CSO

Microsoft Security

SPONSORED CONTENT

Zero-Trust-Sicherheit: **Erkenntnisse von Early Adopters**

CSO Microsoft Security

Inhaltsverzeichnis

CSO Microsoft Security

Einführung

Die Umwälzungen der letzten zwei Jahre haben die traditionellen IT- und Sicherheitsmodelle erschüttert. Im Zuge dieser Entwicklung ist Zero-Trust-Sicherheit schnell von einem interessanten Konzept zur Grundlage der modernen Unternehmenssicherheit geworden.

Laut einer neuen Studie von Foundry befinden sich 52 % der Unternehmen in der Pilotphase oder haben bereits eine Zero-Trust-Architektur bereitgestellt. Weitere 15 % sind gerade dabei, sich über Zero-Trust-Modelle zu informieren. Diese Anwender berichten über zahlreiche Vorteile ihrer Bereitstellungen und führen u. a. einen besseren Schutz von Kundendaten, eine Verringerung der Komplexität und die Möglichkeit eines sicheren, zuverlässigen Zugriffs auf Unternehmensressourcen an.

Dieses E-Book befasst sich mit den Ergebnissen der Foundry-Studie, die deutlich machen, wie wichtig eine Zero-Trust-Strategie für CISOs ist, um ihre Unternehmen besser vor verschiedensten, durch zahlreiche Angriffsvektoren bedingten Risiken schützen zu können. Alle, die erst am Anfang ihres Weges stehen, finden hier auch Ratschläge zur Implementierung von Zero Trust.

Über die Umfrage

Foundry hat im Februar und März 2022 US-amerikanische Unternehmen zum aktuellen Stand ihrer Zero-Trust-Einführung befragt. Bei den Befragten musste es sich um IT-Manager*innen oder Mitarbeitende in einer höheren Position in einem Unternehmen mit mindestens 500 Beschäftigten handeln, die am Kauf von Produkten und Diensten im Bereich Cybersicherheit beteiligt sind.

Insgesamt nahmen 250 Personen an der 23 Fragen umfassenden Umfrage teil.

CSO Microsoft Security

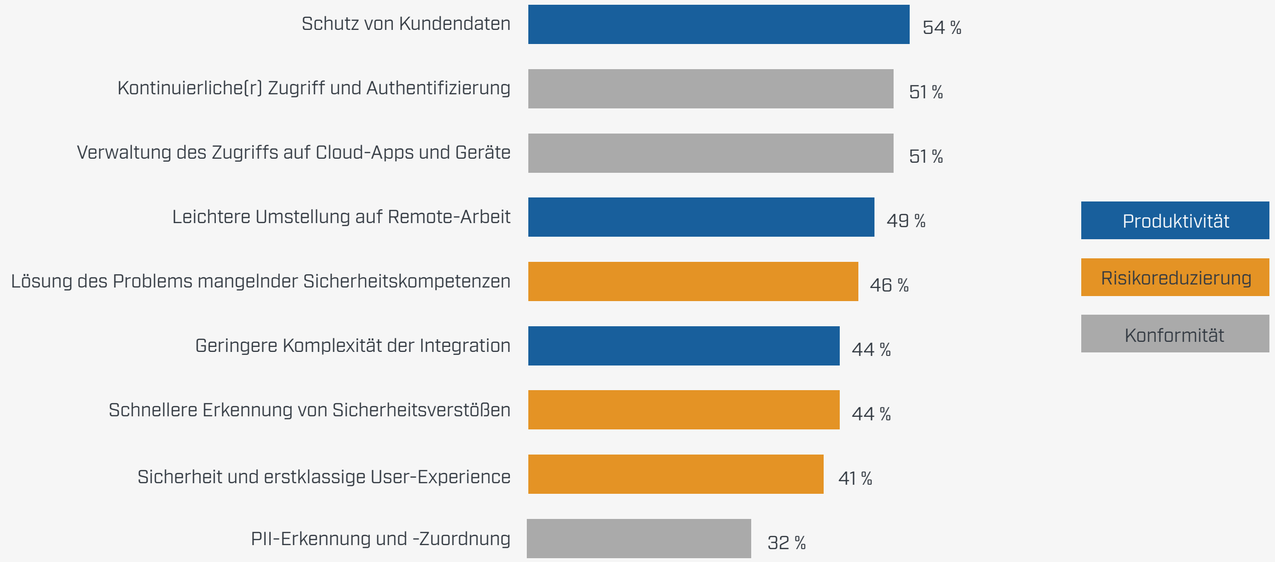
Zero Trust ist Realität und bietet diverse Vorteile

Aus den Umfrageergebnissen sowie den eingehenden Befragungen von Führungskräften aus dem IT- und Sicherheitsbereich geht klar hervor, dass Zero Trust für die meisten Unternehmen höchste Priorität hat. Diejenigen, die schon verschiedene Zero-Trust-Komponenten bereitgestellt haben, stellen bereits die Vorteile hiervon fest.

