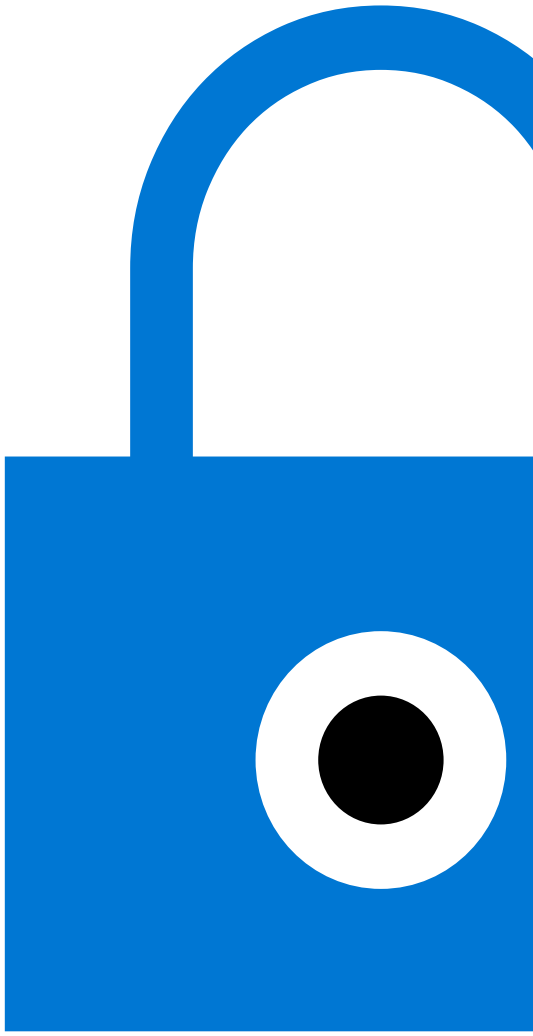
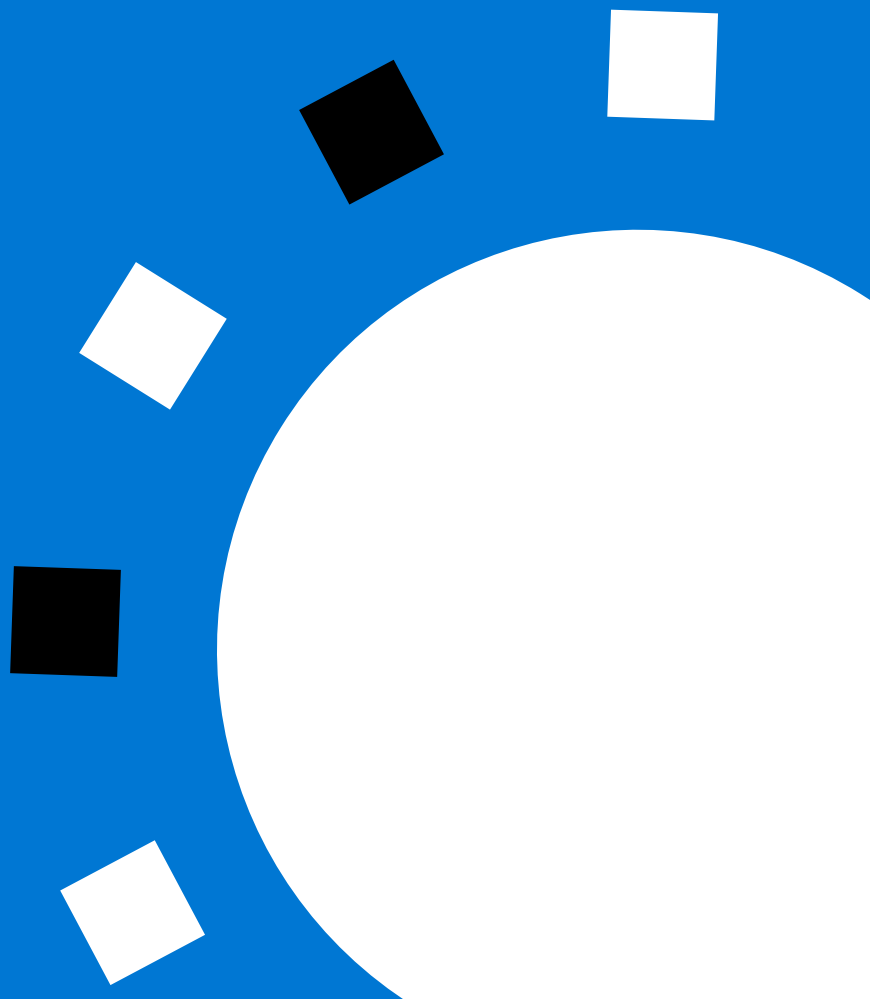
Microsoft



Das Prinzip von Zero Trust

Eine Diskussionsrunde mit Führungskräften

Über die Diskussionsrunde



Am 1. Dezember 2020 veranstalteten Microsoft und die Cloud Security Alliance (CSA) einen virtuellen Roundtable für Führungskräfte, um einen praxisnahen Dialog zu führen und die jeweiligen Visionen zur Zero-Trust-Sicherheit zu erweitern. Ann Johnson, CVP, Security, Compliance, and Identity Business Development bei Microsoft, moderierte die Diskussionsrunde, an der 10 Sicherheitschefs aus namhaften Unternehmen der Energie-, Finanz-, Versicherungs- der Fertigungsbranche teilnahmen. Diese Führungskräfte teilten ihre Erkenntnisse und Erfahrungen, die sie auf ihrer Zero-Trust-Journey gemacht hatten.

Die zentralen Aussagen

Während des Roundtable-Gesprächs diskutierten die Führungskräfte über die Bedeutung, die die Informationssicherheit für die digitale Transformation hat. Sie berichteten von eigenen Erfahrungen und Praxisbeispielen, die ihre strategische Annäherung an die Informationssicherheit geprägt hatten. Außerdem erfahren wir, wie Zero-Trust-Prinzipien umgesetzt wurden, um die gesamte Informationssicherheit zu verbessern.

