netskope

White Paper

Zero-Trust-Leitfaden

ZUSAMMENFASSUNG

Viele Menschen halten die digitale Transformation lediglich für einen Trend. Sie ist eine wirtschaftliche Umwälzung, die sich auf den Rhythmus der Innovation und der Unternehmensentwicklung auswirkt. Unternehmen wollen relevant bleiben, Produkte und Dienstleistungen schneller auf den Markt bringen, agil sein und sich bei passender Gelegenheit neu erfinden können.

Das massive Wachstum des Cloud Computing und die explosionsartige Verbreitung mobiler Geräte haben dazu geführt, dass Nutzer jederzeit und überall auf jedem Gerät Informationen abrufen wollen.

Eine veraltete Denkweise ist ein Hindernis für ein Unternehmen von heute. Unternehmen gehen mit neuen Geschäftsmodellen auf den Markt. Sie interagieren mit Tausenden von externen Beziehungen, was letztendlich zu einer anderen Sichtweise führt, wie wir für die Zukunft gestalten sollten. Heutzutage ist Vertrauen nicht mehr schwarz oder weiß (blockieren oder zulassen) wie in der Vergangenheit, sondern es bedeutet aufmerksames Beobachten im Kontext und Anpassungsfähigkeit. Kein Unternehmen kann implizites Vertrauen voraussetzen, und die Komponenten, die zur Schaffung von Vertrauen verwendet werden, müssen jederzeit überprüft werden. Das ist es, was Zero Trust letztendlich ausmacht. Ein Ansatz mit mehr Systematik und Sicherheit für den Zugang zu Informationen.

Das derzeitige Gefüge an Legacy-Technologien löst sich auf. Offenheit im Denken ist unerlässlich. Die digitale Transformation kann nicht über Nacht oder im Alleingang erfolgen. Sie erfordert als Unterstützungsmechanismus die Transformation von Sicherheit und IT. Wir müssen überdenken, wie wir einen sicheren Zugang zu Informationen durch Transparenz bieten, denn das ist das Einzige, was unsere Nutzer zufriedenstellt und ein starkes Gefühl der Loyalität erzeugt.

Zero-Trust-Konzepte können, wenn sie richtig angewendet werden, genau das bewirken.

Das massive Wachstum des Cloud Computing und die explosionsartige Verbreitung mobiler Geräte haben dazu geführt, dass Nutzer jederzeit und überall auf jedem Gerät Informationen abrufen wollen.

EINFÜHRUNG

Das exponentielle Wachstum des Cloud Computing hat es Unternehmen nicht nur ermöglicht, ihre Hosting-Muster zusammenzuführen und Markteinführungen neu zu gestalten. Es hat auch zu mehr Tempo bei der Ausführung geführt, was traditionelle IT-Teams mit älteren Technologien nur schwer erreichen konnten. Während sich die Vergangenheit als „perimeterbasierte Netzwerkarchitektur" zusammenfassen lässt, sind wir heute sehr viel offener und vielfältiger.

Die Cloud ist jedoch ein „Business Enabler" und hat die Bedrohungslandschaft in einer Weise erweitert, die wir fast vergessen haben. Dieser Trend der „Cloud-Evolution" hat die Art und Weise verändert, wie wir Vertrauen im Zusammenhang mit Geschäftsrisiken bewerten. Heutzutage ist Vertrauen nicht mehr schwarz oder weiß (blockieren oder zulassen) wie in der Vergangenheit, sondern es bedeutet aufmerksames Beobachten im Kontext und Anpassungsfähigkeit. Kein Unternehmen kann implizites Vertrauen voraussetzen, und die Komponenten, die zur Schaffung von Vertrauen verwendet werden, müssen jederzeit überprüft werden. Das ist es, was Zero Trust letztendlich ausmacht. Ein Ansatz mit mehr Systematik und Sicherheit für den Zugang zu Informationen.

Viele Unternehmen treiben Ergebnisse durch standardisierte Ansätze auf Endgeräten voran. Die führenden Unternehmen berücksichtigen jedoch mehr denn je die Wünsche der Endbenutzer. Das führt dazu, dass sich der betriebliche Aspekt dieser Geräte immer schwieriger handhaben lässt, da mehr Gerätetypen unterstützt werden müssen. Andere Unternehmen wenden sich von der Wartung und dem Betrieb von Endgeräten ab. Stattdessen lassen sie zu, dass Benutzer jede Art von Endgerät in die Geschäftsumgebung einbringen, und konzentrieren sich auf die Sicherheit von Informationen.

