BERICHT

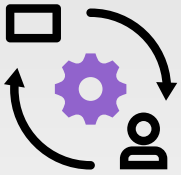
Bericht zum Stand von Zero-Trust

INHALTSVERZEICHNIS

Zusammenfassung

Das Zero-Trust-Modell für die Netzwerk-Sicherheit wird derzeit heiß unter IT-Experten diskutiert. Viele Unternehmen hegen gewisse Erwartungen an einen Zero-Trust-Access (ZTA) oder einen Zero-Trust-Network-Access (ZTNA), die jedoch in der Praxis oft nicht erfüllt werden.

Die meisten Unternehmen haben oder planen nach eigenen Angaben eine ZTA- oder ZTNA-Strategie, berichten aber von Problemen bei der konsequenten Authentifizierung von Anwendern und Geräten, bei der Überwachung von autorisierten Benutzern im Netzwerk oder von einer schwierigen Zero-Trust-Implementierung im erweiterten Netzwerk. Da all das den Kern eines Zero-Trust-Modells ausmacht, stellt sich die Frage, ob viele Unternehmen eine falsche Vorstellung von Zero-Trust haben oder ob ihre Lösungen womöglich nicht richtig implementiert sind.



Die meisten Unternehmen haben oder planen nach eigenen Angaben eine ZTA- oder ZTNA-Strategie, berichten aber von Problemen bei der konsequenten Authentifizierung von Anwendern und Geräten sowie bei der Überwachung von autorisierten Benutzern.

Stand von Zero-Trust

Das Zero-Trust-Modell für die Netzwerk-Security ist kein Novum. Die Zahl der Datenschutzverletzungen steigt – und da Unternehmen immer mehr Geschäftsfunktionen in die Cloud verlagern, machen Angriffe auf Web-Anwendungen mittlerweile 39 % aller Sicherheitsvorfälle aus.[1]

Die meisten Cybersecurity-Verantwortlichen sind sich einig, dass die Konzepte hinter dem Zero-Trust-Sicherheitsmodell sinnvoll sind: Statt wie bei veralteten Authentifizierungslösungen ein für alle Mal einen Vertrauensvorschuss zu gewähren, ist der Zero-Trust-Ansatz eine grundlegende „Misstrauenserklärung“: Niemand gilt per se als vertrauenswürdig – weder außerhalb noch innerhalb des Netzwerk-Perimeters.

Der Wechsel vom implizitem Vertrauen zu Zero-Trust ist die Konsequenz angesichts der zunehmenden Angriffe und finanziellen Folgen von Cyber-Kriminalität. Eine Datenpanne kostet weltweit im Durchschnitt 4,24 Millionen USD. Die drei häufigsten Angriffsvektoren sind gestohlene Zugangsdaten (20 %), Phishing (17 %) und Cloud-Fehlkonfiguration (15 %).[2] Eine robuste Implementierung von Zero-Trust-Lösungen kann die Wahrscheinlichkeit eines Angriffs mit Tools wie der Multi-Faktor-Authentifizierung verringern sowie die Auswirkungen von Sicherheitsverstößen durch Techniken wie eine Mikrosegmentierung minimieren.

Work-from-Anywhere (WFA) ist ein anhaltender Trend in der Wirtschaft und im öffentlichen Sektor: Moderne Arbeitsmodelle wie Telearbeit, Homeoffices, alternierende Arbeitsplätze oder mobiles Arbeiten sind der Grund, warum sich immer mehr Unternehmen für eine ZTNA-Lösung interessieren. Je mehr Menschen aber von überall aus arbeiten, desto unsicher wird der klassische perimeterbasierte Security-Ansatz – und jedes Mal, wenn einem Gerät oder Benutzer automatisch vertraut wird, sind die Daten, Anwendungen und das geistige Eigentum des Unternehmens in Gefahr. Gartner geht deshalb davon aus, dass sich 60 % der Unternehmen bis 2023 vom klassischen VPN verabschieden und auf ein ZTNA-Modell umstellen werden.[3]

Als wegen der Pandemie immer mehr Menschen ins Homeoffice wechselten, wurden die Grenzen herkömmlicher VPN-Verbindungen schnell deutlich. Bessere Lösungen – wie Zero-Trust-Modelle – waren plötzlich zwingend notwendig, um sich vor Bedrohungen durch Mitarbeiter zu schützen, die sich über Heimnetzwerke mit praktisch Null Security mit dem Unternehmensnetzwerk verbinden mussten.[4]

Obwohl man sich über die Notwendigkeit von Zero-Trust einig ist, herrscht viel Verwirrung über das *Wie*. Was genau ist eine effektive Zero-Trust-Strategie? Zero-Trust-Konzepte sind seit Jahren ein Thema, werden aber meistens fälschlicherweise auf eine Art „Zugangsüberprüfung“ reduziert. Im Kern geht es beim Zero-Trust-Modell jedoch darum, das Arbeiten und Lernen überall zu schützen sowie das klassische VPN mit einer besseren Alternative zu ersetzen. Richtig implementiert ist Zero-Trust eine äußerst effektive Strategie für einen zukunftssicheren Schutz hybrider Arbeitsmodelle.

