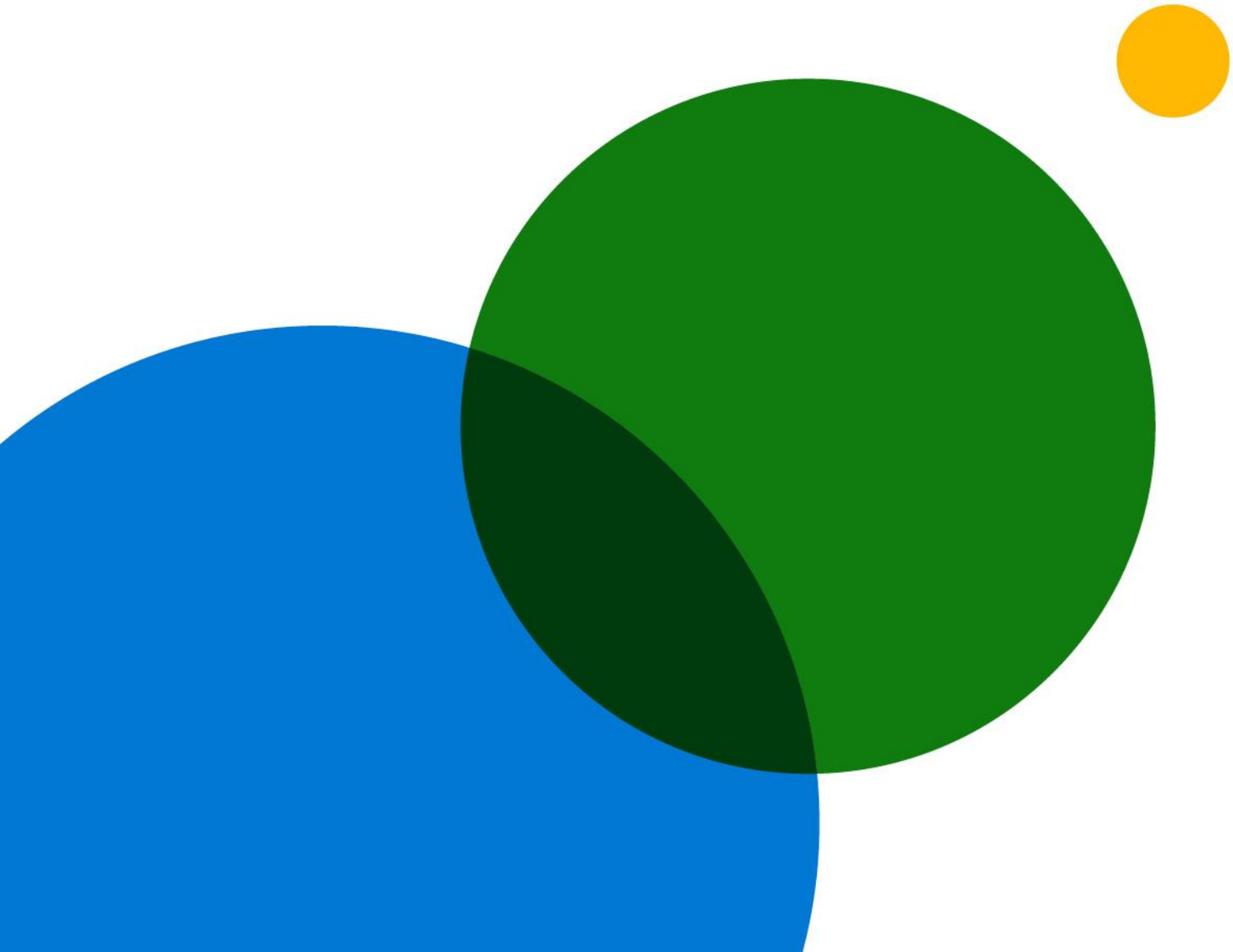
Microsoft Security

hypothesis

Bericht über die Einführung von Zero Trust



Inhaltsverzeichnis

Einführung

Vasu Jakkal / Corporate Vice President, Security, Compliance and Identity

Das vergangene Jahr war im Hinblick auf die Entwicklung der Cyber-Sicherheit und den Aufstieg von Zero Trust als Leitstrategie für unsere Branche und Unternehmen weltweit bemerkenswert.

Zu Beginn der Pandemie wurde fast über Nacht auf die Arbeit im Homeoffice umgestellt. Diese Veränderung zwang viele Unternehmen zu raschen Anpassungen, um ihre Mitarbeiter*innen zu unterstützen, die ihre Arbeit auf jede erdenkliche Weise erledigten und hierfür persönliche Geräte nutzten, über Cloud-Dienste zusammenarbeiteten und Daten außerhalb des Unternehmensnetzwerks teilten. Als sich die Unternehmen an diese Transformation anpassten, sahen sie sich auch mit immer raffinierteren Cyberkriminellen konfrontiert, die ihre Ziele, Taktiken und Ressourcenbeschaffung ständig weiterentwickelten.

Heute sind hybride Arbeitsmodelle die neue Realität. Vor diesem Hintergrund und angesichts des rasanten Wandels gaben die von uns befragten Unternehmen an, auf Zero Trust zu setzen, um in Bezug auf Sicherheit und Compliance agiler zu werden, Bedrohungen schneller zu erkennen und zu beheben und Sicherheitsanalysen einfacher und besser verfügbar zu machen.

Basierend auf den Prinzipien der expliziten Überprüfung, der Nutzung des Zugriffs mit den geringsten Berechtigungen und der Annahme einer mutmaßlichen Sicherheitsverletzung schafft eine umfassende Zero-Trust-Architektur Schutzmaßnahmen innerhalb und zwischen Identitäten, Endpunkten, Anwendungen, Infrastrukturen, Netzwerken und Daten und bietet gleichzeitig eine verbesserte Transparenz, Automatisierung und Orchestrierung. Wir empfehlen diese Herangehensweise nicht nur unseren Kunden und Partnern, sondern beziehen sie auch in unser eigenes Konzept für globale Sicherheit und Softwareentwicklung bei Microsoft ein.

Dieser Bericht befasst sich mit dem Weg zur Einführung von Zero Trust in verschiedenen Märkten und Branchen. Wir hoffen, dass die Erkenntnisse dieser Studie hilfreich für Sie sind, um schneller Ihre eigene Zero-Trust-Strategie einzuführen. Zudem soll die Studie die kollektiven Fortschritte anderer Unternehmen deutlich machen und Insights zum zukünftigen Zustand dieses sich schnell entwickelnden Bereichs vermitteln.

Methodik

Microsoft hat die Hypothesis Group, eine Agentur für Insights, Design und Strategie, mit der Erstellung des Berichts und der Durchführung der Studie zur Einführung von Zero Trust beauftragt. Die Studie wurde in zwei Phasen durchgeführt. Zunächst in den USA, um Trends und die Dynamik bei der Einführung von Zero Trust aufzuzeigen. In der zweiten Phase wurden weitere Länder einbezogen, um globale Trends aufzudecken.

Erste Recherchen fanden im August 2020 statt. In einer 15-minütigen Online-Umfrage wurden dabei 300 Entscheidungsträger*innen aus dem Sicherheitsbereich (Security Decision Maker, SDMs) befragt, die an Entscheidungen zur Zero-Trust-Strategie in großen Unternehmen aus verschiedenen Branchen beteiligt sind. Neben der Online-Umfrage wurden im September 2020 fünf umfassende Befragungen von SDMs aus verschiedenen Branchen in den USA durchgeführt.

Im April 2021 wurde die globale Studie in den USA, Deutschland, Japan und Australien/Neuseeland mit einer ähnlichen Gruppe von Entscheidungsträger*innen aus dem Sicherheitsbereich durchgeführt. Über 900 Teilnehmer nahmen an einer 15-minütigen Online-Umfrage teil. Die Fragen bezogen sich dabei auf die Einführung ihrer Zero-Trust-Strategie, Best Practices, Vorteile, Herausforderungen und ihre Investitionspläne für die Zukunft.