Letztlich wollen Unternehmen ihren Nutzern die Möglichkeit geben, innovativ, produktiv und sicher zu arbeiten, unabhängig von der Art des Geräts, der Zeit und dem Ort, an dem sie arbeiten. Dazu ist es erforderlich, die Offenheit hinsichtlich Architektur und Geschäft im Auge zu behalten. Zero Trust legt den Schwerpunkt auf Folgendes:

- Sicherer Zugriff auf Ressourcen unabhängig von Netzwerkstandort, Benutzer oder Gerät
- Durchsetzung strenger Zugangskontrollen und ständige Überprüfung, Überwachung und Protokollierung des Netzwerkverkehrs

Zero Trust bewertet kontinuierlich alle Aspekte des Verhaltens von Entitäten während einer Netzwerkverbindung und bietet adaptive Zugriffskontrollen auf der Grundlage bestimmter Parameter und akzeptabler Geschäftsrisiken.

Zweck und Umfang

Ziel dieses Dokuments ist es, die wichtigsten Komponenten und Umsetzungsschritte von pragmatischen Zero-Trust-Konzepten zu erläutern.

Der Schwerpunkt des Berichts liegt auf dem Zugang zu Unternehmensressourcen, Verhaltensanalysen und Beobachtungen.

Zielgruppe

Dieser Bericht richtet sich an einen breiten Personenkreis, darunter Sicherheits-, System- und Netzwerkarchitekten sowie Leiter von Sicherheitsprogrammen, die für die technischen Aspekte von Aufbau, Betrieb und Sicherung der Unternehmensressourcen und -anlagen verantwortlich sind. Es ist technisch ausgerichtet, und es wird davon ausgegangen, dass die Leser grundlegende Kenntnisse über Sicherheit, Netzwerke und IT-Systeme haben.

Zero Trust bewertet kontinuierlich alle Aspekte des Verhaltens von Entitäten während einer Netzwerkverbindung und bietet adaptive Zugriffskontrollen auf der Grundlage bestimmter Parameter und akzeptabler Geschäftsrisiken.

PRINZIPIEN

Prinzipien sind allgemeine Regeln und Richtlinien, die verständlich, solide, vollständig und eigenständig sein sollten und nicht dazu gedacht sind, Offensichtliches zu erklären. Sie informieren und unterstützen das Unternehmen bei der Erfüllung ihres Auftrags und sind auf lange Sicht konzipiert, damit sie nur selten geändert werden müssen. Jedes Prinzip sollte eine Aussage enthalten, die den Entscheidungsprozess im Unternehmen unterstützt.

Im Folgenden finden Sie einige allgemeine Prinzipien, die bei der Umsetzung einer Zero-Trust-Strategie eine Orientierungshilfe bieten und für die jeder Architekt offen sein sollte:

- Jeder im Unternehmen muss den geschäftlichen **KONTEXT** verstehen.
  - Bei geschäftlichen Ressourcen (Daten, Informationen muss zum einen die Kritikalität definiert sein. Diese ergibt sich in der Regel aus dem Geschäftskontinuitätsplan und dem von ihm unterstützten Geschäftsprozess. Zum anderen muss die Sensibilität definiert sein, die in der Regel aus der Informationsklassifizierungspolitik des Unternehmens und den notwendigen Integritätsanforderungen an die Daten und den Geschäftsprozess hervorgeht.
- Es darf **KEIN** implizites Vertrauen zwischen Entitäten bestehen.
  - Alle Entitäten müssen während der gesamten Netzwerkinteraktion kontinuierlich überprüft und bewertet werden.
- Vertrauen ist nicht binär, sondern ein Kontinuum.
  - Es gibt verschiedene Stufen des Vertrauens, je nach geschäftlichem Kontext und der akzeptierten Risikobereitschaft.
- Der Zugang wird **NUR** für die einzelne Unternehmensressource gewährt.
  - Es gibt **KEINEN** Netzwerkzugang, sondern nur Zugang zu Ressourcen (Anwendungen, Dienste usw.).
  - Vermeiden Sie „Vertrauenszonen“ und nutzen Sie stattdessen Einzelsitzungen.
- Gehen Sie davon aus, dass alle Netzwerke gleich sind
  - Gehen Sie von der Vorstellung aus, dass Intranet und Internet gleichgestellt sind.