Die meisten Teilnehmer*innen, die Zero Trust implementiert haben (87 %), geben an, dass die Architektur ihre ursprünglichen Ziele in Bezug auf Implementierung, Einführung und Integration erfüllt oder sogar übertrifft.

„[Zero Trust] ist für uns zu einem Standardverfahren geworden. Ich kann mir nicht vorstellen, dass wir noch einmal zum Status vor der Einführung von Zero Trust zurückkehren“, so der IT Director eines globalen Einzelhändlers. (Den Teilnehmer*innen wurde Anonymität zugesichert, damit sie frei über ihre Sicherheitspläne sprechen konnten.)

Seit der Implementierung von Zero Trust erzielte Vorteile



12 % der Befragten gaben an, *alle* diese Vorteile zu erzielen.

Quelle: Zero Trust Adoption Survey, März 2022, Foundry. Basis: 250

CSO Microsoft Security

Ungefähr 44 % der Befragten gaben zudem an, Zero Trust habe die mit der Implementierung einer integrierten Sicherheitsarchitektur einhergehende Komplexität verringert. „Da Sie es mit einem Framework zu tun haben, ist alles weniger kompliziert“, erläutert der CISO eines Callcenter-Unternehmens mit 3.500 Beschäftigten.

Ein VP und CISO für ein Finanzdienstleistungsunternehmen mit 17.000 Beschäftigten berichtet, dass die Multi-Faktor-Authentifizierung, die sein Unternehmen im Rahmen von Zero Trust eingeführt hat, von den Mitarbeitenden begeistert aufgenommen wurde. „Die Mitarbeitenden sind zufriedener, da sie nicht mehr auf ein vom Unternehmen zur Verfügung gestelltes Gerät und einen VPN-Client angewiesen sind, sondern überall auf die Ressourcen zugreifen können“, erläutert er.

Auch das Konzept des Zugriffs mit den geringsten Rechten hat sich bewährt, wie der CISO bemerkt. „Durch die Implementierung dieses Systems des Zugriffs mit den geringsten Rechten hat es bei uns weniger katastrophale Fehler von Systemadministratoren gegeben“, führt er aus. „Sie erhalten Berechtigungen für bestimmte Dinge und bestimmte Zeiträume, wodurch sich die Wahrscheinlichkeit von Fehlern verringert.“

Angesichts der zunehmenden Verbreitung von Phishing und anderen Cyberangriffen fasst der IT Director des Einzelhandelsunternehmens die Vorteile von Zero Trust wie folgt zusammen: „Ohne diese Arten von Tools befänden wir uns wahrscheinlich in einer schwierigen Lage und müssten jetzt im Moment Zahlungen in Bitcoins an irgendjemanden leisten.“

CSO Microsoft Security

Triebkräfte der Zero-Trust-Bereitstellung

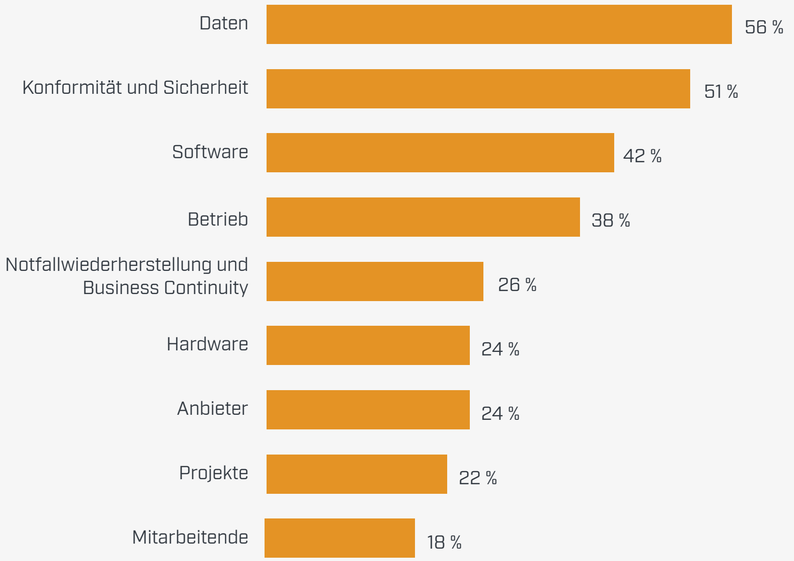
Das Zusammentreffen mehrerer Ereignisse bringt die Unternehmen dazu, zumindest über eine Zero-Trust-Architektur nachzudenken. In erster Linie besteht die Notwendigkeit, die Gefahren zu bewältigen, denen verschiedenste Ressourcen durch zahlreiche Bedrohungen ausgesetzt sind. Die Teilnehmer*innen der Umfrage führten die Sicherheitsvorfälle eines Jahres auf eine Reihe von Ursachen zurück, wobei durch externe Personen oder Unternehmen bedingte Sicherheitslücken an erster Stelle standen. Weitere Ursachen:

