Never Trust, Always Verify – Prinzipien und Komponenten moderner Zero-Trust-Architekturen

1. Einleitung

Definition von Zero Trust und der Relevanz in der heutigen Cybersecurity-Landschaft

Was ist Zero Trust?

Zero Trust ist ein Cybersicherheitsansatz, bei dem alle Zugriffe auf ein Netzwerk und die darin enthaltenen Ressourcen zunächst als potenzielle Bedrohung betrachtet werden. Alle Benutzer, Geräte oder Anwendungen müssen sich also verlässlich verifizieren, um Zugang zu erhalten. Dabei spielt es keine Rolle, ob diese Zugriffe von innerhalb oder von außerhalb des Netzwerks kommen: Das klassische, lange Zeit übliche „Burggraben"-Modell, bei dem ein gut geschützter Perimeter den Übergang zwischen der sicheren internen Umgebung und der unsicheren Außenwelt bildete, hat in den modernen Netzwerkarchitekturen von heute weitgehend ausgedient. An seine Stelle tritt nun der Zero-Trust-Ansatz, der eben nicht nur das Eindringen in ein Netzwerk, sondern auch die laterale Bewegung innerhalb eines Netzwerks verhindern soll: Getreu dem Prinzip „Never trust, always verify" muss dabei jede Zugriffsanfrage authentifiziert, autorisiert und validiert werden, bevor der Zugriff auf das Netzwerk oder die Ressourcen gewährt wird.

Und noch eines unterscheidet moderne Zero-Trust-Umgebungen von den Access-Lösungen vergangener Jahre: Zero Trust gewährt den Zugang zu sensiblen Daten und Ressourcen konsequent auf der so genannten Need-to-know-Basis. Das bedeutet, dass ausschließlich Nutzer, Geräte oder Anwendungen, die auch tatsächlich Zugriff auf bestimmte Informationen benötigen, dafür autorisiert werden. Strenge Kontrollen und kontinuierliche Überwachung sorgen für die Erkennung von Anomalien und verdächtigem Verhalten und ermöglichen angemessene Reaktionen. Im Rahmen dieses Security-Frameworks kommt eine breite Palette moderner Sicherheitstechnologien zum Einsatz, darunter Identity & Access Management (IAM), Multi-Faktor-Authentifizierung (MFA), Netzwerksegmentierung, Verschlüsselung und Verhaltensanalyse. Im Zusammenspiel stellen diese Technologien sicher, dass nur autorisierte Benutzer, Geräte und Anwendungen auf Ressourcen zugreifen können – und dass nicht autorisierte Zugriffsversuche automatisch erkannt und zeitnah unterbunden werden.

Content:

Warum brauchen wir Zero Trust?

Die IT-Landschaften der Unternehmen, Behörden und Organisationen müssen heute einer Vielzahl von Herausforderungen standhalten. Das Zero-Trust-Sicherheitsmodell liefert dafür ein robustes Fundament.

1. Zunehmend professionelle und raffinierte Bedrohungen und Akteure
Die Bedrohungslandschaften entwickeln sich dynamisch weiter und sind in jüngster Zeit vor allem durch eine rasch zunehmende Professionalisierung der Akteure gekennzeichnet. Die Vermarktung von Hacking-Services im Dark Web hat sich weltweit längst als hochgradig profitables Geschäftsmodell etabliert, und führt heute dazu, dass selbst kleinste Unternehmen immer öfter zum Ziel hochgradig professionell geführter Cyberattacken werden können. Dabei nutzen die Angreifer immer raffiniertere Taktiken – etwa mehrstufige Malware, Social Engineering und Supply-Chain-Angriffe –, um in fremde Netzwerke einzudringen und sensible Daten zu stehlen. Die dadurch entstandenen Schäden nehmen von Jahr zu Jahr zu.

Der Ansatz des Zero-Trust-Modells, bei dem alle Zugriffsanfragen als potenziell bösartig eingestuft und strengen Authentifizierungs- und Autorisierungsprüfungen unterzogen werden, kann die potenzielle Angriffsfläche eines Unternehmens nachhaltig verringern und das Schadenspotenzial kompromittierter Identitäten radikal einschränken. So reduzieren Unternehmen das Risiko für schwerwiegende Angriffe erheblich.

2. Die Auflösung des Perimeters
Vor der Verbreitung mobiler und Cloud-basierter Technologien schützten sich Unternehmen in der Regel, indem sie einen sicheren Perimeter um das Netzwerk zogen. Dort wurde der eingehende Traffic im Sinne des mittelalterlichen „Burggraben"-Modells mit Firewalls inspiziert und gefiltert, um externe Bedrohungen zu stoppen. Doch die zunehmende Vernetzung mit externen Systemen, die Anbindung unzähliger Cloud-basierter und mobiler Endpoints, die Integration offener Schnittstellen und die Öffnung für Managed-Service-Modelle haben dieses Perimeter-Modell innerhalb kurzer Zeit weitgehend obsolet gemacht.

Heute gilt es, sämtliche Daten und Anwendungen unabhängig vom Ort der Speicherung oder Ausführung zu schützen.

Kurz: Die Unternehmen können sich nicht mehr darauf verlassen, einen hohen Wall um ihr Netzwerk zu errichten und anschließend nur noch die kleine Zahl fester Zugänge zu kontrollieren. Heute gilt es, sämtliche Daten und Anwendungen unabhängig vom Ort der Speicherung oder Ausführung zu schützen – und genau das ist der Fokus des Zero-Trust-Modells.

3. Remote Work ist auf dem Vormarsch
9-to-5 im Office war gestern. In den meisten Unternehmen verbringen die Anwender heute zumindest einen Teil der Arbeitszeit abseits ihres Büroarbeitsplatzes, sei es zuhause oder unterwegs: Und dieser Trend zum flexiblen hybriden Arbeiten wird uns auch langfristig erhalten bleiben. Remote Work wird auch im New Normal ein wichtiges Merkmal moderner Unternehmenskultur sein – und ein gewichtiges Argument, um im Wettbewerb um mangelnde Fachkräfte die besten Talente zu ergattern. Mit Blick auf die Informationssicherheit und den Datenschutz ist der Siegeszug der hybriden Arbeitswelt aber alles andere als unproblematisch: Die offenen, weit verzweigten Netzwerke mit ihrem bunten Mix beruflich und privat genutzter Endgeräte und Identitäten bieten Cyberkriminellen eine ungleich größere Angriffsfläche.

Die beste Antwort heißt auch hier häufig Zero Trust: Der konsequente Fokus auf kontinuierliche Authentifizierungs- und Autorisierungsprüfungen ermöglicht es den Unternehmen, Remote-Zugriffe auf ihre Netzwerke und Ressourcen zuverlässig zu schützen – und Mitarbeitende so auch im Home Office und unterwegs produktiv und sicher anzubinden.

4. Einhaltung von Compliance-Vorgaben
Unternehmen müssen heute unterschiedlichsten gesetzlichen, branchenspezifischen und internen Compliance-Bestimmungen gerecht werden. Dies erfordert häufig die Implementierung umfassender technischer und organisatorischer Maßnahmen, sowohl mit Blick auf den lückenlosen Schutz von Daten und IT-Systemen als auch mit Blick auf das Monitoring und die Dokumentation der Prozesse.

Der gesamte Zugriffsverlauf kann in Echtzeit protokolliert und als Prüfpfad angezeigt werden.

Das Zero-Trust-Modell liefert einen detaillierten Rahmen für die Umsetzung der entsprechenden Maßnahmen und liefert den Unternehmen ein robustes Fundament, um die Einhaltung der Vorgaben jederzeit lückenlos nachweisen zu können. Aus geschäftsstrategischer Sicht erhöht Zero Trust insbesondere die Transparenz über die Datenzugriffe durch Benutzer, Workloads und Geräte. Auf diese Weise kann der gesamte Zugriffsverlauf in Echtzeit protokolliert und als Prüfpfad angezeigt werden, damit externe Aufsichtsbehörden und Auditoren den Prüfpfad und die Compliance nachvollziehen können.

Mit dem Ansatz, niemals zu vertrauen und jeden Zugriff dediziert zu validieren, stellt das Zero-Trust-Sicherheitsmodell eine wichtige Weichenstellung dar, um Netzwerke und Daten zuverlässig vor der breiten Palette moderner Cyber-Bedrohungen zu schützen – und das unabhängig davon, wo sich die entsprechenden Ressourcen befinden.

Kurze Geschichte und Entwicklung des Zero-Trust-Modells

Das Konzept „Zero Trust" wurde vor rund drei Jahrzehnten erstmals erwähnt und im Laufe der Zeit von verschiedensten Akteuren überarbeitet und weiterentwickelt. Geprägt wurde der Begriff bereits im Jahr 1994 von Stephen Paul Marsh, der in seiner Doktorarbeit „Formalising Trust as a Computational Concept" das Vertrauen zum Zwecke der Computer Security mathematisch beschrieb.

Ab 2003 nahm sich das Jericho Forum, eine internationale Gruppe interessierter CISOs (Chief Information Security Officers), die sich für die Definition und Förderung der „de-perimeterisation" einsetzt, des Themas Zero Trust an. Das Forum formulierte erstmals explizit die Grundidee, dass man nichts oder niemandem vertrauen sollte, nur weil es sich innerhalb des Netzwerks befindet. Schon vor zwanzig Jahren suchten die Beteiligten also nach Lösungen für die bereits erkennbare Auflösung des Perimeters. In den folgenden Jahren befasste sich das Konsortium auch mit Themen wie der sicheren Zusammenarbeit in Clouds sowie mit der wachsenden Bedeutung von Identitäten und dem Management ihrer Zugriffe. Das Jericho Forum erledigte auf diese Weise viel wichtige Grundlagenarbeit für das, was wir heute unter Zero Trust verstehen, ehe es 2014 in das Security Forum der Open Group integriert wurde. Seine Arbeit wurde in Teilen der Cloud Security Alliance und in Teilen der Global Identity Foundation übertragen.

Das Zero-Trust-Sicherheitsmodell in seiner heutigen Form stammt schließlich vom Forrester-Analysten John Kindervag, der ab 2010 in mehreren Arbeiten eine

Zero-Trust-Netzwerkarchitektur beschrieb, die ein datenzentriertes Design besaß und Mikrosegmentierung zur Durchsetzung granularer Regeln nutzte. Kindervag betrachtete dies vor allem als vielversprechenden Ansatz zur Einschränkung lateraler Bewegungen – denn für ihn stand fest, dass der gesamte Netzwerkverkehr nicht vertrauenswürdig ist und folglich jede Zugriffsanfrage auf eine Ressource zuverlässig gesichert erfolgen muss.

Never trust, always verify!

Seinem Ansatz nach sollten daher alle Zugriffsanfragen als potenziell bösartig behandelt und strengen Authentifizierungs- und Autorisierungsprüfungen unterzogen werden. Im Rahmen seiner Forschung formulierte er auch den vielfach zitierten Leitsatz „Never trust, always verify", der auch heute noch untrennbar mit Zero Trust verknüpft ist, und kompromisslos einfordert, dass jeder Zugriff kontinuierlich überwacht und auf der Grundlage von Kontextfaktoren wie Identität, Gerät, Standort und Verhalten des Benutzers zu validieren ist. Mit der Weiterentwicklung des Zero-Trust-Konzepts innerhalb der Branche gewannen in der Folge zunehmend identitätsorientierte Ansätze an Bedeutung – ein Trend, der sich mit dem rasanten Siegeszug von Mobil- und Cloud-Technologien immer weiter beschleunigte.

Im Jahr 2014 folgte ein weiterer wichtiger Meilenstein: Google veröffentlichte im Rahmen eines Forschungsprojekts zur internen Zero-Trust-Einführung sein Beyond-Corp-Modell. Auch dieser Ansatz folgt der Idee, dass die Kombination aus sicherem Netzwerkzugang und geschütztem Intranet allein nicht mehr ausreicht. Daher verlagert das BeyondCorp-Modell die Zugriffskontrollen vom Perimeter auf einzelne Geräte und Nutzer. Ein Ansatz, der in der Praxis hohen Anklang fand: Das Modell wird von Google nach wie vor unterstützt, und von vielen Unternehmen verwendet – in der Regel, weil sie auf ein klassisches VPN verzichten und den Nutzern dennoch die Möglichkeit geben wollen, auch von nicht vertrauenswürdigen Netzwerken aus sicher zu arbeiten.

