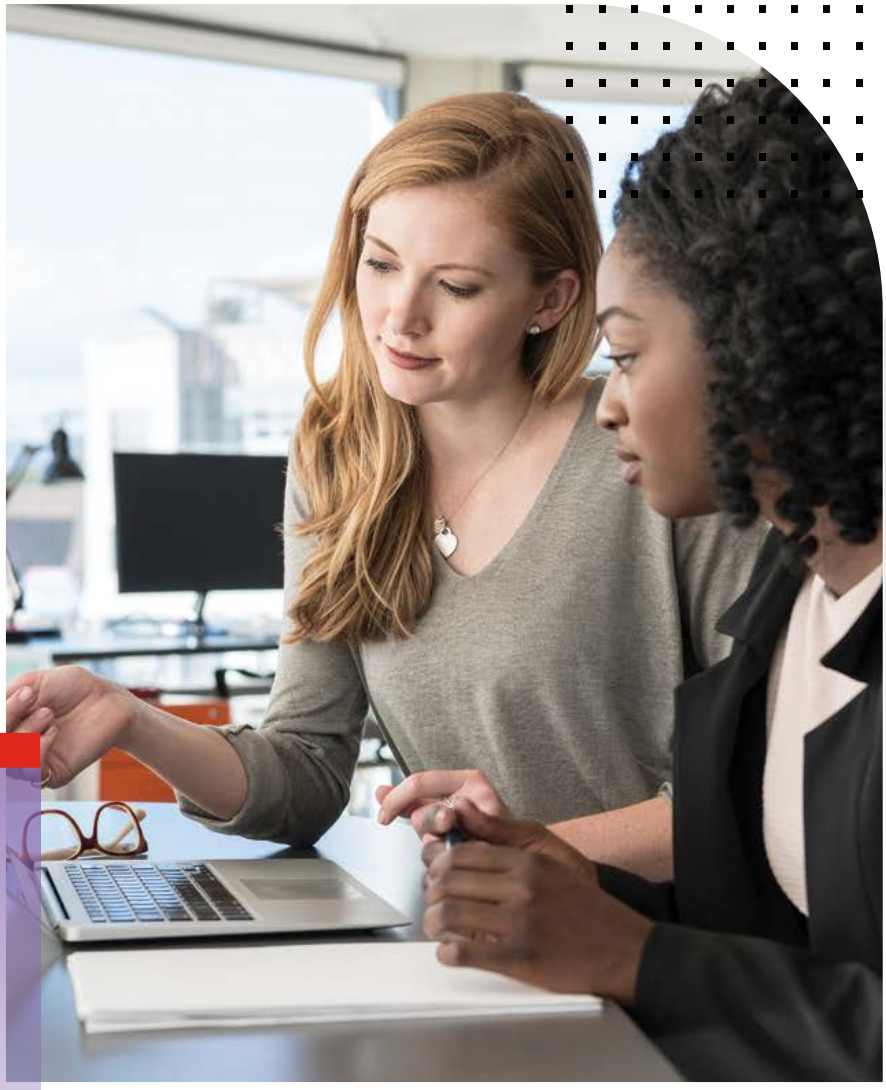
WHITEPAPER

Zero-Trust-Access: Ein Muss für sichere digitale Innovationen

Die wachsende Angriffsfläche bringt neue Risiken, die CISOs angehen müssen



Zusammenfassung

Unternehmen führen heute im Eiltempo digitale Innovationen (DI) ein, um schneller auf Geschäftsanforderungen reagieren zu können und sich Wettbewerbsvorteile zu sichern. Daten und Anwendungen werden zunehmend fernab des zentralen Rechenzentrums im gesamten Unternehmensnetzwerk verteilt, damit Mitarbeiter von vielen Standorten aus auf mehr Ressourcen Zugriff erhalten. Dies führt zur Auflösung des klassischen Netzwerk-Rands und einer ständig wachsenden Angriffsfläche für das ungeschützte interne Netzwerk – ein gravierendes Sicherheitsproblem für jeden CISO.

Als Reaktion auf diese Bedrohungen müssen Unternehmen einen Sicherheitsansatz nach dem Motto „Traue nichts und niemand" praktizieren und das Netzwerk mit einer ZTA-Richtlinie (Zero-Trust-Access) schützen. Nur so lässt sich sicherstellen, dass alle Anwender, Geräte und Web-Anwendungen aus der Cloud vertrauenswürdig und authentifiziert sind und über angemessene Zugriffsrechte verfügen. Ein solches „Null-Vertrauen-Prinzip" ist entscheidend für die Security jeder digitalen Innovation – unabhängig von der Art eines Projekts.