Die folgenden Themen standen im Mittelpunkt der Gesprächsrunde:

- Hinausdenken über Perimetersicherheit und Umstieg auf einen ganzheitlichen Sicherheitsansatz
- Die Zero-Trust-Journey – klein anfangen mit einzelnen Bausteinen, auf denen die spätere Lösung aufbaut
- Optimierte Einführung der Zero-Trust-Sicherheit im ganzen Unternehmen

Die Zero-Trust-Strategie für moderne Sicherheit

Zero-Trust-Sicherheit ist kein Produkt und keine Lösung.

Es handelt sich um eine breit angelegte Strategie für moderne Sicherheit, die sich nahtlos in komplexe moderne Umgebungen einfügt, mobile Mitarbeiter einbezieht sowie Nutzer, Geräte, Anwendungen und Daten an praktisch jedem Ort schützt. Im Unterschied zu traditionellen Ansätzen, durch die alle Ressourcen in ein „sicheres und konformes" Netzwerk gezwängt wurden, konzentriert sich Zero Trust auf die Sicherheit und Compliance von Ressourcen – unabhängig von ihrem physischen oder Netzwerkstandort.

Das Modell räumt auf mit der Annahme, dass alles hinter der Unternehmensfirewall sicher sei. Deshalb wird immer von einem Risiko ausgegangen und jede Anforderung so geprüft, als käme sie aus einem offen zugänglichen Netzwerk. Es gilt das Prinzip „Vertraue niemandem, überprüfe alles" – egal, woher die Anforderung stammt und auf welche Ressource sie abzielt.

Eine Zero-Trust-Strategie muss zunächst die grundlegenden Prinzipien erfüllen und vor Bedrohungen schützen – Vorteile wie die Vereinfachung der IT kommen an zweiter Stelle.

Die Hauptvorteile	
Zuverlässige Eindämmung von Sicherheitsverletzungen	32 %
Schnelle Erkennung und Beseitigung von Bedrohungen	30 %
Zuverlässiger Schutz von Kundendaten	29 %

Quelle: Microsoft Zero Trust Survey 2020

Zur Vermeidung von Sicherheitsverletzungen werden alle Aspekte einbezogen, von der Identität des Nutzers bis hin zur Hostingumgebung der Anwendung. Die Mikrosegmentierung und das Prinzip der geringsten Zugriffsrechte sorgen dafür, die Ausbreitung im System zu minimieren. Gleichzeitig tragen Business Intelligence und Analysen dazu bei, die Sichtbarkeit, die Bedrohungserkennung und die Abwehr zu verbessern. Dabei wird analysiert, was passiert ist, wo ein unbefugter Zugriff stattgefunden hat und wie sich ein solcher Angriff in Zukunft vermeiden lässt.

Die Gründe für die Einführung von Zero Trust

Ein Zero-Trust-Framework erfordert die Implementierung von Kontrollen und Technologien für alle grundlegenden Elemente: Identitäten, Geräte, Anwendungen, Daten, Infrastruktur und Netzwerke. Jedes dieser Elemente ist eine Signalquelle, eine Steuerungsebene zur Durchsetzung von Richtlinien und eine wichtige Ressource, die es zu verteidigen gilt. All dies sind wichtige Bereiche, in denen sich eine Investition lohnt.

Identität – der neue Perimeter

Im Laufe des Gesprächs hat sich eine wichtige Erkenntnis durchgesetzt: Unternehmen müssen sich zuerst auf eine starke Nutzerauthentifizierung und Identitätsprüfung konzentrieren, weil die meisten Sicherheitsverletzungen auf den Diebstahl von Anmeldeinformationen zurückgehen.

Da eine unzulängliche Cyberhygiene das Risiko für einzelne Mitarbeiter und das gesamte Unternehmen erhöht, kommt es auf eine umfassende Identitätsverwaltung an. Auf diese Weise wird sichergestellt, dass nur autorisierte Nutzer auf Geschäftsdaten zugreifen dürfen.

Identität – der neue Perimeter

Den Zugriff über Identitäten steuern

Identitäten, die Personen, Dienste und IoT-Geräte repräsentieren, sind der gemeinsame Nenner für Netzwerke, Endpunkte und Anwendungen. In einem Zero-Trust-Sicherheitsmodell bieten sie eine leistungsfähige, flexible und differenzierte Steuerungsmethode für den Zugriff auf Daten. Wenn eine Identität versucht, auf eine Ressource zuzugreifen, läuft der Verwaltungsprozess wie folgt ab:

- Nachweisen der Identität mithilfe starker Authentifizierung
- Überprüfen des Zugriffs – ob er konform und typisch für die Identität ist
- Bestätigen der Identität – ob die Prinzipien der geringsten Zugriffsrechte eingehalten werden

Ein Teilnehmer betonte, dass man mit einer starken Identitäts- und Zugriffsverwaltung beginnen solle: „Der ursprüngliche Perimeter hat sich aufgelöst. Identität ist der neue Perimeter, und wir brauchen sichere, überprüfte Identitäten... Unser Ausgangspunkt: Da die Zugriffsverwaltung nicht manuell durchgeführt werden kann, muss der Prozess automatisiert werden. Mit reibungsloser Automatisierung und Anmeldung stellen wir sicher, dass alles ordnungsgemäß funktioniert."

Identität – der neue Perimeter

Authentifizierung ausbauen

Die Informationssicherheit lässt sich erheblich verbessern, wenn Unternehmen die mehrstufige oder kontinuierliche Authentifizierung in ihre Identitätsverwaltungsstrategie einbinden. In diesem Zusammenhang betont ein Diskussionsteilnehmer, dass sein Unternehmen die Identitätsverwaltung durch kontinuierliche Authentifizierungsprofile erweitert hat. Auf diese Weise kann die Identität nachgewiesen werden, auch wenn die IP-Adresse oder das Verhaltensmuster des Nutzers abweicht.