- Unerwartete Geschäftsrisiken
- Fehlkonfiguration von Diensten oder Systemen
- Böswillige vorsätzliche Insiderangriffe
- Nicht böswillige Fehler von Benutzer*innen, z. B. Opfer von Phishing-Angriffen
- Kompromittierte Identitäten
- Nicht gepatchte Software
- Gestohlene Anmeldedaten

Diese Vorfälle bergen eine Reihe von Risiken, insbesondere für die Daten.

Infolge des durch die Pandemie bedingten plötzlichen Umstiegs auf Remote-Arbeit trieben viele Unternehmen ihre Pläne zur Einführung von Zero Trust voran, da herkömmliche perimeterbasierte Sicherheitsmodelle allmählich veraltet waren. Viele Unternehmen hatten diesen Weg im Zuge der zunehmenden Verlagerung von Anwendungen und IT-Infrastruktur in die Cloud bereits eingeschlagen, doch die Pandemie gab dem Ganzen einen zusätzlichen Schub.

Am stärksten durch Bedrohungen im Bereich Cybersicherheit gefährdete Bereiche



Quelle: Zero Trust Adoption Survey, März 2022, Foundry. Basis: 250

CSO Microsoft Security

So erläutert beispielsweise der CISO eines Unternehmens aus dem Bereich der Medizintechnik mit 1.700 Mitarbeitenden, dass die Cloud und die Pandemie die Einführung von Zero Trust in seinem Unternehmen vorangetrieben hätten und Zero Trust jetzt eine sichere Grundlage für zukünftige Arbeitsplatzmodelle aller Art bietet.

„Die geschäftliche Motivation war die Tatsache, dass wir ein cloudbasiertes Unternehmen sind und in der Lage sein müssen, unsere Umgebung zu schützen“, führt er aus. „Zudem brauchten wir während der Pandemie eine leistungsfähige Remotebelegschaft. [Dank Zero Trust] konnten wir unseren Bedarf an Immobilien deutlich verringern und werden wahrscheinlich zu mindestens 60 % ein virtuelles Remoteunternehmen bleiben.“

CSO Microsoft Security

Vielzahl von Bedrohungen

Auch Complianceanforderungen haben den Anstoß für robustere Sicherheitsmodelle gegeben. „Die Regulierungsbehörden beobachten uns und erwarten, dass wir unser Sicherheitsframework weiter verbessern“, erklärt der SVP of Global Information Security eines Finanzdienstleistungsunternehmens mit 290.000 Mitarbeitenden.

Manche Unternehmen haben proaktiv Schritte in Richtung Zero Trust unternommen, um viel beachtete Sicherheitsverstöße zu vermeiden, die sie aus den falschen Gründen in die Schlagzeilen bringen. „Es ging darum, proaktiv zu handeln und nicht zum Nachrichtenthema zu werden“, erläutert der CIO einer Hochschuleinrichtung mit 3.500 Mitarbeitenden. „Es gibt wirkliche Horrorgeschichten von anderen lokalen Einrichtungen unserer Größe, bei denen lange Zeit nichts mehr ging.“

Andere haben bereits einen schwerwiegenden Vorfall im Bereich Cybersicherheit erlebt und wurden dadurch zu einer schnellen Überarbeitung ihrer Sicherheitsstrategie veranlasst. Nachdem ein Versicherungsunternehmen mit 6.000 Mitarbeitenden einen Ransomwareangriff erlitten hatte, der das Unternehmensnetzwerk zwei Wochen lahmlegte, kam die Anweisung zur Einführung von Zero Trust direkt vom CEO. „Wir haben die Implementierung schnell vorangetrieben“, erklärt der VP of IT Development des Unternehmens. „Zunächst ging es definitiv nur um bewährte Methoden, doch nach dem Ransomwareangriff wurde die Implementierung erheblich erweitert.“

Ein cloudbasierter Katalysator

Der VP und CISO eines größeren Finanzdienstleistungsunternehmens erklärt, sein Team habe die Notwendigkeit einer neuen Sicherheitsarchitektur schon vor einigen Jahren erkannt, als es begann, mehr cloudbasierte Ressourcen einzuführen, und die Benutzer*innen zunehmend mobil wurden.