Für 81 % der leitenden Führungskräfte sind Mitarbeiter heute das größte Risiko für die mobile Security.[1]

Weiterentwicklung des Netzwerk-Randes

Ob Großkonzern, mittelständischer Betrieb oder Startup: DI-Initiativen fördern das Geschäftswachstum und weiten den Netzwerk-Rand aus. Ständig kommen neue Randbereiche hinzu, die ein exponentiell wachsendes Datenvolumen erzeugen – von Private und Public Clouds, IoT-Geräten (Internet der Dinge) und Mobilgeräten bis hin zu Filialen und Zweigstellen, die mit softwaredefinierten Lösungen (SD) vernetzt werden. Um den Benutzerzugriff zu regeln und Geräte von verschiedenen Standorten inner- und außerhalb des Netzwerks zu verbinden, implementieren Unternehmen immer mehr Geräte am Netzwerk-Rand.

Für CISOs kann das zum Albtraum werden. In den letzten Jahren sind so viele neue Randbereiche zu Netzwerken hinzugekommen, dass sich der klassische Perimeter zunehmend auflöst und das interne Netzwerk zu einer offenen, anfälligen Umgebung wird. Zugleich werden Cyber-Bedrohungen nicht nur vielfältiger, sondern auch anpassungsfähiger. Bislang basierte die Perimeter-Security auf einem Vertrauensvorschuss mit einmaliger Bestätigung nach dem Motto „Trust but verify". Doch angesichts der Masse von Benutzern, Geräten und Anwendungen im Netzwerk lässt sich kaum noch sicher sagen, wem oder was wirklich vertraut werden kann. Exploits wie der Diebstahl von Anmeldedaten und Malware ermöglichen Cyber-Kriminellen den Zugriff auf legitime Benutzerkonten. Sind Angreifer erst einmal ins Netzwerk eingedrungen, finden sie schnell Mittel und Wege, um sich quer durch das Unternehmensnetzwerk zu bewegen und Infektionen in kürzester Zeit zu verbreiten. Die Schwachstellen einer flachen Netzwerk-Topologie mit generellem „Vertrauensvorschuss" für jeden und alles im Netzwerk werden gnadenlos ausgenutzt. Ein Angreifer muss nur ein einziges Gerät am Netzwerk-Rand erfolgreich manipulieren, um in das Netzwerk einzudringen und Betriebsausfälle, Datendiebstahl, finanzielle Verluste und Reputationsschäden zu verursachen.

Für Security-Verantwortliche ist es mit einem herkömmlichen Ansatz für die Netzwerk-Sicherheit unmöglich, mit der wachsenden Anzahl von Angriffen Schritt zu halten. Die Konsequenz lautet: weg vom allgemeinen Vertrauensvorschuss hin zu einer grundsätzlichen Misstrauenserklärung. CISOs benötigen dafür ein gut funktionierendes Modell für den Zero-Trust-Access, um bestimmte Schwachstellen am Netzwerk-Rand als nicht vertrauenswürdig einzustufen: Benutzer, Geräte und Ressourcen – sowohl innerhalb als auch außerhalb des Netzwerks.

Wissen, *wer* mit dem Netzwerk verbunden ist

Security-Verantwortliche müssen jederzeit wissen, wer sich im Netzwerk befindet. Unternehmen sind jedoch einem erhöhten Risiko ausgesetzt, wenn Mitarbeiter für den Netzwerk-Zugang schwache Passwörter verwenden. Da heute für unzählige Konten Anmeldedaten notwendig sind, tendieren Benutzer zu simplen, einfach zu merkenden Passwörtern – die sich leicht durch Exploits wie Phishing-Angriffe knacken lassen. Für Unternehmen ist es wichtig, jeden Benutzer zu kennen und zu wissen, welche Rolle er im Unternehmen spielt. Nur dann lässt sich ein sicherer Zugriff auf die Ressourcen gewähren, die für jede Rolle oder Funktion erforderlich sind – ergänzt durch zusätzliche Berechtigungen in Einzelfällen.

