10 ELEMENTE
eines Zero-Trust-Datencenters

In einem Datencenter, in dem Zero Trust effektiv umgesetzt wird, steht die Endbenutzererfahrung an erster Stelle.

Konkret bedeutet das:

- *Der Zugriff ist schnell, zuverlässig und skalierbar.*
- *Benutzer und Geräte sind geschützt.*
- *Anwendungs- und Workload-Daten sind sicher.*
- *Die Sicherheit verbessert die Geschäftsagilität.*

10 VISIBILITÄT: SICHTBAR MACHEN DES NICHTSICHTBAREN

Man kann nur das schützen, was man sieht.

Deshalb benötigen Sie umfassende Einblicke in alle Netzwerkumgebungen und müssen erkennen können, wie jeder einzelne Bestandteil geschützt wird – vom Client bis zu den Workloads.

9 SEGMENTIERUNG AN MEHREREN STELLEN

Schaffen wir Klarheit.

Für Benutzer und Geräte, Anwendungen und Workloads gilt gleichermaßen: Eine hochpräzise Segmentierung und Kontrolle kann nicht autorisierten Zugriff und Lücken bei der Bedrohungsabwehr verhindern.

8 EIGENE IDENTITÄTEN FÜR BENUTZER, GERÄTE UND WORKLOADS

Nicht nur Benutzer benötigen eine Identität.

Auch Geräte und Workloads müssen eine Identität haben, die sich aus mehreren Faktoren zusammensetzt, damit Sie Risiken im Netzwerk jederzeit erkennen können.

7 STANDORTUNABHÄNGIGE, DURCHGÄNGIG GELTENDE RICHTLINIEN

Behalten Sie Benutzer, Geräte und Anwendungen überall im Blick.

Benutzer, Anwendungen und Workloads sind heute äußerst mobil. Deshalb müssen Sie sicherstellen, dass Sicherheitsrichtlinien in jedem Umfeld durchgängig angewendet werden. Nur so minimieren Sie potenzielle Angriffsvektoren.

6 ERKENNEN DER ABSICHT HINTER DEM NETZWERKDATENVERKEHR

Wohin werden Daten übertragen und was geht im Netzwerk vor sich?

Sie müssen so viel wie möglich über den Netzwerkdatenverkehr in Ihrem Unternehmen wissen – auch über nicht entschlüsselte Übertragungen. Wie das geht? Indem Sie bestimmte Indikatoren und Verhaltensmuster beobachten.

5 AUTOMATISIERUNG WO IMMER MÖGLICH

Machen Sie Automatisierung zu Ihrer Superpower.

Mit automatisierten Abläufen machen Sie sich das Leben leichter und ermöglichen allen Teams effizienteres Arbeiten. Änderungen aus einem Bereich des Datencenters können in anderen Bereichen angewendet werden. Zudem können Sicherheitsteams Angriffsversuche abwehren, bevor es zu einem Sicherheitsvorfall kommt.

4 ÜBERWACHUNG UND NUTZUNG ALLER VERBINDUNGSPUNKTE

Weiten Sie die Sicherheit auf neue Bereiche aus.

Nutzen Sie Ihre Router und Switches, um Bedrohungen zu erkennen und Richtlinien zum Schutz der Datencenter-Umgebungen durchzusetzen.

3 EFFEKTIVE ABWEHR GÄNGIGER BEDROHUNGEN

Tatsache: Eine Sicherheitslösung, die nicht in der Lage ist, bekannte Bedrohungen abzuwehren, ist eine Fehlinvestition.

Daten lügen nicht. Recherchieren Sie gründlich, um einen Anbieter zu finden, dessen Sicherheitstechnologie Angriffe auf Ihr Netzwerk effektiv unterbindet.

2 STÖRUNGSFREIER ANWENDUNGSBETRIEB

Ein Netzwerkausfall ist keine Option.

Der Erfolg eines Unternehmens hängt davon ab, dass das Netzwerk verfügbar ist und Ressourcen vernetzt sind. Effektive Sicherheit darf nicht zu Lasten des Netzwerkbetriebs gehen. Entscheiden Sie sich für zuverlässige Sicherheitslösungen, die blitzschnelle Failover unterstützen und den Durchsatz sicherstellen, den Ihr Geschäft benötigt.

1 SCHRITT FÜR SCHRITT ZUM ERFOLG

Halten Sie an Ihrem Ziel fest.

Sie haben noch nicht alles durchgeplant? Keine Sorge. Ihr Interesse an Zero Trust zeigt, dass Sie auf dem richtigen Weg sind. Legen Sie nun einfach fest, welches Element Sie als Nächstes implementieren. Nach und nach richten Sie so ein Zero-Trust-Datencenter ein. Ein Schritt nach dem anderen ist besser als stillzustehen.

Wir glauben an Sie!

DENKEN SIE AUCH AN DEN EDGE!

Daten sind das Herzstück jeder Sicherheits—initiative. Ein sicheres Datencenter setzt voraus, dass Sie auch den Zugriff auf Ihre Daten schützen. Und dazu gehört effektive Edge-Sicherheit. Schützen Sie Benutzer- und Gerätezugriff auf die Anwendungen und Daten in Ihren Datencenter-Umgebungen, um das gesamte Netzwerk besser abzusichern.

Juniper Networks

3050187-001-DE August 2023