Annahmen

Es ist wichtig zu verstehen, dass bestimmte Bedingungen vorausgesetzt sind, zum Beispiel:

- Die Organisation ist bereit und in der Lage, das Notwendige zu tun.
- Die Organisation wird von der Unternehmensführung unterstützt.
- Die erforderlichen Ressourcen sind vorhanden oder werden der Organisation zugewiesen.
- Der Organisation stehen technologische Möglichkeiten zur Verfügung.

ERSCHLIESSUNG DES KONTEXTES

Die Anwendung der Zero Trust-Prinzipien stellt eine ganzheitliche und strategische Herangehensweise für den Aufbau eines Sicherheitsprogramms dar. Eine Strategie muss festlegen, welche Richtlinie in einem bestimmten Geschäftskontext angewendet wird. Es ist unbedingt notwendig zu verstehen, dass Zero Trust kein Notpflaster oder Produkt ist. Die Implementierung sollte mit einem grob strukturiertem Ansatz beginnen, wobei die Richtlinie mit zunehmendem Verständnis der Benutzerbedürfnisse, der geschäftlichen Anforderungen und der geschäftlichen Auswirkungen immer detaillierter wird.

Das traditionelle Konzept der Kontrollen nach dem Prinzip „Erlauben/Sperren" funktioniert nicht mehr und birgt erhebliche Risiken für ein Unternehmen. Unternehmen müssen bei der Bewertung jeder Art von Zugriff auf Ressourcen eine Risikobetrachtung anstellen, die in hohem Maße kontextabhängig ist.

Die Qualität des Kontextes ergibt sich aus mehreren Komponenten, die bei jeder Verbindungsanfrage berücksichtigt werden müssen, bevor die Verbindung zum endgültigen Ziel hergestellt wird. Diese Komponenten sind:

- Daten
- Identität
- Endgerät
- Anwendung (Ressource)
- Netzwerk
- Sichtbarkeit und Analytik
- Automatisierung und Orchestrierung

Kontinuierliche Bewertung

Die kontinuierliche Bewertung dieser Komponenten liefert den kontextbezogenen Output für die Risikoakzeptanzberechnung, mit der wiederum die Kontrollmechanismen gesteuert werden, die die dynamische Anpassung der Richtlinien vor oder während des Zugriffs auf die Ressourcen beeinflussen.

Daten

Das Geschäft entwickelt sich ständig weiter, aber der Lebenszyklus der Daten bleibt gleich. Daten sind die Seele eines jeden Unternehmens, und so sollten sie auch behandelt werden.

Während viele Unternehmen die typische Klassifizierung ihrer Daten vermeiden oder als schwierig empfinden, ist es zwingend erforderlich, sich an das erste Prinzip von Zero Trust, das „Verstehen des geschäftlichen Kontextes", zu halten und die folgenden Schritte durchzuführen:

- Daten verstehen
  - Ermitteln (Das Unternehmen muss wissen, wo sich die Daten befinden.)
  - Klassifizieren (Das Unternehmen muss den relativen Wert der Daten definieren und sie dann dementsprechend analysieren, kontextualisieren und organisieren.)

- Zuordnen zur Vertraulichkeit (abgeleitet von Sensibilität), Integrität (abgeleitet von Sensibilität) und Verfügbarkeit (abgeleitet vom BCP (business-critical process, geschäftskritischer Prozess))
    - » Falls unbekannt oder unbestimmt, weisen Sie diesen Kategorien (Vertraulichkeit, Integrität und Verfügbarkeit) eine Standardbewertung zu. Anhand dieser Angaben lässt sich zunächst eine Richtlinie festlegen, die dann im Laufe der Zeit weiter verfeinert werden kann.
- Identifizieren von Dateneigentümern und Datenverwaltern.

- Daten schützen
    - Prüfen (Überprüfen aller Daten, z. B. SSL-Entschlüsselung)
    - Governance (Festlegen von Regeln und Leitlinien)
    - Kontrollieren (Anwenden technischer Kontrollmechanismen)

Identität

In jeder Organisation gibt es viele Benutzer, jedoch ist kein Benutzer wie der andere. Sie alle erfordern ein verschiedenes Maß an Zugang zu bestimmten Ressourcen, und die damit verbundenen Kontrollen müssen angemessen durchgeführt werden. Es ist entscheidend, den gesamten Identitätslebenszyklus zu verfolgen, angefangen bei der Bereitstellung über die Verwaltung und Governance bis hin zur Aufhebung der Bereitstellung, wenn die Identität nicht mehr benötigt wird. Die Aufhebung der Bereitstellung ist ein Schritt, an dem viele Unternehmen scheitern, weil es an einem geeigneten Verfahren mangelt.

