Whitepaper

Implementierung eines Sicherheits-Frameworks mit Zero Trust

Einleitung

Mit der Verbreitung von verteilten IT-Umgebungen und dem Internet der Dinge (Internet of Things, IoT) können Unternehmen ihre digitalen Perimeter nicht mehr einfach sichern – ein klar abgegrenzter Unternehmensbereich existiert oft nicht mehr. Während IT-Umgebungen bereits zunehmend komplexer geworden sind, hat die jüngste und schnelle Expansion von Endgeräten und Netzwerken, die neue Arbeitsmodelle ermöglichen, zu einem komplexen Ökosystem geführt, das nur noch schwer zu sichern ist.

Veraltete Ansätze zur Sicherheit sind davon ausgegangen, dass alles innerhalb des Unternehmensnetzwerks vertrauenswürdig sein müsste. Dies ist einfach nicht länger zutreffend. Zurückzuführen ist dies auf Faktoren wie:

Bedarf an Fernzugriff

Mitbringen des eigenen Geräts (BYOD)

IoT

Multi- und Hybrid Cloud-Ansätze

Vermehrte Zusammenarbeit

Notwendigkeit von geschäftlicher Elastizität

Die zunehmende Komplexität der IT-Infrastruktur von Unternehmen hat eine erhöhte Angriffsfläche mit Lücken in der Transparenz und punktuellen Lösungen geschaffen, die das Sicherheitsmanagement zu einer schwierigen Aufgabe machen. Als Ergebnis dieser erweiterten Peripherie erkennen Sicherheitsprotokolle eine notwendige Verschiebung vom Standort zur Identität als Garant für Vertrauen.

Die Kontrolle des Netzwerkzugriffs, die identitätsbasierte Berechtigungen und IT-Zugriff umfasst, ist ein wichtiger Bestandteil für einen zuverlässigen Sicherheitsansatz. Das Zero Trust-Framework, das auf den Prinzipien der geringsten Rechte aufbaut und (wie der Name schon sagt) zunächst keinerlei Vertrauen schenkt, ist ein Ansatz, den das Unternehmen ergreifen kann, um identitätsbasierte Zugriffsrichtlinien methodisch und umfassend im gesamten Unternehmen oder im Betrieb auf Grundlage seiner jeweiligen Anforderungen zu integrieren.

Insight Cloud + Data Centre Transformation (CDCT) unterstützt Unternehmen aller Größen dabei, ihre Sicherheitspositionen zu stärken und ihre Benutzer, Daten und Endgeräte zu schützen, indem sie die Zero Trust-Methodik und unsere Partnerschaften mit führenden Anbietern von Sicherheitstechnologien nutzen. Dieses Whitepaper soll Unternehmen, die interessiert sind, eine Zero Trust-Methodik anzuwenden, unterstützen, die Notwendigkeit und den Nutzen eines solchen Ansatzes und die strategische und technische Unterstützung von Insight zu verstehen, um bei der Identifizierung und Implementierung geeigneter Lösungen zu helfen.

Zero Trust: Die Antwort für immer größer werdende Perimeter

Die Grundlagen von Zero Trust

Die Zero Trust-Methodik legt das Fundament für eine hochgradig geschützte IT-Umgebung und geht davon aus, dass alle Endgeräte bis zum gegenteiligen Nachweis als „nicht vertrauenswürdig" gelten – was unter anderem eine Identitätsprüfung erfordert, um das Vertrauen zu erhöhen und Zugang zu Netzwerken und Ressourcen entsprechend zu gewähren. Diese wichtigsten Arbeitsweisen stützen sich auf die Überzeugung, dass Vertrauen weder binär noch dauerhaft ist und der Betrieb auf Misstrauen basieren muss, um das höchste Maß an Sicherheit aufrechtzuerhalten.

Ein Ansatz von Zero Trust:

Etabliert Vertrauen bei jeder Zugriffsanfrage, unabhängig davon, wo sie herkommt

Sichert den Zugriff über alle Applikationen und Netzwerke hinweg

Weitet das Vertrauen aus, um ein modernes Unternehmen im verteilten Netzwerk zu unterstützen

Zusätzlich zur besseren Zugriffssicherheit unterstützt ein Zero Trust-Ansatz auch moderne Unternehmensmodelle mit BYOD, Cloud-Apps, Hybrid Cloud/On-Premises-Umgebungen und mehr.

Um die Zero Trust-Diskussion zu vereinfachen, wurde die Implementierung geeigneter Sicherheitslösungen in drei Hauptbereiche unterteilt: die Belegschaft, die Workloads und der Arbeitsplatz.