Überblick über die Zero-Trust-Umfrage

Fortinet hat kürzlich 472 Cybersecurity-Experten und Führungskräfte weltweit zum Stand von Zero-Trust in ihrem Unternehmen befragt. Vor allem wollten wir Folgendes wissen:

- Wie gut sind Unternehmen mit dem Konzept von Zero-Trust und ZTNA vertraut?
- Welche Vorteile und Herausforderungen werden mit der Implementierung einer Zero-Trust-Strategie verbunden?
- Soll eine Zero-Trust-Strategie eingeführt werden bzw. wurde sie bereits eingeführt, und wenn ja, welche Sicherheitselemente umfasst diese?

Wichtigste Prioritäten und Vorteile

Die Zunahme von Sicherheitsverletzungen und Ransomware ist ein Dauerthema in den Nachrichten und angesichts zunehmender Angriffe wollen Unternehmen sich besser schützen. Doch obwohl Zero-Trust Teil einer umfassenden Cybersecurity-Strategie ist, variieren die Top-Prioritäten.

„Minimierung der Folgen von Verstößen und Eindringlingen“ führt die Liste mit 34 % an, dicht gefolgt von „Sicherer Fernzugriff“ und „Gewährleistung eines kontinuierlichen Geschäftsbetriebs“ mit 33 %.

