DELL Technologies

5 Empfehlungen zur Erfüllung Ihrer Zero-Trust-Anforderungen

1	2	3	4	5
Planen Sie den Paradigmenwechsel, niemals zu vertrauen, sondern immer zu verifizieren	**Legen Sie Ihren gewünschten Weg fest**	**Das Unternehmen treibt die Zero-Trust-Umgebung voran, nicht umgekehrt**	**Konzentrieren Sie sich auf die Daten**	**Implementieren Sie den Ansatz „niemals vertrauen, immer verifizieren“ im gesamten IT-Ökosystem**
Einen akzeptablen Kompromiss zwischen Risikominderung und geschäftlichen Auswirkungen ermitteln	Inkrementelle Sicherheitsverbesserung	Kontrollen auf der Basis von Geschäftsanforderungen aufbauen	Sicherstellen, dass alle Netzwerk-, Geräte- und Nutzeraktivitäten kontinuierlich protokolliert werden	Zero-Trust-Aktivitäten wie Multi-Faktor-Authentifizierung und Identitätsmanagement universell anwenden, um kritische Lücken zu vermeiden
Die Kosten, die Auswirkungen auf den Betrieb und die StakeholderInnen sowie die Compliancean-forderungen und behördlichen Auflagen berücksichtigen	Hyperscaler	Prozesse, Rollen, Verantwortlichkeiten und Datenklassifizierungen dokumentieren	KI und ML zur Analyse von Daten und Identifizierung von Anomalien nutzen, die auf Bedrohungen hinweisen könnten	Physische und digitale Lieferketten von Drittanbietern in das Zero-Trust-Framework einbeziehen
Von perimeterbasierter Sicherheit zu einem mikrosegmentierten, datenzentrierten Modell übergehen	Dedizierte Umgebung	Nutzererlebnis bleibt entscheidend	Daran denken, dass der Schutz von Daten und Anwendungen die Schlüsselrolle einer Zero-Trust-Architektur ist	
Bei Bedarf externe Hilfe nutzen	Identität ist der neue Perimeter	Sicherheitsverbesserungen wie Zero Trust nicht auf Kosten der Nutzbarkeit gehen lassen		
		Unternehmensziele wie Wachstum und Innovationen bleiben höchste Priorität		

Zero Trust gilt weithin als Best Practice für die Sicherheitsarchitektur.

Daten zeigen, dass die meisten Unternehmen begonnen haben, Zero Trust in Betracht zu ziehen oder den Ansatz bereits implementieren.[1] Die Umstellung auf Zero Trust ist zwar ein großes Unterfangen, aber es gibt einige praktische Überlegungen, die Ihnen dabei helfen können.

Die Dell Technologies Subject Matter Experts Tracy Emmersen, Director of Solution Adoption for Project Fort Zero, und Justin Vogt, Principal Security Engineer, haben ihre Empfehlungen und Erkenntnisse mit Ash Lakshmanan, Security Services Product Manager, geteilt. Ihre wichtigsten Vorschläge sind unten zusammengefasst. Alternativ können Sie sich das ganze Gespräch unter dell.com/cybersecuritymonth ansehen.

> „Wenn wir Zero Trust von einem ganzheitlichen Standpunkt aus betrachten und einen Schritt zurücktreten, dreht sich tatsächlich alles um die Daten.“
>
> ***Tracy Emmersen***
> *Director of Solution Adoption for Project Fort Zero, Dell Technologies*

Planen Sie den (großen) Paradigmenwechsel, niemals zu vertrauen, sondern immer zu verifizieren

Im Grunde stellt die Umstellung auf eine Zero-Trust-Umgebung eine große Abkehr von historischen Sicherheitsmodellen zu einer Umgebung dar, die auf den Prinzipien „niemals vertrauen, immer verifizieren“ und „Zugriff mit der geringsten Berechtigung“ basiert. „Wir müssen unseren Sicherheitsstatus anders betrachten als in der Vergangenheit. Wir müssen weg von herkömmlichen, perimeterbasierten Netzwerksicherheitslösungen und hin zu einer mikrosegmentierten, datenzentrierten Architektur“, merkt Emmersen an.

Legen Sie Ihren gewünschten Weg fest

Emmersen erläutert drei verschiedene Möglichkeiten, die Vorteile von Zero Trust zu erreichen:

- **Inkrementell:** ein iterativer Ansatz, der wichtige Zero-Trust-Prinzipien in die aktuelle Umgebung integriert
- **Hyperscaler:** Nutzung der Zero-Trust-Funktionen der großen Cloud-Anbieter
- **Dedizierte, vollständig konforme Umgebung:** private On-Premise-Umgebung, die von Grund auf neu erstellt wurde und Zero-Trust-Standards strikt einhält

Zusätzlich zu diesen drei Möglichkeiten können virtualisierte, kleine und mittlere Unternehmen auch einen Ansatz namens „Identität ist der neue Perimeter“ verfolgen. Diese Methodik konzentriert sich auf Identitäts- und Zugriffsmanagement und nutzt SaaS-Tools, um einen Zero-Trust-basierten Schutz zu erreichen. Eine wichtige Komponente dieser Methode ist die Implementierung der Multi-Faktor-Authentifizierung (MFA) überall, was die Auswirkungen dieser einen Zero-Trust-Funktion aufzeigt.