Im Laufe der Jahre wurde das Zero-Trust-Sicherheitsmodell von Cybersecurity-Experten weltweit kontinuierlich weiterentwickelt. Heute bündelt die Branche unter dem Schlagwort eine Vielzahl unterschiedlichster Technologien und Strategien, die zum ganzheitlichen Schutz vor Cyberbedrohungen beitragen können. Zu den wichtigsten Leitfäden gehört dabei zweifellos der 2018 vom National Institute of Standards and Technology (NIST) veröffentlichte Guide zur Zero-Trust-Architektur, der einen umfassenden Rahmen für die Umsetzung von Zero-Trust-Prinzipien in Unternehmensumgebungen bietet.

2. Die Prinzipien von Zero Trust

Die Kernprinzipien von Zero Trust

Das Zero-Trust-Sicherheitsmodell basiert auf einer Reihe von Grundprinzipien, die seine Umsetzung leiten. Diese Grundsätze sind:

1. Explicit Verification: Im Rahmen des Zero-Trust-Modells gilt es, den Zugriff auf sämtliche Ressourcen explizit zu überprüfen und authentifizieren – und das auf der Grundlage verbindlicher Richtlinien, die die Identität, das Gerät, den Standort und das Verhalten des Benutzers berücksichtigen.

Diese sechs Kernprinzipien bilden die Grundlage jeder erfolgreichen Zero-Trust-Einführung – und helfen Unternehmen dabei, die Vorteile des Modells zu erschließen.

2. Principle of Least Privilege: Identitäten aller Art erhalten nur die minimalen, für ihre Tätigkeit erforderlichen Rechte, und diese auch nur für den jeweiligen Zeitraum, der für die Durchführung der Aufgabe benötigt wird.

3. Assume Breach: Das Zero-Trust-Modell geht davon aus, dass alle Geräte, Netzwerke und Benutzer potenziell gefährdet sind, und verfolgt einen proaktiven Ansatz zur kontinuierlichen Überwachung und Erkennung von ungewöhnlichem Verhalten.

4. Microsegmentation: Um das Schadenspotenzial lateraler Netzwerkbewegungen konsequent zu minimieren, muss das Netzwerk in kleine, voneinander isolierte und leicht zu verwaltende Segmente untergliedert werden.

5. Continuous Monitoring: Das gesamte Benutzer- und Geräteverhalten wird kontinuierlich überwacht und analysiert, um Anzeichen für verdächtige Aktivitäten oder anormales Verhalten zu erkennen.

6. Strong Access Control: Die Implementierung robuster Zugriffskontrollen stellt sicher, dass Identitäten nur auf die Ressourcen zugreifen können, für die sie die notwendigen Rechte besitzen.

Die Idee hinter Zero Trust – Minimierung der Zone des impliziten Vertrauens

Ein zentrales Konzept von Zero Trust ist die sogenannte „Minimierung der Zone des impliziten Vertrauens" – die Idee, dass Unternehmen versuchen sollten, die Anzahl der Ressourcen zu minimieren, denen ohne Prüfung und Authentifizierung automatisch vertraut wird.

Noch vor einigen Jahren war die Zone des impliziten Vertrauens sehr weit gefasst: Jeder Endpunkt, jeder Anwender und jeder Dienst innerhalb des klassischen Firewall-Perimeters galt zunächst einmal als vertrauenswürdig. Das erleichterte zwar intern die Kommunikation und den Austausch von Ressourcen, machte die Unternehmen aber auch hochgradig angreifbar: Sobald es einem Angreifer gelang, ein internes System zu kompromittieren, konnte er sich dank des Vertrauensvorschusses ungehindert durch das Netzwerk bewegen, und erlangte so über kurz oder lang Zugriff auf die wertvollsten Assets und Daten.

Das Zero-Trust-Modell trachtet deshalb danach, die Zone des impliziten Vertrauens so weit wie möglich zu reduzieren. Es behandelt alle Zugriffsanfragen als potenziell bösartig und unterzieht sie umfassenden Authentifizierungs- und Autorisierungsprüfungen auf der Basis strenger Zugriffsrichtlinien, bei denen kontextbezogene Faktoren wie die Identität des Benutzers, sein Gerät, sein Standort und sein Verhalten Berücksichtigung finden.

Dies ermöglicht es den Unternehmen nicht nur, ihre Angriffsfläche erheblich zu reduzieren. Wenn nicht mehr implizit vertraut wird, sinkt auch das Schadenspotenzial im Falle eines erfolgreichen Angriffs, da sich die Hacker nicht mehr ungehindert lateral bewegen können. Und noch einen wichtigen Mehrwert bietet die kontinuierliche Überwachung und Analyse der Access-Anfragen: Verdächtige Aktivitäten und ungewöhnliches Verhalten fallen wesentlich früher auf und können oft unterbunden werden, bevor echter Schaden entsteht.

Die Vorteile von Zero Trust

Die Vorteile von Zero Trust:

Verbesserung des Security-Standings

Lückenlose Transparenz und Kontrolle

Durchgängige Einhaltung der Compliance

Höhere Produktivität durch Automatisierung

Ob mit Blick auf die Kontinuität der Überprüfung, auf den klaren Fokus auf Ressourcen und Identitäten oder mit Blick auf die dynamische Weiterentwicklung der Policies: Zero Trust bricht in mehr als einer Hinsicht radikal mit den etablierten Security-Architekturansätzen früherer Jahre und läutet damit einen echten, tiefgreifenden Paradigmenwechsel ein. Der kompromisslose Ansatz, die Angriffsfläche zunächst maximal zu reduzieren und dann unter Einhaltung des Least-Privilege-Prinzips sukzessive passgenaue Zugriffe zu ermöglichen, ist wie geschaffen für die offenen und Cloud-basierten Enterprise-Umgebungen von heute – und bietet Unternehmen eine Vielzahl handfester Vorteile.

Verbesserung des Security-Standings
An erster Stelle steht dabei die nachhaltige Verbesserung des Sicherheitsniveaus, die Unternehmen mit der Einführung von Zero Trust erfahrungsgemäß erreichen. Aus der Perspektive eines Risikomanagers betrachtet, gilt dies sogar in doppelter Hinsicht: Durch die Verringerung der Angriffsfläche lässt sich das Risiko eines erfolgreichen Angriffs spürbar reduzieren, während die Umsetzung von Least-Privilege-Access das Schadenspotenzial einer solchen Attacke senkt.

Lückenlose Transparenz und Kontrolle
Ein zweiter wichtiger Pluspunkt von Zero Trust ist die deutlich bessere Transparenz und Kontrolle, die Unternehmen damit erhalten: Die kontinuierliche Überwachung der Zugriffe liefert den IT- und Security-Teams wertvolle Einblicke in das Benutzer- und Geräteverhalten. Auf diese Weise können sie nicht nur ihre Access Policies kontinuierlich optimieren und weiterentwickeln, sondern auch wesentlich schneller auf neue Sicherheitsbedrohungen reagieren.

Durchgängige Einhaltung der Compliance
Wichtig mit Blick auf die Einhaltung von Compliance-Vorgaben: In Zero-Trust-Umgebungen lassen sich äußerst granulare Zugriffsrichtlinien implementieren und anschließend an passgenau implementierten Enforcement-Points durchsetzen. Das macht es den Unternehmen leicht, die Einhaltung regulatorischer Vorgaben sicherzustellen, und diese auch – etwa für anstehende Audits – lückenlos zu dokumentieren.

Höhere Produktivität durch Automatisierung
Und schließlich: Unternehmen mit Zero-Trust-Policy sind in der Regel effizienter und produktiver, da sich über die detaillierten, identitätsbasierten Policies viele Workflows – vom Onboarding neuer Anwendungen bis hin zum User-Lifecycle-Management – umfassend automatisieren lassen. Auf diese Weise können neue Kollegen schneller produktiv einsteigen – und das gesamte Team profitiert früher von technischen Innovationen.

Kurz**:** Das Zero-Trust-Sicherheitsmodell adressiert viele der Security-Herausforderungen, vor denen moderne Unternehmen stehen, von den zunehmend komplexen Bedrohungslandschaften über die hybriden Arbeitswelten bis hin zu zunehmend strengen Compliance-Vorgaben. Kein Wunder also, dass die überwiegende Mehrheit der Unternehmen die Einführung entsprechender Architekturen auf der Agenda hat – und mit Nachdruck vorantreibt. Welche Komponenten es dabei zu berücksichtigen gilt und welche Fallstricke bei der Integration lauern, erfahren Sie im nächsten Kapitel.

Wie sich Zero Trust von traditionellen Security-Modellen unterscheidet

1. Ressourcenbasierte statt Perimeter-basierte Sicherheit:
Klassische Sicherheitsmodelle basieren auf einem Perimeter-basierten Ansatz, bei dem um das gesamte Netzwerk eine hohe Schutzmauer gezogen wird – und der Zugriff auf Ressourcen lediglich an den Ein- und Ausgängen kontrolliert wird. Im Gegensatz dazu folgt das Zero-Trust-Modell einem konsequent ressourcenbasierten Ansatz, bei dem der Zugriff auf jede Ressource über eine dedizierte Policy definiert wird, die klar regelt, wer, wann und wie zugreifen darf.

2. Implizites Vertrauen vs. explizite Überprüfung:
In klassischen Umgebungen galten alle Benutzer und Geräte innerhalb des Perimeters als vertrauenswürdig, und durften sich frei im Netzwerk bewegen. Im Gegensatz dazu geht das Zero-Trust-Modell davon aus, dass alle Zugriffsanfragen potenziell gefährlich sind. Daher müssen sich alle Benutzer und Geräte, die auf Ressourcen zugreifen wollen, zunächst explizit identifizieren und authentisieren.

3. Least Privilege vs. breiter Zugang:
Traditionelle Sicherheitsmodelle gewähren Benutzern und Geräten oft einen relativ breiten, wenn nicht sogar unbegrenzten Zugriff auf Ressourcen. Im Gegensatz dazu implementiert das Zero-Trust-Modell das Prinzip der geringsten Berechtigung: Es gewährt Benutzern und Geräten den Zugriff auf die Ressourcen stets nur für einen begrenzten Zeitraum, und immer nur mit den Rechten, die sie zur Erfüllung ihrer Aufgaben auch wirklich benötigen.

4. Statische vs. dynamische Security:
Traditionelle Sicherheitsmodelle bleiben oft statisch: Einmal definierte Sicherheitsrichtlinien und Kontrollmechanismen bleiben häufig über Jahre hinweg unverändert. Im Gegensatz dazu agiert der Zero-Trust-Ansatz äußerst dynamisch: Aufsetzend auf kontinuierliche Analysen der Bedrohungslage und des Benutzerverhaltens werden die Sicherheitsrichtlinien und -kontrollen kontinuierlich angepasst.

3. Komponenten eines Zero-Trust-Modells

Identity & Access Management
Das Identity & Access Management ermöglicht die durchgängige Überprüfung der Benutzer- und Geräte-Identitäten und überwacht die Legitimität der Zugriffe auf die Ressourcen des Unternehmens – und ist damit die Schlüsselkomponente jeder modernen Zero-Trust-Sicherheitsarchitektur. Denn den Identitäten kommt mit Blick auf alle sechs vorgestellten Kernprinzipien von Zero Trust eine zentrale Rolle zu: Über das IAM lassen sich insbesondere Zugriffskontrollen auf der Grundlage verbindlicher Richtlinien durchsetzen, die kontextbezogene Faktoren wie die Identität des Benutzers, sein Gerät, seinen Standort und sein Verhalten berücksichtigen. Dies trägt dazu bei, die Zone des impliziten Vertrauens zu minimieren und das Risiko eines unbefugten Zugriffs auf sensible Ressourcen zu verringern.