„Uns wurde klar, dass uns die herkömmliche Perimetersicherheitsarchitektur, auf die wir uns bislang verlassen hatten, in Zukunft keinen Schutz vor Angreifern bieten würde“, erläutert er.

Richtig deutlich wurde dies Anfang 2020, als das Unternehmen feststellte, dass ein Angreifer irgendwann im Vorjahr in den Perimeter eingedrungen war und unbemerkt Lateral Movements in der Umgebung durchgeführt hatte. „Wir brauchten eine neue Architektur, in der wir die Verwendung der Ressourcen schützen und authentifizieren konnten, unabhängig davon wo sich diese befanden. Zero Trust ist eine Architektur, die genau hierfür konzipiert ist.“

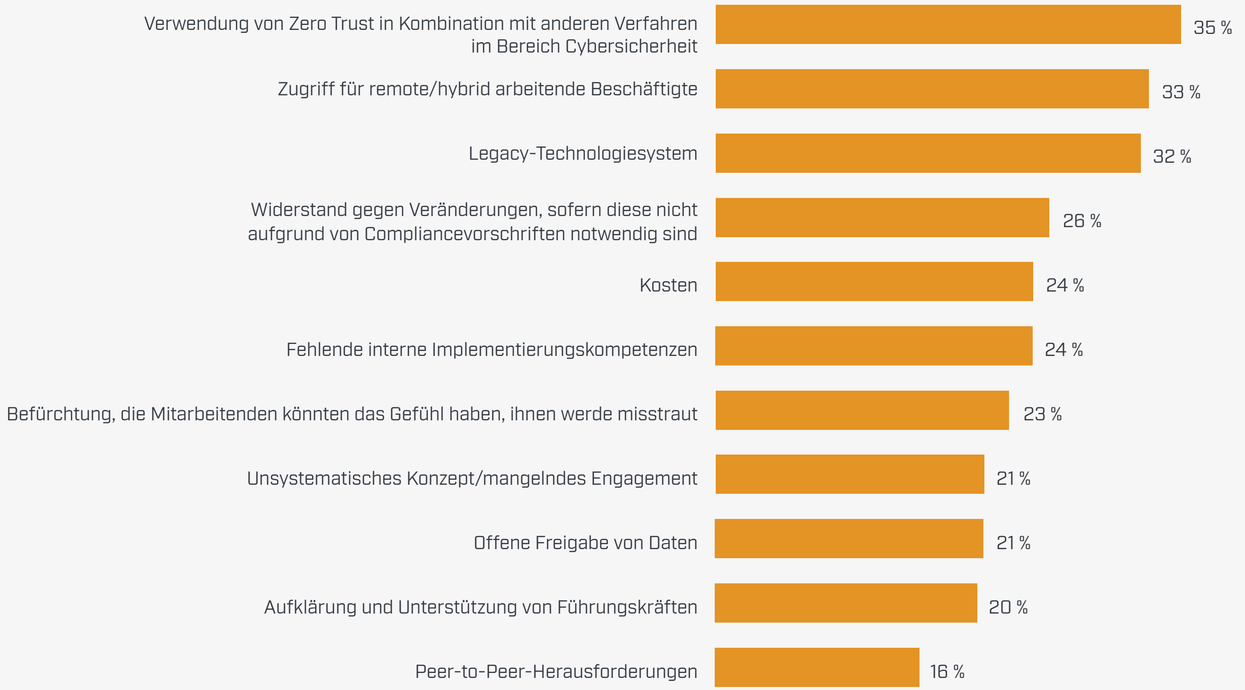
CSO Microsoft Security

Hindernisse für die Einführung von Zero Trust

Für viele Unternehmen bedeutet Zero Trust eine fundamentale Veränderung ihrer Sicherheitsstruktur, ihrer Prozesse und Denkweise. Aus diesem Grund müssen sie einige Hindernisse überwinden, bevor sie Zero Trust einführen.

„Wir sind auf so viele verschiedene Silos in unserem Unternehmen gestoßen“, berichtet der CISO des Callcenters und führt weiter aus, dass die für die Server, das Netzwerk und die Datenbanken zuständigen Teams jeweils ihr eigenes Kontingent an Webservern und -tools hatten. „Das blockierte uns, da jeder eine andere Vorstellung davon hatte, was wir tun sollten und wie dies geschehen sollte.“

Was hält Sie davon ab, Zero Trust einzuführen?



