Fünf vermeidbare Fehler bei Investitionen in die Security

Inhaltsverzeichnis

Zusammenfassung

Wer mit digitalen Innovationen Schritt halten will, muss Investitionen sorgfältig prüfen. Das kostet Zeit und Mühe, insbesondere wenn moderne Technologien integriert werden sollen: Neue Tools und Investitionen erhöhen die Komplexität und Anfälligkeit der Unternehmens-Security – und oft führen neue Software und Dienste zu einer unpraktischen Heterogenität und isolierten Systemen, die Defizite bei der Kommunikation und Zusammenarbeit aufzeigen und Reaktionen ausbremsen. Der Schutz des Unternehmens vor hochkomplexen Cyber-Bedrohungen erfordert eine einheitliche, integrierte und automatisierte Security-Architektur, durch die Abläufe effizienter werden. Diese Architektur muss so umfassend sein, dass sich das Risiko für die gesamte digitale Angriffsfläche verringert. Auch sollte die Security bereits integriert sein, damit Sicherheitslücken geschlossen und Reaktionszeiten verkürzt werden.

Einleitung

Unternehmen sind heutzutage stark vernetzt, immer online und müssen mit schnellen digitalen Innovationszyklen mithalten können. Die Folgen sind weitreichend: Die Zahl der Geräte, Anwendungen und Inhalte im Netzwerk steigt unablässig, der Security-Perimeter wird aufgeweicht, das Netzwerk verliert an Transparenz und das IT-Team wird mit noch mehr manuellen Aufgaben belastet. Dazu kommen immer mehr Angriffsvektoren, die auf die neuen Randbereiche des Netzwerks abzielen. IoT-Geräte (Internet der Dinge), cloudbasierter Datenspeicher, Cloud-Anwendungen, mehr mobile Geräte, neue Zweigstellen und deren Hybridbenutzer – das alles führt zu einzigartigen Sicherheitslücken, Komplexitäten und Risiken. Aber damit nicht genug: Die Fülle an Security-Produkten und -Anbietern schwächt die Sicherheit zusätzlich, wodurch laufende Angriffe oft unbemerkt bleiben – und wenn sie erkannt werden, greifen Sicherheitsmaßnahmen und Abwehrreaktionen viel zu langsam. Während Netzwerke und ihre digitale Angriffsfläche wachsen, werden Cyberangriffe zunehmend automatisierter, ausgefeilter und treffsicherer. Cyber-Kriminelle nutzen gezielt neue Sicherheitslücken aus, die durch die Cloud-Skalierung und Automatisierung entstanden sind. Weiterentwickelte Angriffstechniken – einige mit polymorphen Komponenten, die mehrere Randbereiche gleichzeitig attackieren können –, richten sich speziell gegen solche anfälligen Ziele.

Nur eine einheitliche Sicherheitslösung bietet Schutz vor diesen neuen Risiken und Angriffsvektoren. Notwendig ist ein zukunftsfähiges Sicherheitsprofil, das

- die gesamte Angriffsfläche schützt und sich für neue Randbereiche einfach erweitern lässt,
- alle Phasen eines Angriffszyklus erkennt und Sicherheitsmaßnahmen durchsetzt,
- einheitliche kontextbezogene Sicherheitsrichtlinien ermöglicht,
- Umgebungen mit mehreren Anbietern und Hybrid-Clouds mit cloudnativer Security unterstützt,
- Risiken bewertet und das Sicherheitsprofil automatisch für eine proaktive Bedrohungsabwehr anpasst und
- alle Lösungen überwacht und verwaltet, damit schlanke IT-Teams die Security skalieren und so sämtliche Sicherheitsanforderungen des Unternehmens erfüllen können.

Eine kontextbezogene, leistungsstarke Security, eingebettet auf Konnektivitäts- und Rechnerebene, ist für erfolgreiche, unkomplizierte digitale Innovationen entscheidend. Mit einer einheitlichen, selbstheilenden Umgebung für alle Verbindungen – von Geräten und Benutzern bis hin zu Anwendungen – lassen sich Sicherheitslücken minimieren und zeitnahe, koordinierte Präventiv- und Abwehrmaßnahmen über den gesamten Angriffslebenszyklus hinweg bereitstellen.

Fehler Nr. 1: Zu viel Vertrauen

Angesichts von „vertrauenswürdigen“ Geräten außerhalb des Netzwerk-Perimeters und „nichtvertrauenswürdigen“ Geräten im Netzwerk, die auf Vieles unkontrolliert zugreifen können, hat das perimeterbasierte Sicherheitsmodell ausgedient. Hybridbenutzer, die On-Premises und außerhalb des Unternehmens Public und Private Clouds nutzen, brauchen freien Zugriff auf das Netzwerk und auf Anwendungen. Das bedeutet: Noch strengere Zugriffsberechtigungen sind notwendig.