Mitarbeiter

Benutzer und Geräte, die auf Unternehmensapplikationen zugreifen

Workloads

Applikationen, Services, Microservices usw., die auf Datenbanken, Server usw. zugreifen

Arbeitsplatz

IoT-Geräte, Endgeräte und Kontrollsysteme, die auf das Netzwerk zugreifen

Mitarbeiter

Der erste Bereich, der im Zero Trust-Framework behandelt wird, ist die Belegschaft. Die Belegschaft setzt sich aus Unternehmensbenutzern und den Geräten zusammen, von denen aus sie auf Unternehmensapplikationen zugreifen, sei es in der Cloud oder in physischen Rechenzentren. Die Prinzipien von Zero Trust, die auf die Belegschaft angewendet werden, stellen sicher, dass nur verifizierte Benutzer und gesicherte Geräte auf Unternehmensapplikationen zugreifen können.

Es gibt drei wichtige Komponenten, um Ihre Angriffsfläche durch ein verifiziertes Vertrauen zu minimieren: die Transparenz des Geräts verbessern, die Sicherheitslage des Geräts beurteilen und eine kontinuierliche Risikobewertung ermöglichen. Wenn diese Funktionen aktiviert sind, können Unternehmen ihre Daten schützen und gleichzeitig ihrer gesamten Belegschaft einen nahtlosen Zugriff auf kritische Applikationen und Netzwerke bieten.

Die richtigen Lösungen für einen gesicherten Zugriff ermöglichen Ihrem Unternehmen Folgendes:

- Überprüfen von Benutzeridentitäten mit Multi-Faktor-Authentifizierung (MFA)
- Erlangen von Transparenz für das Gerät und Schaffen von Vertrauen
- Durchsetzen von Zugriffsrichtlinien mit adaptiven Zugriffskontrollen

Workloads

Die nächste Facette der Unternehmensumgebung, die in einer Zero Trust-Diskussion behandelt wird, sind die Workloads. Zero Trust-Sicherheit für Workloads bedeutet ein verifiziertes Vertrauen für Ihre Applikationen, Services und Microservices, die mit Datenbanken, Containern und Servern in Ihrer gesamten Unternehmensumgebung kommunizieren – ob lokal, in der Cloud oder über hybride Infrastrukturen hinweg.

Effektive Technologien zur Sicherung Ihrer Workloads sollten mit minimalem Aufwand das Risiko für Ihre IT-Ressourcen reduzieren und Funktionen bieten, die Ihnen Folgendes ermöglichen:

- Erlangen von Transparenz über die gesamte Umgebung hinweg
- Identifizierung individueller Workloads
- Programmieren und Durchsetzen von Richtlinien
- Eindämmung von Verstößen
- Aufrechterhalten von Compliance
- Kontinuierliche Überwachung von Aktivität
- Automatisches Reagieren auf Kompromisse

Arbeitsplatz

Schließlich sollten Zero Trust-Protokolle auch den Arbeitsplatz umfassen und sich auf den sicheren Zugriff für alle Endgeräte und IoT-Geräte konzentrieren, die mit dem Unternehmensnetzwerk verbunden sind – von Gäste-Laptops über Ausweisscanner bis hin zu Point-of-Sale-Geräten. Spezifische Zugriffsprotokolle müssen vorhanden sein, da viele der Geräte am Arbeitsplatz Zugriff auf dieselben Applikationen und Workloads wie Ihre Benutzer benötigen, aber keinen vollständigen Netzwerkzugriff brauchen (und diesen auch nicht bekommen sollten).

Die Implementierung geeigneter Netzwerksicherheitslösungen ermöglicht es Benutzern, sich sicher mit Unternehmensnetzwerken zu verbinden und gleichzeitig den Zugriff von nicht-konformen Geräten einzuschränken. Die sicheren Lösungen für den Netzwerkzugriff, die Sie auswählen, sollten Ihnen Folgendes ermöglichen:

- Gewähren eines angemessenen Netzwerkzugriffs für Benutzer und Geräte mit Netzwerkauthentifizierung und -autorisierung
- Klassifizieren und Segmentieren von Benutzern, Geräten und Applikationen
- Isolieren von infizierten Endgeräten
- Widerrufen eines Netzwerkzugriffs, soweit erforderlich

Umsetzung von Zero Trust mit Insight

Branchenführende Lösungen und Support-Services von Insight und unseren Partnern machen es möglich, mit der Implementierung von Zero Trust-Methoden in jeder Phase der Entwicklung von Sicherheitsstrategien zu beginnen. Dieser Ansatz bietet deutliche Vorteile, auch über die entscheidende Komponente einer erhöhten Sicherheit hinaus. Mit einer stärkeren Sicherheitsumgebung und einheitlichen Sicherheitslösungen können Unternehmen von einem effizienteren Betrieb, geringeren Sicherheitskosten und einer benutzerfreundlicheren sowie optimierten Technologieumgebung profitieren.