Die Vermeidung von Sicherheitsverstößen und Datenverfälschungen sind die wichtigsten Ergebnisse guter Identitäts-Governance- und Zugriffsverwaltungsprogramme. Wenn die richtigen Benutzer zur richtigen Zeit Zugriff auf die richtigen Daten erhalten, wird das Risiko von Verstößen und Verfälschungen, die den Unternehmensbetrieb beeinträchtigen und sich auf Kunden auswirken, minimiert. Identitäts-Governance- und Zugriffsverwaltungsprogramme müssen in der Lage sein, die folgenden Punkte zu erfüllen:

- Zugriffsverwaltung
    - Zuordnung von Benutzerprofilen
    - Provisionierung, Deprovisionierung und Übertragungen
- Bewertung von Zugangsdaten
    - Authentifizierung und Autorisierung
    - SSO und MFA
    - Privilegierter Zugriff
- Governance
    - Zugriffs-Governance
    - Anfrage- und Genehmigungsprozess
    - Abstimmungs- und Fehlerprozesse

Endgerät

Die Zeiten haben sich geändert, seit Unternehmen „ausschließlich“ vom Unternehmen verwaltete Geräte benötigten. Heutzutage erfordern die Benutzer eine Vielzahl von Geräten, um ihre Arbeit zu erledigen. Viele Unternehmen sind deshalb inzwischen einverstanden, dass Benutzer ihre eigenen Geräte mitbringen (BYOD, bring your own device). Für eine verwaltete Gruppe von Geräten ist ein solider Bestand an Geräten unerlässlich, denn sie müssen alle identifiziert, isoliert und durch die Implementierung richtlinienbasierter Kontrollen gesichert sein. Unternehmen müssen jedoch sicheren Zugriff auf Ressourcen bieten, der über ein vom Unternehmen bereitgestelltes Gerät hinausgeht.

Registrieren Sie nicht vertrauenswürdige oder nicht verwaltete Geräte. Unternehmen müssen zunehmend den Zugriff von Dritten zulassen, was wiederum den Zugriff von nicht vertrauenswürdigen Endgeräten zur Folge hat, zusätzlich zu dem bereits erwähnten BYOD.

Bei der Erarbeitung der Zero-Trust-Zugangsrichtlinie muss eine Organisation Endgeräte berücksichtigen (vertrauenswürdige oder nicht vertrauenswürdige/verwaltete oder nicht verwaltete). Hierfür gibt es keine Einheitslösung, vielmehr ist es notwendig, den Benutzer- und Geschäftskontext zu verstehen. In einigen Szenarien erhalten nicht verwaltete Geräte den gleichen Zugriff auf Anwendungen (und damit auf Daten) wie verwaltete Geräte. In einigen Fällen jedoch nicht – mehr dazu folgt im Abschnitt über die Risikoeinstufung.

Anwendung

Mit der zunehmenden Verbreitung von Cloud- und SaaS-Anwendungen sowie -Diensten haben sich die Geschäfts- und Betriebsmodelle verändert. Einer der wichtigsten Sicherheitsaspekte besteht darin, den Zugang zu Ressourcen, in diesem Fall zu Anwendungen, auf ein Minimum zu beschränken. Hier wird Zero Trust extrem leistungsfähig, da die Benutzer keine Verbindung zu Netzwerken mehr herstellen müssen, sondern sich stattdessen über einzelne isolierte Sitzungen mit einer bestimmten Anwendung oder einem Dienst verbinden.