Wissenswertes über die Einführung von Zero Trust

01 / Unternehmen sind bereit, die Vorteile einer Zero-Trust-Strategie zu nutzen – eine durch den Umstieg auf einen hybriden Arbeitsplatz und COVID-19 beschleunigte Entwicklung

Die Entscheidungsträger*innen im Sicherheitsbereich (SDMs) sehen die Entwicklung einer Zero-Trust-Strategie als ihre höchste Sicherheitspriorität an. 96 % erachten dies als entscheidend für den Erfolg ihres Unternehmens. Die Hauptmotivation für die Einführung einer Zero-Trust-Strategie besteht in einer Verbesserung des allgemeinen Sicherheitsstatus und der User-Experience. Der Übergang zu einem hybriden Arbeitsplatz – eine Entwicklung, die durch COVID-19 beschleunigt wurde – führt auch zu einer umfassenderen Einführung der Zero-Trust-Strategie: 81 % der großen Unternehmen haben mit dem Umstieg auf einen hybriden Arbeitsplatz begonnen, 31 % haben dies bereits erfolgreich umgesetzt. 94 % haben allerdings Bedenken hinsichtlich des Übergangs, die sich vor allem auf eine mögliche falsche Verwendung durch Mitarbeiter*innen, die größeren IT-Workloads und Cyberangriffe beziehen. Zu den wichtigsten Überlegungen im Zusammenhang mit der Strategie gehören daher verstärkte Schulungen für Mitarbeiter*innen und eine Multi-Faktor-Authentifizierung (MFA), um eine reibungslose User-Experience und Umstellung zu gewährleisten.

02 / Bei einer Zero-Trust-Strategie sind die Unternehmen flexibel in Bezug auf den Bereich, in dem sie mit der Umsetzung beginnen – das Konzept kann somit auf die Anforderungen der Unternehmen zugeschnitten werden

Weniger als 15 % der Unternehmen haben mit der Umsetzung der Zero-Trust-Strategie in demselben Sicherheitsrisikobereich begonnen. Dies ist größtenteils darauf zurückzuführen, dass die Umsetzung als durchgängiger Prozess über Säulen und Funktionen der Sicherheitsarchitektur hinweg erfolgt, nicht in Form einer Reihe von unterschiedlichen individuellen Technologien. Auch die Reihenfolge, in der die einzelnen Komponenten von Zero Trust innerhalb eines Sicherheitsrisikobereichs implementiert werden, schwankt stark. Die Sicherheitsexperten haben sehr unterschiedliche Herangehensweisen, wenn es darum geht, welche Komponenten sie zuerst implementieren.

03 / Zwar ist die Zero-Trust-Strategie bereits weit verbreitet und bietet den Unternehmen bessere Möglichkeiten zur Bewältigung von Bedrohungen, doch es gibt noch einiges zu tun

76 % der Unternehmen haben zumindest mit der Umsetzung einer Zero-Trust-Strategie begonnen, 35 % geben an, die Strategie bereits vollständig umgesetzt zu haben. Doch auch diejenigen, die die Strategie laut eigenen Angaben bereits vollständig umgesetzt haben, räumen ein, dass sie die Umsetzung der Zero-Trust-Strategie noch nicht in allen Sicherheitsrisikobereichen und für alle Komponenten abgeschlossen haben. Die Zero-Trust-Strategie überzeugt, da sie mehr Agilität, eine schnellere Erkennung von Bedrohungen und bessere Möglichkeiten zur Verwaltung der Sicherheit in den Bereichen Internet of Things (IoT) und Operational Technology (OT) bietet. Die Einführung von Zero Trust in den USA nimmt zu (von 70 % im August 2020 auf 79 % im April 2021). Die USA sind in Bezug auf die Implementierung von Zero Trust auch im Vergleich zu anderen Ländern, die erst später mit der Einführung begonnen haben, schon etwas weiter. Die Unternehmen in den USA geben an, weniger Budgeteinschränkungen zu unterliegen. Während jedoch 57 % der Unternehmen erklären, im Hinblick auf die Einführung von Zero Trust anderen voraus zu sein, haben etwa die Hälfte der Unternehmen noch Arbeit vor sich, da sie Zero Trust noch nicht vollständig in allen Sicherheitsrisikobereichen und für alle Komponenten implementiert haben.

04 / Mit Blick auf die Zukunft wird die Zero-Trust-Strategie weiterhin oberste Priorität haben und sorgfältige Entscheidungen im Hinblick auf Mitarbeiter*innen und Anbieter erfordern

Die Zero-Trust-Strategie wird voraussichtlich auch in zwei Jahren weiterhin höchste Priorität im Sicherheitsbereich haben. Die Unternehmen rechnen damit, dass sie ihre Investitionen erhöhen werden. Die Überwindung von Herausforderungen im Zusammenhang mit den Mitarbeiter*innen (einschließlich der Besetzung von Sicherheitsteams und der Unterstützung seitens der Führungskräfte) wird entscheidend für eine Verdopplung der Investitionen in Zero Trust sein. Was die Anbieterstrategie betrifft, tendieren die Entscheidungsträger*innen im Sicherheitsbereich etwas mehr zur Zusammenarbeit mit ganzheitlichen oder konsolidierten Anbietern, da die Auswahl der Anbieter häufig von der Verfügbarkeit interner Fachkenntnisse abhängt. Ein Best-in-Suite-Ansatz hat den Vorteil, dass mehr Know-how und mehr Ressourcen zur Verfügung stehen und dieser Ansatz einfacher ist. Allerdings kann die Umsetzung länger dauern, die Integration in die bestehende Sicherheitsarchitektur kann schwieriger sein und das potenzielle Sicherheitsrisiko kann erhöht sein.

Unsere Studienteilnehmer

Global

Entscheidungsträger *innen aus dem Sicherheitsbereich,
die in großen Unternehmen arbeiten*

90 %
vertraut mit Zero Trust
Selbsteinschätzung, Bestehen eines Wissenstests

76 %
sind gerade dabei, Zero Trust zu implementieren

24 % planen/erwägen Zero Trust

*1000+ Mitarbeiter*innen in den USA; 500+ Mitarbeiter*innen in Deutschland, Japan, Australien/Neuseeland

Allgemeine Forschungs-erkenntnisse

Die Unternehmen sind bereit, die Vorteile der Zero-Trust-Strategie zu nutzen

Die Zero-Trust-Strategie hat heute im Sicherheitsbereich höchste Priorität in allen Märkten und Branchen. Zahlreiche Unternehmen haben in den letzten Jahren eine Zero-Trust-Strategie eingeführt. Zero Trust steht für alle (53 %) an erster Stelle, hat jedoch eine besonders hohe Priorität für Unternehmen in den USA (56 %) und Deutschland (53 %).

Fast alle Sicherheitsexperten (96 %) sehen eine Zero-Trust-Strategie als entscheidend für den Erfolg ihres Unternehmens an. (Siehe Abbildung 1) Neben der Stärkung ihres allgemeinen Sicherheitsstatus und der Verbesserung der User-Experience versprechen sich die Sicherheitsexperten von der Zero-Trust-Strategie eine Vereinfachung der Sicherheitsverfahren für die Mitarbeiter*innen. (Siehe Abbildung 2)

Wie ein US-amerikanischer Entscheidungsträger aus dem Sicherheitsbereich im Gastgewerbe erklärt, *„besteht das Ziel darin, den Sicherheitsstatus insgesamt zu verbessern, dabei es geht aber darum, Barrieren in der User-Experience abzubauen und den Endanwendern das Leben zu erleichtern."*

Darüber hinaus sehen 31 % der Sicherheitsexperten die Zero-Trust-Strategie als wichtiges Instrument für den bevorstehenden Übergang zu einem hybriden Arbeitsplatz in der Zeit nach der Pandemie. Dieser Faktor spielt in Australien/Neuseeland (44 %) eine besonders große Rolle.