Moderne IAM-Systeme erfüllen dabei eine Vielzahl von Aufgaben – allen voran die Identitätsüberprüfung. Die Identitäten aller Benutzer und Geräte müssen vor jedem Zugriff zweifelsfrei verifiziert werden. Traditionell diente dafür ein Passwort, das heutzutage als alleiniger Faktor allerdings in der Regel nicht mehr ausreicht, da es mit einer Reihe von Nachteilen einhergeht – etwa mit Blick auf die Usability und die Überwindbarkeit. Stattdessen hat sich Multi-Faktor-Authentifizierung als State-of-the-Art etabliert. Dabei müssen die Benutzer ihre Identität durch mehrere, voneinander unabhängige Faktoren authentifizieren, um Zugriff auf die gewünschten Ressourcen zu erhalten.

Die wichtigsten Authentifizierungsfaktoren

„Knowledge“ bezeichnet etwas, das der Nutzer weiß, also beispielsweise ein Passwort.

„Ownership“ ist etwas, das der Nutzer physisch oder auch digital besitzt – vom Mobiltelefon über eine Chipkarte bis zum kryptografischen Schlüssel.

„Inherence“ beschreibt biometrische Merkmale des Nutzers, wie etwa einen Fingerabdruck, Gesichtserkennung oder Iris-Scan.

„Location“ nutzt den Ort des Nutzers zu dessen Authentifizierung. Meldet sich ein Nutzer z.B. von einem ungewöhnlichen Standort oder innerhalb kurzer Zeit von zwei weit entfernten Orten an, so könnte ein Sicherheitsverstoß vorliegen.

Die zweite zentrale IAM-Funktionalität ist die **Zugriffskontrolle**. Dabei validiert die Lösung vor einem Zugriff auf eine Ressource, ob die entsprechende Identität über die erforderlichen Rechte verfügt. Die Basis für diese Entscheidung bilden Richtlinien, die kontextbezogene Faktoren wie die Identität des Benutzers, sein Gerät, seinen Standort und sein Verhalten berücksichtigen. Auf diese Weise lässt sich zuverlässig gewährleisten, dass Benutzer und Geräte stets nur auf die Ressourcen zugreifen können, die sie zur Erfüllung ihrer Aufgaben benötigen.

Durch die **kontinuierliche Überwachung** von Benutzern und Geräten sollten IAM-Systeme permanent nach Anzeichen für verdächtige Aktivitäten oder ungewöhnliches Verhalten suchen. Denn diese könnten auf Sicherheitsbedrohungen hindeuten.

Und schließlich ist auch die **Verwaltung des Identity Lifecycles** eine wichtige IAM-Funktion, da veraltete und nicht mehr benötigte Identitäten stets einen zusätzlichen Risikofaktor darstellen – erst recht, wenn es sich dabei um privilegierte Accounts handelt. Vor allem bei großen Unternehmen mit einer Vielzahl unterschiedlicher Identitäten – vom Mitarbeiter, über Partner und Lieferanten bis zum Kunden – verspricht die Automatisierung des Lifecycles zudem attraktive Einsparpotenziale, und bedeutet für die überlasteten Teams häufig eine wertvolle Entlastung.

Privileged Access Management

Privilegierte Accounts mit weitreichenden Berechtigungen sind bei bösartigen Akteuren besonders beliebte Ziele. Um zu verhindern, dass sich Cyberkriminelle nach dem erfolgreichen Eindringen in das Netzwerk lateral von System zu System bewegen, um ihre Privilegien zu skalieren, gilt es, konsequent das Least-Privilege-Prinzip umzusetzen: Anwender sollten stets nur ein Mindestmaß an Privilegien erhalten, das gerade so ausreicht, um die für sie vorgesehene Aufgabe zu bewältigen. Darüber hinaus sollten die Rechte stets auch nur für das notwendige Zeitfenster und nicht dauerhaft vergeben werden, Stichwort: Just-in-Time-Zugriff. Auf diese Weise lässt sich die Angriffsfläche kritischer Netzwerkfunktionen so klein wie möglich halten.

Die Strategien für moderne PAM-Lösungen unterscheiden sich zwar von Hersteller zu Hersteller, die Grundrichtung weist jedoch meist viele Parallelen auf: Hochrangige

Tier0- oder Tier1-Ressourcen, wie der Domänencontroller, verdienen allerhöchsten Schutz. Daher muss der privilegierte Zugriff darauf zunächst in einer isolierten Umgebung und erst nach einer robusten Multi-Faktor-Authentifizierung erfolgen. Dasselbe gilt auch für Zugriffe auf IDs von SaaS-Admins und privilegierten Business-Usern. Darüber hinaus sollten Unternehmen eine konsequente Strategie für das Passwortmanagement implementieren, die automatische Passwortwechsel für Netzwerkkonten einschließt, ebenso wie die Speicherung kritischer Zugangsdaten in sicheren Vaults – unter anderem für Infrastruktur-Accounts, DevOps-Zugangsdaten oder SSH-Schlüsselpaare. Eine Reihe weiterer Maßnahmen, von regelmäßigen Red-Team-Übungen bis hin zu umfassendem Auditing und Reporting, tragen zusätzlich zur Cyber-Resilienz bei.

Netzwerk- und Mikrosegmentierung setzen richtlinienbasierte Zugangskontrollen zu einzelnen Segmenten durch.

Netzwerk- und Mikrosegmentierung

Die Segmentierung eines Netzwerks in kleinere, logische und sichere Einheiten kann den möglichen Impact, den ein kompromittierter Account verursachen kann, nachhaltig reduzieren. In einem Zero-Trust-Modell kommt der Netzwerk- und Mikrosegmentierung daher eine Schlüsselrolle zu, um richtlinienbasierte Zugangskontrollen zu einzelnen Segmenten durchzusetzen. Die Unterteilung schränkt den Datenverkehr zwischen verschiedenen Netzwerkbereichen ein und stellt – ganz im Sinne des Least-Privilege-Prinzips – sicher, dass Benutzer und Geräte stets nur auf die Ressourcen zugreifen können, die sie zur Erfüllung ihrer Aufgaben benötigen.

Die Mikrosegmentierung ermöglicht eine so feingranulare Zugriffskontrolle, dass Unternehmen den Zugriff auf einzelne Anwendungen oder Dienste auf der Grundlage der Identität, des Geräts, des Standorts und des Verhaltens des Benutzers einschränken können. Dies trägt zur Minimierung der Angriffsfläche und dem Risiko von lateralen Netzwerkbewegungen bei.

Umgesetzt wird die Netzwerk- und Mikrosegmentierung in der Regel mithilfe von Software-definierten Netzwerktechnologien (SDN), Next-Generation Firewalls (NGFWs) und Software-definierten Perimeter-Lösungen (SDP). Diese ermöglichen es den Unternehmen, dynamische Zugriffskontrollen auf der Grundlage von Richtlinien durchzusetzen und dabei auch kontextbezogene Faktoren zu berücksichtigen.

Access Policies und deren Enforcement

Wenn es gilt, die Zugriffe unterschiedlichster Identitäten und Identitätstypen auf weltweit verteilte, kritische Ressourcen zu regeln, bedarf es granularer, kontextbasierter Access Policies. Die Kombination aus der Geräte- oder Benutzeridentität und unterstützenden, kontextbezogenen Daten steuert den Entscheidungsprozess darüber, welche Identities Zugang zu Anwendungen und Segmentgruppen erhalten – und welcher Grad an Zugang und Berechtigung gewährt wird.

Vor der Erstellung der Zugriffsrichtlinien gilt es zunächst jedoch, klare Benutzergruppen zu definieren (z.B. Marketing, Sales, Kunden) und auf dieser Basis passende Arbeitsprofile zu erstellen. Anschließend sollte in enger Zusammenarbeit mit den Fachabteilungen festgelegt werden, welche Benutzergruppen den Zugriff auf welche Ressourcen benötigen.

Vor der erstmaligen Definition der Zugriffsrichtlinien sollten die Sicherheitsteams umfassend analysieren und dokumentieren, welche Rollen für ihre Benutzer und Teams wirklich benötigt werden, und welche Anwendungen diese jeweils benötigen. Darüber hinaus gilt es, die konkreten Anforderungen an den Datenschutz zu ermitteln und die Arbeitsprofile mit bestehenden Risikobewertungen – typischerweise auf Grundlage der Rolle einer Identität – abzugleichen. Dabei hat es sich bewährt, die Zugriffsrichtlinien zunächst eher weiter zu fassen und die Granularität im Laufe der Zeit zu erhöhen. Auf diese Weise minimieren Unternehmen den Aufwand für das Troubleshooting und notwendige Aktualisierungen in der Anfangsphase, die die Akzeptanz unter den Beschäftigten beeinträchtigen und zusätzlich die Arbeit für das Security-Team erhöhen würden.

Threat Intelligence

Threat Intelligence Techniken und Prozesse identifizieren Cyberbedrohungen und spüren Sicherheitslücken auf.

Der Begriff Threat Intelligence bezeichnet Techniken und Prozesse zur Identifizierung von Cyberbedrohungen. Dazu gehört sowohl die interne und externe Erfassung von Bedrohungsdaten als auch die Analyse dieser Daten vor dem Kontext der eigenen Infrastruktur, um sicherheitsfördernde Maßnahmen einleiten zu können. Ein Threat-Intelligence-Programm dient also dem Aufspüren eigener Sicherheitslücken, der Risikominimierung von Datenverlusten, der Etablierung robuster Richtlinien und Security-Maßnahmen sowie der Schaffung einer Wissensdatenbank, die organisationsübergreifend den Kampf gegen die organisierte Cyberkriminalität unterstützt.

Bei der Erfassung der Bedrohungsdaten sind Unternehmen gut beraten, eine möglichst breite Palette von Quellen einzubeziehen. Das Fundament liefern dabei in der Regel die Metadaten der internen Netzwerke und Security-Systeme. Darüber hinaus bieten zahlreiche kommerzielle Anbieter und Analysten sowie unabhängige Organisationen wie die MITRE Corporation heute Zugang zu ihren Datenbanken mit aktuellen Informationen zu Cyberangriffen.

Besonders wichtig: Auch die allgegenwärtigen Open-Source-Komponenten sind trotz ihrer aufmerksamen und agilen Community globaler Entwickler oft nicht zuverlässig vor Schwachstellen geschützt, wie nicht zuletzt der Log4Shell-Vorfall aus dem Jahr 2021 zeigte. Auch für diese Komponenten sind aber aktuelle Bedrohungsinformationen verfügbar, beispielsweise von Nonprofit-Organisationen wie der OWASP (Open Worldwide Application Security Project).

Security-Analyse und Monitoring

Weil ein erfolgreicher Security Breach nie gänzlich ausgeschlossen werden kann, kommen die Security-Teams heute nicht umhin, die eigenen Netzwerke durchgehend aufmerksam zu überwachen. Nur so lassen sich mögliche Threats schnellstmöglich identifizieren und stoppen, bevor sie echten Schaden anrichten können. Daher sollte auch jede Zero-Trust-Architektur eine dedizierte Analyse- und Monitoring-Lösung umfassen, die Daten aus multiplen Quellen erfasst und nach Korrelationen und Anomalien sucht. Auch hier kommt der Threat Intelligence externer Anbieter eine Schlüsselrolle zu, aber auch Echtzeitwarnungen von Endpoints, Alarmmeldungen interner Security-Systeme, Traffic-Analysen und Server-Protokolle sollten bei der Analyse berücksichtigt werden.

Die Analyse- und Monitoring-Lösung umfasst eine Reihe verschiedener Komponenten. Dazu gehört die **Verhaltensanalyse**, die die Verhaltensmuster von Benutzern, Anwendungen und Geräten analysiert, um Anomalien zu identifizieren: zum Beispiel könnte ein Mitarbeiter im Kundendienst, der außerhalb der Geschäftszeiten auf für seine Tätigkeiten nicht notwendige Systeme zugreifen möchte, auf einen kompromittierten Account hinweisen. Ein zweites wichtiges Tool ist die **Netzwerkanalyse** zur Visualisierung des gesamten Datenverkehrs, der durch das Netzwerk fließt. So lassen sich beispielsweise ungewöhnlich hohe Download-Datenraten identifizieren, die auf einen Informationsdiebstahl hinweisen könnten.