Auch wenn der Einsatz mitarbeitereigener Geräte (BYOD) bei Anwendern und Führungskräften gleichermaßen beliebt sein mag, müssen sich CISOs der damit verbundenen Gefahren bewusst sein: Private Geräte, die geschäftlich genutzt werden, erweitern die Angriffsfläche. Besonders neue Bedrohungen können hierüber leichter die klassische Perimeter-Security aushebeln und sich quer im internen Netzwerk verbreiten. Viele laterale Angriffe sind nur möglich, weil Schwachstellen sehr lange unentdeckt blieben. Einige der verheerendsten Sicherheitsvorfälle gehen z. B. auf Netzwerk-Zugriffe von unbefugten Benutzern oder zu weit gefasste Zugriffsrechte für autorisierte Benutzer zurück. Offensichtlich scheint bei der Begeisterung für BYOD-Konzepte die Sicherheit auf der Strecke zu bleiben: 83 % der Security-Verantwortlichen sehen ihr Unternehmen durch Bedrohungen gefährdet, die von Mobilgeräten ausgehen.[2]

Eine weitere Herausforderung für Unternehmen ist eine geografisch verteilte Belegschaft, wenn Mitarbeiter von verschiedenen Standorten aus arbeiten – z. B. im Hauptsitz, in Filialen oder im Homeoffice. Wenn derart viele Benutzer von außerhalb auf das

Netzwerk zugreifen, erweitert sich die Angriffsfläche gewaltig. Mitarbeiter verbinden sich z. B. häufig über Hotspots oder öffentliche WLAN-Zugänge in Cafés, Flughäfen, Fahrzeugen oder öffentlichen Verkehrsmitteln mit dem Unternehmensnetzwerk. Diese Art der Konnektivität führt zu erheblichen Sicherheitsrisiken: Dritte können alle Informationen abfangen, die zwischen dem Benutzer und dem Unternehmensnetzwerk übertragen werden. Auch können Angreifer ungepatchte Software-Schwachstellen ausnutzen, um Malware in Endgeräte einzuschleusen – nicht nur um die Daten auf dem Gerät zu stehlen, sondern auch, um über das Endgerät in das Unternehmensnetzwerk einzudringen.

Diese Sicherheitsprobleme verschärfen sich, wenn der Großteil der Belegschaft wie bei der Corona-Pandemie 2020 im Homeoffice arbeiten muss. Die meisten Unternehmen waren wahrscheinlich vorher von 15 % externen Mitarbeitern ausgegangen. Nun mussten plötzlich die richtige Infrastruktur und geeignete Sicherheitskontrollen für über 90 % der Belegschaft bereitgestellt werden.

Viele der verheerendsten Angriffe auf Unternehmen in den letzten Jahren konzentrierten sich auf Geräte am Netzwerk-Rand.[3]

Diese Anforderungen sind teilweise der Grund, warum ein Zero-Trust-Access so wichtig ist. Da Geräte ständig im Netzwerk „ein- und ausgehen", müssen Security-Verantwortliche genau wissen, welche Benutzer sich im Netzwerk befinden und ob sie über die richtigen Zugriffsrechte verfügen. Ändern sich Aufgabenbereiche – z. B. bei einem Wechsel vom Vertrieb in den Kundenservice –, benötigen Mitarbeiter möglicherweise andere Zugriffsrechte als in der vorherigen Rolle. Security-Teams sollten die reibungslose Umstellung bei betriebsinternen Versetzungen gewährleisten können.

Wissen, *was* mit dem Netzwerk verbunden ist

Security-Verantwortliche müssen nicht nur jederzeit wissen, wer sich im Netzwerk befindet, sondern auch, welche Geräte mit dem Netzwerk verbunden sind. Die Verbreitung von IoT- und Mobilgeräten hat jedoch den bisherigen Netzwerk-Perimeter aufgelöst. Heutige Netzwerke haben viele „Mikro-Perimeter" mit einer weitaus größeren Angriffsfläche für das Unternehmen. Da jeder dieser Mikro-Randbereiche einem Benutzergerät entspricht, sind Endpunkte zunehmend die Hauptziele von Malware-Infektionen und hochkomplexen Exploits.