Abbildung 1: Zero Trust ist entscheidend

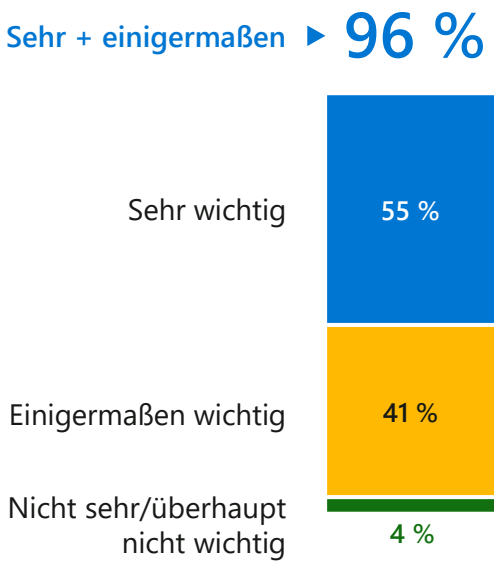


Abbildung 2: Motivatoren für Zero Trust

Wichtigste Motivatoren	
Insgesamt besserer Sicherheitsstatus	47 %
Verbesserung der User-Experience und Produktivität	44 %
Transformation der Zusammenarbeit der Sicherheitsteams	38 %
Vereinfachter Sicherheitsstack	35 %
Geringere Kosten für Sicherheit	35 %

Der Umstieg auf einen hybriden Arbeitsplatz fördert eine umfassendere Einführung der Zero-Trust-Strategie

81 % der großen Unternehmen haben mit der Umstellung auf einen hybriden Arbeitsplatz begonnen, 31 % haben dieses Modell bereits vollständig eingeführt. Allerdings ist der Anteil der Unternehmen, die das Hybridmodell bereits vollständig eingeführt haben, nicht in allen Märkten gleich. Während Australien und Neuseeland mit 37 % führend sind, liegt Deutschland weit zurück. Hier haben nur 20 % der Unternehmen bereits auf ein Hybridmodell umgestellt. (Siehe Abbildung 3)

Auch wenn die globalen Märkte unterschiedlich schnell auf das Modell des hybriden Arbeitsplatzes umsteigen, geht die überwiegende Mehrheit (91 %) der Unternehmen, die den Übergang noch nicht abgeschlossen haben, davon aus, dies in den nächsten fünf Jahren zu tun. Entscheidend ist, dass sich 94 % Sorgen wegen der Umstellung machen. Ihre größten Bedenken beziehen sich dabei auf eine falsche Verwendung durch Mitarbeiter*innen, größere IT-Workloads und Cyberangriffe. (Siehe Abbildung 4)

Abbildung 3: Pläne bezüglich des hybriden Arbeitsplatzes

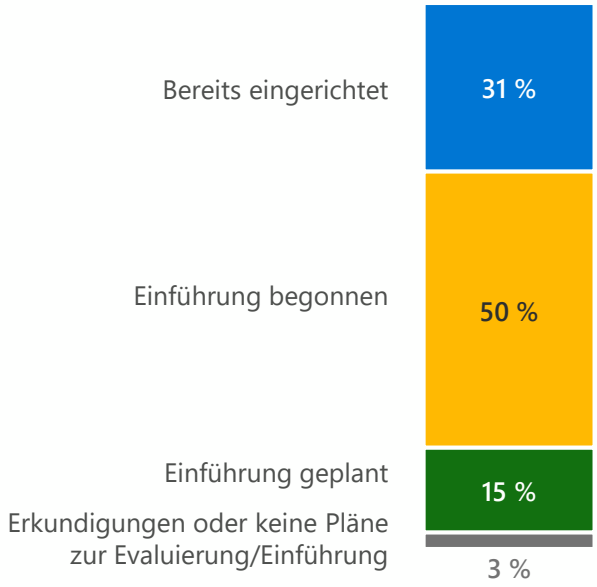
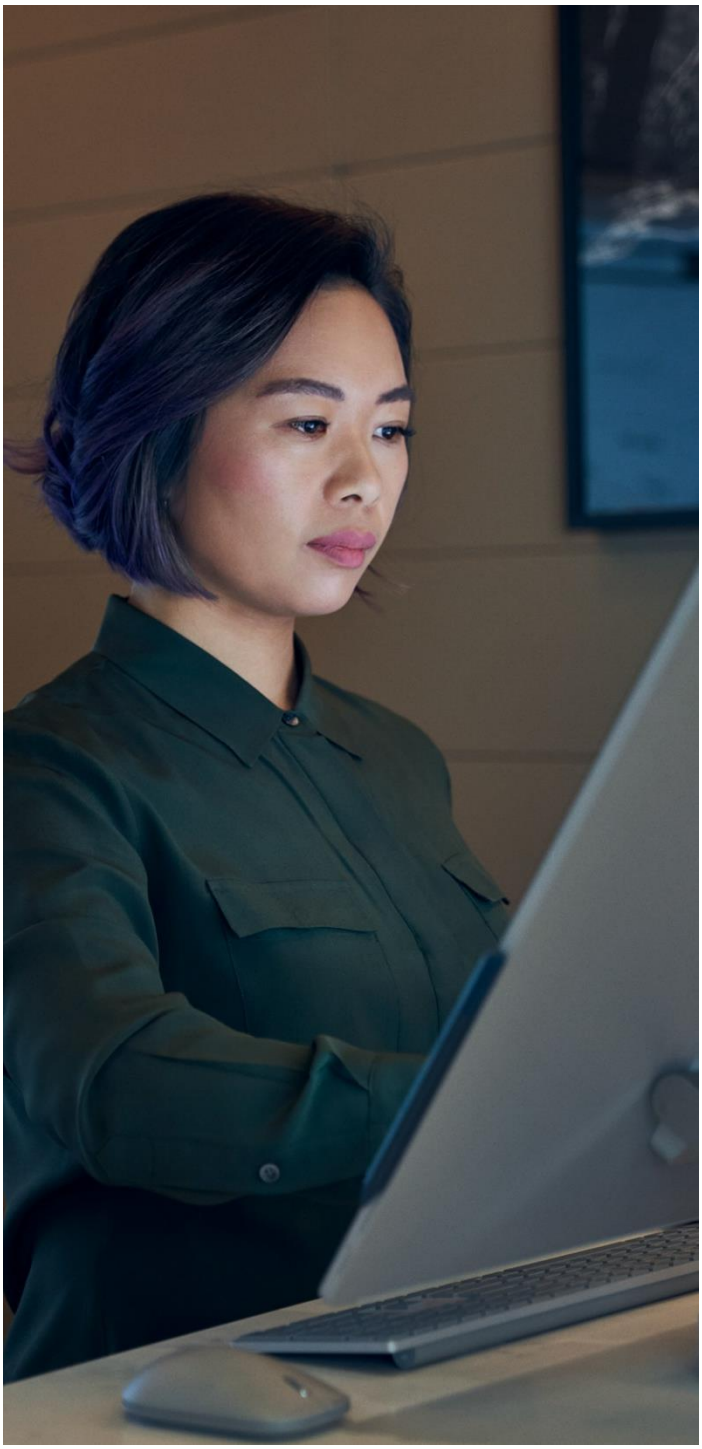


Abbildung 4: Bedenken bezüglich des hybriden Arbeitsplatzes

Mitarbeiter*innen laden unsichere Apps herunter	37 %
Größerer Workload für die IT	37 %
Ransomware-Angriffe	36 %
Phishing-Angriffe	35 %
Unsachgemäße Nutzung persönlicher Geräte	34 %
Unbefugter Datenzugriff	31 %
Unmöglichkeit, alle Geräte zu verwalten	30 %
Nutzung persönlicher E-Mail-Konten	30 %
Nichteinhaltung der Datenschutzbestimmungen	24 %

Im Zuge der COVID-19-Pandemie haben sich neue Überlegungen ergeben, die den Umstieg auf die Zero-Trust-Strategie beschleunigen



Um potenzielle Probleme auf ein Minimum zu reduzieren, betonen Stakeholder die Bedeutung von vermehrten Schulungen für die Mitarbeiter*innen (54 %) (insbesondere in Japan (61 %) und Deutschland (58 %)) sowie einer Multi-Faktor-Authentifizierung (MFA) (50 %) (insbesondere in den USA (52 %) und in Deutschland (56 %)), damit eine reibungslose User-Experience und ein problemloser Umstieg gewährleistet werden können.

Da sicheres Arbeiten im Homeoffice und hybrides Arbeiten durch eine Zero-Trust-Strategie unterstützt werden können, hat die COVID-19-Pandemie für 72 % der Unternehmen die Einführung einer Zero-Trust-Strategie beschleunigt. Es bestehen allerdings Asymmetrien zwischen den Märkten. Während die Einführung in rund sieben von zehn Unternehmen in den USA (76 %), Japan (71 %) und Australien/Neuseeland (69 %) durch die Pandemie beschleunigt wurde, waren die Umsetzungsraten in Deutschland (62 %) deutlich niedriger. Dies ist möglicherweise auf einen langsameren Übergang zu einem hybriden Arbeitsplatz zurückzuführen.