Betriebliches

Eines der wichtigsten Probleme bei einem traditionellen Sicherheitsansatz ist die Komplexität. Zero Trust kann IT- und Sicherheitsteams mehr Kontrolle und Transparenz bei Benutzern, Geräten, Zugriffsebenen und laufenden Aktivitäten bieten. Wenn Zero Trust richtig verstanden und implementiert wird, reduziert es sowohl die Komplexität als auch die Ressourcenüberlastung – zwei Hauptfaktoren für das betriebliche Risiko.

Finanzen

Die Wahl eines Zero Trust-Ansatzes mag aufgrund der voraussichtlichen Kosten für die Neugestaltung und Entwicklung entmutigend erscheinen. Unternehmen können aber von langfristigen Vorteilen profitieren, indem sie Punktlösungen reduzieren, das Sicherheitsrichtlinien-Management zentralisieren und Verhaltens-Analytik einsetzen, um die ständige Bewertung eines Benutzer-und Geräterisikos für das Unternehmen zu unterstützen. Zero Trust bietet eine fokussierte Sicherheitslösungsumgebung und reduzierte Ressourcenaktivitäten, um die ständige Flut von Warnmeldungen und potenziellen Vorfällen zu verwalten, mit denen Sicherheitsexperten täglich umgehen.

Technologie

Einer der wichtigsten Aspekte eines gut gestalteten Zero Trust-Frameworks ist das einfache, zentralisierte Richtlinienmanagement. Je komplexer eine Softwareumgebung ist, desto wahrscheinlicher ist es, dass Lücken vorhanden sind, die Risiken bergen. Im Idealfall sollten Technologien, die Zero Trust unterstützen, Integrationen liefern, welche die IT-Umgebung rationalisieren, das maschinelle Lernen (ML) und eine Analyse des Nutzerverhaltens begünstigen, eine kontinuierliche Aktivitätsüberwachung anbieten und automatisierte Abhilfemaßnahmen schaffen.[1]

Zusammenfassung

Als Unternehmen, das solide Industriepartnerschaften mit erstklassigen OEMs und Lösungsanbietern unterhält, möchte Insight seine Kunden bei der Bewertung und Implementierung optimaler Sicherheitslösungen unterstützen, die auf den jeweiligen organisatorischen Anforderungen basieren, um so eine Zero Trust-Umgebung mit innovativen, umfassenden und benutzerfreundlichen Technologien zu schaffen.

Ein Zero Trust-Ansatz, der durch die professionellen Ressourcen von Insight ermöglicht und unterstützt wird, bietet den Unternehmen Folgendes:

- Verhindern von Datenschutzverletzungen, bevor sie passieren, indem für jeden Zugriffsversuch auf Unternehmens-Applikationen, Workloads und Netzwerke richtlinienbasierte Kontrollen ermöglicht werden.
- Erlangen einer erhöhten Transparenz darüber, wer und was auf Applikationen, Workloads und Netzwerke zugreift, um Risiken und Indikatoren für eine Datenschutzverletzung zu identifizieren.
- Reduzieren der Gesamtangriffsfläche, Eingrenzen von Datenschutzverletzungen und Stoppen von lateralen Aktivitäten durch die Umsetzung granularer Kontrollen und die Segmentierung von Netzwerken und Workloads.

Viele Unternehmen erkennen mittlerweile die Notwendigkeit eines Zero Trust-Ansatzes, sind sich aber nach wie vor unschlüssig, wo und wie sie mit der Implementierung beginnen sollen. Das Ziel von Insight ist es, unsere Kunden zu unterstützen, ihnen in jeder Phase ihrer Entwicklung der Sicherheitsstrategie zur Seite zu stehen und mit ihnen gemeinsam optimale Lösungen zu entwickeln bzw. die nächsten Schritte zu identifizieren, und zwar in Übereinstimmung mit einem Zero Trust-Framework und den organisatorischen Anforderungen der Unternehmen. Insight ermöglicht dies durch Partnerschaften mit Anbietern und professionelle Dienstleistungen und bietet Unternehmen alle Bestandteile eines umfassenden und effektiven Sicherheitsansatzes, um optimale Kundenergebnisse zu erzielen.

Weitere Informationen zur Implementierung einer Zero Trust-Methodik als Teil der Sicherheitsstrategie Ihres Unternehmens finden Sie unter Insight Security Services.

---

1 Rowell, E. (2021, March 5). Zero Trust: What's Driving Its Adoption in Enterprise Environments? Insight.

Sinnvolle Lösungen für den Geschäftserfolg

Wir unterstützen unsere Kunden bei der Modernisierung und Sicherung kritischer Plattformen zur Transformation der IT. Wir glauben, dass Daten ein wichtiger Faktor und Hybridmodelle Beschleuniger sind und dass sichere Netzwerke gut integriert sein müssen. Unsere End-to-End-Services befähigen Unternehmen, Technologielösungen effektiv zu nutzen, um Herausforderungen zu überwinden, Wachstum und Innovation zu unterstützen, Risiken zu reduzieren und das Unternehmen zu transformieren.

Weitere Informationen:
www.insight.de

www.insight.de