In Bezug auf Identitäten und die in der Praxis eingesetzte Technologie wurde ein Teilnehmer gefragt, welche Identität kritischer einzuschätzen sei: Mensch oder Maschine? Seine Antwort: „Beide. Menschliche Unterstützung – insbesondere von Technikpersonal – ist wichtig, um die mehrstufige Authentifizierung vor Ort zu aktivieren. Das war in der Vergangenheit sehr kompliziert, ist heute aber ziemlich einfach. Die größte Herausforderung ist die Authentifizierung von Maschine zu Maschine. Worauf beruht der zweite Faktor, wenn es keinen Menschen gibt, der [ihn] in Frage stellt?"

Kennwortlose Authentifizierung einbinden

Mit der Verbreitung von Zero Trust wird es immer selbstverständlicher, Biometrie und weitere Innovationen in die moderne Informationssicherheit einzubinden. Die kennwortlose Authentifizierung ist eine weitere MFA-Methode, bei der das herkömmliche Kennwort durch eine sichere Alternative ersetzt wird. Diese Art der Authentifizierung erfordert mindestens zwei Verifizierungsfaktoren, die mit einem kryptografischen Schlüsselpaar gesichert sind. Bei der Registrierung wird vom Gerät ein öffentlicher und ein privater Schlüssel erstellt. Der private Schlüssel kann nur über eine lokale Geste wie eine PIN oder eine biometrische Authentifizierung entsperrt werden. Die Nutzer können sich direkt über biometrische Merkmale – per Fingerabdruck-, Gesichts- oder Iriserkennung – oder über eine PIN anmelden, die in unlesbarer Form auf dem Gerät gesichert ist.

Auf die Frage, wie sich die kennwortlose Authentifizierung auf die Wirksamkeit von Zero Trust auswirkt, antwortete ein Teilnehmer: „Ich denke, die Wirksamkeit steigt. Nach einem Machbarkeitsnachweis für Microsoft Windows Hello, der auf ein Jahr angelegt war, führen wir diese Methode gerade unternehmensweit ein. Zero Trust funktioniert nur, wenn der Ansatz transparent für den Endnutzer ist. Einfachheit und Transparenz sind unverzichtbar. Wer die Authentifizierung alle fünf Minuten oder jede Sekunde wiederholen will, kann dies tun, solange der Endnutzer nicht aktiv werden muss – vorausgesetzt, es gibt weitere Validierungsmethoden. Ein Endpunkt kann z. B. als einer der MFA-Faktoren fungieren.“

Unternehmensnetzwerk segmentieren

Das Thema Netzwerksegmentierung wurde während der Gesprächsrunde lebhaft diskutiert. Ein Teilnehmer äußerte die Ansicht, dass bei zu starker Segmentierung alles auseinanderbrechen könnte. Sobald einzelne Teile konzipiert werden und das Perimeternetzwerk segmentiert wird, hat man kein einheitliches IT-Netzwerk mehr. Die Herausforderung für die Unternehmens-IT besteht darin, dass Firewalls eine frühe Segmentierung darstellen. Dies kann zu inhärenten Schwierigkeiten bei der Entwicklung und beim Testen führen. Letztendlich ist das IT-Team stärker auf die Sicherheitsteams angewiesen, um Netzwerk-, Verbindungs- und Zugriffsprobleme zu beheben.

Doch in einer „Mobile First"- und „Cloud First"-Welt erfolgt der Zugriff auf alle unternehmenswichtigen Daten über die Netzwerkinfrastruktur. Netzwerkkontrollen bieten wichtige Funktionen, um die Sichtbarkeit zu verbessern und Angreifer daran zu hindern, sich im Netzwerk auszubreiten. Folglich sollten Unternehmen bei der Netzwerksegmentierung bleiben und eine stärkere netzwerkinterne Mikrosegmentierung durchführen – und zwar zusätzlich zu Echtzeit-Bedrohungsschutz, End-to-End-Verschlüsselung, Überwachung und Analysen.

> Ein Teilnehmer bemerkte: „Unser Plan war die Mikro- und Markrosegmentierung unseres Netzwerks. Wir begannen in den Rechenzentren und Büros, was zu einer Anwendungssegmentierung führte. Dadurch konnten wir Nutzer – die sich über VDI oder VPN verbinden – auf einen bestimmten App-Stack beschränken. Wir können [Nutzer] also so segmentieren, dass sie keinen uneingeschränkten Zugriff erhalten, sobald sie sich im VPN befinden."

Im weiteren Verlauf der Diskussion über die Segmentierung wurden die Teilnehmer gefragt, ob das Zero-Trust-Framework auch auf lokale Ressourcen ausgedehnt werden kann oder auf Cloudumgebungen beschränkt werden sollte. Ein Teilnehmer beschrieb seine Erfahrungen wie folgt: „Wir fingen lokal an und werden auch lokal weitermachen. Schließlich ist die Mikrosegmentierung wichtig, um die Ausbreitung im System zu verhindern. So gesehen, bleibt alles gleich, außer dass wir die Funktionen jetzt auf die Cloud ausweiten. Finanzdienstleister werden nie alles in der Cloud hosten, sondern immer eine Mischung aus lokalen und cloudbasierten Ressourcen beibehalten.... [Wir müssen] herausfinden, wie wir die verschiedenen Perimeter intakt halten und das Paradigma flächendeckend ausweiten können."

Ein anderer Teilnehmer bemerkte: „Ich fing ebenfalls mit intensiver Mikrosegmentierung und NAC an. Mein Vertrauen in das nächste VLAN war nicht besonders groß. Man musste eine Firewall passieren, und wenn man nicht autorisiert war, war kein Durchkommen. Wir mussten sicherstellen, dass der Zugriff segmentweise erfolgt, und zwar bidirektional und unidirektional. So hat alles angefangen."