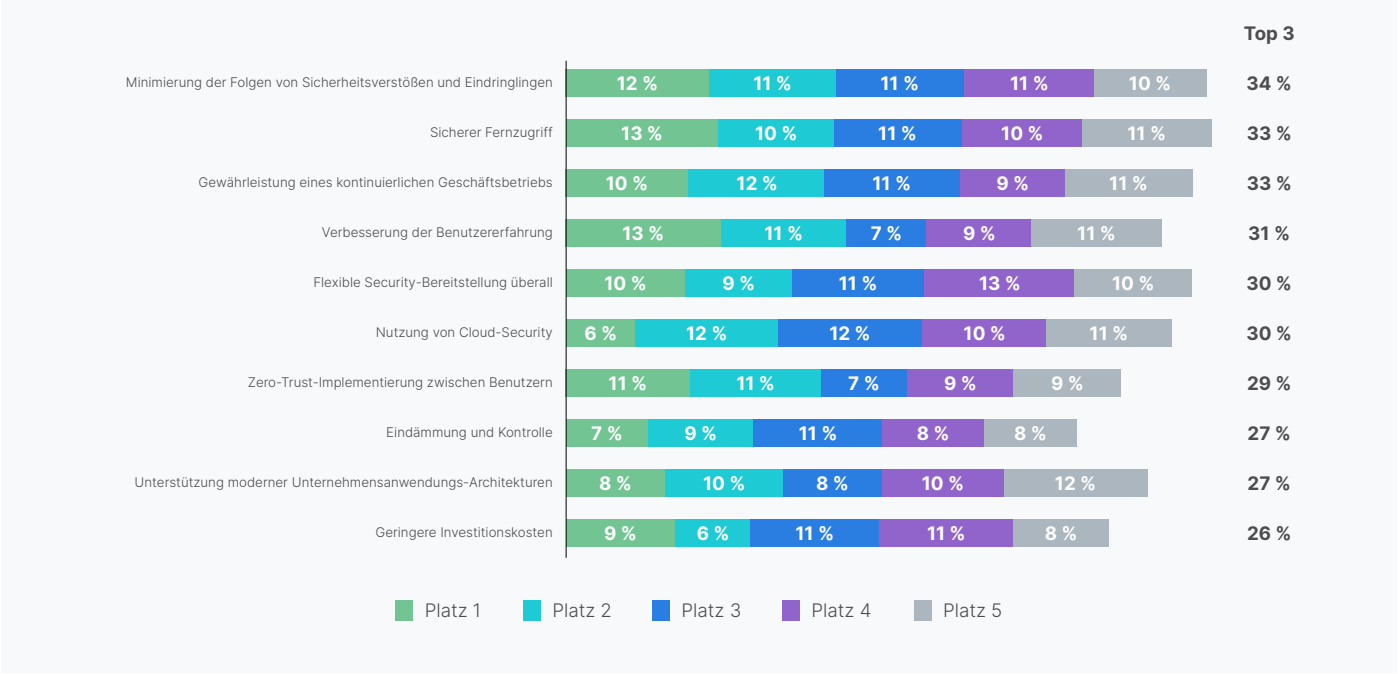
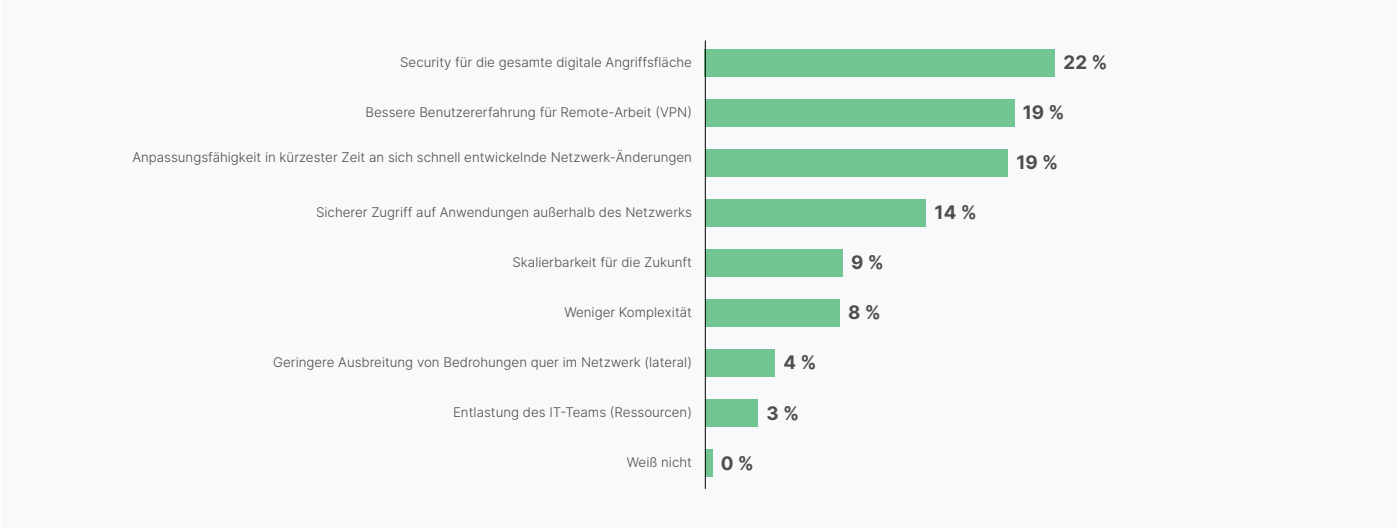


Abbildung 1: Prioritäten bei einer Zero-Trust-Strategie

Auf die Frage nach dem wichtigsten Vorteil einer Zero-Trust-Lösung nannten 22 % der Unternehmen „Security für die gesamte digitale Angriffsfläche“, dicht gefolgt von einer „besseren Benutzererfahrung für Remote-Arbeit (VPN)“ und „Anpassungsfähigkeit in kürzester Zeit an sich schnell entwickelnde Netzwerk-Änderungen“ (beide 19 %).



Die Umfrage zeigte auch, dass ein sicherer Fernzugriff in allen Regionen Priorität genießt, wohingegen es bei anderen Prioritäten weltweit Unterschiede gibt.

	Nordamerika	EMEA	Asien-Pazifik	Lateinamerika
Gewährleistung eines kontinuierlichen Geschäftsbetriebs	36 %	40 %	29 %	24 %
Sicherer Fernzugriff	35 %	34 %	32 %	32 %
Zero-Trust-Implementierung zwischen Benutzern	33 %	26 %	28 %	24 %
Nutzung von Cloud-Security	33 %	27 %	30 %	28 %
Minimierung der Folgen von Sicherheitsverstößen und Eindringlingen	32 %	30 %	34 %	46 %
Flexible Security-Bereitstellung überall	31 %	29 %	32 %	24 %
Eindämmung und Kontrolle	27 %	22 %	27 %	32 %
Verbesserung der Benutzererfahrung	26 %	37 %	31 %	32 %
Geringere Investitionskosten	25 %	30 %	25 %	26 %
Unterstützung moderner Unternehmensanwendungs-Architekturen	22 %	25 %	31 %	32 %

