ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

Cloud Security

Zero Trust Ganzheitliche Sicherheit statt Perimeterschutz.

Die Regulatorien nehmen laufend zu, die Bedrohungen durch Cyberangriffe ebenso. Unternehmen müssen ihre Sicherheitskonzepte verschärfen, um das Risiko unautorisierter Datenzugriffe zu minimieren. Zugleich steigen die Anforderungen an die Verfügbarkeit von Daten und Applikationen. Das klingt wie ein Widerspruch – doch das Sicherheitskonzept Zero Trust löst ihn auf.

Interne und externe Bedrohungen unterbinden

Daten und Applikationen müssen in zunehmendem Masse nicht mehr nur im klassischen Unternehmensperimeter verfügbar sein, sondern auch ausserhalb von ihm und auf unterschiedlichen Endgeräten. Cloud Computing, SaaS, Homeoffice und neue Arten des Datenaustauschs bieten immer mehr Einfallstore für Cyberangriffe. Das Zero-Trust-Modell ist einer der wirksamsten Ansätze, um solche Schwachstellen zu schliessen.

Zero Trust von ISPIN macht keinen Unterschied mehr zwischen Applikationen, Anwendern und Geräten, die sich im Firmennetzwerk oder ausserhalb von ihm befinden. Es behandelt eine interne Bedrohung, die im eigenen Firmennetz entsteht, genauso restriktiv wie eine externe. Das Sicherheitskonzept prüft jeglichen Datenverkehr und verlangt die eindeutige Authentifizierung aller Anwender.

Ihre Vorteile auf einen Blick

- Schutz sämtlicher Benutzer, Applikationen, Daten, VMs, Container und des Netzwerkverkehrs
- Sichtbarkeit in Echtzeit bis hin zur Prozessebene
- Bereitstellung aller Ressourcen für den Umstieg von Blacklist- auf Whitelist-Sicherheit
- Neue Ebene der Sicherheitsanalytik durch Kombination von maschinellem Lernen, der Erkennung anomaler Verhaltensweisen und intelligenter Algorithmen

Daten und Applikationen greifen über das Firmennetz hinaus

Der Paradigmenwechsel von einer reinen Sicht auf das interne Netzwerk hin zu einer ganzheitlichen Betrachtung hat erhebliche Auswirkungen auf die IT-Security-Architektur. Heute muss eine Sicherheitslösung den Schutz von Daten und Applikationen nicht mehr nur bis zu den Grenzen firmeneigener Perimeter, sondern innerhalb des kompletten Netzwerks gewährleisten. Ein Netzwerk, das durch die Cloud und ausgelagerte Services weit über die Grenzen der unternehmenseigenen IT-Architektur hinausragt.

Mit dem Zero-Trust-Modell gewinnen Unternehmen die Kontrolle über sämtliche Zugriffe auf Daten zurück. Seine praktische Umsetzung bedeutet für Firmen einen grossen Schritt hin zu umfassender Sicherheit. Denn alle Bereiche der IT sind betroffen und müssen kontrolliert werden: Netzwerke, Workloads, Geräte und Anwender. Eine zentrale Bedeutung kommt dabei der Sichtbarkeit zu; Zero Trust befähigt Unternehmen, ihre gesamte IT-Umgebung lückenlos zu überblicken und zu überwachen.

Mikrosegmentierung minimiert Angriffsflächen

Eine Herausforderung bei der Implementierung von Zero Trust stellt die Mikrosegmentierung dar. Es gilt, die richtige Granularität zu finden, um grosse Netzsegmente in kleinere aufzuteilen, die sich dann individuell überwachen lassen. Das garantiert sowohl die Minimierung der Angriffsflächen als auch den sparsamen Einsatz der Ressourcen für die Konfiguration und Verwaltung der Segmente.