Geräte schützen

Während die meisten zustimmen würden, dass moderne Unternehmen beim Datenzugriff eine unglaubliche Vielfalt an Endgeräten verwalten müssen, äußerte ein Gesprächsteilnehmer die Sorge, dass die Geräte selbst weitestgehend unbeachtet blieben. Nicht alle Endgeräte werden vom Unternehmen verwaltet oder befinden sich in dessen Besitz. Dies kann zu abweichenden Gerätekonfigurationen und Softwarepatchebenen führen. Wie bereits erwähnt, gilt für Zero Trust das Prinzip „Vertraue niemandem, überprüfe alles“. Im Endeffekt bedeutet das, dass immer alle Endpunkte überprüft werden müssen. Das gilt nicht nur für Geräte von Auftragnehmern, Partnern und Gästen, sondern auch für Apps und Geräte, über die Mitarbeiter auf Arbeitsdaten zugreifen – egal, wem das Gerät gehört.

Beim Zero-Trust-Modell werden einheitliche Sicherheitsrichtlinien angewendet – unabhängig davon, ob es sich um ein firmeneigenes oder privates Gerät handelt, ob das Gerät vollständig durch die IT verwaltet oder ob nur Apps und Daten geschützt werden. Die Richtlinien gelten für alle Endpunkte wie PC, Mac, Smartphone, Tablet, Wearable oder IoT-Gerät. Dabei spielt es keine Rolle, ob sie mit dem sicheren Firmennetzwerk, dem ortsfesten Breitband oder dem öffentlichen Internet verbunden sind.

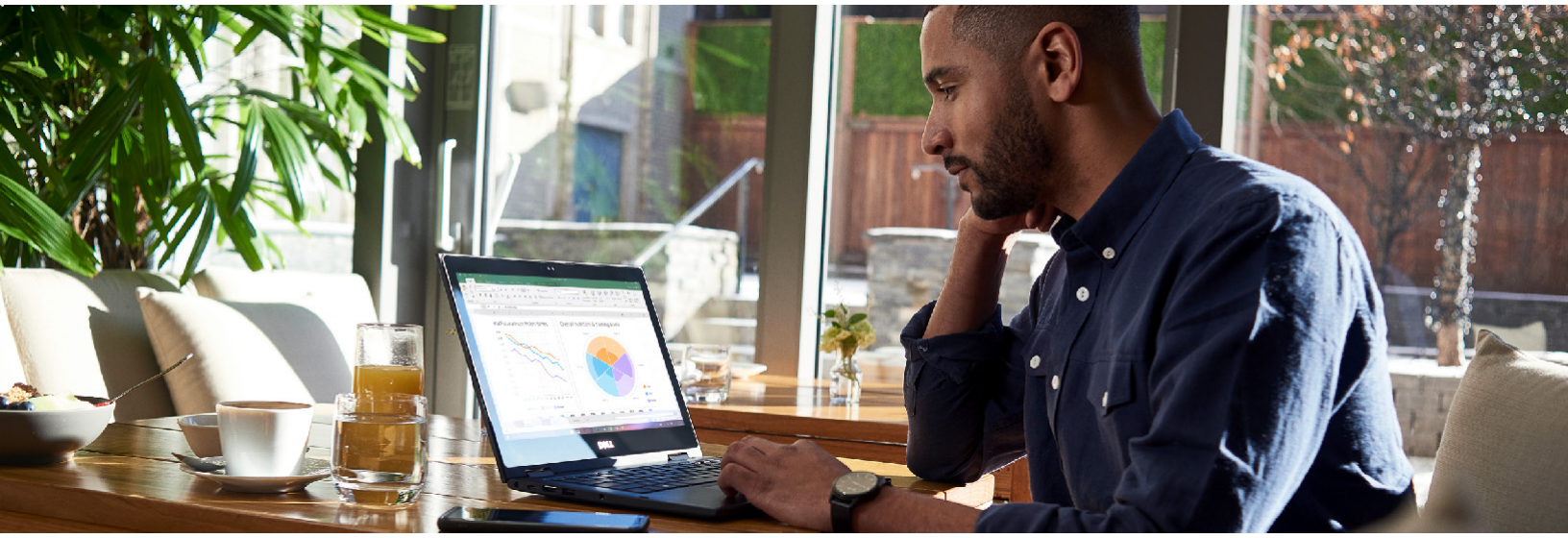
In der Diskussion über Gerätesicherheit lieferte ein Teilnehmer ein besonders treffendes Beispiel: „In einer BYOD-Welt geht die größte Gefahr vom Gerät aus. Wenn sich nicht gepatchte Geräte mit dem Netzwerk verbinden dürfen, ist es, als würde man mit einer entsicherten Handgranate hantieren. Das kann leicht schief gehen. Warum also nicht von vornherein auf externe Sicherheit achten? Mit der Zeit gewöhnen sich die Menschen an die Aufforderung, für Sicherheit zu sorgen (z. B. Geräte zu patchen) – sie erwarten es geradezu. Bald wird es für die Nutzer zur Normalität, sicherheitsrelevante Erinnerungen zu erhalten und das Gerät zu schützen.“

Anwendungen segmentieren

Besonders erwähnenswert: Einige Gesprächsteilnehmer lenkten die Diskussion auf ihre Bedenken bezüglich der Sicherheit auf Anwendungsebene. Sie betonten, dass der bedarfsgerechte Zugriff auf Anwendungen – ob über SaaS oder in Rechenzentren – entscheidend für die erfolgreiche Umsetzung einer Zero-Trust-Strategie ist.

Um die Vorteile von Cloud-Apps und -Diensten voll ausschöpfen zu können, müssen Unternehmen die richtige Balance zwischen Zugänglichkeit und Kontrolle finden. Nur so können sie sicherstellen, dass Apps und die darin enthaltenen Daten geschützt sind. Kontrollen und Technologien dienen dazu, die Schatten-IT zu erkennen, angemessene In-App-Berechtigungen bereitzustellen, den Zugriff auf der Basis von Echtzeitanalysen einzuschränken, anomales Verhalten zu überwachen, Nutzeraktionen zu beschränken und sichere Konfigurationsoptionen zu validieren.