Abbildung 3: Prioritäten bei Zero-Trust-Strategien (Top 3)

Kenntnisstand und Implementierung

Als eines der Hauptziele der Umfrage wollten wir mehr über den Kenntnisstand und die Implementierung von Zero-Trust erfahren. Zwar werben viele Netzwerk- und Security-Anbieter implizit oder direkt mit dem Begriff „Zero-Trust“, was aber damit gemeint ist, kann sich stark unterscheiden. Für weitere Verwirrung sorgen zudem die Begriffe „Zero-Trust-Access“ (ZTA) und „Zero-Trust-Network-Access“ (ZTNA), die oft synonym verwendet werden.

Die Befragten gaben an, dass sie die Konzepte hinter Zero-Trust (77 %) und ZTNA (75 %) verstünden und zuversichtlich seien, einen sicheren Zugang bereitzustellen.

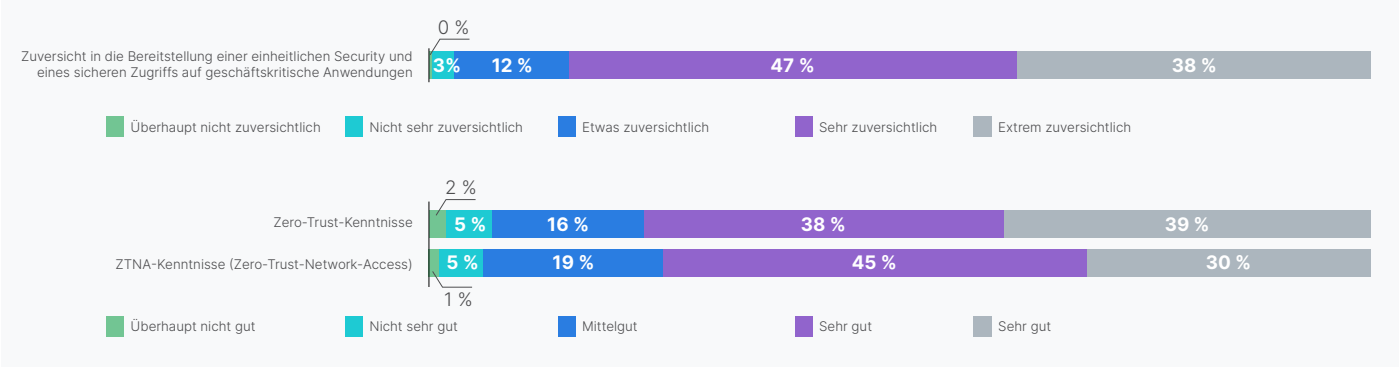


Abbildung 4: Kenntnisstand und Implementierung

Diskrepanz zwischen Implementierung und tatsächlicher Sicherheit

Interessanterweise gaben die meisten Umfrageteilnehmer an, dass sie bereits eine Zero-Trust- und/oder ZTNA-Strategie haben oder derzeit entwickeln. Ein Drittel hat die Implementierung nach eigenen Angaben bereits abgeschlossen und nur 6 % haben noch nicht damit begonnen.

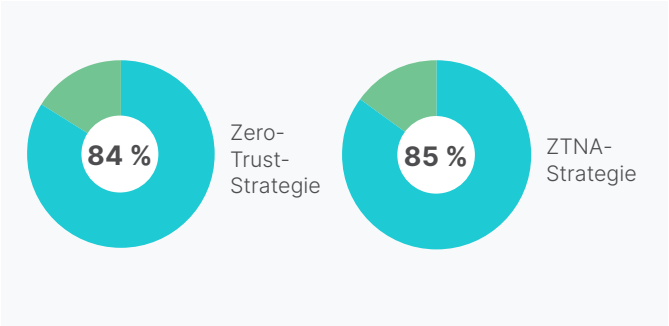


Abbildung 5: Vorhanden oder in Entwicklung

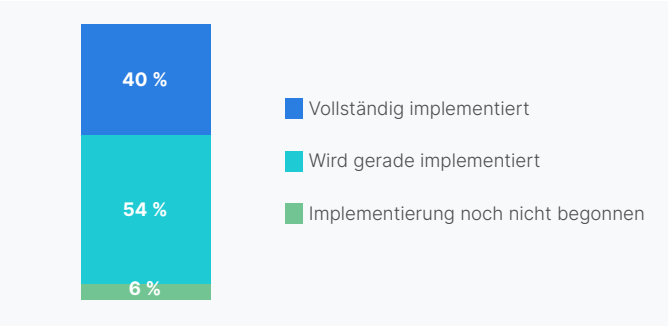


Abbildung 6: Stand der Implementierung

Obwohl eine beträchtliche Anzahl von Unternehmen angeben, dass sie eine ZTNA- oder Zero-Trust-Strategie entweder vollständig implementiert haben oder gerade daran arbeiten, kann über die Hälfte davon Benutzer und Geräte nicht kontinuierlich authentifizieren und hat Schwierigkeiten mit der Überwachung von Benutzern nach der Authentifizierung.