Zero Trust ist weltweit weit verbreitet und nimmt in den USA weiter zu

Zero Trust ist nicht nur ein Schlagwort, es ist Realität. 76 % der Unternehmen haben zumindest begonnen, diese Strategie umzusetzen, und 35 % sind der Meinung, Zero Trust bereits vollständig implementiert zu haben. Diese Daten zeichnen jedoch ein zu optimistisches Bild, da viele Unternehmen, die der Auffassung sind, Zero Trust bereits vollständig implementiert zu haben, nach eigenen Angaben noch nicht alle Sicherheitsrisikobereiche abdecken. Was die Einführung der Zero-Trust-Strategie anbelangt, sind die USA heute anderen Ländern voraus. Die Einführung dieser Strategie nimmt weiter stark zu: Im Vergleich zum August 2020 ist die Umsetzung der Zero-Trust-Strategie in den USA von 70 % auf 79 % gestiegen, ein beachtlicher Sprung in nur acht Monaten.
(Siehe Abbildung 5)

Auch wenn die Zero-Trust-Strategie derzeit im Sicherheitsbereich dominiert, ist ihre Allgegenwärtigkeit relativ neu. 82 % der Unternehmen haben in den letzten drei Jahren Zero-Trust-Strategien umgesetzt, 21 % haben dies in den letzten zwölf Monaten getan. 26 % der US-Unternehmen haben vor mindestens drei Jahren mit der Umsetzung begonnen, in Japan sind es 19 %, in Australien/Neuseeland 6 % und in Deutschland 3 %. Diese frühere Umsetzung in den USA – in Verbindung mit weniger Budgeteinschränkungen – könnte erklären, warum die Unternehmen in den USA den Unternehmen in anderen Ländern bei der Zero-Trust-Einführung voraus sind. In ähnlicher Weise könnte das relativ neue Aufkommen von Zero Trust in Deutschland die geringeren Einführungsraten verständlich machen: 97 % der deutschen Unternehmen haben erst in den letzten drei Jahren mit der Umsetzung begonnen.

Abbildung 5: Implementierung von Zero Trust

	USA (2020)	USA	DE	JP	AUS/NZ
Implementierung von Zero Trust	70 %	79 %	75 %	76 %	71 %
• Vollständig implementiert	27 %	44 %	19 %	32 %	28 %
• Im Gange	43 %	35 %	56 %	44 %	43 %

35 % vollständig implementiert

42 % Implementierung im Gange

Es gibt kein universelles Konzept für die Implementierung von Zero Trust, es kann also überall begonnen werden

Es gibt keinen einzelnen Sicherheitsrisikobereich (Identitäten, Endpunkte, Anwendungen, Netzwerk, Infrastruktur, Daten, Automatisierung und Orchestrierung), der als bevorzugter Ausgangspunkt für die Zero-Trust-Strategie heraussticht. Weniger als 15 % beginnen mit demselben Sicherheitsrisikobereich. Die Unternehmen beginnen an verschiedenen Stellen, wahrscheinlich basierend auf ihren Anforderungen und den verfügbaren internen Ressourcen. Letztendlich streben sie die Einführung der Zero-Trust-Strategie in allen Sicherheitsrisikobereichen an, um einen noch besseren Schutz vor Bedrohungen zu gewährleisten. Zero Trust wird also als End-to-End-Strategie wahrgenommen, die über einen gewissen Zeitraum erfolgt. (Siehe Abbildung 6)

Neben den Sicherheitsrisikobereichen der Zero-Trust-Strategie müssen die Unternehmen die einzelnen Komponenten jedes Sicherheitsrisikobereichs identifizieren, die vorrangig behandelt werden sollen. Für Endpunkte, Anwendungen, Netzwerke, Daten und Automatisierung/Orchestrierung gibt es keinen klaren Ausgangspunkt. Die Sicherheitsexperten haben sehr unterschiedliche Vorstellungen davon, welche Komponenten für sie höchste Priorität haben. Eine starke Authentifizierung wird in der Regel jedoch für Identitäten zuerst implementiert, und Tools zur Erkennung von Bedrohungen haben in der Infrastruktur klare Priorität. (Siehe Abbildung 7)

Abbildung 6: Aktuelle Implementierung von Zero Trust – Sicherheitsrisikobereiche

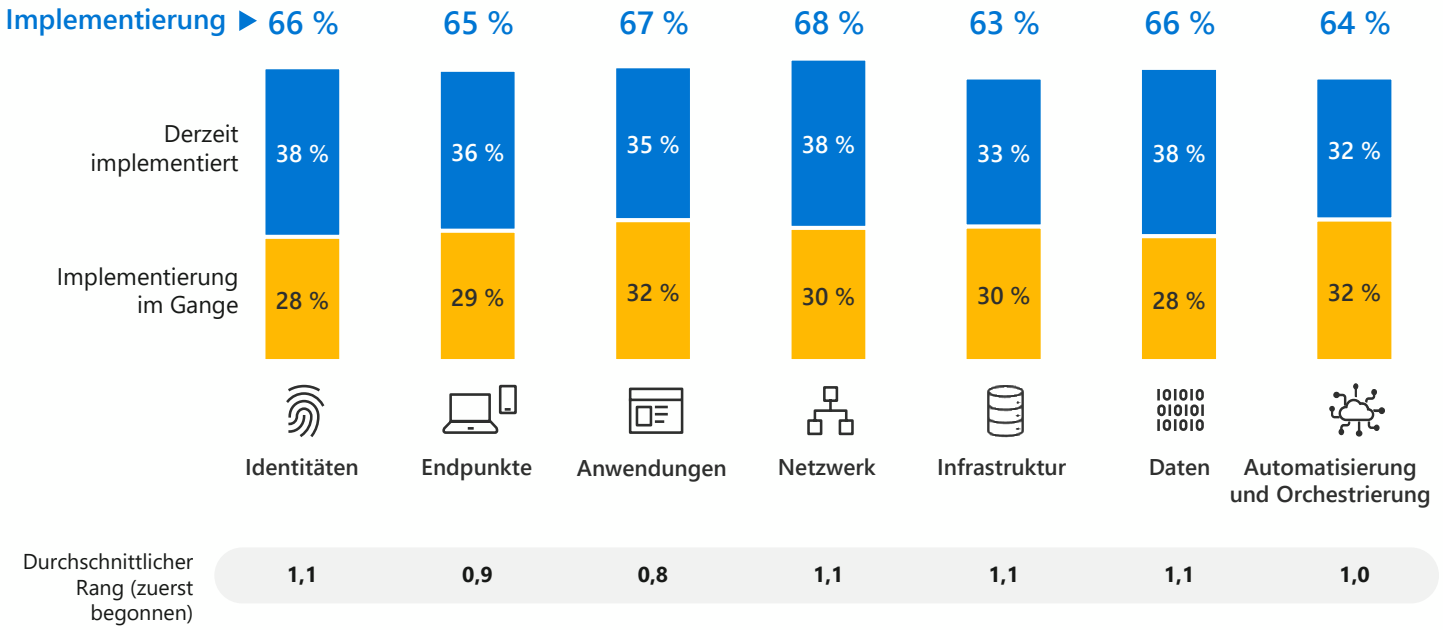


Abbildung 7: Implementierung von Zero-Trust-Komponenten (Top 3) – Rang 1 (zuerst implementiert)

Identitäten	
Starke Authentifizierung (d. h. Multi-Faktor-Authentifizierung, kennwortfreie Authentifizierung)	32 %
Automatisierte Erkennung und Eindämmung von Risiken	27 %
Adaptive Zugriffsrichtlinien, um den Zugriff auf Ressourcen zu beschränken	22 %

Endpunkte	
Data-Loss-Prevention-Richtlinien/-Kontrollen für alle nicht verwalteten und verwalteten Geräte	27 %
Bewertung des Geräterisikos in Echtzeit / Bedrohungserkennung für Endpunkte	26 %
Geräteregistrierung bei Identitätsanbieter	24 %

Anwendungen	
Kontinuierliche Ermittlung von Schatten-IT und Risikobewertung	23 %
Differenzierte Zugriffssteuerung für Anwendungen (z. B. eingeschränkte Sichtbarkeit oder nur Lesezugriff)	22 %
Richtlinienbasierte Zugriffssteuerung für Apps	20 %