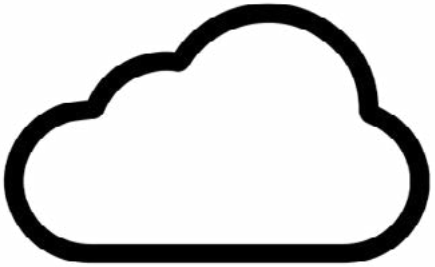
Best Practices sehen deshalb ein Zero-Trust-Security-Modell vor. Bei diesem Modell wird standardmäßig keinem Benutzer oder Gerät vertraut. Stattdessen wird der Zugriff auf Ressourcen anhand der Benutzeridentität gewährt und Berechtigungen werden abhängig von den Zuständigkeiten eines Benutzers erteilt. Zero-Trust-Prinzipien verringern Risiken durch anfällige oder infizierte Geräte sowie nachlässige oder böswillige Benutzer. Das ist heute ein besonders wichtiger Aspekt, da der Perimeter durch Homeoffices und den massiven Anstieg neuer Endgeräte im Netzwerk nicht nur größer, sondern auch fragmentierter geworden ist. Richtig implementiert, wird das Zero-Trust-Modell zudem mit Bedrohungsinformationen in Echtzeit „gefüttert“. So lassen sich auch ultraschnelle, ausgefeilte Cyberangriffe erkennen und abwehren. Auch bietet dieses Modell viele weitere Möglichkeiten, um die Verbreitung von Angriffen im Netzwerk und den Missbrauch von Berechtigungen proaktiv zu verhindern.

Angesichts mehrerer Möglichkeiten für den Zugriff auf und die Nutzung von Daten in Multi-Cloud-Umgebungen muss es eine starke Netzwerk-Segmentierung und Zugangskontrolle geben. Das ist eine Voraussetzung für die Implementierung und Durchsetzung eines Zero-Trust-Security-Modells. Die unternehmenseigene Sicherheitsarchitektur sollte Geräte, die sich mit dem Netzwerk verbinden, automatisch erkennen, Benutzer sicher identifizieren und den Zugang anhand der Benutzerberechtigungen bei der Anmeldung erteilen oder verweigern können.

Eine konsequent durchgesetzte Zero-Trust-Security erfordert zudem eine interne Netzwerk-Segmentierung, die die seitliche Bewegung von Angreifern und Malware begrenzt sowie die Wahrscheinlichkeit und Folgen einer Datenpanne verringert. Es spielt keine Rolle, ob sich Anwendungen im Netzwerk oder in der Cloud befinden: Benutzer und Applikationen können beim Zero-Trust-Modell unabhängig vom Aufenthaltsort sichere, zuverlässige Verbindungen herstellen.

Eine Lösung für den Zero-Trust-Network-Access (ZTNA) basiert auf diesem Sicherheitskonzept. Sie regelt den Anwendungszugriff mithilfe zahlreicher Komponenten wie Clients, Proxys, Authentifizierung und Schutzfunktionen. Tatsächlich ist das Ganze aber noch komplizierter als es sich anhört, weil in den meisten Unternehmen die einzelnen Komponenten von verschiedenen Anbietern stammen, unterschiedliche Betriebssysteme haben und über mehrere Management- und Konfigurations-Konsolen gesteuert werden müssen. Fakt ist: Auf so einer Grundlage ist es nahezu unmöglich, ein ZTNA-Modell zu schaffen, dass alle Anbieter abdeckt.

Über 94 % der Unternehmen haben Cloud Computing eingeführt, davon sind 84 % Multi-Clouds.[1]



Unternehmen nutzen durchschnittlich fast fünf verschiedene Cloud-Plattformen.[2]

Fehler Nr. 2: Isolierte Bewertung von Cloud-Plattformen und Anwendungssicherheit

Unternehmen haben damit zu kämpfen, einheitliche Sicherheitsrichtlinien in Multi-Cloud-Umgebungen durchzusetzen. Das Management der Multi-Cloud-Security mit selbstentwickelten Lösungen ist komplex. Konsequente Sicherheitskontrollen, die Regelung und Optimierung des Anwendungszugriffs sowie die Aufrechterhaltung der unternehmensweiten WAN-Performance sind alles andere als einfach. Dies gilt umso mehr, wenn mehrere Lösungen von unterschiedlichen Anbietern in verschiedenen Instanzen eingesetzt werden.