Auf relevante Bedrohungsinformationen sollte eine möglichst schnelle, im Idealfall automatisierte Reaktion erfolgen. Eine Zero-Trust-Infrastruktur erfordert dafür eine angemessene **Kommunikation zwischen Datenerfassung, Analyse-Tools und Response-Anwendungen.** Dies ermöglicht beispielsweise eine SOAR-Lösung (Security Orchestration, Automation and Response) oder eine SIEM-Anwendung (Security Information and Event Management). Ein weiteres wichtiges Analyseelement stellt die **Forensik** dar, die vergangene oder laufende Angriffe untersucht, um die verursachenden Schwachstellen ausfindig zu machen. Dies verhindert das Auftreten ähnlicher Vorfälle in der Zukunft.

4. Zwischenfazit

Agile und fortschrittliche Unternehmen benötigen flexible Netzwerk-Infrastrukturen, die dennoch sicher sind.

Das Zero-Trust-Modell und sein Leitspruch „Never trust, always verify" löst viele aktuelle Herausforderungen, die Unternehmen und Security-Verantwortliche derzeit beschäftigen. Obwohl Security Researcher und Analysten das Konzept bereits seit Jahrzehnten untersuchen und entwickeln, ist es erst in den letzten Jahren zum State-of-the-Art gereift – und gilt heute zurecht als Best-Practice in der IT-Sicherheit.

Viele der Ansätze und Prinzipien von Zero Trust brechen allerdings radikal mit den traditionellen Security-Modellen, was die Adaption spürbar verzögert hat. Erst die enormen gesellschaftlichen Veränderungen im Rahmen der globalen Pandemie, der geopolitischen Krisen und der stark zunehmenden Cyber-Bedrohungslage haben die Verantwortlichen zu einem nachhaltigen Umdenken gezwungen: Agile und fortschrittliche Unternehmen benötigen flexible Netzwerk-Infrastrukturen, die dennoch sicher sind – und kommen daher nicht um Zero Trust herum.

Die Security-Hersteller bieten heute unzählige Tools und Plattformen für verschiedenste Architektur-Ansätze. Unternehmen und Security-Teams haben also die Qual der Wahl – und sind damit nicht selten allein. Spezialisierte Beratungsunternehmen wie iC Consult unterstützen mit einer fachkundigen Bewertung der bestehenden Infrastruktur und einem herstellerunabhängigen Blick auf das umfassende Lösungsangebot, das der Security-Markt bietet.

Im zweiten Teil des Whitepapers erfahren interessierte Leser alles über die Optionen und Herausforderungen bei der Implementierung einer Zero-Trust-Lösung – und über die Möglichkeiten, die ihnen moderne Cloud- und Managed-Service-Modelle in diesem Umfeld bieten.

Im ersten Teil dieses Whitepapers haben Sie viel über die Geschichte, die Prinzipien und die Komponenten von Zero Trust erfahren. In diesem zweiten Teil geht es nun in die Praxis: Wir schildern die Herausforderungen bei der Planung, der Implementierung und dem Betrieb und gehen auf die Chancen und Fallstricke beim Outsourcing ein. Im

letzten Kapitel geben wir Ihnen schließlich noch einen Ausblick auf die Zukunft von Zero Trust.

Für eine erfolgreiche Implementierung von ZTNA sind richtige Weichenstellungen in der Entwurfs- und Planungsphase unerlässlich.

5. Implementierung von Zero Trust

Worauf Sie bei der Entwicklung und Planung eines Zero-Trust-Modells achten müssen: Die Einführung von Zero Trust Network Access (ZTNA) ist ein aufwendiges und komplexes Projekt. Es strahlt auf alle Bereiche Ihres Unternehmens aus und lässt sich dementsprechend nicht von heute auf morgen umsetzen. Mit Blick auf eine reibungslose und erfolgreiche Implementierung sind – wie so oft in der IT – vor allem die Weichenstellungen in der Entwurfs- und Planungsphase von entscheidender Bedeutung.

Die folgende Checkliste kann Ihnen dabei helfen:

Analysieren Sie sorgfältig Ihre Geschäftsprozesse
Untersuchen Sie vor dem Projektstart Ihre Geschäftsprozesse und identifizieren Sie die kritischen Assets und Daten, die besonders geschützt werden müssen – auch und besonders mit Blick auf die Cloud-Ressourcen Ihres Unternehmens. Dies hilft Ihnen, Ihre Abläufe an den Zero-Trust-Prinzipien auszurichten und ein angemessenes Schutzlevel für alle Assets zu bestimmen.

Erstellen Sie einen Kosten- und Ressourcenplan
Da die Umstellung auf ein Zero-Trust-Modell mit einem vergleichsweise hohen Zeit- und Kostenaufwand verbunden ist, sollten Sie darauf achten, die dafür eingesetzten Ressourcen auch effektiv zu nutzen. Ein detaillierter Plan, der die vorhandenen Ressourcen den zugehörigen Kosten gegenüberstellt, hilft Ihnen dabei, die Einhaltung der Zeit- und Kostenbudgets sicherzustellen.

Priorisieren Sie die geplanten Schutzmaßnahmen
Im Rahmen des Projekts werden Sie die Security-Architektur Ihres Unternehmens umfassend modernisieren – und in vielen Teilbereichen ganz neu denken müssen. Daher lohnt es sich, die konkreten Sicherheitsmaßnahmen detailliert zu priorisieren, und so zu planen, dass Ihre kritischen Systeme auch während der Umstellung jederzeit zuverlässig geschützt sind. Umgekehrt gilt es aber auch, sich auf die wichtigsten Bedrohungen zu konzentrieren und ein unkontrolliertes Ausufern der Security zu vermeiden. Ihr Security-Stack muss jederzeit kontrollierbar bleiben, um Sicherheitslücken durch zu hohe Komplexität oder fehlende Transparenz zu vermeiden. Behalten Sie jederzeit die Compliance-Anforderungen im Blick.

Der Umgang mit kritischen Daten – ob On-Premises oder in der Cloud – unterliegt heute zunehmend strengen gesetzlichen, branchenspezifischen und internen Regulierungen. Verschaffen Sie sich zum Start Ihres Zero-Trust-Projekts einen Überblick über alle Compliance-Anforderungen, die es zu berücksichtigen gilt. Dies wird unter Umständen zusätzliche Sicherheitsmaßnahmen erfordern, und auch dabei gilt es einen Weg zu finden, die Komplexität in Maßen zu halten.

Erstellen Sie eine detaillierte Access Control Policy
Die Access Control Policy ist die zentrale, unternehmensspezifische Richtlinie, die festlegt, welche Personen unter welchen Bedingungen auf welche Daten und Ressourcen zugreifen dürfen. Best Practice ist es dabei heute, die Berechtigungen

nach dem „Need-to-know"-Prinzip zu beschränken, sprich: Jedem Anwender nur die Zugriffsrechte zuzugestehen, die er bei seiner Arbeit auch wirklich benötigt. Dies erreichen Unternehmen am besten durch die Implementierung rollenbasierter und dynamischer Zugriffssteuerungen.

Definieren Sie Benutzer- und Geräteprofile
Um das Zero-Trust-Prinzip kontinuierlich umzusetzen, müssen Unternehmen verbindliche Profile für alle Benutzer und Geräte definieren, die auf das Unternehmensnetzwerk zugreifen werden, einschließlich derer, die remote arbeiten – und diese bei allen Zugriffsanfragen durchgehend validieren. Der Access Control Policy kommt dabei eine Schlüsselrolle zu, um verdächtige oder veraltete Nutzerprofile zu identifizieren. Auf diese Weise lässt sich sicherstellen, dass ausschließlich vertrauenswürdige Benutzer und Geräte auf die Ressourcen zugreifen können.

Schaffen Sie die Voraussetzungen für eine starke Netzwerksegmentierung
Mit einer robusten Netzwerk- oder Mikrosegmentierung verhindern Sie, dass kompromittierte Benutzer-Accounts oder Geräte lateral auf andere Teile Ihres Netzwerks zugreifen können – im Falle eines Angriffs eine wichtige Schutzmaßnahme. Wie, wann und in welchem Rahmen eine solche Netzwerksegmentierung erfolgen wird, sollten Sie bereits in der Planungsphase thematisieren.

Stellen Sie die Weichen für starke Multi-Faktor-Authentifizierung
Die klassische Kombination aus Passwort und Benutzerkennung reicht heute nicht mehr aus, um Benutzer und Geräte zuverlässig zu authentisieren – und ist auch mit Blick auf den Bedienkomfort und die hohen Kosten nicht länger zeitgemäß. Stellen Sie daher vom ersten Tag an die Weichen für eine moderne Multi-Faktor-Authentifizierung, und machen Sie sich rechtzeitig Gedanken über geeignete (und von den Anwendern akzeptierte!) Identifikationsmethoden, von biometrischen Faktoren bis hin zu Token- und Push-App-Verfahren.

Stellen Sie Ihren Technologie-Stack auf den Prüfstand
Die Implementierung von Zero Trust erfordert ein reibungsloses Zusammenspiel unterschiedlichster, hochkomplexer Technologien: von IAM-Systemen über Monitoring-Tools und Access-Control-Plattformen bis hin zu IGA-Lösungen. Analysieren Sie deshalb frühzeitig, wie es um die Interoperabilität Ihrer vorhandenen Systeme bestellt ist, welche Legacy-Systeme abgelöst werden müssen und wo Bedarf nach neuen Lösungen besteht.

Planen Sie Schulungs- und Awareness-Maßnahmen
Bevor die neue Lösung live geht, müssen Ihre Mitarbeitenden die Bedeutung und den Mehrwert von Zero Trust kennen – und auch wissen, vor welchen Bedrohungen und Risiken sie die neue Architektur schützen wird. Führen Sie daher rechtzeitig vor dem Roll-out geeignete Schulungs- und Awareness-Maßnahmen durch, in denen Sie die verschiedenen Rollen gezielt informieren – wahlweise in Eigenregie oder mit Unterstützung externer Experten.

Integrieren Sie ein durchgängiges Monitoring
Um Ihr Unternehmen zuverlässig zu schützen, müssen Sie durchgehend über neue Bedrohungen und ungewöhnliche Aktivitäten in Ihrer IT-Umgebung auf dem Laufenden bleiben. Dafür können Sie wahlweise selbst geeignete Monitoring-Tools implementieren oder externe Provider hinzuziehen – wobei die meisten Unternehmen heute mit Blick auf die notwendige 24/7-Abdeckung das Outsourcing favorisieren.

Denken Sie schon heute an morgen!
Entwickeln Sie für Ihre Zero-Trust-Umgebung schon jetzt ein verbindliches Validierungs- und Aktualisierungsmodell, das turnusmäßige Überprüfungen der Funktionalitäten, der Skalierung und der Bedürfnisse vorsieht. So stellen Sie sicher, dass Ihre Systeme jederzeit auf dem neuesten Stand sind, neue Anforderungen zeitnah umgesetzt werden und alle Systeme einwandfrei funktionieren – kurz: dass Ihre Architektur mit der Zeit geht.

Die Planung- und Entwurfsphase ist für den Erfolg Ihres Zero-Trust-Projekts von zentraler Bedeutung – Sie sollten sich also nicht scheuen, bereits in dieser frühen Phase externe Unterstützung hinzuzuziehen. Je nachdem, wo Sie Entlastung wünschen und wie Ihre konkreten Anforderungen aussehen, stehen Ihnen die Experten von iC Consult gerne mit maßgeschneiderten Consulting, Professional und Managed Services zur Seite.

Build or Buy?

Vor der eigentlichen Implementierung gilt es noch eine weitere, zentrale Frage zu beantworten: Verfügt Ihr Unternehmen über die internen Ressourcen und das Know-how, ein so komplexes und umfangreiches Projekt eigenverantwortlich anzugehen und seine Zero-Trust-Umgebung vollständig in Eigenregie zu entwickeln? Oder sind Sie besser beraten, eine bestehende Best-of-Breed-Lösung auszuwählen – und diese dann als Cloud-basierten Service über einen externen Experten bereitstellen zu lassen?