Netzwerk	
Sichere Zugriffssteuerung zum Schutz der Netzwerke	25 %
Bedrohungsschutz und Filterung mit kontextbasierten Signalen	24 %
Verschlüsselung des gesamten Datenverkehrs	20 %

Infrastruktur	
Zugriff des Sicherheitsteams auf Tools zur Erkennung von Bedrohungen	25 %
Schutz der Cloud-Workloads in Hybrid- und Multi-Cloud-Umgebungen	19 %
Differenzierte Sichtbarkeit und Zugriffssteuerung für alle Workloads (virtuelle Maschinen, Server usw.)	17 %

Daten	
Steuerung von Zugriffsentscheidungen über die Sicherheitsrichtlinien-Engine	21 %
Klassifizierung und Kennzeichnung von Daten	21 %
Dauerhafter Schutz hochvertraulicher Dateien durch Verschlüsselung	20 %

Automatisierung und Orchestrierung	
Umfassende Einblicke durch eine zentralisierte Plattform für die Untersuchung und Reaktion	29 %
Erfassung und Analyse von Bedrohungsdaten über Domänen hinweg (Identitäten, Endpunkte, Anwendungen, Netzwerk, Infrastruktur)	28 %
Aktivierung einer automatisierten Untersuchung und Reaktion	22 %

Wir haben dies nicht nur als eine Reihe von Technologien betrachtet, sondern als Strategie und Konzept zur Behandlung jeder Benutzerressource – ob innerhalb oder außerhalb unseres Netzwerks – als nicht vertrauenswürdig, bis sie verifiziert werden konnte."

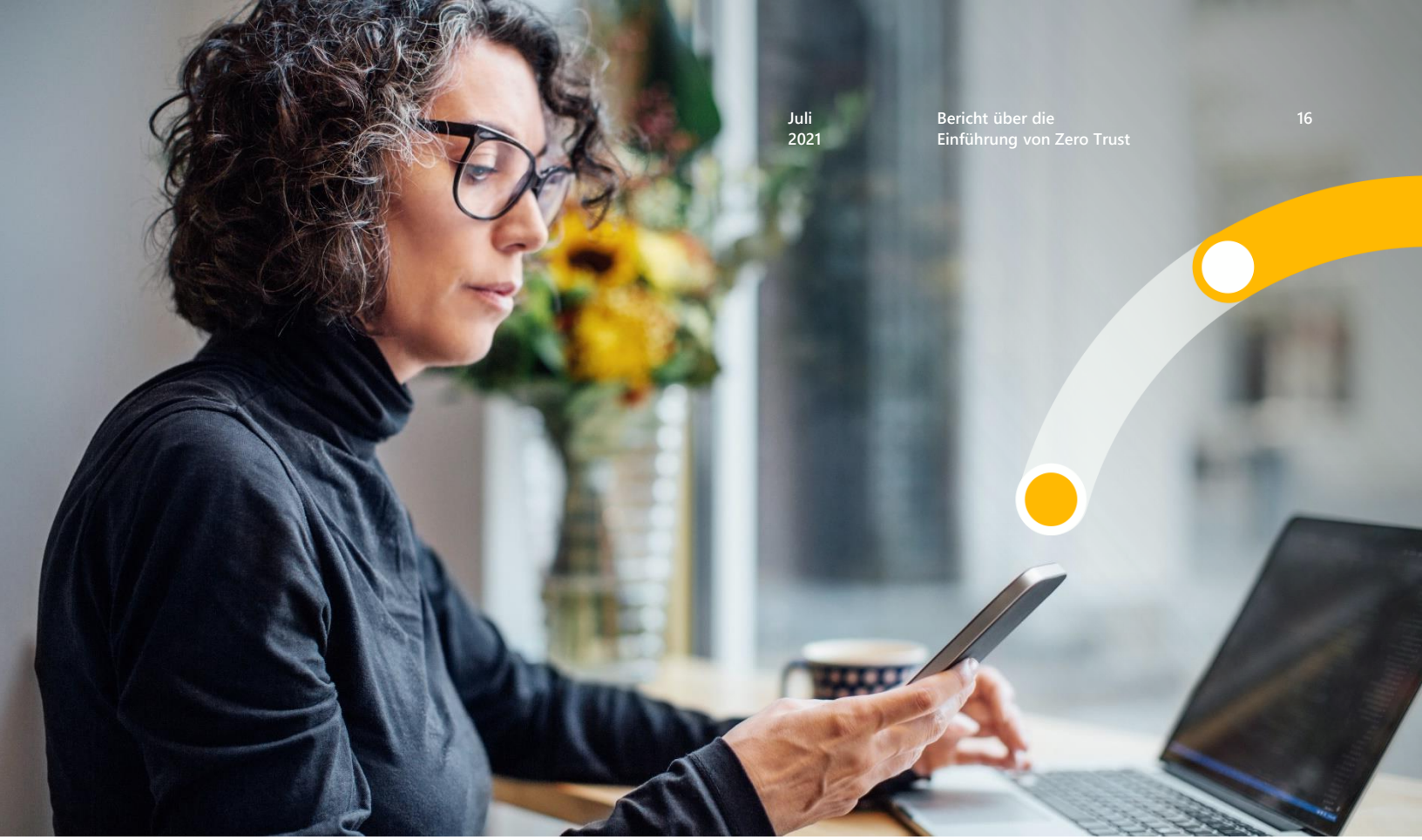
US-amerikanischer Entscheidungsträger aus dem Sicherheitsbereich im Gastgewerbe

Zu den wichtigsten Vorteilen für Unternehmen, die mit der Umsetzung einer Zero-Trust-Strategie beginnen, gehören eine größere Agilität, eine höhere Geschwindigkeit und ein besserer Schutz. Ressourcenvorteile sind weniger häufig.

Nach Umsetzung der Zero-Trust-Strategie profitieren die Unternehmen von einer größeren Agilität (37 %), einer höheren Geschwindigkeit (35 %) und einem besseren Schutz von Kundendaten (35 %). (Siehe Abbildung 8.) Direkte Vorteile für die Mitarbeiter*innen, wie z. B. eine Entlastung des Sicherheitsteams (27 %) und ein geringerer Bedarf an Ressourcen für die Verwaltung der Infrastruktur (22 %), werden weniger häufig erzielt.

Wichtig ist, dass die Unternehmen davon überzeugt sind, dass sie mithilfe der Zero-Trust-Strategie die meisten Bedrohungen und Veränderungen in der Umgebung bewältigen können, insbesondere in Bezug auf IoT- und OT-Sicherheit (47 %).

Abbildung 8: Vorteile von Zero Trust



Die Unternehmen sind zuversichtlich, dass sie das Beste aus ihrer Zero-Trust-Strategie herausholen können

79 % sind zuversichtlich, dass sie Sicherheitsbedrohungen insgesamt bewältigen können. Diese Zuversicht schwindet jedoch, wenn die Bedrohung eine Vortäuschung der Wahrheit beinhaltet: Am wenigsten sicher fühlen sich die Entscheidungsträger*innen im Sicherheitsbereich (SDMs), wenn es um Bedrohungen mit synthetischen Identitäten (20 %) und Deepfakes (10 %) geht.