Quelle: Zero Trust Adoption Survey, März 2022, Foundry. Basis: 250

CSO Microsoft Security

Die Aufdeckung solcher Probleme kann laut Anthony Mocny, Senior Product Marketing Manager für Zero Trust bei Microsoft, sogar ein positiver Nebeneffekt von Zero Trust sein. „Als Architektur ist Zero Trust darauf ausgelegt, die technologiebasierten Silos der Sicherheitsteams aufzubrechen und eine effektive Zusammenarbeit der Teams zu ermöglichen“, erläutert er. „Zero Trust kann auch einen kulturellen Wandel bedeuten, was die Art und Weise der Zusammenarbeit der Teams anbelangt.“

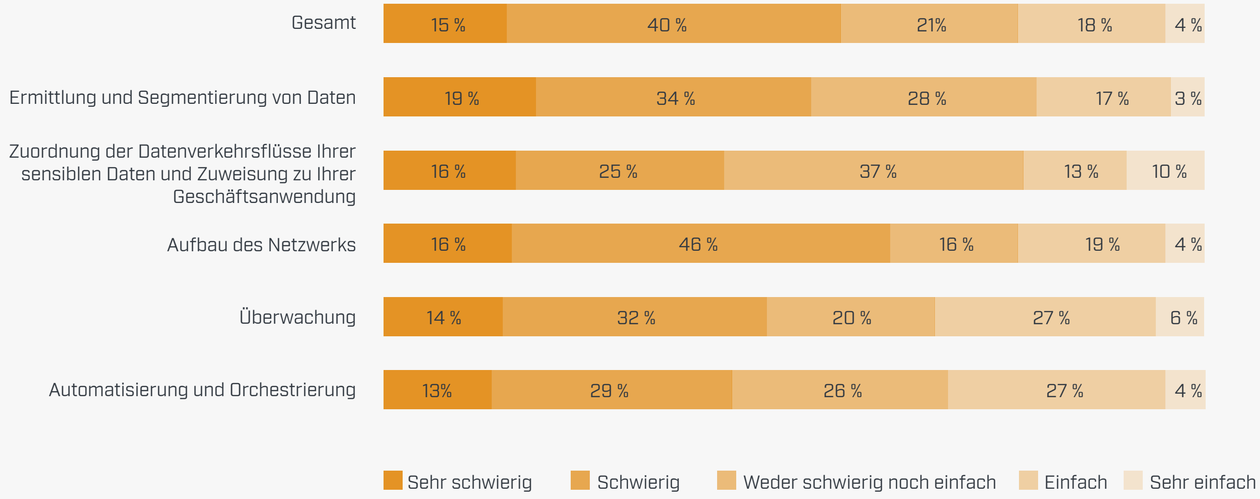
Für den VP/CISO des Finanzdienstleistungsunternehmens stellten ältere Anwendungen ein Hindernis auf dem Weg zu Zero Trust dar. „Sie müssen mit moderner Authentifizierungstechnologie nachgerüstet werden“, erläutert er. „Je nachdem, wie alt sie sind, ist dies unter Umständen nicht leicht möglich.“

CSO Microsoft Security

Herausforderungen bei der Bereitstellung

Unternehmen, die sich für die Einführung von Zero Trust entschieden haben, können bei der Implementierung vor einer Vielzahl von Herausforderungen stehen. Mehr als die Hälfte der Umfrageteilnehmer*innen (56 %) empfand die Implementierung von Zero Trust als schwierig oder sehr schwierig. Insbesondere folgende Probleme traten auf:

Wie schwierig ist die Implementierung von Zero Trust?



Quelle: Zero Trust Adoption Survey, März 2022, Foundry. Basis: 168

CSO Microsoft Security

Herausforderungen im Zusammenhang mit der Segmentierung und Mikrosegmentierung wurden bei den eingehenden Befragungen häufig angeführt.

„Sie segmentieren Ihr Netzwerk bis zum einzelnen Host“, erklärt der VP/CISO des Finanzdienstleistungsunternehmens. „Das ist ein bisschen so, als würden Sie zwischen den einzelnen Hosts im internen Netzwerk eine kleine Firewall einrichten, sodass Sie den gesamten Datenverkehr verfolgen und bis hin zum einzelnen Rechner kontrollieren können. Das bietet enorme Sicherheitsvorteile, ist aber extrem schwer zu implementieren, da Sie jetzt im Prinzip Zehntausende Firewalls verwalten müssen.“

Auch die Zuordnung von Datenverkehrsflüssen kann mehrere Monate dauern. Dies macht der CTO eines Verlags- und Medienunternehmens mit 5.000 Mitarbeitenden deutlich. Nach der Definition der kritischen Daten, Anwendungen und Netzwerkdienste, die geschützt werden mussten, „haben wir die Transaktionsflüsse im Netzwerk zugeordnet und versucht, sie als Informationsgruppen zu verstehen“, erklärt er. „[Anschließend] haben wir Teile dieser Informationen segmentiert und untersucht, wie diese das Netzwerk durchqueren. Dabei gingen wir sogar bis auf die Ebene einzelner Informationspakete.“ An diesem Punkt hat das Unternehmen Zero-Trust-Richtlinien auf jede Art von Datenverkehrsfluss angewendet. „Wir haben auch neue Möglichkeiten zur Überwachung und Unterhaltung unseres Netzwerks geschaffen.“

