

Ganzheitliche IT-Sicherheit erfordert ein Umdenken

In Security-Ökosystemen agieren

Lesedauer: 5 min

- » Ernste Sicherheitslage erfordert umfassende Konzepte.
- » Wirkungsvolle Maßnahmen wie der Aufbau eines Security Operations Center stellen für Unternehmen eine große Herausforderung dar.
- » Kompetenzträger und Integrationsspezialisten gesucht.
- » Konsequenz für den Channel: Kooperationen anstreben und ständig dazu lernen.
- » Kommunikations- und Wissensplattformen helfen weiter.

Der IT-Security-Markt befindet sich in einem grundlegenden Wandel. Die Komplexität der Herausforderungen steigt beständig und kann von einem Akteur allein nicht mehr bewältigt werden. „Für viele Systemhäuser und Integratoren bedeutet dies, noch stärker miteinander zu kooperieren und das eigene Security-Know-how kontinuierlich zu erweitern“, sagt Patrick Olschewski, Senior Business Development Manager bei Tech Data Advanced Solutions. Value-Added-Distributoren können hierbei ihren Partnern wertvolle Unterstützung bieten.

Die Sicherheitslage in IT-Infrastrukturen verschärft sich weiter. Internet-of-Things (IoT)-Anwendungen und die mobile Arbeitswelt mit Smartphones und Tablets schaffen neue Angriffspunkte für Cyberkriminelle.

Zudem steigt die [Professionalität und Aggressivität der Cyberangriffe](#). Kennzeichen dafür sind zum Beispiel Attacken mit Verschlüsselungstrojanern, die Unternehmensprozesse komplett zum Stillstand bringen können. Stark ansteigend sind auch gezielte Angriffe, die einen dauerhaften Zugriff auf die IT-Ressourcen des Unternehmens zum Ziel haben. Die als „Advanced Persistent Threats (APT)“ bezeichneten Attacken setzen ein hohes technisches Know-how voraus.

Vor diesem Hintergrund sind strategische Investitionen in die IT-Sicherheit nötig. „IT-Security muss als ganzheitlicher Prozess betrachtet werden, der technische, organisatorische und personelle Maßnahmen miteinander verbindet“, betont Patrick Olschewski.

Unternehmen sind oft überfordert

Zu den wichtigsten Handlungsfeldern einer ganzheitlichen IT-Security gehören laut einem [aktuellen Trendpaper](#) von Crisp Research im Auftrag von Tech Data Advanced Solutions der Aufbau eines Security Operations Center (SOC) und das Identity & Access Management (IAM).

Das SOC lässt sich wie eine Kommandozentrale der NASA beschreiben. Security-Experten sitzen dort vor großen Bildschirmen, die in Echtzeit den Zustand der Infrastrukturen anzeigen, über die aktuelle Bedrohungslage informieren und im Security-Ernstfall die sicherheitsrelevanten Maßnahmen einleiten.

Um Cyber-Angriffen wirkungsvoll vorzubeugen, müssen Identitäten und Zugriffsrechte definiert und verwaltet werden. Das IAM enthält klare Regeln und Rollen, wer zu welchem Zeitpunkt auf die Netzwerke und Unternehmensdaten zugreifen darf und wie er sich gegenüber den IT-Systemen auszuweisen hat.

Mit der Umsetzung beider Maßnahmen sind Unternehmen oftmals überfordert, zudem fehlen personelle Ressourcen.

Diese Situation eröffnet Systemhäusern und Integratoren interessante Geschäftspotenziale. „Ob beim Aufbau und Betrieb eines Security Operations Center oder bei der Einführung eines Identity & Access Managements: Unternehmen suchen nach Kompetenzträgern, die bei diesen Aufgaben tatkräftig helfen“, erläutert Patrick Olschewski.