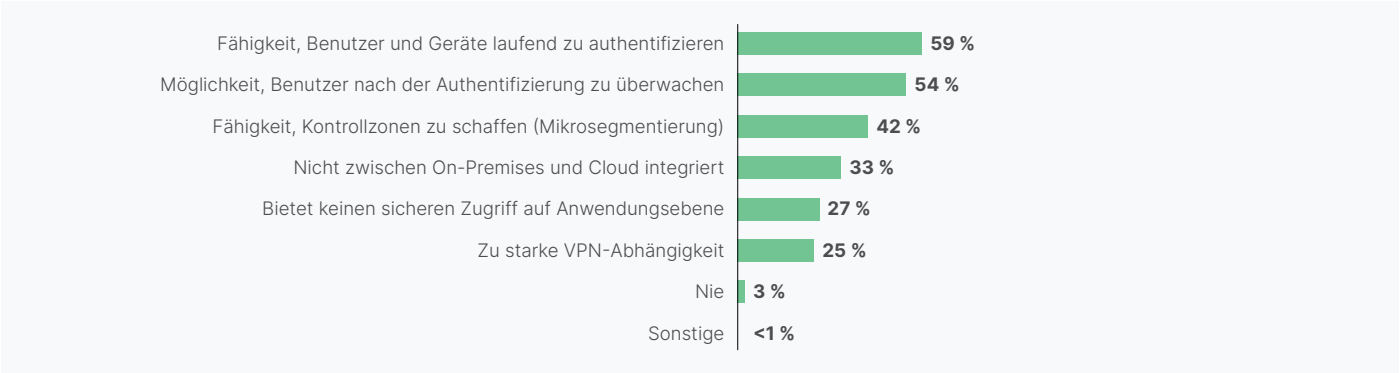


Abbildung 7: Defizite, die bei Zero-Trust-Strategien behoben werden müssen

Diese Probleme sind besorgniserregend, da beide Sicherheitsfunktionen zu den Grundelementen von Zero-Trust zählen. Das wirft die Frage auf, was für eine Art von Zero-Trust-Konzept bei Unternehmen tatsächlich implementiert ist. Es könnte gut sein, dass die Befragten nur annehmen, sie *hätten* eine funktionierende Zero-Trust-Lösung, oder sich nicht bewusst sind, dass die Implementierung unvollständig ist.

Die Umfrageergebnisse zeigen eine Diskrepanz zwischen den bestehenden Lösungen in Unternehmen und dem Grad an Sicherheit, den sie de facto für einen vollständigen Schutz brauchen.

Von solchen Sicherheitsproblemen berichten Unternehmen aus allen Regionen – die Authentifizierung und Überwachung von Benutzern scheint also weltweit ein Problem zu sein.

