool eine Sicherheitsverletzung an einer bestimmten IP-Adresse erkennt, sollte die Security-Architektur automatisch komplexe Bedrohungen schnell und effizient entschärfen und so die Risikoexposition reduzieren.

3. Fehlende automatisierte Workflows: Viele veraltete Prozesse, wie z. B. die Bereitstellung, erfordern ein manuelles Eingreifen des IT-Personals. Dies kann die Einarbeitung neuer Mitarbeiter verlangsamen, Möglichkeiten für menschliche Fehler schaffen kann, die die Risikoexposition erhöhen, die IT-Arbeitslasten erhöhen und die Effizienz des gesamten Sicherheitsbetriebs verringern.

Diese Lösungen bieten zwar Kontrolle über herkömmlich verwaltete Geräte, der unaufhaltsame Weg in Richtung IoT und BYOD bringt jedoch besondere Herausforderungen mit sich. Das größte Problem ist, dass es praktisch keine Standardisierung der Gerätekonfiguration für BYOD oder IoT gibt. Es gibt Hunderte von Permutationen von Gerätetypen, Marken, Betriebssystemen und Sicherheitszuständen – und die meisten Geräte sind nicht auf Unternehmenssicherheit ausgelegt. Dieses Problem wird mit zunehmender Zeit immer gravierender, da Roboter, Wärmewächter, Insulinpumpen, HVAC-Sensoren, automatisierte Sicherheitszutrittssysteme und andere IoT-Verbindungen rasant zunehmen.

Experten schätzen, dass **heute ca. 9 Milliarden IoT-Geräte** verwendet werden, und dass diese Zahl **bis 2025 auf über 55 Mrd. anwachsen wird.**[4]

SECURITY MUSS SICH WEITERENTWICKELN, UM DIE ZUGANGSRISIKEN ZU KONTROLLIEREN

Durch die zunehmende Verbreitung von BYOD- und IoT-Geräten haben sich die Sicherheitsanforderungen für Endgeräte über die Möglichkeiten der Zugangskontrollen der vorherigen Generation hinaus ausgeweitet. Da sich gezielte Zero-Day-Angriffe und komplexe persistente Bedrohungen weiterentwickeln und vervielfachen, wird die Notwendigkeit, diese Abwehrlücken zu schließen, von Tag zu Tag dringlicher. Security-Architekten müssen die Netzwerkzugangskontrollen neu bewerten, um Endgeräte, Benutzer und das gesamte Unternehmen vor den potenziell katastrophalen Auswirkungen eines über Geräte in das Netzwerk gelangten Angriffs und dadurch verursachten Datenschutzverletzungen zu schützen.

[1] „IDC Forecasts Worldwide Spending on the Internet of Things to Reach $772 Billion in 2018“, IDC, 7. Dezember 2017.

[2] Nick Elia, „Mobile Worker Report Announcement“, VDC Research, 11. August 2017.

[3] „The Cost of Insecure Endpoints“, Ponemon Institute, Juni 2017.

[4] Peter Newman, „IoT Report: How Internet of Things technology is now reaching mainstream companies and consumers,“ Business Insider, 27. Juli 2018.

Februar 19, 2019 5:07 nachm.

271964-A-1-DE

WP-the-evolution-of-NAC-final-A4_DE