Trotz der Herausforderungen sind viele Umfrageteilnehmer*innen der Auffassung, dass Zero Trust letztendlich die täglichen Abläufe vereinfacht. Mit herkömmlichen Technologien „brauchen wir Tage, um Änderungen vorzunehmen. Diese müssen auf alle Hardware- und Softwarekomponenten übertragen werden, und wir benötigen viele Ressourcen hierfür“, erörtert der SVP for Global Information Security des Finanzdiensleistungsunternehmens. „Mit Zero Trust können wir die Komplexität der Architektur langfristig wirklich minimieren und benötigen weniger Mitarbeitende für dieselbe Art von Arbeit.“

Bewährte Methoden für die Implementierung von Zero Trust

Immer mehr Unternehmen implementieren eine Zero-Trust-Architektur und entwickeln dabei Roadmaps und bewährte Methoden, denen andere folgen können. Im Folgenden sprechen wir über fünf Dinge, die bei der Planung einer Bereitstellung zu berücksichtigen sind.

Nehmen Sie sich am Anfang nicht zu viel vor

Eine Zero-Trust-Strategie auszuarbeiten, kann schwierig erscheinen, wenn Sie sie nur im breiteren Kontext sehen und direkt daran denken, dass Sie Richtlinien und Schutzmaßnahmen für Netzwerke, Daten, Anwendungen, Identitäten, Endpunkte und die Infrastruktur überarbeiten müssen. „Zunächst sahen wir nur diesen riesigen Berg, den wir erklimmen mussten, und fragten uns, ob wir das wirklich schaffen würden“, erklärt der CIO der Hochschuleinrichtung. „Sie müssen Schritt für Schritt vorgehen.“

Letztendlich entschieden sich der CIO und sein Team für ein „Follow the Money“-Konzept und räumten der Segmentierung von Finanz- und Lohnbuchhaltungsanwendungen in einem separaten Netzwerk Priorität ein.

Die Assets zu ermitteln, die am dringendsten geschützt werden müssen, ist laut Mocny eine vernünftige Vorgehensweise. „Denken Sie daran, warum Sie Zero Trust überhaupt implementieren“, meint er.

Beginnen Sie im Zweifelsfall mit der Multi-Faktor-Authentifizierung

Bei der Priorisierung des Sicherheitsstacks empfehlen viele CISOs und Sicherheitsanbieter zunächst eine Fokussierung auf die Authentifizierung und andere identitätsbasierte Schutzmaßnahmen. „Wenn Sie nicht wissen, wo Sie beginnen sollen, ist Multi-Faktor-Authentifizierung ein guter Ausgangspunkt“, führt Mocny aus. Nach Einschätzung von Microsoft lassen sich mit Multi-Faktor-Authentifizierung über 90 % der identitätsbasierten Angriffe verhindern.

Der VP/CISO des Finanzdienstleistungsunternehmens stimmt dem zu. „Authentifizierung ist ein grundlegendes Element der Implementierung einer Zero-Trust-Architektur. Die anderen Komponenten funktionieren alle nicht, wenn es nicht möglich ist, die Identität des Anwenders zu prüfen. Daher haben wir damit begonnen.“

Im nächsten Schritt befasste sich der VP/CISO des Finanzdienstleistungsunternehmens mit der Netzwerkkomponente. Dies brachte unmittelbare Vorteile im Hinblick auf die Unterstützung von remote arbeitenden Beschäftigten. Das Team verschob die Mikrosegmentierung auf einen späteren Zeitpunkt, da diese Maßnahme für das gesamte Unternehmen nicht ohne weiteres sichtbar ist. „Wenn dieser Schritt geschafft ist, sind Sie wesentlich sicherer, doch niemand bemerkt den Unterschied“, meint er.