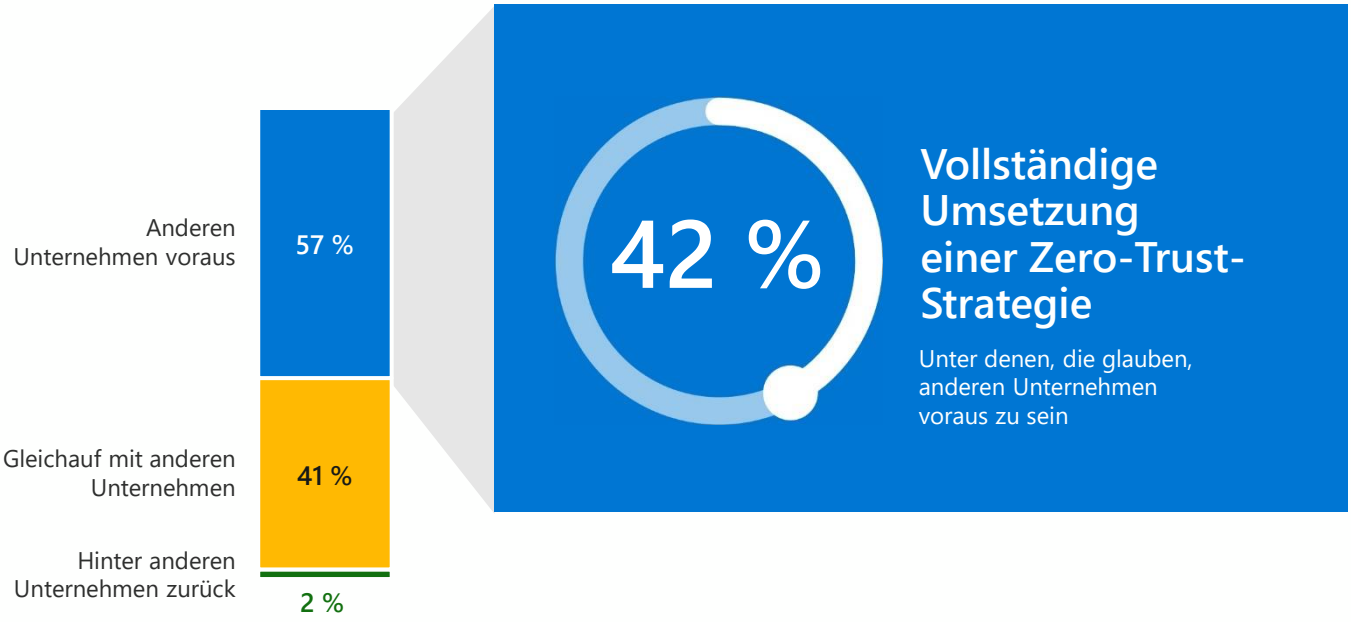
Angesichts der gewonnenen Vorteile wird Zero Trust im Allgemeinen positiv gesehen. In allen vier Märkten sehen die SDMs die Herangehensweise ihrer Unternehmen als gleichzeitig praktisch und ambitioniert an und beschreiben sie als selbstbewusst (37 %), effizient (31 %), motivierend (25 %), inspirierend (25 %) und aufregend (25 %). Insbesondere in Japan bezeichnen Sicherheitsexperten Zero Trust als anspruchsvoll (27 %) und transformativ (25 %), ein Zeichen dafür, dass die Strategie zwar nicht leicht umzusetzen ist, nach ihrer Einführung jedoch weitreichende Vorteile bietet.

Viele sind der Meinung, bei der Implementierung von Zero Trust führend zu sein, doch es bleibt noch viel zu tun

Zwar haben nur 35 % der Unternehmen ihre Zero-Trust-Strategie vollständig umgesetzt, doch 52 % geben an, schon weiter zu sein als geplant, und 57 % sind der Auffassung, anderen Unternehmen voraus zu sein. Insbesondere in Japan (66 %) und Australien/Neuseeland (63 %) haben die Unternehmen den Eindruck, schon weiter als andere zu sein. Das Vertrauen in den Ländern ist groß, doch es scheint eine Kluft zwischen Wahrnehmung und Realität zu geben: Von den Unternehmen, die den Eindruck haben, anderen voraus zu sein, geben nur 42 % an, eine Zero-Trust-Strategie vollständig umgesetzt zu haben. (Siehe Abbildung 9)

Auch wenn viele Unternehmen von ihrer Zero-Trust-Strategie überzeugt sind und sich bereit fühlen, zukünftige Sicherheitsbedrohungen zu meistern, muss noch viel Arbeit geleistet werden, um alle Risikobereiche vollständig abzudecken. Von den Unternehmen, die ihre Zero-Trust-Strategie als vollständig umgesetzt ansehen, hat beispielsweise fast die Hälfte noch nicht alle Sicherheitsrisikobereiche abgedeckt. Dabei ist die Wahrscheinlichkeit, dass die Strategie bereits umgesetzt wurde, in den Bereichen Infrastruktur und Identitäten am geringsten.

Abbildung 9: Vergleich der Implementierung von Zero Trust



	USA	DE	JP	AUS/NZ
Voraus	59 %	46 %	66 %	63 %
Gleichauf	40 %	52 %	34 %	32 %
Zurück	2 %	2 %	0 %	6 %

Mit Blick auf die nächsten zwei Jahre hat die Zero-Trust-Strategie weiterhin oberste Priorität im Sicherheitsbereich

Die Unternehmen haben sich voll und ganz der Zero-Trust-Strategie verschrieben, und die Entscheidungsträger*innen erklären, dass Zero Trust in den nächsten zwei Jahren weiterhin oberste Priorität im Sicherheitsbereich haben wird. Die relative Bedeutung der Zero-Trust-Strategie als Sicherheitsinitiative wird bis 2023 voraussichtlich noch zunehmen (von 53 % auf 58 %), da die SDMs davon ausgehen, dass die Strategie für den Gesamterfolg entscheidend bleiben wird (96 %). (Siehe Abbildung 10)

Die erwartete Bedeutung ist bei japanischen Unternehmen besonders hoch. Hier geben 70 % an, dass die Zero-Trust-Strategie in den nächsten zwei Jahren sehr wichtig sein wird. Der Gesamtdurchschnitt liegt dagegen bei 56 %. Auch die Budgets für die Zero-Trust-Strategie werden voraussichtlich wachsen. 73 % der Unternehmen rechnen mit einer Erhöhung ihrer Budgets. In Deutschland ist diese Zahl allerdings etwas niedriger (67 %), hier gehen 31 % davon aus, dass ihre Budgets unverändert bleiben werden. (Siehe Abbildung 11)