In der Praxis sprechen für beide Ansätze gute Gründe, und es ist nicht immer leicht zu beantworten, welcher Weg für ein Unternehmen der Richtige ist. Im Folgenden fassen wir für Sie die wichtigsten Argumente zusammen, die Sie bei der Entscheidungsfindung bedenken sollten.

Eine selbst entwickelte Zero-Trust-Lösung garantiert einen hohen Individualisierungsgrad.

Für die eigenverantwortliche Entwicklung spricht in erster Linie der hohe Individualisierungsgrad, der mit einem solchen Ansatz realisiert werden kann: Wer seine Zero Trust-Lösung von Grund auf selbst entwickelt, kann auch sicherstellen, dass sie optimal an seine spezifischen Anforderungen und Bedürfnisse angepasst ist. Anders als bei schlüsselfertigen Services, bei denen mitunter die Hersteller oder Betreiber der Lösung die Weichen stellen, entscheidet das Unternehmen bei einer eigenentwickelten Lösung selbst, welche Komponenten es implementieren will und wie diese zu einem leistungsfähigen Ganzen kombiniert werden sollen. Gerade für KRITIS-Unternehmen mit besonders hohen Sicherheitsanforderungen – etwa in der Rüstungsindustrie – ist das ein wichtiger Aspekt.

Lückenlose Kontrolle und Flexibilität
Hinzu kommt, dass Unternehmen mit einer eigenen Zero-Trust-Lösung jederzeit die volle Kontrolle über die Implementierung und den Betrieb behalten. Dies macht es in der Praxis oft etwas einfacher, die Einhaltung regulatorischer Vorgaben sicherzustellen. Und: Das tiefe Verständnis für die selbst entwickelte Lösung hilft dabei, schnell und flexibel auf neue Bedrohungen und Anforderungen zu reagieren und die Lösung nach Bedarf selbst anzupassen.

Einsparpotenziale bei den laufenden Kosten
Und schließlich: Viele Unternehmen, die sich für die Entwicklung einer eigenen Lösung entscheiden, berichten, sie hätten auf diese Weise nachhaltige Einsparungen bei

den laufenden Kosten erzielt. Dieses Argument ist unter Experten allerdings nicht unumstritten: Erstens, weil dieser Weg überhaupt nur gangbar ist, wenn intern das entsprechende Knowhow und die passende Infrastruktur vorhanden ist. Und zweitens, weil die angeführten Einsparungen bei den OpEx mit deutlich höheren CapEx in der Frühphase des Projekts erkauft werden.

Umgekehrt sprechen aber auch viele Gründe für die Wahl eines As-a-Service-Modells:

Etablierte ZTNA-Service-Provider garantieren wertvolles Experten-Knowhow.

Externes Expertenwissen
Der für viele Unternehmen wichtigste Grund, das Thema Zero Trust auszulagern, dürfte der Zugang zu wertvollem Experten-Knowhow sein: Immerhin verfügen etablierte ZTNA-Service-Provider über jahrelange Erfahrung bei der Implementierung passgenauer Zero-Trust-Lösungen und sind mit den Märkten, Komponenten und Technologien bestens vertraut. Darüber hinaus bringen solche Experten tiefes Know-how im Bereich Compliance mit – und das über alle Branchen und Regionen hinweg. Mit diesen erfahrenen Partnern an ihrer Seite können Unternehmen fundiert alle wichtigen Weichen stellen, ohne in entsprechende interne Ressourcen zu investieren.

Flankierende Services für eine nachhaltige Entlastung
Hinzu kommt, dass die Service-Provider ihre Kunden nicht nur bei der Auswahl und der Implementierung ihrer ZTNA-Lösung unterstützen, sondern ihnen darüber hinaus mit umfangreichen Services zur Seite stehen: zum Beispiel bei der 24/7-Überwachung und Wartung der Systeme, die gewährleisten, dass der implementierte Technologie-Stack stets auf dem neusten Stand ist, oder indem sie das Team des Kunden mit Schulungen und Informationsmaterial auf die Einführung von Zero Trust vorbereiten.

Grenzenlose Skalierbarkeit
Und auch mit Blick auf einen agilen Geschäftsbetrieb bieten Managed Services wichtige Vorteile: Aufsetzend auf innovative Cloud-Technologien können die Service-Provider in der Regel sehr schnell und einfach auf neue Geschäftsanforderungen ihrer Kunden reagieren. Dies ist insbesondere mit Blick auf die Skalierbarkeit der Umgebung wichtig: Ganz egal, ob das Unternehmen wächst oder ob es den Funktionsumfang seiner Lösung erweitern oder ganz neu definieren möchte: Mit dem richtigen Service-Provider an seiner Seite können jederzeit neue Lizenzen oder Ressourcen bereitgestellt oder neue Funktionen integriert werden, ohne, dass der Kunde seine Umgebung anpassen müsste.

Attraktive OpEx statt hoher CapEx
Wie bereits angesprochen geht die eigenverantwortliche Entwicklung einer ZTNA-Umgebung mit hohen Einmalinvestitionen einher – sowohl mit Blick auf das erforderliche Equipment als auch mit Blick auf die Zeit- und Personalressourcen. Bei einem As-a-Service-Modell lassen sich all diese Investitionen vermeiden und in transparente monatliche Raten überführen. Hinzu kommt, dass durch die Zusammenarbeit mit erfahrenen Experten auch teure Fehlentwicklungen und gefährliche Sicherheitslücken ausgeschlossen sind – und die Skaleneffekte der Cloud voll greifen.

Schneller zum Ziel
Und auch mit Blick auf die immer kürzeren Innovationszyklen haben sich As-a-Service-Modelle bewährt: Wird die Zero-Trust-Architektur von einem etablierten Service-Provider bereitgestellt, sparen Unternehmen viel Zeit, die für die Planung, Implementierung, Wartung und Verwaltung der eigenen Lösung erforderlich wäre. Dies erlaubt es ihnen, sich schnell wieder auf ihre Kernkompetenzen zu konzentrieren und den Fokus auf eigene Innovationsprojekte zu richten.

Sie sehen: Auch wenn viele gute Gründe für die Einführung einer eigenentwickelten ZTNA-Umgebung sprechen, profitieren in der Praxis die meisten Unternehmen davon, frühzeitig externe Experten hinzuzuziehen. Dabei können diese im Sinne eines Outsourcings das Gesamtprojekt – von der Planung über die Implementierung bis hin zum Betrieb – übernehmen oder im Rahmen eines individuellen Out-Taskings in einzelnen Projektphasen unterstützen und lediglich für bestimmte Komponenten verantwortlich zeichnen.

Grundsätzlich gilt aber: Mit vereinten Kräften lassen sich die Aufgabenstellungen bei der Implementierung in der Regel besser meistern.

Best Practices für die Zero-Trust-Einführung

So unterschiedlich, wie die Einführung von Zero Trust von Unternehmen zu Unternehmen erfolgt, gibt es keine allgemeingültige Formel, die den Erfolg des Projekts garantieren würde: Jedes Unternehmen startet mit individuellen Anforderungen in die Zero-Trust-Einführung, und jedes Unternehmen muss bei der Integration andere Hindernisse überwinden.

Es gibt aber eine Reihe bewährter Frameworks, die sich mit überschaubaren Anpassungen für zahlreiche Unternehmen adaptieren lassen und ihnen die Integration erleichtern. iC Consult hat beispielsweise einen eingängigen Schritt-für-Schritt-Leitfaden entwickelt, der die Umsetzung von Zero-Trust-Modellen nachhaltig erleichtert – und den wir seit vielen Jahren optimieren und erfolgreich bei eigenen Projekten nutzen.

Planung

- Kickoff-Meeting
- Planungs-Workshop
- Wöchentliche Meetings
- Projektplan-Monitoring

Die **Planungsphase** dient vorrangig dazu, den Leistungsumfang Ihres Zero-Trust-Projekts auszuloten. Eine zentrale Rolle spielen dabei die erforderlichen Security-Standards und Compliance-Vorgaben, denen die Zero-Trust-Lösung gerecht werden muss. Gleichzeitig verschafft sich Ihr Unternehmen in dieser Phase einen umfassenden Überblick über die bestehende Infrastruktur und entwickelt erste To-Dos für das Projektteam. Vor der eigentlichen Planung sollte zudem ein dedizierter Planungsworkshop mit einem Kickoff-Meeting stehen. Anschließend werden alle Beteiligten im Zuge wöchentlicher Meetings über den aktuellen Stand informiert.

Design

- Technische Workshops
- Anwendungs-Workshops
- Design-Workshops

In der anschließenden **Designphase** gilt es, die Zero-Trust-Lösung passgenau auf die Anforderungen, die Architektur und die Anwendungslandschaft des Unternehmens zuzuschneiden. So entsteht ein erster Designentwurf, der in enger Abstimmung aller Projektbeteiligten weiterentwickelt wird. Wird das Management der Identitäten an einen Zero-Trust-Provider ausgelagert, sollte dieser auch das Design übernehmen, um die am besten geeigneten Technologien auszuwählen.

Implementierung

- Setup & Testing
- Integrationen
- Erster Benutzerimport

Sind die ersten beiden Projektphasen abgeschlossen, steht die **Implementierung** der Zero-Trust-Lösung in der bestehenden Infrastruktur an. Nach einem ersten Setup und einer ersten Testphase werden sukzessive alle erforderlichen Konnektoren und Anwendungen integriert und die bestehenden Benutzer importiert. Auch hier können externe Dienstleister dem Unternehmen tatkräftig zur Seite stehen und bei Bedarf sogar die gesamte Implementierung übernehmen.

Deployment

- Support, Terminierung & Koordinierung
- Testverfahren
- Post Go-Live Support

Die **Deployment-Phase** ist zunächst in aller Regel von weiteren Testreihen geprägt, um sicherzustellen, dass die integrierte Lösung für den alltäglichen Betrieb fit ist. Ist

Betrieb

- Support & Instandhaltung
- Entwicklungserweiterungen
- Service Delivery Manager
- Zertifizierte Okta Administratoren

ein externer Experte involviert, steht dieser dem internen Projektteam zur Seite, um einen reibungslosen Ablauf bei der Bereitstellung zu gewährleisten.

Nach der Überführung der Lösung in den **Echtbetrieb** kommt dem Projektteam die Aufgabe zu, den stabilen und sicheren Betrieb zu überwachen und weiter zu optimieren. Hierzu gehört es beispielsweise auch, für die Zero-Trust-Lösung automatische Patch- und Update-Prozesse zu definieren, um sicherzustellen, dass das System stets auf dem neusten Stand ist. Sind externe Zero-Trust-Anbieter involviert, ist jetzt die Zeit, um die Kommunikation mit deren Ansprechpartnern auf den Prüfstand zu stellen und zu verbessern und gegebenenfalls proaktive Wartungsabläufe mit automatisiertem Service-Monitoring zu definieren. Zu diesem Zeitpunkt sollte für das Unternehmen auch ein dedizierter Service Delivery Manager benannt werden, der bestenfalls bereits im Entwicklungsprozess eingebunden war – und der dem Inhouse-Team nun beratend zur Seite steht.

Zero-Trust-as-a-Service (ZTaaS)

Hohes Knowhow rund um Zero Trust

Kurze Reaktionszeiten durch etablierte und standardisierte Prozesse

Schlüsselfertige Integrationen reduzieren den Ressourcenaufwand und entlasten das Team

Zero-Trust-as-a-Service – ist das eine Option?

Von Zero-Trust-as-a-Service (ZTaaS) sprechen wir, wenn ein Service-Provider die gesamte Planung, Implementierung und Verwaltung der Zero-Trust-Infrastruktur für ein Unternehmen übernimmt. Auf diese Weise profitieren Unternehmen ganz ohne eigenes Investment vom starken Schutz und allen anderen Vorteilen von Zero Trust.

ZTaaS-Dienstleister bringen umfassendes **hohes Knowhow** rund um Zero Trust mit: Sie verfügen über breite Marktkenntnis und Expertise und kennen die Lösungen aller führenden Hersteller mit ihren individuellen Vor- und Nachteilen. Auf diese Weise können sie fundiert bei der Auswahl beraten, die Kompatibilität mit Bestandssystemen einschätzen und ganzheitliche Lösungen entwickeln. Die Praxiserfahrung und die eingespielten Teams garantieren einen schnellen Go-Live und eine effiziente Administration.