Jede Organisation sollte sich über die folgenden Punkte in den Anwendungsvereinbarungen im Klaren sein:

- Art der Anwendung
- Hosting-Modell
- Vertraulichkeit, Integrität und Verfügbarkeit der Anwendung (abhängig von den Daten, auf die sie zugreift, die sie speichert oder verarbeitet, oder den Geschäftsprozessen, die sie unterstützt)
- Transaktionsströme – vor- und nachgelagert
- Anforderungen an den Zugriff durch Dritte
- Das Ergebnis einer Risikobewertung für eine Anwendung

Netzwerk

Frühere abgegrenzte Modelle verschwinden, Konnektivität ist allgegenwärtig, und Sicherheit ist nun verteilt. Es ist von entscheidender Bedeutung, die Transaktionsströme und Interaktionen zwischen zwei oder mehreren Punkten zu verstehen. Netzwerkisolierung und Mikrosegmentierung in stärker lokalisierte Segmente sind einige taktische Maßnahmen zur Minimierung von Lateralbewegungen, ermöglichen aber auch eine genauere Kontrolle des Ressourcenzugriffs.

Netzwerkteams kennen bereits die Topologie, die Bereitstellung von Inhalten und die Servicequalität durch Leistungsüberwachung und -optimierung, aber Zero Trust führt zu dynamischeren Änderungen innerhalb der Netzwerkarchitektur, wo Anpassungen erforderlich sind.

Endgeräte und Benutzer greifen nicht mehr auf Netzwerke zu. Dennoch haben sie eine direkte Verbindung zu einem einzelnen Dienst, einer Anwendung oder einer Arbeitslast (was die Stärke von Zero Trust ausmacht, denn wir können nun die Angriffsfläche erheblich verkleinern): Daher ist die Anwendung der folgenden Konzepte entscheidend:

- Einführung der Sicherheitseinstellung „Standardverweigerung“
- Vermeidung von „Vertrauenszonen“
- Isolierung der Sitzung
- Mikrosegmentierung

Sichtbarkeit und Analytik

Die Einsicht in die Transaktionen zwischen den oben genannten Komponenten mit Einzelheiten zum Kontext und der Fähigkeit, diese gegenüberzustellen und auszuwerten, ist ein absolutes Muss. Dadurch können wir die Interaktion, die Qualität und die Leistung eines konstruierten Ökosystems besser verstehen, was uns wiederum in die Lage versetzt, neue feinkörnige Richtlinien zu entwickeln und umzusetzen und somit die Einführung von Kontrollen zu fördern. Die Funktionen müssen auf bestimmte Ergebnisse und Zwecke ausgerichtet sein, beispielsweise auf die schnelle Erkennung von und Reaktion auf Bedrohungen, bei denen das IR-Team der größte Verbraucher ist, auf die Suche nach Bedrohungen, auf forensische Untersuchungen, Compliance-Aktivitäten usw.

Ausgereifte Zero Trust-Programme müssen zu Folgendem in der Lage sein:

- Untersuchen des gesamten Datenverkehrs (Deep Packet Inspection, die über die reine Netzwerktelemetrie hinausgeht)
- Korrelieren von Daten zwischen mehreren unterschiedlichen Quellen mit Security Information and Event Management (SIEM)
- Identifizieren von anomalem Verhalten mit User-Environment Behavior Analysis (UEBA)
- Ganzheitlicher Blick auf die Umgebung

Automatisierung und Orchestrierung

Eine der größten Herausforderungen für viele Organisationen ist heute die Verfügbarkeit von qualitativ hochwertigen Ressourcen. Die Sicherheit ist einer der am stärksten betroffenen Bereiche, in dem es zu Kapazitätsnachteilen kommt. Einzelpersonen können nicht schnell genug und in ausreichendem Umfang auf solche komplexen Zusammenhänge im Ökosystem reagieren. Die zunehmende Komplexität macht den Einsatz von Automatisierung erforderlich.

Automatisierung und Orchestrierung bieten unvergleichliche Möglichkeiten, ein effizienteres und effektiveres Sicherheitsprogramm bereitzustellen. Es geht um den richtigen Prozess zur richtigen Zeit. Durch Automatisierung können Unternehmen die Identifizierung und Beseitigung bestimmter Bedrohungen mit einer Präzision beschleunigen, mit der Menschen nicht mithalten können.

Risikobewertung und Definition der Zugriffsrichtlinie

Der Zugriff auf Ressourcen wie Anwendungen, Dienste oder Daten wird durch richtlinienbasierte Kontrollen verwaltet. Die Richtlinien setzen dann die Zugriffsregeln durch, die von der Risikobereitschaft des Unternehmens bestimmt werden. Die Definition der Richtlinie und damit die Auswahl der Kontrollen sollte sich an einer Reihe von Kriterien zur Bewertung der einzelnen oben genannten Komponenten orientieren.