Während der Diskussion über die Zero-Trust-Journey äußerte sich ein Teilnehmer wie folgt über die Anwendungssicherheit: „Die Segmentierung zwischen Anwendungen lässt sich inzwischen einfach und zielführend umsetzen. Die Möglichkeit, übermäßige Berechtigungen/ rollenbasierten Zugriff zu gewähren, wird in das Richtlinienmodul integriert. Je mehr Zeit vergeht, desto intelligenter wird der Umgang mit Anwendungen. Dies bestätigt sich jedes Mal, wenn ich höre, dass ein Endnutzer in der Lage ist, ein Problem selbst zu beheben."

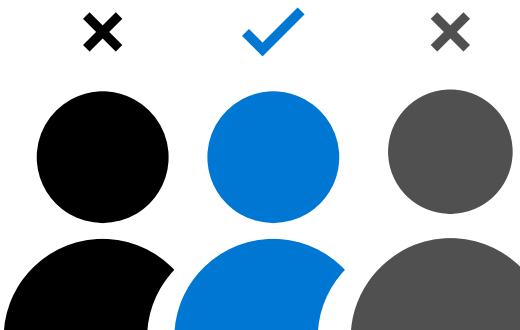


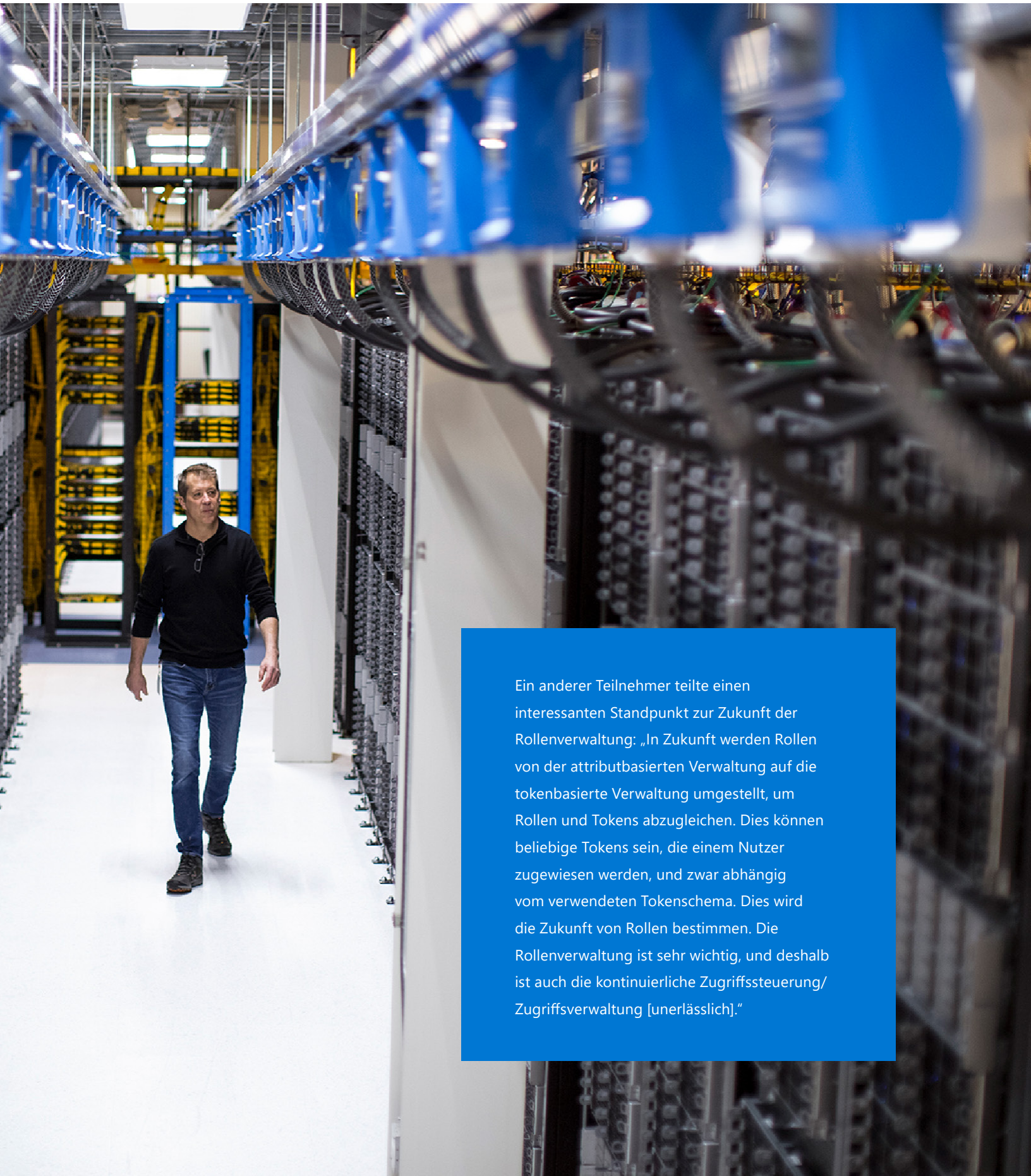
Rollen und Zugriffssteuerungen definieren

Auch aktuelle Themen wurden in der Diskussionsrunde erörtert wie z. B. die rasante Zunahme von Remotearbeitskräften. Da die meisten Mitarbeiter heute per Remotezugriff arbeiten, müssen Unternehmen alternative Lösungen finden, um moderne Sicherheitskontrollen umzusetzen. Ein Teilnehmer kam direkt auf den operativen Bereich zu sprechen und erklärte, dass die richtlinienbasierte Verwaltung von Nutzerrollen ein wichtiger Teil der ganzheitlichen Informationssicherheit sei. Diese Idee wurde dann weiter ausgeführt, um auf die Notwendigkeit einer effektiven Rollenverwaltung – und auf die Verknüpfung von Rollen mit Richtlinien – hinzuweisen, z. B. im Rahmen von Autorisierung, Single Sign-On (SSO), kennwortlosem Zugriff, Segmentierung usw.