Die Fülle neuer Endgeräte im Netzwerk und die ständig wachsende Angriffsfläche führen in vielen Unternehmen zu einem fundamentalen Kontrollverlust: Niemand weiß mehr, welche Geräte mit dem Netzwerk verbunden sind. Tatsächlich gibt es praktisch keine standardisierten Gerätekonfigurationen für BYOD oder IoT. Besonders mobile BYOD-Geräte stellen ein hohes Risiko für Netzwerke dar, z. B. durch Datenlecks, ungeschützte WLAN-Zugänge, Netzwerk-Spoofing, Phishing, Spyware, fehlende Verschlüsselung oder keine Abmeldung nach Online-Sitzungen. Am stärksten wächst die Angriffsfläche jedoch durch das Internet der Dinge – IoT-Geräte, die als neue Endpunkte ins Netzwerk kommen.

Cyber-Angriffe auf IoT-Geräte sind stark im Kommen. Das liegt daran, dass Unternehmen immer mehr intelligente Geräte ins Netzwerk einbinden. Diese Geräte werden von Angreifern missbraucht, um DDoS-Angriffe (Distributed Denial-of-Service) sowie viele andere bösartige Aktionen durchzuführen.

Um BYOD- und IoT-Endpunkte richtig zu schützen, müssen Unternehmen wissen, wo sich die einzelnen Geräte befinden, was sie tun und wie sie über die Netzwerk-Topologie mit anderen Geräten verbunden sind. Mangelnde Transparenz macht ein Unternehmen anfällig, da man sich gewisser Risiken gar nicht bewusst ist. Security-Verantwortliche müssen deshalb Geräte an den Randbereichen des Netzwerks überwachen können. Fast die Hälfte der Cyber-Security-Experten gibt jedoch an, keinen Plan zur Bekämpfung von Angriffen auf IoT-Geräte zu haben – obwohl neun von zehn der Befragten sich wegen künftiger Bedrohungen besorgt zeigen.[4]

Einige Unternehmen setzen auf eine herkömmliche Netzwerk-Segmentierung. Damit lassen sich jedoch nur schwer sichere netzwerkbasierte Segmente definieren, auf die allein autorisierte Benutzer und Anwendungen gleichzeitig und vollständig zugreifen können. Selbst die bestmögliche Segmentierung führt unweigerlich zu einer lückenhaften Netzwerk-Security, die Angreifern zuspielt – weil Netzwerk-Architekten nicht alle Zugangsszenarien bedacht haben.

Beruhen Zugriffsberechtigungen nur auf einem angenommenen Vertrauen in überprüfte Geräte, bleibt das Unternehmen weiterhin anfällig. Viele Firmen wurden bereits von Angriffen überrascht, die von als vertrauensvoll geltenden Mitarbeitern und Auftragnehmern ausgingen. Durch ein verlorenes oder gestohlenes Gerät können Passwörter in die falschen Hände gelangen und werden dann irgendwann in der Zukunft für Angriffe missbraucht. Genau deshalb ist ein Zero-Trust-Ansatz so wichtig. Da Cyber-Kriminelle möglichst viele unterschiedliche Netzwerk-Geräte kompromittieren wollen, benötigen Security-Verantwortliche mehr Transparenz über Netzwerk-Verbindungen und eine bessere Erkennung jedes Geräts, das auf das Netzwerk zugreifen will.

Schutz für Ressourcen überall – innerhalb und außerhalb des Netzwerks

Ein weiteres zentrales Problem für Security-Verantwortliche ist die zunehmende Verwendung mobiler Geräte außerhalb des Unternehmensnetzwerks oder in anderen Netzwerken, durch die sich Sicherheitsbedrohungen wie Malware oder Botnets einschleichen können. Beispielsweise verwenden viele Mitarbeiter ihre BYOD-Geräte sowohl für private als auch für

geschäftliche Zwecke: Sie surfen im Internet, interagieren in sozialen Medien und erhalten z. B. private E-Mails, wenn sie nicht beim Unternehmensnetzwerk angemeldet sind. Greift ein Mitarbeiter nach privaten Online-Aktivitäten wieder mit dem gleichen Gerät auf das Unternehmensnetzwerk zu, können versehentlich Bedrohungen wie Viren, Malware und andere Exploits eingeschleust werden.

Diese Kombination aus privater und geschäftlicher Gerätenutzung trifft mit einer anderen Entwicklung zusammen: Die meisten Unternehmen haben keinen Überblick mehr über die vielen Endgeräte, die auf ihr Netzwerk zugreifen. In einem aktuellen Bericht des Ponemon Institute gaben 63 % der Unternehmen an, dass sie Endgeräte nicht außerhalb ihres Netzwerks überwachen können, und über der Hälfte der Unternehmen fehlen Kontrollmöglichkeiten, ob ein Gerät die Compliance-Anforderungen erfüllt.[5] Transparenz über alle Endpunkte scheint an der schieren Masse der Endgeräte im Netzwerk zu scheitern. Infolgedessen haben CISOs und Security-Teams Schwierigkeiten, dieses enorme Risiko in den Griff zu bekommen.