Investitionen steigen zweistellig

Eine weitere Hürde für ganzheitliche Konzepte sind klassische Security-Silos. Nicht selten sind in großen Unternehmen bis zu 80 Security-Lösungen im Einsatz, die einzeln betrachtet gut funktionieren, aber in der Summe keinen ausreichenden Schutz mehr bieten. „Der Weg zur ganzheitlichen IT-Security führt über die Integration vorhandener Technologien, Produkte und Services – eine Aufgabe, für die der Channel prädestiniert ist“, so Patrick Olschewski.

Eine Umfrage im Rahmen des [Trendpaper ‚Security‘](#) fasst die Geschäftspotenziale in konkrete Zahlen. Demnach will fast die Hälfte der befragten IT- und Business-Entscheider im nächsten Geschäftsjahr zwischen 10 und 20 Prozent mehr Budget für Security bereitstellen.

Aufeinander zugehen, miteinander arbeiten

Die Komplexität einer ganzheitlichen IT-Security erfordert aber auch beim Channel ein Umdenken. Viele Systemhäuser oder Integratoren können heute allein die Themen und Aufgaben nicht abdecken.

Erfolg versprechen Security-Ökosysteme, in denen Value-Added-Distributoren, Channel-Partner und Hersteller eng zusammenarbeiten. Mit diesem Schritt lassen sich alle Security-Komponenten zusammenführen und auf die individuellen Sicherheitsanforderungen des jeweiligen Kunden zuschneiden.

Für Tech Data Advanced Solutions ist es wichtig, dass die Channel-Partner aufeinander zugehen und gemeinsam individuelle Lösungen für die Kunden entwickeln. Patrick Olschewski: „Wichtig für den Erfolg von Security-Ökosystemen sind Kommunikationsplattformen, auf denen Partner sich persönlich treffen, untereinander austauschen und wertvolle Impulse für Ihr Geschäft bekommen.“

Zu diesem Zweck veranstaltet Tech Data Advanced Solutions regelmäßige TrendUps. Die Tagesveranstaltungen sind von Experten für Experten. Sie informieren über Themen, die die Investitionen von morgen bestimmen werden. Zu den Inhalten der TrendUps gehören neben Vorträgen zu aktuellen Entwicklungen auch konkrete Anwendungsszenarien. Wichtig bei den TrendUps ist ein offener Dialog. Das Veranstaltungsformat bietet deshalb den Teilnehmern genügend Raum, sich persönlich mit den Experten auszutauschen und ihr Netzwerk zu erweitern.

Ende letzten Jahres startete die Veranstaltungsreihe erfolgreich mit dem Thema ‚Security‘. Aufgrund der positiven Resonanz ist ein weiterer TrendUp Security für die zweite Jahreshälfte geplant.

Vorher findet Mitte März in Frankfurt/M ein Executive Circle zu IT-Security und AI statt. Top-Entscheider und Experten diskutieren dort zentrale Fragen zum Einsatz Künstlicher Intelligenz in der IT-Security. Einer der inhaltlichen Schwerpunkte sind die Geschäftschancen für den Channel.

Know-how-Transfer stärken

Nur Systemhäuser und Integratoren, die ihr Wissen und ihre Expertise kontinuierlich erweitern, werden sich langfristig im IT-Markt behaupten können. Tech Data Advanced Solutions unterstützt seine Partner dabei mit Marktuntersuchungen und Trendanalysen.

Beispiel dafür ist die Studie [„Digital Infrastructure 2020 – IT-Infrastruktur für das digitale Zeitalter“](#).

„Die Studie enthält eine detaillierte Analyse der aktuellen IT-Infrastrukturrends und konkrete Handlungsempfehlungen für den Anwender. Mit diesem Werkzeug können sich unsere Channel-Partner auf den digitalen Wandel in den Rechenzentren rechtzeitig einstellen und ihr Geschäft entsprechend ausrichten“, beschreibt Patrick Olschewski die Vorteile.

Neben der Studie gibt es noch [sieben Trendpapiere](#) mit vertiefenden Informationen, darunter eines zu ‚Security‘. Die Trendpapiere können von den Partnern als ‚White Label-Lösung‘ mit eigenem Logo für Marketing-Zwecke genutzt werden.