Eine Frage bleibt: Wie sinnvoll ist es, Rollen auf der operativen Ebene zu verwalten und sie mit der Richtlinienverwaltung zu verknüpfen? Wie ein Teilnehmer sagte, ist die Operationalisierung von Rollen unerlässlich. Schließlich müssen die richtigen Rollen definiert werden, um SSO und kennwortlose Funktionen zu unterstützen. Dieser Teilnehmer mahnte aber auch zur Vorsicht und warnte davor, zu viele Rollen zu verwenden. Jede definierte Rolle muss jetzt und in Zukunft verwaltet werden. Dies kann zu Wildwuchs und Risiken führen, da Rollen möglicherweise nicht überwacht werden oder über mehr Berechtigungen als nötig verfügen.

> Zum effizienten Umgang mit Rollen bemerkte ein Teilnehmer: „Viele wollen die Autorisierung sehr genau angehen. Aber wenn man schließlich tausend Rollen im Unternehmen definiert, um diese Ebene zu erreichen, treten später definitiv Probleme bei der Verwaltung auf. Es kommen immer mehr Konten hinzu, die nicht aktualisiert werden, und das sind die Ursachen für Sicherheitsverletzungen – z. B. wenn ich intern den Tätigkeitsbereich wechsele und die Berechtigungen [die ich nicht mehr brauche] mitnehme."





Ein anderer Teilnehmer teilte einen interessanten Standpunkt zur Zukunft der Rollenverwaltung: „In Zukunft werden Rollen von der attributbasierten Verwaltung auf die tokenbasierte Verwaltung umgestellt, um Rollen und Tokens abzugleichen. Dies können beliebige Tokens sein, die einem Nutzer zugewiesen werden, und zwar abhängig vom verwendeten Tokenschema. Dies wird die Zukunft von Rollen bestimmen. Die Rollenverwaltung ist sehr wichtig, und deshalb ist auch die kontinuierliche Zugriffssteuerung/ Zugriffsverwaltung [unerlässlich].“

Die Zero-Trust-Journey

Während die Gesprächsteilnehmer ihre Zero-Trust-Erfahrungen diskutierten – sowohl ihre Anfänge als auch den Status quo – kristallisierten sich mehrere gemeinsame Muster heraus.
Ein Hauptanliegen war die Notwendigkeit, den Umfang der Informationssicherheit zu analysieren und einen Einstiegspunkt zu finden. Einige Teilnehmer hatten ihre Zero-Trust-Journey mit der Identitäts- und Zugriffsverwaltung für Nutzer begonnen, andere mit der Makro- und Mikrosegmentierung von Netzwerken und wieder andere mit Anwendungen. Letztlich näherten sich alle dem Zero-Trust-Reifegrad „Vertraue niemandem und prüfe alles“ – innerhalb und außerhalb der Firewall, am Endpunkt, auf dem Server oder in der Cloud. Sie waren sich einig, dass mit der Weiterentwicklung von Zero Trust eine Erkenntnis wächst: Der Weg ist das Ziel.

Ein Teilnehmer erzählte, dass er seine Journey in Richtung Zero-Trust-Sicherheit mit der Identitätsverwaltung begonnen hatte. Es sollten SSO-Funktionen implementiert werden, doch dann erkannte man, dass sich diese auch auf das Homeoffice ausweiten lassen.

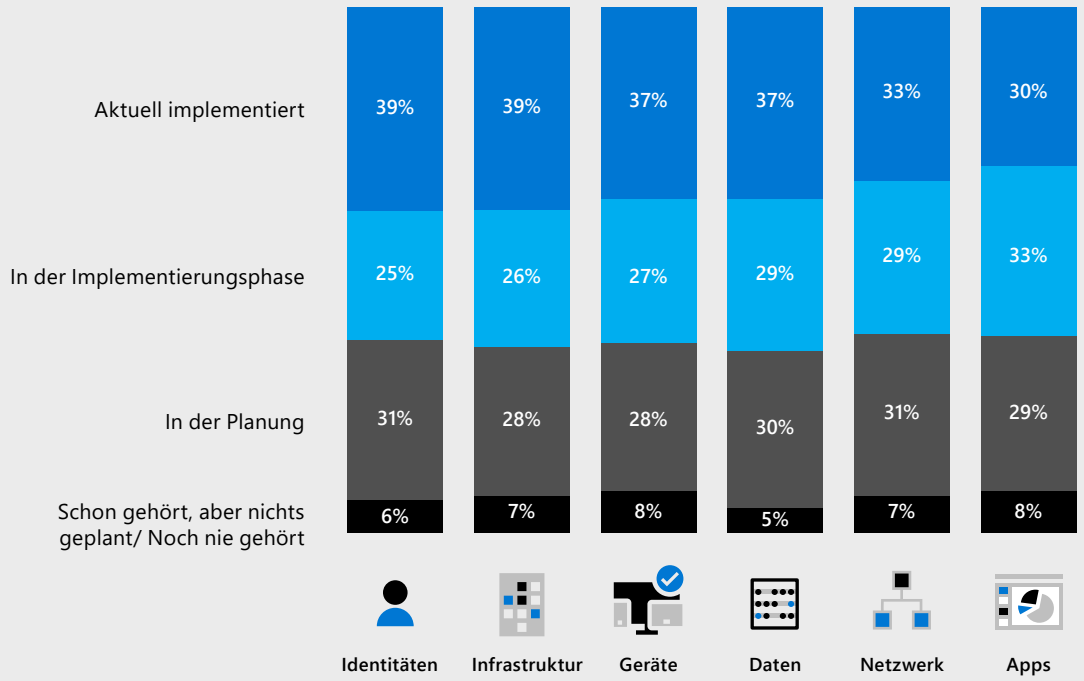
Bei Zero Trust kommt es auf die Entwicklung einer ganzheitlichen Strategie an. Um eine erfolgreiche Zero-Trust-Journey zu planen und umzusetzen, muss ein Unternehmen die Prioritäten, Technologien, Prozesse und sogar die Auswirkungen von Veränderungen im Blick behalten.

Die Diskussionsrunde ist sich einig:

Um optimalen Schutz zu gewährleisten, müssen Unternehmen klein anfangen, Vertrauen aufbauen und Zero Trust unternehmensweit einführen.