Service-Provider verfügen über **etablierte und standardisierte Prozesse.** Das beschleunigt den Ablauf der Projekte – von der Planung und Moderation über die Implementierung und Verwaltung bis zur Integration neuer Anwendungen – und stellt kurze **Reaktionszeiten** bei Cyberangriffen und Ausfällen sicher.

Externe Dienstleister bieten ein breites Portfolio **schlüsselfertiger Integrationen.** Dies reduziert die Komplexität des Projekts, minimiert den Ressourcenaufwand und verkürzt die Time-to-Market der Anwendungen. Das entlastet das interne Team und schafft wertvolle Zeiträume für Innovationen.

Die Entscheidung für einen Managed Service hat auch handfeste wirtschaftliche Vorteile: CapEx wird zu OpEx. Hohe Einmal-Investitionen werden in überschaubare monatliche Betriebsausgaben überführt. Unternehmen schonen so ihr Eigenkapital, schaffen Freiräume für weiter Investitionen, senken die TCO und stellen die Weichen für einen schnellen Return-on-Investment.

8 Fragen, um die Scope Ihres ZTNA-Projekts zu definieren

Wollen Sie das Thema ZTNA demnächst angehen – tun sich aber noch schwer damit, den Projektumfang klar zu definieren? Dann beantworten Sie im nächsten Planungsmeeting zusammen mit Ihrem Team die folgenden Fragen:

1. Welche Art von Daten und Ressourcen müssen wir schützen, und welchen konkreten Risiken sind diese ausgesetzt?
2. Wie ist die IT-Infrastruktur unserer Organisation aufgebaut, und wie können darin die Zero-Trust-Prinzipien am besten implementiert werden?
3. Welchen Compliance-Anforderungen müssen wir Rechnung tragen? Wie kann uns ein Zero-Trust-Modell dabei helfen?
4. Welche Ressourcen stehen uns für die Implementierung und das Management der Zero-Trust-Umgebung zur Verfügung?
5. Wie gut ist das interne Security-Knowhow? Welche Skills sind bei uns intern vorhanden, und wo benötigen wir Unterstützung von externen Experten?
6. Wie stellen wir die Akzeptanz für das Zero-Trust-Modell sicher, und welche Schulungs- und Sensibilisierungsmaßnahmen sind notwendig?
7. Wie können wir den Erfolg des Zero-Trust-Modells messen? Welche Metriken werden zur Bewertung verwendet?
8. Wie stellen wir die kontinuierliche Weiterentwicklung des Zero-Trust-Modells sicher? Wer ist dafür verantwortlich?

Auch wenn am Ende noch einige Fragen offen sein sollten, legen Sie mir dieser Checkliste einen soliden Grundstein, um das Projekt Zero Trust anzugehen – und gegebenenfalls nach einem passenden Partner zu suchen. Für die ersten Sondierungsgespräche sind Sie auf jeden Fall bestens gerüstet.

6. Outsourcing von Zero Trust

Die hohe Komplexität und Integrationstiefe moderner Zero-Trust-Umgebungen ist nicht zu unterschätzen – immerhin gilt es, multiple Access Gateways, Authentifizierungsserver, Policy-Engines und Network-Security-Systeme passgenau zu integrieren und zu einem leistungsfähigen Ganzen zusammenzuführen. Schon das verlangt ein tiefes technisches Verständnis für die Cybersecurity. Erschwerend kommt hinzu, dass die Interoperabilität der Komponenten auch in einem hoch dynamischen Umfeld funktionieren muss. Die Zero-Trust-Lösung erfordert also eine kontinuierliche Pflege, Aktualisierung und Skalierung, um mit steigenden Anforderungen des Unternehmens und dynamischen Threat-Landschaften Schritt zu halten.

Viele Unternehmen tun sich erfahrungsgemäß schwer damit, all dies mit Bordmitteln zu leisten. Angesichts von Fachkräftemangel, fehlendem Knowhow und knappen Ressourcen ist daher in den meisten Szenarien das Hinzuziehen externer Experten sinnvoll. Je nach Anforderungen und Bedarf unterstützen sie mit Consulting Diensten, mit Professional Services oder mit Managed-Zero-Trust-Angeboten.

Im Folgenden werden wir uns alle drei Service-Ansätze genauer ansehen. Bevor wir das tun, haben wir aber noch einige Empfehlungen, die Ihnen auf der Suche nach dem richtigen Partner helfen sollen.

Folgende Aspekte sollte ein Zero-Trust-Partner abdecken:

- **Herstellerunabhängigkeit**
- **Kontinuierliche Optimierung**
- **Agilität und Skalierbarkeit**

Wie Sie den richtigen Partner für Ihr Zero-Trust-Projekt finden

Schon eine schnelle Internetsuche offenbart, dass im Security-Markt derzeit kein Mangel an selbsternannten Zero-Trust-Experten herrscht. Allein in Deutschland wetteifern heute hunderte von Systemintegratoren, Beratern und MSSPs um die Gunst der Unternehmen, und sie alle nehmen für sich in Anspruch, Ihr Unternehmen professionell und kompetent zu unterstützen und nachhaltig zu entlasten. Wie aber finden Sie in diesem breiten Angebot den Partner, der perfekt zu Ihrem Zero-Trust-Projekt passt?

Auch wenn es sehr viele Faktoren gibt, die in Ihre Entscheidung einfließen werden, empfehlen wir Ihnen, vor allem auf drei Aspekte zu achten:

Der erste, und vielleicht wichtigste Punkt ist, dass Ihr Zero-Trust-Partner **herstellerunabhängig** agieren sollte. Schließlich muss Ihre neue Zero-Trust-Lösung passgenau auf die Anforderungen und Bedürfnisse Ihres Unternehmens zugeschnitten sein. Und weil nicht jeder Hersteller jedes Feature und Funktionalität unterstützt, werden naturgemäß nicht alle Hersteller für Sie in Frage kommen. Daher ist es von entscheidender Bedeutung, dass Ihr Zero-Trust-Partner Ihnen auch wirklich die gesamte Bandbreite verfügbarer Lösungen vorstellt, und nicht versucht, Sie gezielt in eine Richtung zu drängen. Berater und Integratoren wie iC Consult agieren Technologie- und Anbieter-unabhängig – und können Sie unvoreingenommen bei der Zusammenstellung der perfekten Lösung unterstützen.

Das zweite Kriterium ist es, einen ZTNA-Partner zu suchen, der den Fokus nicht ausschließlich auf den Betrieb der Zero-Trust-Lösung legt – sondern auch die **kontinuierliche Optimierung des Technologie-Stacks** im Blick behält. So bleibt die Zero-Trust-Lösung durchgehend auf der Höhe der Zeit. Achten Sie insbesondere beim Abschluss von Managed-Services-Verträgen darauf, dass diese eine agile und kontinuierliche Weiterentwicklung der Zero-Trust-Architektur umfassen.

Und schließlich: Moderne Zero-Trust-Lösungen müssen sich immer schneller und häufiger an neue Anforderungen anpassen – und dem internen Team die Möglichkeit bieten, schnell auf Probleme zu reagieren. Achten Sie bei der Wahl eines Zero-Trust-Providers deshalb darauf, dass er zu den Vorreitern im Markt gehört, und **agile und skalierbare Ansätze** wie Self-Services, Accelerators und Factory Patterns in den Fokus rückt. So bleiben Sie dauerhaft wettbewerbsfähig.

Consulting Services

Consulting Services kommen bei Zero-Trust-Projekten vor allem in der Planungs- und Designphase zum Tragen. Aber auch bei der Implementierung und bei der Optimierung vorhandener Zero-Trust-Strategien können erfahrene Berater Ihrem Unternehmen eine wertvolle Hilfe sein.

Die wichtigsten Consulting Services im Zero Trust im Überblick:

Consulting-Anbieter können Unternehmen mit individueller **Strategie- und Architekturberatung** bei der grundlegenden Planung der Zero-Trust-Strategie unterstützen. Dies umfasst in der Regel die Bewertung der aktuellen Infrastruktur, der Identifizierung von Schwachstellen und die Entwicklung einer Roadmap für die Migration auf eine Zero-Trust-Umgebung.

Bei der **Risiko- und Sicherheitsbewertung** führen die Consultants eine detaillierte Analyse durch, um bestehende Sicherheitslücken und Bedrohungen im Unternehmen zu identifizieren. Basierend auf diesen Erkenntnissen sprechen sie anschließend konkrete Empfehlungen zur Stärkung der IT-Security aus und stellen Best Practices für die Umsetzung von Zero Trust vor.

Bei der **Compliance-Beratung** steht die Entwicklung geeigneter Maßnahmen zur Einhaltung geltender regulatorischer Anforderungen im Fokus. Die Berater analysieren dafür zunächst die gesetzlichen, branchenspezifischen und internen Vorgaben, denen das Unternehmen gerecht werden muss (etwa in Bezug auf Datenschutz- und Sicherheitsstandards). Anschließend richten sie die Zero-Trust-Strategie gemeinsam mit dem internen Team an den Vorgaben aus und definieren geeignete Kontrollen und Überwachungsmaßnahmen.

Nahezu alle Consulting-Anbieter bieten **Schulungen und Sensibilisierungsmaßnahmen** für Mitarbeiter an. Auf diese Weise schärfen sie vom ersten Tag an das Bewusstsein für die Zero-Trust-Prinzipien und vermitteln konkrete Security-Best-Practices. Darüber hinaus haben sich spezielle Workshops für Abteilungen bewährt, die von den Zero-Trust-Maßnahmen besonders betroffen sind, etwa die Personalabteilung. Und auch wenn sich die Bedrohungslage verändert und neue Angriffsstrategien bekannt werden, nehmen dies viele Unternehmen zum Anlass für regelmäßige Schulungen.

Consulting-Dienste von iC Consult

iC Consult bietet Unternehmen ein breites Portfolio von Consulting-Services in zwei Kategorien:

1. Business- und Prozess-Beratung
iC Consult unterstützt Unternehmen als Enabler und Gestalter bei der Definition der ZTNA-Strategie. Unsere Consultants verfügen über tiefe Expertise entlang der gesamten Wertschöpfungskette und beraten bei der Konzeption und Umsetzung entsprechender Strategien. Die Beratung erfolgt dabei herstellerunabhängig – und fokussiert sich darauf, Unternehmen einen umfassenden Blick auf ihre Prozesse zu geben und darauf aufsetzend passgenaue Lösungen zu entwickeln. Diese Consulting-Dienste erbringt iC Consult auf Unternehmenswunsch auch vor Ort – das garantiert kurze Abstimmungswege und ermöglicht schnelle Reaktionen auf neue Anforderungen.

2. Technology Advisory
Bei der Entwicklung der ZTNA-Strategie spielt die Auswahl der passenden Technologien eine wichtige Rolle. Als herstellerunabhängiger Systemintegrator, der mit über 30 führenden Security-Anbietern zusammenarbeitet, kann iC Consult in diesem Bereich exakt auf die individuellen Anforderungen jedes Unternehmens eingehen – und ohne Scheuklappen bei der Auswahl und Integration einer passenden Lösung unterstützen.

Professional Services

Im Rahmen von Professional Services unterstützen externe Experten Ihr Unternehmen von der Planung über die Implementierung bis hin zum Betrieb und zur Verwaltung ihrer Zero-Trust-Lösung. Die Palette von Dienstleistungen, die unter diesem Begriff subsummiert werden, ist breit – grundsätzlich lassen sich aber vier Schwerpunkte bestimmen:

Die **Implementierungsdienste** fokussieren auf die Unterstützung bei der Integration einer Zero-Trust-Infrastruktur. Hierzu gehören die Implementierung und die Einrichtung der benötigten Security-Technologien, die Einrichtung von Zugriffsrichtlinien sowie die Durchführung und Validierung von Tests. Auch die nahtlose Verzahnung mit vorhanden Systemen, Netzwerk-Devices und anderen Sicherheitskomponenten fällt in diese Kategorie.