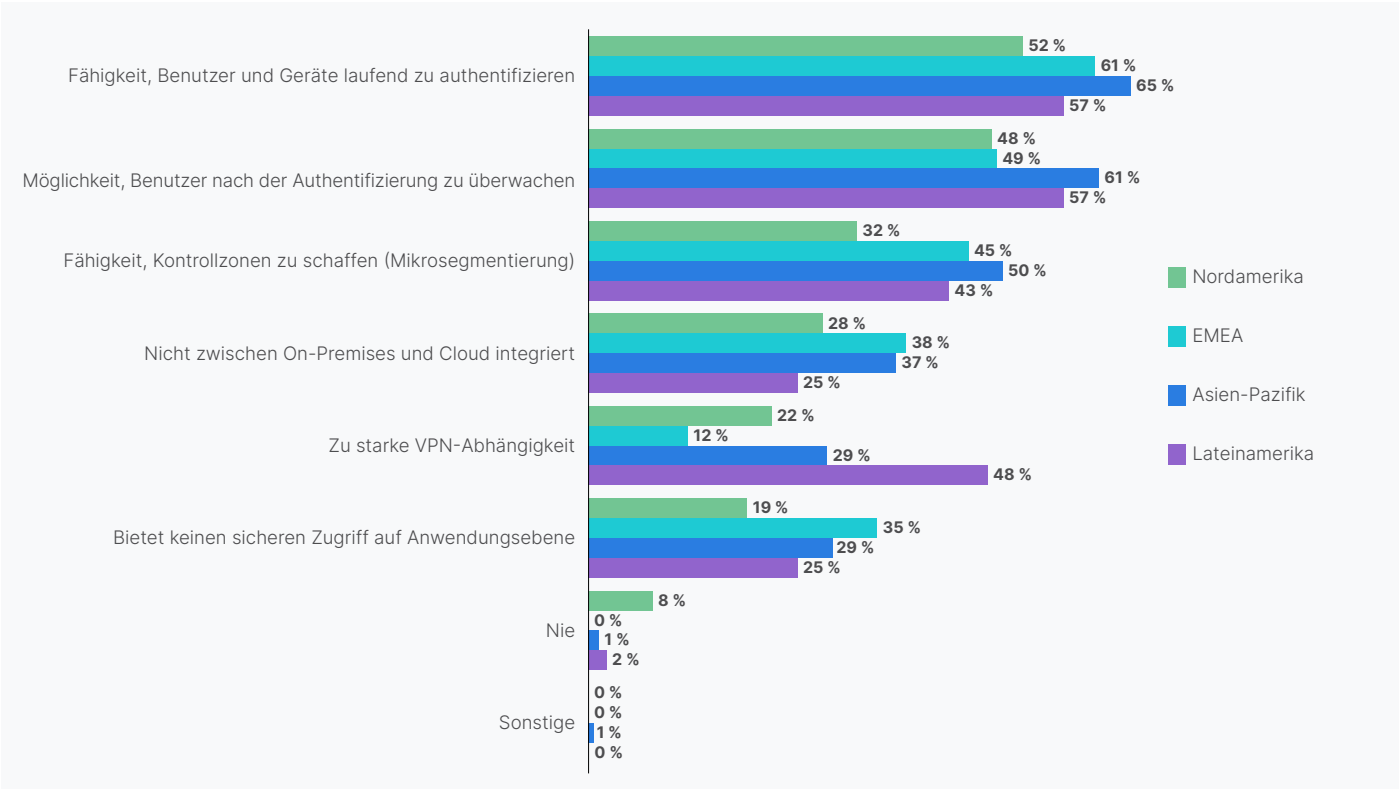


Abbildung 8: Defizite, die bei Zero-Trust-Strategien behoben werden müssen

Obwohl die Befragten angeben, sich mit Zero-Trust-Konzepten gut auszukennen, waren über 80 % der Ansicht, dass die Implementierung einer Zero-Trust-Strategie in einem erweiterten Netzwerk nicht leicht sein würde. Die meisten (60 %) gehen davon aus, dass dies etwas oder sehr schwierig werde, weitere 21 % rechnen mit großen Hindernissen.

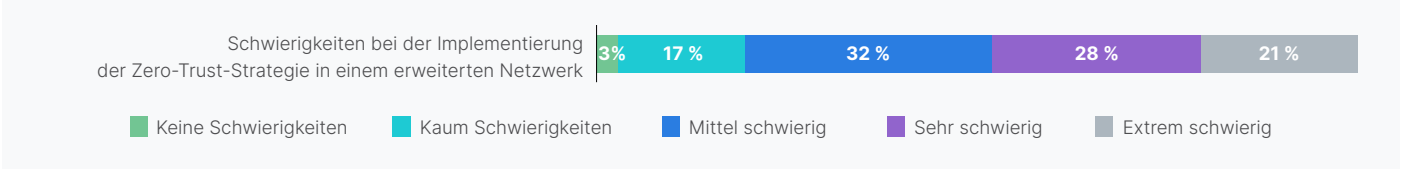


Abbildung 9: Schwierigkeiten bei der Implementierung

Diese Diskrepanzen aus der Studie bekräftigen die Vermutung, dass Unternehmen zwar über einige Zero-Trust-Komponenten verfügen, viele jedoch nicht alle wesentlichen Funktionen implementiert haben.

Hindernisse für die Zero-Trust-Implementierung

Dass Zero-Trust-Konzepte eine gute Idee sind, bezweifelt kaum ein Unternehmen. Aber das Hinzufügen eines weiteren Produkts oder einer Produkt-Suite zu einer bereits hochkomplexen Netzwerk-Umgebung ist in der Praxis abschreckender, als viele zugeben möchten.