CSO Microsoft Security

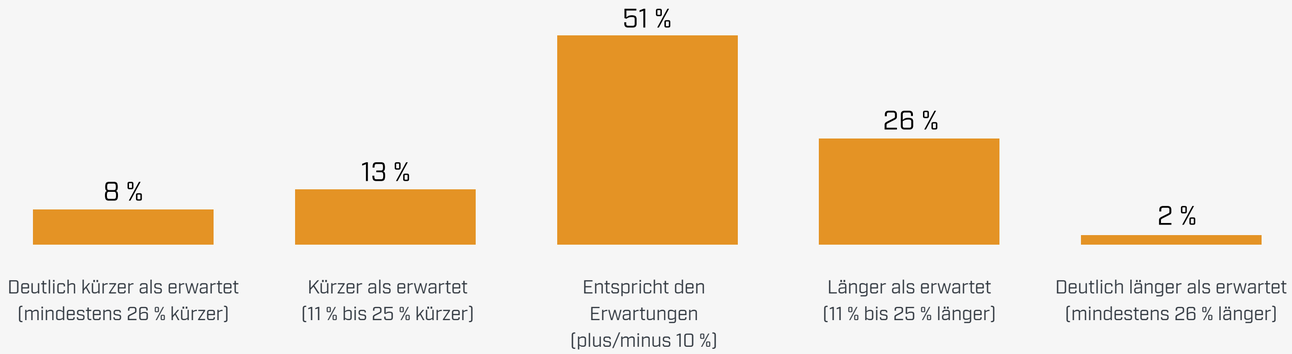
Legen Sie einen realistischen Zeitrahmen fest

Es ist wichtig, dass CISOs realistische Erwartungen in Bezug auf Zero-Trust-Bereitstellungen stellen. „Die Implementierung einer Zero-Trust-Architektur ist ein Programm und kein Projekt“, meint der VP/CISO des Finanzdienstleistungsunternehmens. „Das ist eine gewaltige Veränderung. Um dies richtig zu machen, sind zahlreiche Projekte erforderlich, und wahrscheinlich wird es Jahre dauern. Eine Zero-Trust-Architektur lässt sich nicht schnell und einfach implementieren.“

Sein Kollege, der SVP des Finanzdienstleistungsunternehmens stimmt zu. „Ich denke nicht, dass wir überhaupt jemals fertig werden, denn es wird immer neue Technologien, neue Malware und neue Bedrohungen geben“, meint er.

Die Mehrheit der Umfrageteilnehmer*innen (72 %) gab an, mit ihrer Bereitstellung entweder im Zeitplan zu liegen oder sogar schneller als geplant voranzukommen. Die restlichen Teilnehmer*innen erklärten, die Implementierung dauere länger als erwartet.

Entspricht die Zero-Trust-Bereitstellung Ihren Zeitvorgaben?



Quelle: Zero Trust Adoption Survey, März 2022, Foundry. Basis: 168

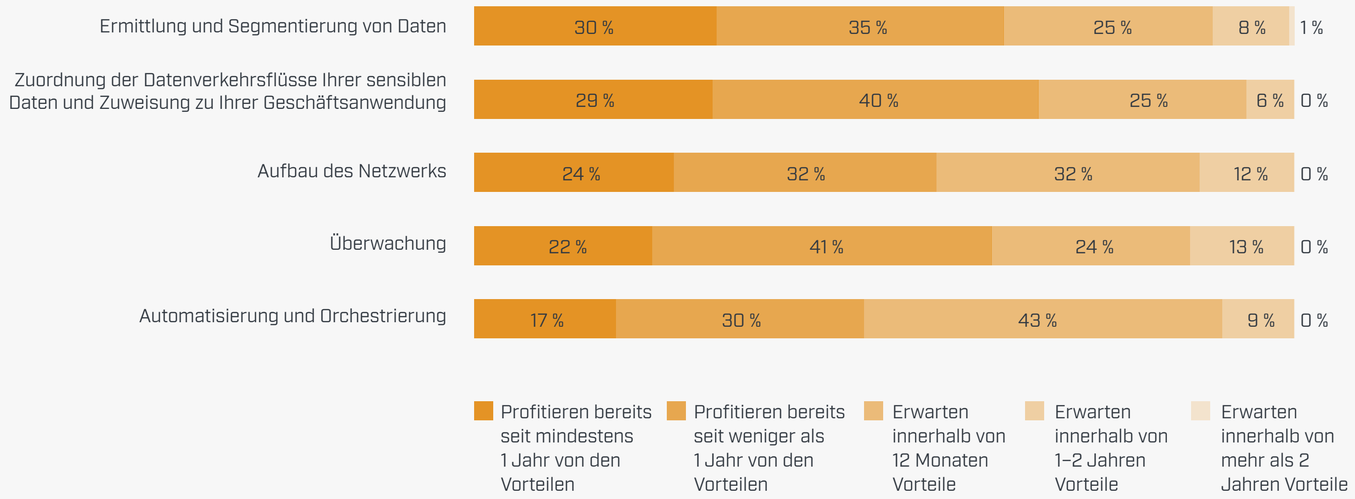
CSO Microsoft Security

Messen Sie Ihre Fortschritte

Im Verlauf einer Zero-Trust-Bereitstellung können und sollten CISOs Meilensteine festlegen, um die Fortschritte zu messen. Es ist ein gutes Zeichen, dass rund zwei Drittel der Umfrageteilnehmer*innen angeben, innerhalb eines Jahres in Bezug auf die meisten Aspekte ihrer Projekte profitiert zu haben, und mindestens ein weiteres Viertel dies innerhalb von 12 Monaten erwartet, und zwar bei wichtigen Aktivitäten wie der Ermittlung und Segmentierung von Daten, der Zuordnung von Datenverkehrsflüssen und dem Aufbau des Netzwerks.