Professional Services im Bereich **Konfiguration und Anpassung** helfen Unternehmen bei der individuellen Einrichtung ihrer Zero-Trust-Lösung und stellen sicher, dass die neue Umgebung den spezifischen Anforderungen und Geschäftsprozessen entspricht. Zu den Services in dieser Kategorie gehört etwa die Feinabstimmung von Zugriffsrichtlinien, die genaue Definition von Benutzerrollen und die Anpassung der Benutzeroberflächen und Dashboards für mehr Transparenz.

Professional Services im Bereich **Performance-Optimierung** sollen den Unternehmen dabei helfen, das Potenzial ihrer neuen ZTNA-Architektur voll zu erschließen. Dies beinhaltet die Überprüfung der Netzwerktopologie, die Analyse von Durchsatzraten und das Monitoring der Latenzzeiten. Auf diese Weise können Engpässe oder Flaschenhälse identifiziert und proaktiv behoben werden, um eine reibungslose und effiziente Bereitstellung sicherzustellen.

Im Zuge von **Migrations- und Upgrade-Services** unterstützen die Dienstleister Ihr Unternehmen bei der Modernisierung oder der Zusammenführung bestehender Security-Lösungen und Datenbanken. Diese umfassen die Bewertung der Bestandssysteme sowie die Planung und Umsetzung des Projekts. Verbindliche Upgrade-Services stellen sicher, dass Ihre Zero Trust-Lösung jederzeit auf dem neuesten technologischen Stand bleibt und stabil läuft.

Professional Services von iC Consult

Bei den Professional Services von iC Consult stehen drei Schwerpunkte im Fokus, die alle Projektphasen vom Kickoff bis zum Betrieb der Zero-Trust-Lösung abdecken:

1. Architecture & Design
Aufsetzend auf maßgeschneiderte und agile Lösungen unterstützt iC Consult Ihr Unternehmen bei der Entwicklung von Architekturen und Designs, die Ihre konkreten Anforderungen bis ins Detail abbilden. Dabei profitieren Sie von unserer langjährigen Erfahrung aus Hunderten von ZTNA-Projekten und unserer umfassenden Kenntnis der führenden ZTNA-Produkte auf dem Markt.

2. Implementation & Integration
iC Consult setzt bei der Implementierung und Integration von ZTNA-Architekturen auf bewährte Methoden aus der agilen Software-Entwicklung – und verbindet diese mit langjähriger Praxiserfahrung. So entstehen ganzheitliche und innovative Lösungen, die sich nahtlos in bestehende Architekturen eingliedern und kontinuierlich mitwachsen.

3. Support & Operations
Im Anschluss an die Implementierung unterstützt iC Consult Ihr Unternehmen im laufenden Betrieb mit kompetentem 3rd-Level-Support und steht Ihnen auch bei der Weiterentwicklung der ZTNA-Services zur Seite. Etablierte Methoden, professionelle DevOps-Abläufe und zertifizierte ITIL-Prozesse stellen die Weichen für standardisierte Support-Services, die höchsten Ansprüchen gerecht werden.

Managed Services

Im Rahmen von Managed Zero Trust Services können Unternehmen die Integration, Verwaltung und Überwachung ihrer Zero-Trust-Architekturen vollständig an spezialisierte Managed Security Services Provider (MSSP) auslagern. In diesem Szenario übernimmt der MSSP die gesamte Verantwortung für den Betrieb der Zero-Trust-Lösung – und damit auch für den Schutz und die kontinuierliche Pflege der Komponenten. Typischerweise umfassen Managed Zero Trust Services die folgenden Dienste:

Managed Security Services (MSS) fokussieren sich auf die Absicherung, Überwachung und Verwaltung der Zero-Trust-Infrastruktur. Hierzu gehört beispielsweise die Überwachung des Netzwerkverkehrs, die Analyse von Bedrohungen und Anomalien, das Management von Zugriffsrichtlinien und Incident Response im Falle eines Angriffs. Im Rahmen von Identity and Access Management as a Services (IAMaaS) stellen die Provider individuelle Services rund um das Handling von Identitäten und Zugriffsrechten bereit. Der Anbieter übernimmt dabei die Technologieauswahl, die Verwaltung und Pflege der Identitäten, das Management der Zugriffsrechte und Policies und die Durchsetzung der Zero-Trust-Prinzipien.

Managed SASE Services führen eine Reihe wichtiger Security- und Netzwerkfunktionen in einer integrierten, Cloud-basierten Plattform am Secure Service Edge zusammen. Auf diese Weise können Unternehmen über einen zentralisierten Cloud-Service auf alle wichtigen Zero-Trust-Funktionalitäten zugreifen – und diese jederzeit flexibel anpassen und bedarfsgerecht skalieren.

Bei sogenannten **Incident Response as a Service** Angeboten beauftragen Unternehmen ihren MSSP mit der Erkennung und Behebung von Sicherheitsvorfällen in der Zero-Trust-Umgebung. Die Services reichen dabei von der Überwachung und Analyse von Security-Events über die forensische Analyse bis hin zur Einleitung von Sofortmaßnahmen zur Eindämmung von Bedrohungen.

Managed Services von iC Consult

Als der weltweit führende Anbieter von Managed Services und Consulting-Dienstleistungen im Bereich Identity & Access Management bieten wir weltweit verfügbare Managed IAM Services, die Ihr Unternehmen beim sicheren Betrieb Ihrer ZTNA-Umgebung unterstützen. Aufsetzend auf Best-of-Breed-Lösungen führender Anbieter bieten die Services ein Höchstmaß an Flexibilität und unzählige Individualisierungsoptionen – eine spannende Alternative zu tradierten und aufwendigen On-Premises-Installationen.

Die Services sind in zwei Varianten verfügbar:

1. IAM Cloud Ops
Mit diesem Fully-Managed-Service-Angebot profitieren Unternehmen vom ersten Tag an von den Vorzügen einer ganzheitlichen IAM-Plattform, ohne in eine eigene IAM-Architektur investieren zu müssen. Die Planung und Einführung übernehmen dabei die Experten von iC Consult – so kommen die Lizenzen, die Architektur und die Implementierung komfortabel aus einer Hand. Ein dedizierter Service Delivery Manager und ein rund um die Uhr erreichbares Support-Team stellen eine hochwertige Betreuung sicher und sorgen dafür, dass Ihr Unternehmen frühzeitig von neuen Funktionalitäten profitiert.

2. IAM Cloud Ops Advanced
Für besonders anspruchsvolle Umgebungen bietet iC Consult eine Service-Plattform, die deutlich über klassische IDaaS-Angebote hinausgeht. Die All-in-One-Plattform basiert auf den marktführenden Lösungen von ForgeRock und Ping Identity und ist durch den Einsatz von DevOps, IaC und Configuration-as-Code für einen weitgehend automatisierten Betrieb optimiert. Das macht es Ihnen leicht, Ihre Services hochgradig individuell aufzusetzen – und sie weltweit flexibel in Public, Private oder Hybrid Clouds einzubinden.

Was macht die Managed Services von iC Consult besonders

End-to-End Scope: Unsere IAM Managed Services gehen über die traditionelle Implementierung und den Betrieb hinaus und umfassen auch Beratungsfunktionen. Wir bieten ganzheitliche Unterstützung für Ihr gesamtes Identitätsprogramm und gewährleisten eine umfassende Lösung für alle Ihre IAM-Anforderungen.

Exzellenz: Bei iC Consult leben wir #IAMExcellence. Unser großes Team von IAM-Experten liefert durchweg hochmoderne und qualitativ hochwertige Dienstleistungen. Mit einer beeindruckenden Erfolgsbilanz in verschiedenen Branchen, Unternehmensgrößen und -umfängen sind wir darauf spezialisiert, individuelle Probleme und komplexe Anwendungsfälle zu lösen.

Flexibilität: Wir passen uns Ihren Bedürfnissen an und bieten Ihnen die ultimative Flexibilität, um Ihr Unternehmen zu vergrößern und gleichzeitig eine robuste IAM-Strategie aufrechtzuerhalten. Darüber hinaus bietet Ihnen unser Smart Managed Service Configurator die Flexibilität, Ihre IAM Managed Services an Ihre spezifischen Anforderungen anzupassen.

Auch komplexe ZTNA-Projekte lassen sich erfolgreich umsetzen.

Ganz egal, wie komplex und anspruchsvoll Ihr ZTNA-Projekt auch ist: Mit dem richtigen Mix aus Consulting, Professional und Managed Services können Sie heute nahezu jedes Szenario erfolgreich adressieren – und Ihr Inhouse-Team nachhaltig vom Betrieb der Security-Infrastruktur entlasten. Dabei wird es mitunter unvermeidlich sein, dass es bei einzelnen Services zu Überschneidungen kommt. Solange die internen Stakeholder und die externen Partner aber eng zusammenarbeiten, wird dies aber nicht etwa zu aufwändigen Mehrarbeiten führen – sondern kann im Gegenteil wertvolle Impulse für alle beteiligten Teams liefern.

7. Die Zukunft von Zero Trust

Hypes und Trends im Bereich Zero Trust
Trotz seiner langen Vorgeschichte ist Zero Trust ein junger Technologie-Ansatz, der dem schnellen Rhythmus von Veränderung und Wandel in der IT folgt – und dabei immer wieder durch neue Trends und Impulse beeinflusst wird. Wie sich Zero Trust in der Zukunft weiterentwickeln wird, ist daher schwer abzusehen, doch bei einigen Prognosen sind sich die Experten einig.

Ausblick 1: Zero Trust wird die Software- und DevOps-Prozesse verändern
Entwicklungsumgebungen können in besonderem Maße von ZTNA profitieren: Wenn der Zugriff auf Entwicklertools und IDEs nur noch nach den Prinzipien „Just-in-Time" und „Just-enough-Access" funktioniert, lässt sich das Risikopotenzial für kritische Informationen und Ressourcen nachhaltig minimieren. Integrierte Access-Management-Systeme überprüfen in diesem Szenario kontinuierlich die Zugriffe und können in Echtzeit Richtlinien durchsetzen, um kritische Geschäftsdaten zu schützen. Neue native Integrationen, implementierte Konnektoren und frei konfigurierbare APIs reduzieren den Implementierungsaufwand und erlauben es Unternehmen, Zero Trust umzusetzen, ohne etablierte Anwendungen nachzurüsten.

Ausblick 2: Es wird multiple Authentifizierungs-Ebenen geben
In der zunehmend Cloud- und Mobility-zentrierten Welt greifen schon heute immer mehr Mitarbeiter über multiple Geräte auf geschäftskritische Daten zu. Die Sessions können je nach Anwendung mitunter Stunden oder Tage dauern – gerade mit mobilen Geräten. Bei Diebstahl oder kompromittierten Devices sind die anfänglichen Schutzmaßnahmen also bedeutungslos. Moderne Zero-Trust-Lösungen werden daher schon bald multiple Authentifizierungsebenen unterstützen müssen, um nach bestimmten Fristen, Zugriffsversuchen oder Standortveränderungen erneut die Identität des Nutzers und Gerätes abfragen zu können.

Ausblick 3: Zero Trust wird die IoT-Umgebungen erobern
Das Internet der Dinge (IoT) stellt mit Blick auf die Sicherheit kritischer Systeme eine enorme Herausforderung dar. Nicht nur, weil dort tausende Geräte miteinander vernetzt sind, so dass sich Angreifer ungleich schneller ausbreiten können. Sondern auch, weil die Vernetzung ungleich performanter ist als früher: Die höhere Geschwindigkeit bedeutet, dass sich erfolgreiche Angreifer mit rasantem Tempo durch das Netzwerk bewegen können. Zero Trust ist unverzichtbar, um automatische Zugangskontrollen zu errichten und die Identität von Nutzer und Gerät zu validieren.

Ausblick 4: Zero Trust wird neue Standards erfordern
Aktuell gibt es kaum einheitliche Standards für Zero Trust. Um die Umsetzung von ZTNA zu erleichtern und zu vereinheitlichen, wird es aber notwendig sein, weltweit einheitliche Frameworks zu etablieren. Diese werden es den Unternehmen ermöglichen,

wichtige Partner aus der Supply-Chain einfach und ohne komplizierte Work-Arounds an ihre Netzwerke anzubinden. Das wird die Produktivität verbessern und viele Prozesse beschleunigen und vereinfachen – ohne Abstriche bei der Sicherheit in Kauf zu nehmen.