Mit einem ZTA-Framework, das alle Geräte identifiziert, segmentiert und kontinuierlich überwacht, können Unternehmen risikoreiche, flach aufgebaute Netzwerke ersetzen und interne Ressourcen, Daten, Anwendungen sowie geistiges Eigentum jederzeit zuverlässig schützen. Diese Strategie hat mehrere Vorteile: Sie verringert die mit einem perimeterorientierten Sicherheitskonzept verbundenen Risiken, sorgt für mehr Transparenz und Kontrolle über Geräte außerhalb des Netzwerks und vereinfacht zugleich das gesamte Netzwerk- und Security-Management.

63 % der Unternehmen sind nicht in der Lage, Endgeräte zu überwachen, wenn sie nicht mehr im Unternehmensnetzwerk sind. 53 % geben an, dass die Zahl der mit Malware infizierten Endgeräte in den letzten 12 Monaten gestiegen ist.[6]

Fazit: Ein Zero-Trust-Ansatz ist notwendig

DI-Initiativen führen zu schnelleren geschäftlichen Erfolgen, aber auch zu einer erweiterten Angriffsfläche und neuen Anfälligkeit für Cyber-Bedrohungen. Digitale Innovationen stellen daher auch eine Mehrbelastung für CISOs, ihre Teams und Ressourcen dar. Erschwerend kommt hinzu, dass Angreifer ständig dazulernen und immer ausgefeiltere, komplexere Angriffsformen entwickeln, denen sich mit herkömmlichen Sicherheitsstrategien für den Netzwerk-Rand nichts entgegensetzen lässt. Bedingt durch die Art und Komplexität von Bedrohungen gibt es heutzutage keinen einzigen Punkt mehr in der Security-Infrastruktur eines Unternehmens, an dem alle Aspekte einer Bedrohung sichtbar sind. Mit einem Zero-Trust-Access (ZTA) lässt sich dieses Problem lösen: CISOs können sich bei einem ZTA-Konzept auf die Benutzer und Geräte konzentrieren, die sich mit dem Netzwerk verbinden, deren Identität bestätigen und sicherstellen, dass nicht mehr Vertrauen und Zugriffsrechte als unbedingt notwendig gewährt werden.

Einer der Hauptgründe für die wachsende Angriffsfläche liegt in der zunehmenden Verbreitung von IoT- und intelligenten Geräten im Netzwerk. Security-Verantwortlichen fehlt oft ein vollständiger Überblick über die Fülle an Geräten, die auf das Netzwerk zugreifen. Die meisten CISOs wissen aus eigener Erfahrung, dass mangelnde Transparenz das Unternehmen großen Risiken aussetzt. Um aber sämtliche Endgeräte vollständig zu schützen, müssen Unternehmen im gesamten Netzwerk eine Zero-Trust-Access-Richtlinie (ZTA) durchsetzen. Damit lässt sich dann genau sehen, wo sich einzelne Geräte befinden, was sie tun und wie sie mit anderen Geräten im Netzwerk interagieren. Auch wird so eine kontinuierliche Überwachung möglich, um bedrohungsrelevante Verhaltensanomalien zu erkennen.

[1] „Mobile Security Index 2019".Verizon, 2019.

[2] Ebd.

[3] Neil Jenkins und Natasha Cohen: „Living on the Edge". Cyber Threat Alliance, 30. April 2019.

[4] „Only 47% of cybersecurity pros are prepared to deal with attacks on their IoT devices". Help Net Security, 8. November 2019.

[5] „The Cost of Insecure Endpoints". Ponemon Institute, 2020.

[6] Ebd.

Deutschland
Feldbergstraße 35
60323 Frankfurt
Deutschland
Telefon: +49 69 310 192 0

Schweiz
Riedmuehlestr. 8
CH-8305 Dietlikon/Zürich
Schweiz
Telefon: +41 44 833 68 48

ÖSTERREICH
Wienerbergstraße 11
Turm A, 9. OG
1100 Wien
Österreich
Verkaufsabteilung:
Telefon: +43 1 3760013-0

www.fortinet.com/de

696181-A-0-DE