„Zero Trust ist ein Weg, denn Sie müssen ständig Evaluierungen durchführen, um angesichts der sich ändernden Art der Angriffe geschützt zu bleiben“, meint Mocny. „Halten Sie immer Ausschau nach Verbesserungsmöglichkeiten.“

Zeitdauer, bis Zero-Trust-Vorteile erzielt werden



Quelle: Zero Trust Adoption Survey, März 2022, Foundry. Basis: 103

Fokussieren Sie sich auf Menschen, nicht nur auf Technologie

In Anbetracht seiner großen Reichweite hat das Zero-Trust-Sicherheitsmodell Auswirkungen auf alle Mitarbeitenden, einschließlich der IT- und Sicherheitsteams, die mit der Umsetzung des Modells beauftragt sind. Daher ist es wie bei jedem großen Technologieprojekt wichtig, dass die Bereitstellungen mit neuen Prozessen und Änderungsmanagementverfahren abgestimmt sind, um eine reibungslose und erfolgreiche Einführung zu gewährleisten.

„Neben technologischen Veränderungen findet auch ein kultureller Wandel statt“, meint Mocny. „Wenn bei Ihnen mehrere Teams für die Sicherheit zuständig sind – darunter auch Netzwerkarchitekt*innen oder Identitätsexpert*innen – müssen Sie auch die Art und Weise der Zusammenarbeit dieser Teams ändern. Sie müssen Silos einreißen, um sicherzustellen, dass alle Technologien effektiv zusammenwirken.“

Um die Silos zu beseitigen, müssen die Teams aus allen diesen Fachbereichen eng in Pilot- und Proof-of-Concept-Projekte (POC) eingebunden werden. Diese Erfahrung musste ein IT Systems Director eines Telekommunikationsunternehmens mit rund 2.000 Mitarbeitenden machen, nachdem es während der Bereitstellung an mehreren Single Points of Failure Probleme gegeben hatte. So konnten sich verschiedene Dienste beispielsweise nicht authentifizieren und galten plötzlich als „nicht vertrauenswürdig“, was dazu führte, dass die betreffenden Dienste sowie einige Systeme nicht verfügbar waren.

„Die Bereitstellung eines Dienstes kann einen Dominoeffekt auslösen und dazu führen, dass andere Dienste nicht mehr funktionieren“, führt er aus. In Zukunft „werden wir viel vorsichtiger vorgehen – mehr POC-Zeit, mehr Überprüfungen, mehr Beurteilungen der Architektur mit Fachexperten vor der Bereitstellung.“

Zero-Trust-ROI

Eine 2021 in Auftrag gegebene **Total Economic Impact™-Studie von Forrester Consulting** beziffert die Kosteneinsparungen und geschäftlichen Vorteile der Zero-Trust-Lösungen von Microsoft. Auf der Grundlage der fünf Unternehmen, die von Forrester befragt wurden, erreichte ein Mischunternehmen durch die Implementierung einer Zero-Trust-Architektur mit Microsoft einen 3-Jahres-ROI von 92 %.

Dieses Mischunternehmen erzielte darüber hinaus Einsparungen in Höhe von durchschnittlich 20 USD pro Mitarbeiter*in pro Monat, da im Rahmen von Zero Trust verschiedene Sicherheitstools überflüssig wurden, darunter Endpunkt-Management-, Antiviren- und Antischadsoftwarelösungen.

CSO Microsoft Security

An welchem Punkt auf dem Weg zu Zero Trust stehen Sie?

Wie die Umfrage zeigt, überwiegen die Vorteile eines Zero-Trust-Sicherheitsmodells eindeutig gegenüber den Herausforderungen, mit denen CISOs und ihre Sicherheitsteams bei der Bereitstellung konfrontiert sind. Wenn Sie diesen Herausforderungen mit einem gut durchdachten Plan begegnen, kann Ihr Unternehmen schnell seinen Schutz verbessern, die Risiken reduzieren und unternehmensweit Mehrwert schaffen.

Wenn Sie den Zero-Trust-Reifegrad Ihres Unternehmens bewerten und weitere praktische Ressourcen zur Bereitstellung erhalten möchten, können Sie die **Bewertung mit dem Zero-Trust-Reifegradmodell** von Microsoft nutzen.