Viele Unternehmen implementieren separate Security-Komponenten, weil sie keinen Anbieter mit einer passenden Komplettlösung finden konnten. Das Ergebnis ist oft eine unvollständige, nicht integrierte Lösung mit einer komplexen Bereitstellung und Maintenance, die zu wenig Transparenz über das gesamte Netzwerk bietet.

Die große Mehrheit der Befragten weiß, dass eine Zero-Trust-Sicherheitslösung in die Infrastruktur integriert werden, in der Cloud sowie On-Premises funktionieren und Schutz auf Anwendungsebene bieten muss.

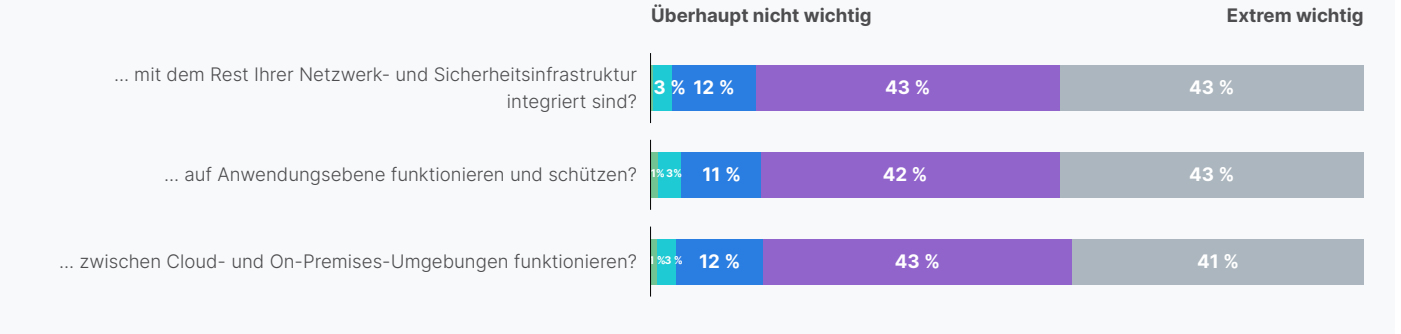


Abbildung 10: Wie wichtig ist es, dass eine Zero-Trust-Strategie Sicherheitslösungen umfasst, die ...

Ungeachtet dieser Erkenntnis besteht jedoch die größte Herausforderung für Unternehmen bei einer Zero-Trust-Strategie darin, dass es nur wenige qualifizierte Anbieter einer Komplettlösung gibt.

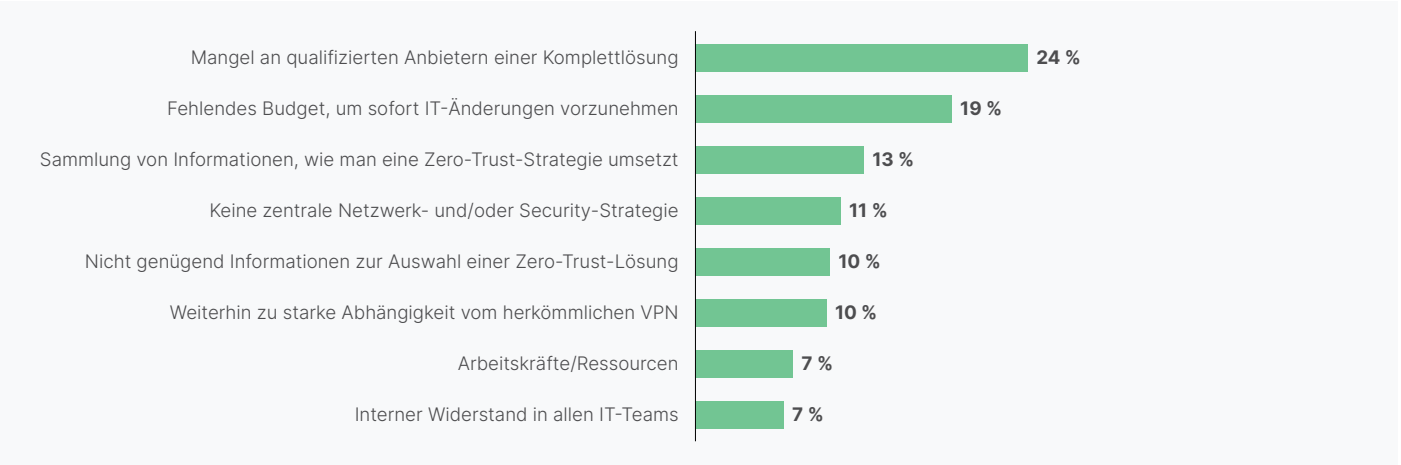


Abbildung 11: Größte Herausforderung bei der Umsetzung einer Zero-Trust-Strategie