Zwar gehört die Mikrosegmentierung seit Langem zum Zero-Trust-Ansatz, doch erst heute lässt sie sich praktisch nutzen. Sie löst sich von infrastrukturbedingten Gegebenheiten wie VLANs, operiert mit softwaredefinierten Overlay-Elementen und erlaubt eine flexible Abbildung von Policies auf der abstrahierten Infrastruktur. Dadurch lassen sich die Regelwerke viel engmaschiger definieren und konfigurieren. Ein softwaredefiniertes Framework ermöglicht die genaue Segmentierung von Workloads und Anwendungen, eine hohe Individualisierung der Regelwerke und dadurch einen äusserst soliden Schutz.

Die ISPIN-Lösung

Die Lösung von ISPIN betrachtet jedes Element der IT-Umgebung, um die Zero-Trust-Strategie umzusetzen. Sie verschafft eine lückenlose Sichtbarkeit – unabhängig davon, ob sich die Workloads und Applikationen im Rechenzentrum, in der Cloud oder in einer dynamischem VM-Umgebung befinden. Ein Whitelisting lässt nur diejenigen Applikationen und Protokolle zu, die erlaubt sind und sämtliche Sicherheitsanforderungen erfüllen. Alle anderen Elemente blockiert Zero Trust – oder es löst einen Alarm aus, um eine genaue Untersuchung zu ermöglichen.

Sensoren liefern Erkenntnisse in Echtzeit

Die ISPIN-Lösung basiert auf einer Kombination von Server- und Softwaresensoren sowie Netzwerk- und Hardwaresensoren mit einem schlanken Überbau. Die Sensoren sind mit einem Big-Data-Analyse-Cluster verbunden, der die Erkenntnisse durch anschauliche Grafiken in Echtzeit vermittelt. Weiter zeigt die Lösung Applikationsabhängigkeiten auf, schlägt automatisch Empfehlungen für das Regelwerk vor und reagiert sofort, wenn Abweichungen auftreten.

Migration von Blacklist zu Whitelist-Sicherheit

Die Segmente basieren nicht auf der Zugehörigkeit zu einer Infrastruktur, sondern bilden Scopes innerhalb der Lösung. Diese Scopes lassen sich anhand von operationellen Abhängigkeiten und Sicherheitsanforderungen verwalten. Für jedes Segment können IT-Verantwortliche ein eigenes Regelwerk definieren. Eine Enforcement Engine führt die Regelwerke aus, der Enforcement Agent konfiguriert die Host Firewall und gewährleistet eine durchgehende Kommunikation gemäss der Whitelist Policy.

Mit der Technologie von ISPIN können Unternehmen die Zero-Trust-Strategie in fünf Schritten erfolgreich umsetzen. Sie erlaubt die Migration von Blacklist- zu Whitelist-Sicherheit und verkleinert die Angriffsfläche massiv:

- Schritt 1: Durchgehende Sichtbarkeit der IT-Umgebung in Echtzeit
- Schritt 2: Abbildung von Applikationsabhängigkeiten
- Schritt 3: Automatische Empfehlung von Whitelist-Regelwerken
- Schritt 4: Einsatz von Whitelist-Regelwerken
- Schritt 5: Laufender Betrieb und automatische Überwachung der Zero-Trust-Prozesse

Zero Trust für Ihre Sicherheit

Seit über 20 Jahren plant und realisiert die ISPIN AG aus ihrer Zentrale in der Schweiz Sicherheitslösungen für die Netzwerk- und IT-Umgebungen ihrer Kunden. Unsere Zero-Trust-Lösung gibt Unternehmen ein hochleistungsfähiges Werkzeug in die Hand, um ein robustes Sicherheitskonzept mit Whitelists zu etablieren. Die Grundlagen für Ihren Erfolg mit dem Zero-Trust-Konzept bilden das grosse Fachwissen unserer IT-Spezialisten, das eigene lokale Cyber Defence Center und zahlreiche Zertifizierungen.

Möchten Sie mit Zero Trust Ihre IT-Sicherheit markant erhöhen, oder möchten Sie weitere Details zur ISPIN-Lösung erfahren?
Wir beraten Sie gerne. Senden Sie uns Ihre Anfrage:
cloudsecurity@ispin.ch

Alina Besmer, Sales Executive

ISPIN AG
Grindelstrasse 6
CH-8303 Bassersdorf
Tel.: +41 44 838 31 11
www.ispin.ch