Abbildung 10: Erwartete Bedeutung von Zero Trust in den nächsten zwei Jahren

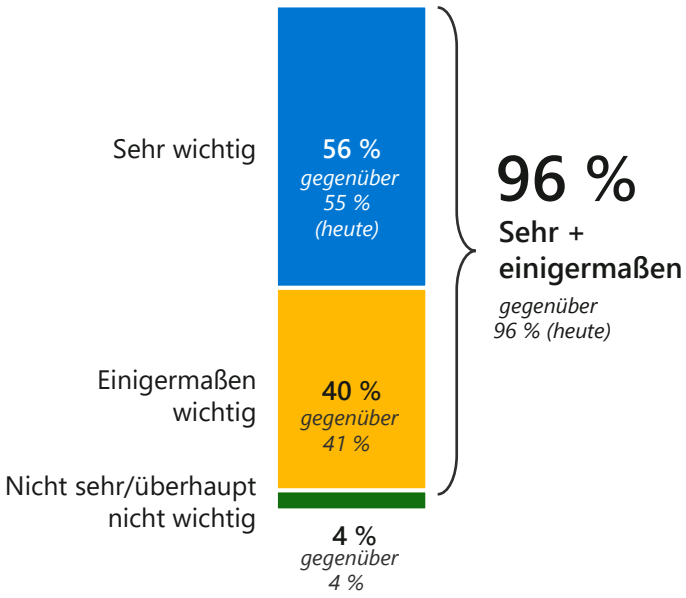
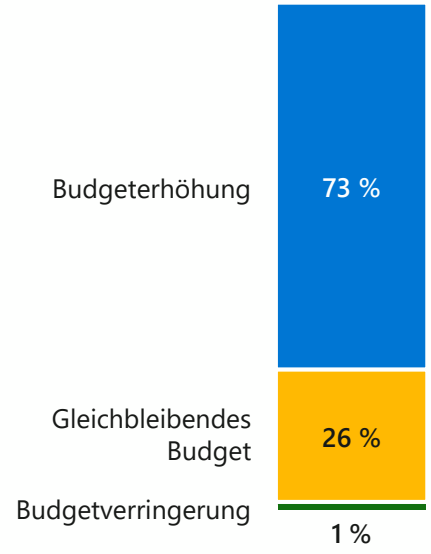
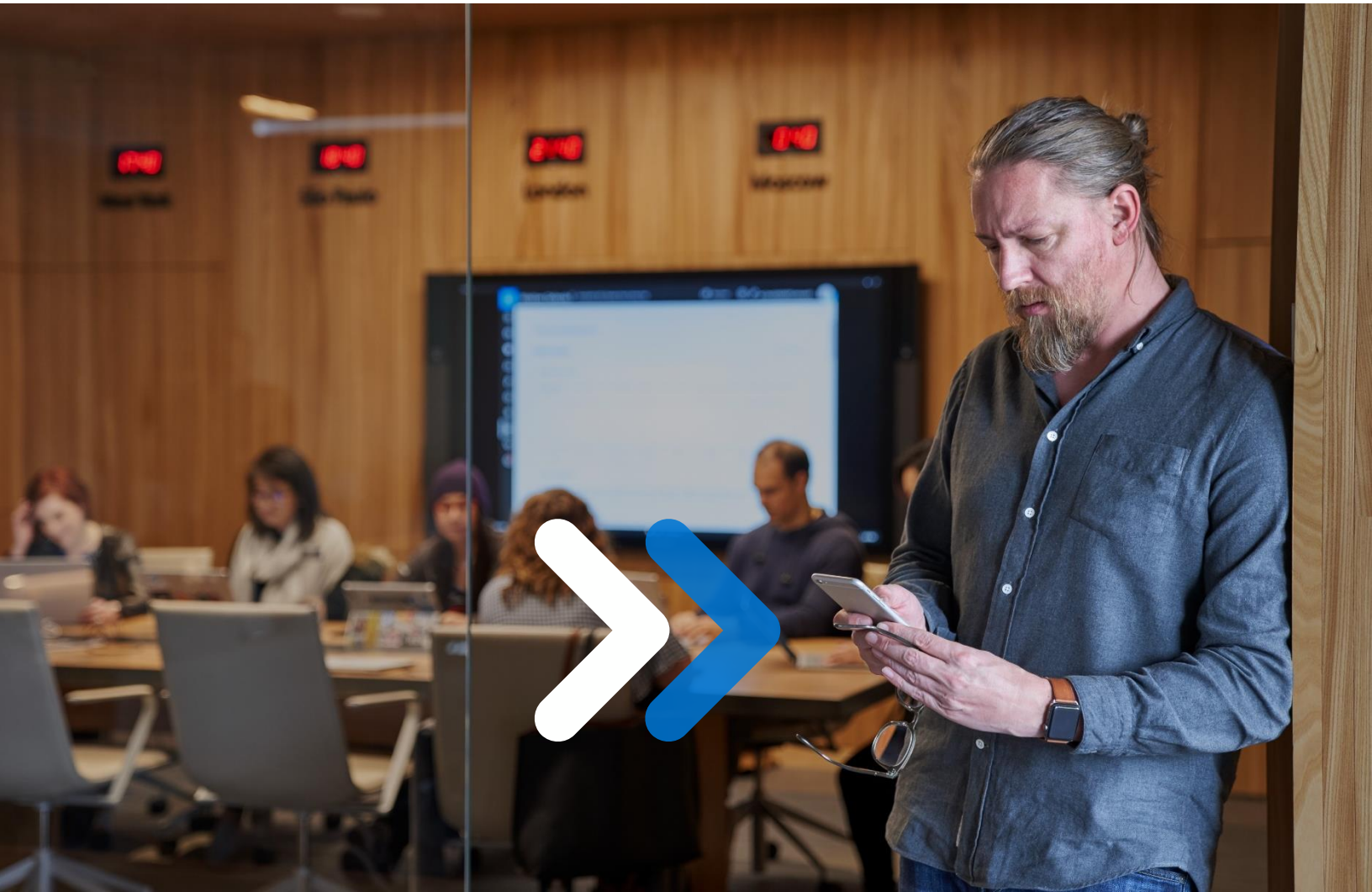


Abbildung 11: Erwartetes Zero-Trust-Budget in den nächsten zwei Jahren



Nachweisliche Erfolge der Zero-Trust-Strategie könnten weitere Investitionen fördern

Unternehmen, die sich ohne Vorbehalte auf Zero Trust eingelassen haben, rechnen damit, ihre Investitionen in den nächsten zwei Jahren zu verdoppeln. Diejenigen, die noch nicht mit der Einführung begonnen haben, laufen Gefahr, weiter zurückzufallen. Diese Unternehmen liegen hinter denen, die Zero Trust bereits vollständig implementiert haben, nicht nur in Bezug auf die Priorisierung von Zero Trust in ihren Sicherheitsplänen (42 % gegenüber 66 %) und erwartete Budgeterhöhungen (66 % gegenüber 72 %) zurück, sie sind auch deutlich weniger zuversichtlich, die IoT- und OT-Sicherheit in Zukunft bewältigen zu können (40 % gegenüber 53 %).



Die Überwindung von Herausforderungen im Zusammenhang mit den Mitarbeiter*innen wird entscheidend für eine Verdopplung der Investitionen in Zero Trust sein

Trotz der schnellen Fortschritte bei der Einführung der Zero-Trust-Strategie müssen Unternehmen eine Vielzahl von Herausforderungen meistern, wenn sie die Implementierung weiter voranbringen möchten. (Siehe Abbildung 12.) Die Herausforderungen in Bezug auf Ressourcen und Führungskräfte sind in diesen Kategorien am größten. An oberster Stelle der Liste der Barrieren stehen die für die Umsetzung von Zero-Trust-Strategien erforderliche Zeit und die mangelnde Unterstützung seitens der Geschäftsführung. Letzterer Aspekt ist besonders auffällig in Australien/Neuseeland (65 %).

Darüber hinaus spielen Budgetbeschränkungen – die 45 % der Unternehmen als Barriere angeben – wahrscheinlich ebenfalls eine Rolle bei den Herausforderungen im Zusammenhang mit Ressourcen und Führungskräften.

So nennen beispielsweise 21 % der SDMs Schwierigkeiten beim Nachweis des ROI einer Investition in Zero Trust als Barriere für die Implementierung – ein Problem, das zu einer mangelnden Unterstützung seitens der Unternehmensleitung führen kann. Da es in den Märkten außerhalb der USA eher Budgetbeschränkungen gibt (60 % der Unternehmen in Japan, 57 % der Unternehmen in Deutschland, 57 % der Unternehmen in Australien/Neuseeland), kann es zu einem Dominoeffekt kommen, der wiederum dazu führt, dass Zero-Trust-Strategien in Japan, Deutschland und Australien/Neuseeland in geringerem Maße und langsamer umgesetzt werden als in den USA.

Abbildung 12: Barrieren für Zero Trust

Herausforderungen im Zusammenhang mit Ressourcen 60 %	Geschäftsführung 53 %	Technologisch 46 %	Anbieter 46 %	Budgeteinschränkungen 45 %
20 % Implementierung dauert zu lange	**20 %** Mangelnde Unterstützung seitens einer breiteren Führungsebene	**21 %** Schwierigkeit bei der Integration von Sicherheitslösungen	**21 %** Implementierungssupport durch die Anbieter benötigt	**21 %** Kosten der Umsetzung einer Zero-Trust-Strategie
19 % Fehlendes internes Änderungsmanagement	**19 %** Mangelnde Unterstützung durch Stakeholder	**19 %** Inkompatibilität mit älteren Systemen	**21 %** Schwierigkeit, die richtigen Anbieter zu finden	**21 %** Schwierigkeit beim Nachweis des ROI
18 % Notwendigkeit von mehr Schulungsmaterialien	**19 %** Hilfe benötigt, um überzeugenden Business Case zu erstellen	**19 %** Schwierigkeit bei der unternehmensweiten Skalierung	**17 %** Unfähigkeit, innovative Partner zu finden	**14 %** Kein ausreichendes Budget
17 % Keine Notwendigkeit bei einem Unternehmen unserer Größe	**18 %** Mangelnde Unterstützung seitens des Unternehmens			
16 % Fehlen qualifizierter Mitarbeiter*innen für eine ordnungsgemäße Umsetzung				

„ Anfangs war es schwierig, Unterstützung zu erhalten, doch sobald wir uns als Stakeholder einig waren, dass wir in das Projekt investieren würden, waren alle mit an Bord.“

US-amerikanischer Entscheidungsträger aus dem Sicherheitsbereich im FinTech

Entscheidungsträger*innen im Sicherheitsbereich tendieren etwas mehr zu ganzheitlichen oder konsolidierten Anbietern