Ausblick 5: Zero Trust wird einfacher
Die Standardisierung schafft auch die Voraussetzungen für eine nachhaltige Vereinfachung der Zero-Trust-Lösungen – und wird den Boden für innovative neue Systeme bereiten, die sich wesentlich effizienter in die zunehmend komplexen Security-Ökosysteme der Unternehmen eingliedern lassen. Die hohe Skalierbarkeit der Lösungen stellt zudem sicher, dass die ZTNA flexibel mit dem Unternehmen mitwachsen kann.

Ausblick 6: Der Beratungsbedarf rund um Zero Trust bleibt hoch
Angesichts des anhaltenden Personalmangels werden sich Unternehmen auch in Zukunft schwertun, das für den Betrieb und den Support erforderliche Zero-Trust-Knowhow vollständig intern vorzuhalten. Dies gilt umso mehr, da die Technologie-Stacks immer komplexer und die Bedrohungen immer raffinierter werden. Experten mit einem tiefgreifenden Verständnis für Zero Trust dürften also auch in Zukunft hoch im Kurs stehen.

5 Security-Trends, die untrennbar mit Zero Trust verbunden sind

Zero Trust ist eine tragende Säule der Next-Generation Security – und Teil eines Ökosystems spannender Technologien, die sich dynamisch weiterentwickeln und gegenseitig kontinuierlich verändern. Zu den wichtigsten Trends, die die Zukunft der Zero-Trust-Technologie prägen werden, gehören.

1. SASE
„Secure Access Service Edge" ist ein Technologieansatz, der die wichtigsten Netzwerk- und Security-Funktionalitäten in eine durchgängig Cloud-basierte Plattform am Service Edge auslagert. SASE und Zero Trust bedingen einander und sind schon heute untrennbar verbunden. Es lohnt sich also, beide Ansätzen gemeinsam zu betrachten und sorgsam im Blick zu behalten.

2. XDR
Bei der „Extended Detection and Response" dreht sich alles darum, die Transparenz und Reaktionsfähigkeit von Security-Lösungen zu verbessern. Moderne XDR-Lösungen führen sicherheitsrelevante Daten aus unterschiedlichsten Quellen zusammen, um umfassende Einblicke in die Bedrohungslandschaft zu erhalten und proaktiv nach Angreifern in Netzwerken zu suchen. Auch dieser Ansatz ist eng mit dem Zero-Trust-Gedanken verknüpft, und wird zweifellos näher mit dem Konzept zusammenrücken.

3. Identity-Centric Security
Die identitätszentrierte Security geht davon aus, dass klassische Perimeter mehr und mehr obsolet werden und stattdessen die Identitäten der Benutzer und Devices der Schlüssel zur Sicherheit werden. Zero Trust kommt in diesem Modell seit jeher eine Schlüsselrolle zu.

4. Cloud-native Zero Trust
Die zunehmende Verlagerung von Anwendungen und Diensten in Cloud-Infrastrukturen ist in zweifacher Hinsicht mit dem Zero-Trust-Ansatz verquickt: Zum einen, weil mit der Zahl Cloud-basierter Systeme auch die Zahl der Cloud-Identitäten und der Cloud-Zugriffe rasant steigt – eine starke Zero-Trust-Security also immer wichtiger wird. Zum anderen aber auch, weil Cloud-basierte Infrastrukturen den Grundstein für Cloud-native Zero-Trust-Architekturen legen, und damit eine ganz neue Generation von ZTNA ermöglichen werden.

5. Machine Learning und Künstliche Intelligenz
Der Einsatz von Machine Learning (ML) und Künstlicher Intelligenz (KI) gewinnt über alle Segmente der Cybersecurity rasant an Bedeutung – auch im Zero-Trust-Umfeld: Die Analyse immer größerer Datenmengen und die ML- und KI-gestützte Erkennung von Mustern und Anomalien kann entscheidend dazu beitragen, Sicherheitsbedrohungen in ZTNA-Umgebungen frühzeitig zu erkennen und erfolgreich zu bekämpfen.

Die Chancen und Herausforderungen von Zero Trust

Die Einführung von Zero Trust bietet Unternehmen viele Ansatzpunkte, um ihre Daten und Ressourcen besser zu schützen und die durchgängige Einhaltung regulatorischer Bestimmungen zu gewährleisten. Doch um diese Chancen nutzen zu können müssen Unternehmen zunächst eine Reihe von Herausforderungen adressieren. Einige davon haben wir im Rahmen des Whitepapers bereits angesprochen.

Besonders die **Komplexität** einer Zero-Trust-Lösung macht nach wie vor vielen Unternehmen zu schaffen: Zero Trust erfordert eine breite und tiefe Infrastruktur, die eine Vielzahl komplexer Einzelsysteme umfasst – von Access Gateways bis Monitoring-Tools. All diese Technologien müssen nahtlos zusammengefügt und in die ZTNA-Plattform eingebunden werden, was mitunter aufwendige Anpassungen des bestehenden Netzwerks erforderlich macht.

Verschärft wird diese Problematik durch die **unübersichtliche Vendor-Landschaft:** Wer sich einen lückenlosen Überblick über das Lösungsangebot verschaffen will, muss Dutzende von Anbietern und Hunderte von Produkten recherchieren und evaluieren. Angesichts der dünnen Personaldecken und der erforderlichen tiefen Fachkenntnisse ist dies für viele Teams schlichtweg nicht zu leisten.

Kurz: ZTNA geht mit einem **hohen Planungs- und Implementierungsaufwand** einher und erfordert viel Zeit, Geld und Fachkräfte mit passendem Knowhow. Letztere sind dabei besonders rar gesät. Mit Blick auf den Fachkräftemangel und die kleine Zahl verfügbarer Zero-Trust-Experten auf dem Markt können die meisten Unternehmen ein ZTNA-Projekt also kaum ohne externe Partner umsetzen.

Eine weitere Herausforderung für viele Unternehmen ist die **fehlende Benutzer-akzeptanz**. Immerhin bedeutet die Einführung von Zero Trust in der Regel eine tiefgreifende Veränderung der Unternehmenskultur, die auf viele etablierte Prozesse ausstrahlt. Mitarbeiter fühlen sich schnell gegängelt – und stehen dem Konzept skeptisch gegenüber. Dem gilt es frühzeitig mit Trainings und Awareness-Schulungen entgegenzuwirken.

Und schließlich: Jeder noch so kleine Fehler bei der Zero-Trust-Implementierung kann zu **kritischen Sicherheitsrisken** führen. Nur wenn die Technologien nahtlos integriert sind, verbindliche Prozesse definiert wurden, die Mitarbeiter geschult sind und ein durchdachter Plan zu Überwachung und Aktualisierung der Systeme steht, ist ein sicherer Betrieb gewährleistet.

Der Lohn der Mühen: Wie Sie von Zero Trust profitieren

So viel zur Soll-Seite. All diesen Herausforderungen steht eine noch deutlich umfangreichere Liste von Vorzügen gegenüber, die Zero Trust unter dem Strich zu einer lohnenden Herausforderung machen:

Der offensichtlichste, aber auch wichtigste Punkt auf der Liste der Vorzüge ist die **verbesserte IT-Sicherheit.** Zero Trust hebt das Schutzniveau im hybriden, perimeterlosen Unternehmen von heute auf einen ganz neuen Level – und ist Ihre beste Waffe im Kampf gegen die rasant expandierenden Angriffsflächen. Denn mit Zero Trust werden die Identitäten der Anwender zu einem starken, neuen Perimeter, an dem sämtliche Zugriffe überwacht, verifiziert und autorisiert werden können. Neue Technologien wie XDR eröffnen Ihrem Unternehmen überdies die Option, proaktiv gegen Angreifer im Unternehmensnetzwerk vorzugehen.

Auf diese Weise ermöglicht es Ihnen Zero Trust, endlich wieder die **volle Kontrolle** über ihre Netzwerke und Ressourcen zurückzugewinnen. Aufsetzend auf dem „Need-to-know"-Prinzip lassen sich die Zugriffsrechte der Benutzer automatisch auf das erforderliche Minimum reduzieren. Darüber hinaus stellt die Zero-Trust-Lösung das durchgehende Monitoring aller Aktivitäten sicher – und kann bei verdächtigen Vorgängen automatisch intervenieren.

Von jedem Standort und jedem Gerät aus auf kritische Ressourcen zugreifen zu können – natürlich nur, solange der Nutzer und das Gerät authentifiziert und autorisiert sind – garantiert im Geschäftsalltag auch ein deutliches **Plus an Flexibilität** für Ihre Mitarbeiter. Das gilt übrigens auch für das Unternehmen als solches, das damit wesentlich schneller auf neue Bedrohungslagen und neue Vorgaben reagieren und die Zero-Trust-Lösung einfach anpassen kann.

Technologisch spannend: Mit der Einführung von Zero Trust legen Sie auch ein robustes Fundament für eine natürliche **Segmentierung von Netzwerken und Ressourcen,** da die Autorisierung und Authentifizierung auf einer wesentlich granularen Ebene möglich wird. Dies ermöglicht es Ihnen, Ihre Umgebung sukzessive in unterschiedlichste Zugriffsebenen zu unterteilen. So verringern Sie die Angriffsfläche und reduzieren das Schadenspotenzial, wenn ein Angriff erfolgreich ist.

Und zu guter Letzt unterstützt Sie Zero Trust auch nachdrücklich bei der **Einhaltung von Compliance-Anforderungen.** Da Zugriffe auf Ressourcen durch strenge Authentifizierungs- und Autorisierungsmaßnahmen beschränkt werden und die Aktivitäten von Benutzern jederzeit dokumentiert sind, tun Sie sich wesentlich leichter damit, Compliance-konforme Abläufe durchzusetzen und nachzuweisen.

8. Fazit

Zero-Trust-Architekturen werden zweifellos die Zukunft der IT-Security prägen – doch sie in Eigenregie zu planen, zu implementieren und zu betreiben ist für viele Unternehmen eine enorme Herausforderung. Ein solches Projekt bindet nicht nur wertvolle Zeit-, Personal- und Kapital-Ressourcen, sondern erfordert auch ein tiefes Verständnis der technologischen Zusammenhänge und einen robusten Überblick über einen fragmentierten und dynamisch wachsenden Technologiemarkt. Hinzu kommt, dass jeder noch so kleine Fehler bei der Umsetzung gravierende Sicherheitsrisiken und teure Compliance-Verstöße nach sich ziehen kann. Die Fallhöhe bei einem eigenverantwortlich umgesetzten ZTNA-Projekt ist also beträchtlich.

Unternehmen sind daher gut beraten, frühzeitig externe Experten als Projektpartner hinzuzuziehen. Aufsetzend auf ihre jahrelange Erfahrung bei der Umsetzung von Zero-Trust- und Identity-Projekten können diese Spezialisten Ihr Unternehmen herstellerunabhängig in allen Projektabschnitten unterstützen. So können Sie Ihre maßgeschneiderte Lösung aus einem breiten Best-of-Breed-Portfolio auswählen – und mit individuell zusammengestellten Consulting-, Professional und Managed Services die Weichen für einen erfolgreichen Projektverlauf stellen.

Das sind wir

iC Consult ist der führende unabhängige Berater, Systemintegrator und Managed Services Anbieter für Identity & Access Management (IAM) mit mehr als 800 Mitarbeitenden weltweit.

Mit unserer Hingabe zu Exzellenz und Innovation und den besten Technologien im IAM-Umfeld bieten wir unseren Kunden erstklassige Cyber Security Lösungen. Unser Service-Portfolio umfasst Managed Services für IAM einschließlich Beratung, Architektur, Implementierung, Integration, Support und Betrieb.

iC Consult hat seinen Hauptsitz in München und Niederlassungen in Deutschland, der Schweiz, Österreich, Frankreich, Belgien, Spanien, Bulgarien, Großbritannien, den USA, Kanada, Indien und China. Die größten Marken der Welt vertrauen auf unsere Expertise, um ihre wertvollsten Güter zu schützen und zu verwalten: Ihre Identitäten.

Mehr Informationen unter www.ic-consult.com