Fazit

Obwohl Unternehmen an der Implementierung von Zero-Trust arbeiten, zeigt die Umfrage eklatante Sicherheitsdefizite auf. Das lässt darauf schließen, dass die Zero-Trust-Bereitstellung bei weitem nicht so reibungslos oder einfach funktioniert, wie es manche Anbieter vermuten lassen.

Eine gute Zero-Trust-Lösung bietet umfassende Transparenz auf ganzer Linie: Security- und Netzwerk-Teams können jederzeit genau sehen, wer und was sich zu einem bestimmten Zeitpunkt im Netzwerk befindet. Auch werden authentifizierten Benutzern und Geräten nur die absolut notwendigen Zugriffsrechte gewährt. Beklagen Unternehmen also, dass sie Benutzer und Geräte nicht kontinuierlich authentifizieren können und Schwierigkeiten haben, die Benutzer-Authentifizierung zu überwachen, funktioniert die Zero-Trust-Lösung nicht richtig.

Authentifizierung, Zugangskontrolle und Benutzeridentität sind allesamt wichtige Elemente von Zero-Trust. Um zu wissen, was sich im Netzwerk befindet, sollten Unternehmen eine Netzwerk-Zugangskontrolle (Network Access Control, NAC) haben. Damit lässt sich jedes Gerät im Netzwerk (oder das auf das Netzwerk zugreifen will) erkennen und identifizieren sowie sicherzustellen, dass ein Gerät nicht bereits kompromittiert wurde.

Die Benutzeridentität ist ein weiterer Eckpfeiler von Zero-Trust. Genau wie die Geräte muss auch jeder Benutzer identifiziert werden. AAA-Dienste (Authentifizierung, Autorisierung und Accounting), Zugangs-Management und Single Sign-On (SSO) dienen zur Identifizierung und Anwendung der richtigen Zugriffsrechte für einen Benutzer je nach seiner Aufgabe im Unternehmen. Der Zugriff sollte mit weiteren Sicherheitsmaßnahmen wie einer Mikrosegmentierung kombiniert werden. Nur so lässt sich die Kontrolle darüber behalten, auf welche Netzwerk-Bereiche ein Anwender zugreifen darf. Ebenfalls sollten Benutzer und Geräte kontinuierlich überwacht werden, um die jederzeitige Einhaltung von Richtlinien zu gewährleisten. Auch müssen diese Kontrollen einheitlich und konsequent an jedem Ort im Netzwerk angewendet sowie nahtlos zwischen Netzwerk-Umgebungen übernommen werden.

Eine effektive Zero-Trust-Lösung muss all diese Aufgaben erfüllen. Ist dies nicht möglich, sollten Unternehmen ihre Zero-Trust-Strategien und -Produkte überdenken. Es gibt schließlich integrierte Komplettlösungen zur Implementierung von Zero-Trust im gesamten Netzwerk, einschließlich in der Cloud und On-Premises.

Die Entwicklung einer Ad-hoc-Lösung mit unterschiedlichen Security-Tools kann zu Sicherheitslücken sowie Management- und Konfigurationsproblemen führen. Im Gegensatz dazu reduziert eine einheitliche, plattformbasierte Lösung – mit nahtlos integrierten Sicherheitskontrollen sowie konsolidierten Management-, Orchestrierungs- und Reporting-Tools – den Mehraufwand bei der Bereitstellung, Konfiguration und Fehlerbehebung erheblich.

Eine effektive Zero-Trust-Lösung braucht Security-Elemente, die von Grund auf als integriertes System zusammenarbeiten. Das ist notwendig, um genau die Sicherheits- und Transparenzlücken beim Management zu vermeiden, die die Umfrageteilnehmer als problematisch anführten.

[1] „Verizon 2021 Data Breach Investigations Report“. Verizon, 2021.

[2] „Cost of a Data Breach Report 2021“. IBM und Ponemon Institute, Juli 2021.

[3] Mike Wronski: „Since Remote Work Isn’t Going Away, Security Should Be the Focus“. Dark Reading, 24. September 2020.

[4] „Global Threat Landscape Report“. FortiGuard Labs, August 2020.

20. Juni 2022, 00:03

1310666-0-1-DE