INSEYA
simply secure

Zero Trust

Grundlagen

Inhalt

Zero Trust
Grundlagen.

Zero Trust Grundlagen.

#1

Was ist Zero Trust?

Das Konzept Zero Trust basiert auf dem Grundsatz, dass keinem Gerät, Benutzer oder Prozess mehr einfach so vertraut wird. Dabei ist es nicht von Bedeutung, ob sich die Quelle, welche die Anfrage stellt, sich innerhalb oder ausserhalb des Perimeters befindet. Nach dem Prinzip „Never Trust, Always Verify“ erfordert jede einzelne Anfrage eine neue Verifizierung. Erst nach erfolgreicher Überprüfung wird ein policybasierter, granularer, zeitlich begrenzter Zugang zu einem Netzwerk, System oder einer Unternehmensressource freigegeben. Das Vertrauen wird ständig neu überprüft und wird auf Basis von einer Kombination von internen und externen Faktoren (MFA, Standort etc.) bestimmt und authentifiziert

#2

Was ist Zero Trust nicht?

Zero Trust kann man nicht kaufen, es ist kein fertiges Produkt und keine fixfertige Lösung. Ebenso kann Zero Trust nicht einfach implementiert und abgeschlossen werden. Mittlerweile gibt es eine Vielzahl von Anbietern, welche mit dem Begriff Zero Trust werben und damit einzelne Sicheheitskomponenten mit einem Bezug zu Zero Trust anbieten. Aber erst der gesamtheitliche Ansatz mit der Auswertung einzelner Parameter und einer kontextbasierten Entscheidung ermöglichen ein «richtiges» Zero Trust welches einen Sicherheitsgewinn bringt.

#3

Wie schnell kann ein Zero Trust Framework eingesetzt werden?

Zero Trust ist eine lange Reise, auf welcher die Einstellung bezüglich Sicherheit auf organisatorischer, strategischer und technischer Ebene angepackt werden muss. Im grösseren Sinne ist ein «Culture Change», worin alle beteiligten Personen von einem gleichen IT-Verständnis ausgehen müssen. Darum gibt es auch nicht ein allgemein gültiges Konzept, dass man aus einer Schublade ziehen kann. Das Sicherheitskonzept muss individuell auf die Bedürfnisse und Anforderungen der Unternehmung adaptiert werden.

#4

Ist CARTA ein Zero Trust Konzept?

Teilweise ja, CARTA ist wie Zero Trust ein theoretisches Konzept, wozu keine fertigen Produkte oder Lösungen existieren. Die Beratungsfirma Gartner prägte die Entwicklung dieses Begriffs, welche für „Continuous Adaptive Risk and Trust Assessment“ steht. CARTA ist auf dem Modell von «Zero Trust Extended» von Forrester entstanden, legt den Fokus sehr stark auf Automatisierung und die kontinuierliche Überwachung und Controlling der Massnahmen.

#5

Was sind die Treiber von Zero Trust?

Cloud Services - Zunehmend werden Services aus den Cloud genutzt weil diese schnell verfügbar, einfach skalierbar und flexibel genutzt werden können.

Work from Home - Mitarbeitende arbeiten häufiger ausserhalb des Unternehmens. Die Pandemie und die Homeoffice Pflicht haben dies noch weiter verstärkt.

Digitalisierung - Prozesse und Dienstleistungen werden digitalisiert und mit unterschiedlichsten Endgeräten von unterschiedlichen Standorten aus genutzt.

Klassische Perimeter - Sicherheitskonzepte mit durch Firewall getrennte Zonen können die Anforderungen an oben genannten Gründe nicht erfüllen.

#7

Was sind die Ziele von Zero Trust?

Jede Unternehmung möchte Ihre wichtigsten Ressourcen schützen. Das Ziel von Zero Trust ist es, den Zugriff von nicht autorisierten Identitäten auf Informationen und Systeme, welche für das Un-ternehmen wertvoll sind, zu schützen. Dies ist im Grundsatz nicht komplett neu, auch die bisherige Sicherheitsarchitekturen folgen diese Ziele. Bei Zero Trust kommt aber das dynamische, kontextbasierte Regelwerk hinzu, welches situativ entscheiden soll, ob der Zugriff gewährt wird.

#7

Was ist der Mehrwert von Zero Trust?

Durch die notwendigen, konzeptuellen Vorarbeiten für eine Zero Trust Umsetzung lernt das Unternehmen sehr viel darüber, wie Informationen im Unternehmen verarbeitet werden. Was muss ich wirklich schützen? Welche sind unsere «Kronjuwelen»? Wie und wo werden Daten verarbeitet? Wo sind unsere Schwachstellen? Wieviel Aufwand soll betrieben werden?

- Eine effektiv umgesetzte Zero Trust Architektur **erhöht die Sicherheit** durch granulare Zugriffskontrolle für alle wichtigen Ressourcen

- Das Zero Trust Konzept **verbessert die Reaktionsfähigkeit** auf Bedrohungen da sämtliche Parameter im Netzwerk zentral kontrolliert und ausgewertet werden

- Eine Zero Trust Umsetzung **erhöht die Agilität**, weil auf neue Sicherheitsanforderungen mittels der zentralen Steuerungskomponente dynamisch reagiert werden kann

- Der Zero Trust Ansatz **optimiert den Zugriff** den Mitarbeitenden auf die verwendeten Ressourcen da die neuen Sicherheitskomponenten auf ein Arbeiten mit Cloud Ressoucen und hybriden Infrastrukturen ausgerichtet sind

- Die Verwendung von einheitlichen Identitäten **vereinfacht die Nutzung von Diensten für die Mitarbeitenden** und steigert die Sichereit durch das „least privilege“ Prinzip Arbeiten mit Cloud Ressoucen und hybriden Infrastrukturen ausgerichtet sind

#8

Was sind die Herausforderungen von Zero Trust?

Die erste grosse Herausforderung ist eine tragfähige und unternehmensweit akzeptierte Zero Trust Strategie zu entwickeln. Dabei ist es wichtig von Anfang an die Unterstützung der entscheidenden Kräfte für sich zu gewinnen (Interne Stakeholder), um den Budgetprozess zu beschleunigen und die Ressourcen freizugeben. Die Zero Trust Strategie muss sich den bestehenden IT-Prozessen und Geschäftsanforderungen angleichen und diese unterstützen.

Die zweite grosse Herausforderung ist die technische Abstimmung der Schnittstellen zwischen den einzelnen Sicherheitskomponenten. Alle Komponenten müssten mit einer zentralen Entscheidungsinstanz kommunizieren können und diese muss alle Sicherheitskomponenten ansteuern können, um den Zugang zu einer Ressource zu gewähren

#9

Was sind Zero Trust Prinzipen

Das Zero Trust Konzept baut auf vier grundlegenden Prinzipien auf: Assume breach, Never Trust – Always Verify, Least privileged access & Mikrosegsegmentation. Diese bilden die Grundlage für die zu definie-rende Zero Trust Strategie.