Zero Trust ist eine End-to-End-Strategie, die alle Bereiche umfasst

Aktueller Status von Zero-Trust-Aktivitäten
Gesamt (n=300)



Quelle: Microsoft Zero Trust Survey 2020

Klein anfangen und Vertrauen aufbauen

Betriebliche Anforderungen, vorhandene Technologien und Sicherheitsstufen beeinflussen die Planung einer Zero-Trust-Implementierung. Obwohl Zero-Trust-Sicherheit am effektivsten ist, wenn sie in die gesamte digitale Umgebung integriert wird, müssen viele Unternehmen einen schrittweisen Ansatz verfolgen, der je nach Zero-Trust-Reife, verfügbaren Ressourcen und Prioritäten auf bestimmte Bereiche abzielt. Jede Investition muss sorgfältig überlegt und auf die aktuellen Geschäftsanforderungen abgestimmt sein. Die erste Etappe der Journey muss nicht zwingend eine „Lift & Shift"-Umstellung auf cloudbasierte Sicherheitstools sein.

Genauso erfordert der Einstieg in Zero Trust keine vollständige Neuerfindung der Infrastruktur. Lösungen sind dann erfolgreich, wenn sie auf einer Hybridumgebung aufsetzen und diese unterstützen, ohne frühere Investitionen vollständig abzulösen.

Unabhängig von der Größe des Unternehmens sollte die Zero-Trust-Einführung mit kleinen Schritten beginnen. Viele scheitern an dem Versuch, mehrere größere Änderungen gleichzeitig durchzuführen. Der Erfolg wird in der Regel dadurch erzielt, dass man entweder mit einem neuen Projekt in der Cloud beginnt oder in einer Entwicklungs- und Testumgebung experimentiert.

Ein Teilnehmer untermauerte die Idee einer kleinen Einstiegslösung wie folgt: „Man muss mit den Kronjuwelen beginnen, ohne alles auf einmal zu wollen. Es ist nicht möglich, parallel zur Zero-Trust-Bereitstellung viele andere Dinge zu stemmen."

Ein anderer Teilnehmer erzählte ein Beispiel aus der Praxis, nämlich wie er ein großes Unternehmen davon überzeugte, mit einer kleinen Zero-Trust-Lösung anzufangen: „Ich leitete einen Workshop bei einer großen Bank und riet zu einer kleinen Einstiegslösung. Daraufhin sagte man mir, dass man mit 5.000 Nutzern anfangen wolle. Aus der Perspektive der Bank war das klein. Aber ich empfahl ihnen, auf 50 runterzugehen. Die Bank setzte sich darüber hinweg und startete mit ca. 2.500 Nutzern. Etwa acht Wochen später meldete sich die Bank erneut, um den Umfang neu bewerten zu lassen und einen Pilotplan anzufordern. Der neue Versuch umfasste 25 Nutzer. Nach zwei Jahren lassen sich jetzt echte Fortschritte erkennen."

Zero Trust auf die ganze Umgebung ausweiten

Nachdem die ersten Schritte getan und Vertrauen aufgebaut war, sollte das Zero-Trust-Modell auf die gesamte digitale Umgebung ausgeweitet und gleichzeitig als integrierte Sicherheitsphilosophie und End-to-End-Strategie umgesetzt werden. Wenn eine Zero-Trust-Strategie flächendeckend angewendet wird, muss sie den gesamten Sicherheitsstatus abdecken.

Jede Zugriffsanforderung sollte streng auf Unregelmäßigkeiten geprüft werden, bevor der Zugriff gewährt wird. Von der Identität des Nutzers bis hin zur Hostingumgebung der Anwendung sollte alles authentifiziert und autorisiert werden. Um die Ausbreitung im System zu minimieren, müssen Mikrosegmentierung und Prinzipien der geringsten Zugriffsrechte angewendet werden.

Kurz gesagt: Die konsistente und umfassende Implementierung eines Zero-Trust-Sicherheitsmodells setzt voraus, dass alle wesentlichen Elemente berücksichtigt werden – einschließlich Identität, Geräten, Anwendungen, Daten, Infrastruktur und Netzwerk. Darüber hinaus sollten folgende Überlegungen einbezogen werden:

- Alle Nutzer und Geräte, die versuchen, auf Ressourcen zuzugreifen, müssen im Hinblick auf die Zielressource (basierend auf ihrer Vertraulichkeitsstufe) als vertrauenswürdig bestätigt werden.
- Ein einheitliches Zero-Trust-Richtlinienmodul wird vorausgesetzt, um die Unternehmensrichtlinien konsistent auf alle Ressourcen anzuwenden (statt mehrere Module mit abweichenden Konfigurationen zu verwenden).
- Je mehr Messdaten, die das normale Verhalten widerspiegeln, in eine Vertrauensentscheidung einfließen, desto schwieriger und kostspieliger ist es für Angreifer, legitime Anmeldeversuche und -aktivitäten zu imitieren. Dadurch werden Angreifer abgeschreckt oder in ihren böswilligen Absichten eingeschränkt.
- Der sichere Systembetrieb muss immer gewährleistet sein, auch nach einer versäumten oder falschen Entscheidung (damit die Lebensdauer/Sicherheit und der Geschäftsnutzen durch stabile Vertraulichkeit, Integrität und Verfügbarkeit gewahrt werden kann).
- Der Erhalt eines sicheren Zustands ist besonders wichtig für Unternehmen, die sich auf veraltete oder statische Kontrollen verlassen, die die Vertrauenswürdigkeit eingehender Zugriffsversuche nicht dynamisch messen und durchsetzen können (z. B. statische Netzwerkkontrollen für ältere Anwendungen, Server oder Geräte).

Bewerten der Zero-Trust-Bereitschaft

Unternehmen, die ihre Zero-Trust-Bereitschaft bewerten und einen verbesserten Schutz für ihre gesamte digitale Umgebung planen wollen, sollten die folgenden Schlüsselinvestitionen für eine reibungslose und effektive Zero-Trust-Implementierung in Betracht ziehen.