In Bezug auf die Zero-Trust-Anbieterstrategie haben die Unternehmen die Wahl zwischen einem Best-in-Suite- und einem Best-in-Breed-Ansatz. Die erstgenannte Strategie umfasst den Kauf einer Reihe von Produkten für die gesamte Zero-Trust-Architektur bei einem ganzheitlichen oder konsolidierten Anbieter. Bei dieser Lösung stehen nach Ansicht der SDMs mehr Know-how und mehr Ressourcen zur Verfügung, zudem ist die Lösung einfacher. Ein Vorteil für Unternehmen, die intern über zu wenig Ressourcen verfügen. Bei diesem Ansatz bestehen allerdings Bedenken hinsichtlich des größeren Sicherheitsrisikos und einer mangelnden Flexibilität. (Siehe Abbildung 13)

Bei der zweiten Strategie, Best-in-Breed, werden einzelne Komponenten der Zero-Trust-Technologie von spezialisierten Anbietern erworben. Im Gegensatz zu Best-in-Suite stützt sich diese Strategie auf Anbieter, die sich auf verschiedene Bereiche spezialisiert haben und daher mehr Flexibilität bieten und sich besser auf die Strategie des Unternehmens ausrichten können. Sicherheitsexperten sind allerdings der Meinung, dass Best-in-Breed-Lösungen kostenintensiver sind, mehr Ressourcen erfordern und nur beschränkte Einblicke ermöglichen – Nachteile, die letztendlich zu anbieterbezogenen Herausforderungen und Budgetproblemen führen. (Siehe Abbildung 14)

Zwar haben sich unter den Unternehmen zwei weitgehend gleich große Gruppen gebildet, die jeweils eine dieser Strategien nutzen, eine leichte Mehrheit der SDMs (55 %) bevorzugt jedoch die Zusammenarbeit mit ganzheitlichen (Best-in-Suite-)Anbietern. (Bei den Unternehmen in Australien/Neuseeland ist dagegen eine Tendenz in die andere Richtung erkennbar, 52 % bevorzugen hier Best-in-Breed-Strategien.)

Abbildung 13: Vorteile und Barrieren von Best-in-Suite-Lösungen – unter den Top 2 eingestuft

⊕ Vorteile von Best-in-Suite	
Der Anbieter verfügt über branchenspezifisches Know-how für verschiedene Lösungen	24 %
Mehr Ressourcen zur Unterstützung bei der Planung der Zero-Trust-Strategie verfügbar	23 %
Vereinfachtes Sicherheitsportfolio	22 %

⊖ Nachteile von Best-in-Suite	
Höheres Sicherheitsrisiko aufgrund der Abhängigkeit von einem einzelnen Anbieter	34 %
Erfordert eine komplexere Integration mit älterer Architektur	33 %
Weniger Flexibilität für spezielle Aufgaben	29 %

Abbildung 14: Vorteile und Barrieren von Best-in-Breed-Lösungen – unter den Top 2 eingestuft

⊕ Vorteile von Best-in-Breed	
Flexibilität, für jede Komponente der Zero-Trust-Strategie die besten Lösungen zu nutzen	33 %
Bessere Abstimmung auf die Architektur oder Strategie des Unternehmens möglich	30 %
Bessere Chancen für Innovationen mit verschiedenen Anbietern	26 %

⊖ Nachteile von Best-in-Breed	
Höhere Kosten	29 %
Unfähigkeit, Daten über verschiedene Lösungen hinweg gemeinsam zu nutzen	26 %
Viele Lösungen, die von den internen Teams eingeführt und verwaltet werden müssen	26 %

Fazit

Da es nicht nur immer häufiger zu Sicherheitsrisiken kommt, sondern diese auch immer gravierender werden, entscheiden sich die Unternehmen in allen Ländern und Branchen für eine Zero-Trust-Strategie nach dem Prinzip „Vertrauen ist gut, Kontrolle ist besser“. Die Zero-Trust-Strategie hat im Bereich Sicherheit oberste Priorität für Unternehmen, die ihren allgemeinen Sicherheitsstatus, die User-Experience und die Produktivität verbessern, die Sicherheitsverfahren für ihre Mitarbeiter*innen vereinfachen und die Kosten senken möchten. Doch auch wenn die Vorteile einer Zero-Trust-Strategie allseits bekannt sind, stehen begrenzte Ressourcen und Skepsis seitens der Geschäftsführung einer universellen Umsetzung im Weg.

In den letzten drei Jahren wurden verstärkt Zero-Trust-Strategien eingeführt. Dies ist zum Teil auf die COVID-19-Pandemie zurückzuführen. Entscheidend ist, dass der Umstieg auf die Arbeit im Homeoffice und hybride Arbeitsplätze eine umfassendere Einführung von Zero-Trust-Strategien fördert, die versprechen, Systeme und Daten auch dann zu schützen, wenn Mitarbeiter*innen jenseits der Unternehmensgrenzen und manchmal mit persönlichen Geräten darauf zugreifen. Die beschleunigte Einführung aufgrund der COVID-Pandemie ist ein guter Indikator für die Zero-Trust-Bereitschaft insgesamt. Unternehmen, die die Strategie während der Pandemie eingeführt haben, haben dabei mehr Sicherheitsrisikobereiche abgedeckt als andere Unternehmen.

Allerdings haben selbst diejenigen, die mit der Einführung ihrer Zero-Trust-Strategie schon am weitesten vorangekommen sind, noch einiges zu tun. Die Fehleinschätzung der Unternehmen hinsichtlich ihres Zero-Trust-Reifegrads kann dazu führen, dass einige Unternehmen Sicherheitslücken aufweisen, von denen sie nicht einmal etwas wissen.

Die Mehrheit der Unternehmen in allen Märkten ist der Meinung, dass die Bedeutung von Zero-Trust-Strategien mit der Zeit noch zunehmen wird. Sie rechnen mit einer entsprechenden Erhöhung der Budgets. Diese zu erwartende Verschiebung der Prioritäten ist besonders wichtig für Märkte außerhalb der USA, in denen Bedenken bezügliche des Budgets ein wesentliches Hindernis für die Einführung darstellen. Das Streben nach einer umfassender Umsetzung kann zu einer finanziellen und logistischen Überforderung führen. Dennoch sind die Vorteile eines Zero-Trust-Ansatzes unbestreitbar, und Microsoft wird die Unternehmen auf ihrem Weg in diesen boomenden Bereich begleiten und unterstützen.

Wenn Sie mehr über Zero Trust erfahren und den Zero-Trust-Reifegrad Ihres Unternehmens beurteilen möchten, besuchen Sie

aka.ms/zerotrust

Detaillierte Forschungsziele und Rekrutierung der Studienteilnehmer

Die Zielsetzungen der Studie lauteten wie folgt:

Verständnis des aktuellen Stands von Zero-Trust-Ansätzen

Aufdeckung von Denkansätzen, Best Practices, Vorteilen und Herausforderungen im Zusammenhang mit der Einführung von Zero-Trust-Ansätzena

Erkundung der Zukunft von Zero-Trust-Ansätzen

Kontextualisierung von Innovationen und Trends bei Zero-Trust-Ansätzen

Um die Screening-Kriterien zu erfüllen, mussten die Entscheidungsträger*innen aus dem Sicherheitsbereich folgenden Vorgaben entsprechen:

Verantwortung für die Sicherheit in ihrem Unternehmen, einschließlich Cyber-Sicherheit, Security-Operations, Schutz vor Bedrohungen, Identitätsverwaltung, Risikomanagement, Anwendungssicherheit, digitaler Forensik und Reaktion auf Sicherheitsverletzungen (Incident Response)

Vollzeitbeschäftigung in einem großen Unternehmen (1000+ Mitarbeiter*innen in den USA; 500 Mitarbeiter*innen in DE/JP/AU/NZ)

Altersgruppe: 25 bis 75

Vertraut mit Zero Trust

Beteiligung an der Entscheidungsfindung für die Entwicklung/Umsetzung einer Zero-Trust-Strategie

Von den 911 Entscheidungsträger*innen aus dem Sicherheitsbereich, die im Rahmen der Umfrage vom April 2021 befragt wurden:

wurden in den USA 477 SDMs befragt

wurden in Deutschland 201 SDMs befragt

wurden in Australien/Neuseeland 126 SDMs befragt

wurden in Japan 107 SDMs befragt

Hinweis: Die Studie wurde während der globalen COVID-19-Pandemie durchgeführt, die sich in verschiedenen Phasen der Eskalation/Eindämmung befand.