Die Hyperscaler- und Identitätsansätze sind in der Regel kostengünstiger, während die inkrementellen und dedizierten Umgebungen höhere Investitionen erfordern.

Das Unternehmen treibt die Zero-Trust-Einführung voran, nicht umgekehrt

Im Grunde genommen ist eine Zero-Trust-Architektur darauf ausgelegt, die Workflows, Nutzerrollen und zugehörigen Berechtigungen, Geräte, Daten, Anwendungen und Netzwerke eines Unternehmens zu verwalten und zu schützen. Der erste Teil einer Implementierung erfordert eine solide Dokumentation dieser Aspekte. Anschließend werden die Steuerungsebene und die Infrastruktur so konzipiert, dass die sie regelnden Policies durchgesetzt werden.

Wenn die Zero-Trust-Umgebung den Geschäftsbetrieb zum Nachteil des Unternehmens behindert oder erheblich verändert, lohnt sich die erreichte verbesserte Sicherheit wahrscheinlich nicht. Vogt erklärt: „Wenn [Sicherheit] … der Kernmission des Unternehmen im Weg steht, … sind wir nicht wirklich besser als die GegnerInnen, die wir zu unterbrechen versuchen. Wir haben lediglich unseren eigenen Denial of Service bereitgestellt.“

Konzentrieren Sie sich auf die Daten

Emmersen merkt an: „Wenn wir Zero Trust von einem ganzheitlichen Standpunkt aus betrachten und einen Schritt zurücktreten, dreht sich tatsächlich alles um die Daten.“ Der Schutz von Unternehmensdaten ist einer der wichtigsten Vorteile der Umstellung auf Zero Trust. Prinzipien wie kontinuierliche Überprüfung und Segmentierung schützen Daten und Anwendungen, indem sie verhindern, dass sich Bedrohungen lateral im Netzwerk verschieben.

Protokollierung und kontinuierliches Monitoring sind wichtige Komponenten von Zero Trust. Diese Daten und die Telemetriedaten werden analysiert, um Anomalien zu identifizieren, die auf ein Risiko oder eine Bedrohung hinweisen könnten. Beispielsweise kann eine Änderung der Datennutzungsmuster ein Hinweis auf eine potenzielle Exfiltration oder einen Ransomwareangriff sein.

1 Aus einer von Dell in Auftrag gegebenen Studie der Enterprise Strategy Group, „Assessing Organizations' Security Journeys: Insights Spanning the Attack Surface, Threat Detection and Response, Attack Recovery, and Zero Trust“, November 2023.

DELL Technologies

Angesichts der enormen Datenmenge, die durch die Protokollierung aller Aktivitäten erzeugt wird, müssen moderne Analysetools KI und maschinelles Lernen nutzen, um effektiv zu sein.

Der Ansatz „niemals vertrauen, immer verifizieren“ muss durchgängig angewendet werden

Während ein Großteil der Fokussierung auf Daten, Anwendungen, NutzerInnen und Geräte intern stattfindet, muss die mit einer Zero-Trust-Architektur verbundene Überprüfung während des gesamten IT-Lebenszyklus angewendet werden. Andernfalls können kritische Sicherheitslücken entstehen.

Die Lieferkette ist ein gutes Beispiel. Vogt empfiehlt, wichtige Fragen zu Hard- und Software von Drittanbietern zu stellen:

- „Wer konnte noch darauf zugreifen?
- Woraus besteht sie?
- Was wird unter der Oberfläche noch ausgeführt?
- Wie können wir diese Prinzipien des Nichtvertrauens [sowie] eine Art Verifizierungsprozess und einen Status der geringsten Berechtigung für die von uns genutzte Technologie umsetzen? Selbst wenn sie in der Technologielieferkette vorgelagert ist?“

Die Umstellung auf eine Zero-Trust-Architektur oder die Implementierung ihrer Prinzipien ist derzeit die Best Practice zur Förderung des Cybersicherheitsreifegrads. Dabei gibt es mehrere Wege, die unterschiedliche Kompromisse zwischen Kosten, Risiken und dem Level der Sicherheitsverbesserung darstellen. Der erste Schritt sollte darin bestehen, die einzigartige Position des Unternehmens zu ermitteln und sie als Grundlage für Technologieentscheidungen zu nutzen.

Erfahren Sie, wie Sie einige der größten Herausforderungen von heute im Bereich der Cybersicherheit bewältigen können: **dell.com/cybersecuritymonth**.