Starke Authentifizierung: Sorgen Sie für sichere MFA und Erkennung von Sitzungsrisiken. Dies sind die Grundlagen jeder Zugriffsstrategie, durch die sich das Risiko von Identitätsdiebstahl minimieren lässt.

Richtlinienbasierter adaptiver Zugriff: Definieren Sie angemessene Zugriffsrichtlinien für Ressourcen, und setzen Sie diese mit einem konsistenten Sicherheitsrichtlinien-Modul durch, das sowohl Governance als auch Erkenntnisse über Abweichungen bietet.

Mikrosegmentierung: Lassen Sie den einfachen, zentralisierten Netzwerkperimeter hinter sich, um über softwaredefinierte Mikroperimeter eine umfassende und verteilte Segmentierung zu erreichen.

Automatisierung: Investieren Sie in ein automatisiertes Warn- und Abwehrsystem, um die durchschnittliche Reaktionszeit auf Angriffe zu verkürzen.

Business Intelligence und KI: Nutzen Sie Cloud Intelligence und alle verfügbaren Signale, um Anomalien beim Zugriff in Echtzeit zu erkennen und angemessen zu reagieren.

Daten klassifizieren und schützen: Erkennen, klassifizieren, schützen und überwachen Sie vertrauliche Daten, um Risiken durch böswillige oder versehentliche Exfiltration zu minimieren.

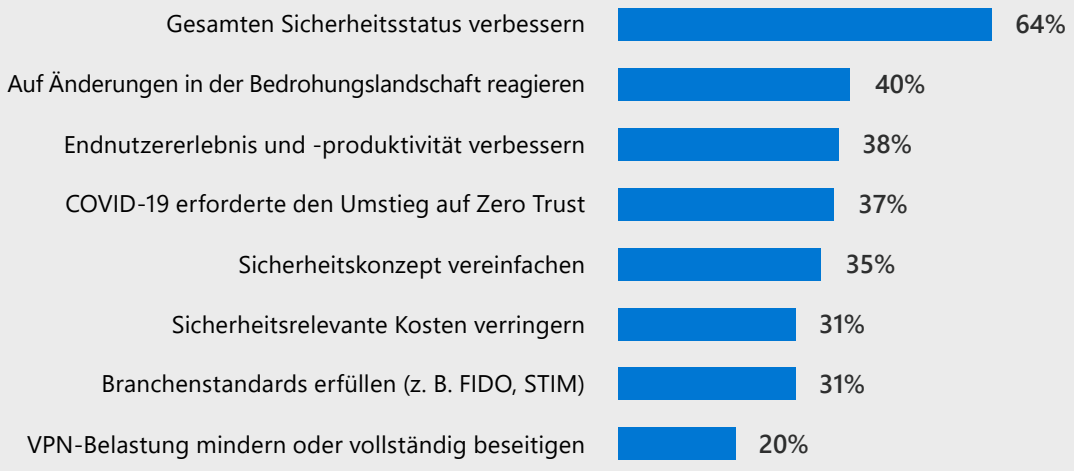
Quelle: Microsoft Zero Trust-Reifegradmodell

Ein Teilnehmer berichtete von den Erfahrungen, die sein Unternehmen auf dem Weg zum Zero-Trust-Reifegrad gemacht hatte:

„[Wir starteten] ganz klassisch mit manueller Mikrosegmentierung (bevor es SDP gab) und implementierten dann NAC. Mit der Einführung von IoT und Cloud sowie der Auflösung der Grenze zwischen internem und externem Perimeter wird das System um weitere Zero-Trust-Merkmale erweitert: z. B. Segmentierung von Anwendungen und Netzwerk, Identitätsverbund, kontinuierliche Autorisierung und mehrstufige Authentifizierung. Das Ergebnis ist ein umfassendes Ökosystem."

Die Verbesserung des allgemeinen Sicherheitsstatus ist der größte Anreiz für die Einführung einer Zero-Trust-Strategie, gefolgt von steigenden Sicherheitsbedenken.

Anreize für Zero Trust
Gesamt (n=300)



Quelle: Microsoft Zero Trust Survey 2020

Vertraue niemandem, prüfe alles!

Das Zero-Trust-Sicherheitsmodell bietet effektive Kontrollen für geschäftskritische Informationen und Systeme und stellt sicher, dass die richtigen Personen zur richtigen Zeit Zugriff auf die richtigen Daten haben. Basierend auf dem Prinzip „Vertraue niemandem, prüfe alles“ schützt Zero Trust Ihre Unternehmensressourcen, indem unbekannte und nicht verwaltete Geräte verbannt werden und die Ausbreitung im System eingeschränkt wird. Zero Trust bietet eine End-to-End-Strategie für die ganze Umgebung: einschließlich Identität, Infrastruktur, Geräten, Daten, Anwendungen und Netzwerk. Deshalb erfordert die Implementierung eines echten Zero-Trust-Modells, dass alle diese Elemente validiert und als vertrauenswürdig eingestuft werden.

Die Umsetzung eines Zero-Trust-Modells ist nicht immer einfach, aber unverzichtbar für jeden langfristigen Modernisierungsplan. Jedes Unternehmen, das Zero Trust einführen möchte, sollte zunächst Sicherheitskontrollen in kleinen Teilbereichen umsetzen, statt mehrere, weitreichende Kontrollen gleichzeitig durchzusetzen. Sobald die Sicherheitskontrollen Schritt für Schritt erfolgreich implementiert wurden, kann die Zero-Trust-Sicherheit auf die gesamte digitale Umgebung ausgeweitet werden. Eine optimale Zero-Trust-Umgebung umfasst eine starke Identitätsauthentifizierung, Geräte, bei der Geräteverwaltung registrierte Geräte, geringstmögliche Nutzerrechte und eine bestätigte Dienstintegrität.

Mehr erfahren

Zero-Trust-Sicherheit entdecken

Den Fortschritt der Zero-Trust-Journey bewerten

Microsoft Zero Trust Deployment Center