Organisationen können zwei Wege einschlagen:

- Bewerten Sie für jedes Attribut jedes mögliche Implementierungsszenario. Legen Sie dann eine Regel fest, die eine bestimmte Zugriffsebene ermöglicht (bzw. einschränkt), und wenden Sie diese kumulativ an.
- Erstellen Sie ein Risikomodell, bei dem die Implementierungsszenarien aller Attribute gewichtet werden, und legen Sie auf der Grundlage der Summe dieser Punktzahl Zugriffsrichtlinien fest.

Bei Ansatz eins kann die Organisation beispielsweise nicht verwaltete Geräte nur auf solche Anwendungen den Zugriff erlauben, die Daten mit niedriger Vertraulichkeits- und Integritätseinstufung verarbeiten, speichern oder abrufen. Darüber hinaus kann der Benutzerkontext in diese Richtlinienentscheidung einbezogen werden, z. B. kann ein interner Benutzer, der von einem nicht verwalteten Gerät kommt, auf Anwendungen zugreifen, die Daten mit einer höheren Vertraulichkeits- und Integritätseinstufung verarbeiten, speichern oder abrufen. Dennoch haben sie keinen Zugriff auf die kritischsten Anwendungen oder Daten.

Jede Permutation kann zu einer anderen Richtliniendefinition und damit zur Anwendung eines anderen Kontrollsatzes führen.

Ein paar Musterpermutationen sind unten aufgeführt. Die Organisation muss jedoch eine eigene Dokumentation und Bewertung durchführen, passend zur Arbeitsweise und den bestehenden Standards und Praktiken:

- **Benutzer:** Intern und fest angestellt, interner Auftragnehmer, Drittpartei
- **Bewertung der Vertraulichkeit der Daten:** Streng vertraulich, vertraulich, privat, öffentlich
- **Bewertung der Datenintegrität:** Sehr hoch, hoch, mittel, niedrig
- **Bewertung der Datenverfügbarkeit:** Hoch verfügbar, 0–4 Stunden, 4–24 Stunden, länger als 24 Stunden
- **Endgerät:** Verwaltet, nicht verwaltet
- **Anwendung:** Kritisch, wichtig, unbedeutend

Im Sinne des Konzepts der kontinuierlichen Bewertung sollten diese Komponenten während einer Benutzersitzung jederzeit bewertet und überprüft werden. Sollte eine Veränderung festgestellt werden, sind Maßnahmen zu ergreifen: zum Beispiel die Sitzung beenden, die erneute Authentifizierung erzwingen oder das Set-up-Authentifizierung durchführen.

Ein Szenario könnte sein, dass die Sitzung plötzlich von einem nicht verwalteten Gerät auszugehen scheint, obwohl sie zuvor für ein verwaltetes Gerät gehalten wurde. Es könnte auch sein, dass der Benutzer versucht, auf Daten zuzugreifen, die inzwischen mit einer höheren Vertraulichkeit eingestuft sind als zuvor.

FAZIT

Die meisten aktuellen Sicherheitsarchitekturen wurden für ein Technologiegefüge entwickelt, das nicht mehr aktuell ist. Um neue Wege zu beschreiten und Ihr Unternehmen voranzubringen, ist eine neue Denkweise erforderlich. Die Sicherheitsarchitektur muss sich auf ein klares Verständnis des Geschäftsrisikos, des Kontextes sowie auf die Anwendung adaptiver Kontrollen konzentrieren, um eine Reihe neuer Herausforderungen zu bewältigen und gleichzeitig Benutzern und Unternehmen ein schnelles Vorankommen zu ermöglichen.

Ein angemessenes Gleichgewicht zwischen Sicherheit, Datenschutz und Benutzerfreundlichkeit ist unerlässlich.

Netskope, ein weltweit führendes Unternehmen im Bereich Cybersicherheit, definiert Cloud-, Daten- und Netzwerksicherheit neu, um Unternehmen bei der Anwendung von Zero Trust-Prinzipien zum Schutz von Daten zu unterstützen. Die Netskope Intelligent Security Service Edge(SSE)-Plattform ist schnell und leicht zu bedienen; sie schützt Menschen und sichert Geräte sowie Daten überall. Besuchen Sie netskope.de und erfahren Sie, wie Netskope Kunden dabei unterstützt, auf alles vorbereitet zu sein.