Die größten Risiken bei Multi-Cloud-Bereitstellungen entstehen durch viele zusätzliche Security-Einzellösungen und Fehlkonfigurationen. Zudem können Hybrid-Cloud-Implementierungen außerhalb des Netzwerk-Perimeters, die über das öffentlich zugängliche Internet erreichbar sind, zu Problemen mit unautorisierten Zugriffen führen.

Um das Potenzial der Cloud voll auszuschöpfen, muss die Security die effektive Nutzung von Cloud-Ressourcen mit Funktionen wie einer automatischen Skalierung unterstützen und verschiedene Netzwerk-Bereiche erkennen können. Nur so lässt sich die Granularität erreichen, die eine integrierte cloudnative Sicherheit in mehreren Cloud-Implementierungen erfordert.

Ein integriertes Management von Security-Konfigurationen ist daher für die Cloud-Sicherheit unverzichtbar. Für Multi-Cloud-Umgebungen müssen sich Erkennung und Durchsetzung für die gesamte digitale Angriffsfläche koordinieren lassen, damit schnell auf Bedrohungen reagiert werden kann, die Fehlkonfigurationen ausnutzen. Cloudnative, einheitliche und kontextbezogene Sicherheitslösungen, die Risiken anhand von Daten bewerten und den Schutz automatisch anpassen, sind für Hybrid-Cloud-Anwendungen in unterschiedlichen Clouds ein Muss.

Fehler Nr. 3: Schwerpunkt auf Erkennung statt auf schnelle Prävention

Cyber-Kriminelle setzen zunehmend auf automatisierte, gezielte Angriffe. Bei diesen gut koordinierten Attacken gibt es nur ein begrenztes Zeitfenster, in dem der Angriffsablauf erkannt und gestoppt werden kann. Mit Automatisierung, Cloud-Skalierung und künstlicher Intelligenz (KI) können Cyber-Kriminelle sogar noch komplexere polymorphe Angriffskomponenten lancieren. Solche Angriffe lassen sich mit einer manuellen Erkennung und Reaktion nicht abwehren – schon gar nicht bei weitläufigen Netzwerk-Perimetern.

Um das Unternehmen wirksam vor neuen, schnellen Angriffstaktiken zu schützen, müssen Sie Ihr Sicherheitsprofil rechtzeitig „umprogrammieren“ können. Nur so lässt sich der Ablauf eines Angriffs unterbrechen, bevor er erfolgreich ist. Dafür müssen Sie wissen, wie gut Ihre Security nach der Erkennung eines Angriffs zu einer Bedrohungsabwehr übergeht, die für alle unterschiedlichen Umgebungen funktioniert, wie präzise und schnell Erkennungsfunktionen arbeiten – und noch mehr: Gibt es z. B. einheitliche Datensätze, die eine ganzheitliche Erkennung statt einer symptombasierten Erkennung ermöglichen? Bewerten Sie die Qualität der KI sowie den weltweiten Austausch von Bedrohungsinformationen in Communitys, damit Sie niemals zum „zweiten Patient Null“ werden. Sehen Sie sich außerdem an, ob die Lösung über den gesamten Angriffszyklus hinweg neue Präventionsmaßnahmen entwickelt und diese automatisch an verschiedenen Technologien und Geräte sendet. Denn das ist der Moment, in dem Ihre Verteidigung beginnt.

Zweitens muss Ihr Security-Team in Echtzeit die neuesten Bedrohungsinformationen erhalten. Ein gut trainierter Klassifikator für maschinelles Lernen (ML) kann echte Bedrohungen von falsch-positiven Ergebnissen unterscheiden. Security-Teams können so ihre Untersuchungen und Bedrohungsabwehr auf tatsächliche Angriffe konzentrieren. Diese Klassifikatoren lassen sich in unterschiedlichste Sicherheitslösungen integrieren. Inline-Lösungen können Bedrohungen auch automatisch an Verhaltensanomalien erkennen und mithilfe vordefinierter Playbooks reagieren. ML kann zusätzlich die Datenerfassung und -analyse unterstützen und bietet Threat Huntern und SOC-Analysten (Security Operations Center) die notwendigen Informationen, um hochkomplexe, schnell fortschreitende Angriffe in kürzester Zeit zu erkennen und abzuwehren.

Ein robustes Netzwerk- und Sicherheitsprofil nutzt die Cloud-Skalierung und eine fortschrittliche KI, um automatisch in nahezu Echtzeit den Benutzerzugriff auf Anwendungen in der gesamten Umgebung zu schützen. Der strategische Einsatz von KI ist entscheidend: Hiermit erreichen Sie eine koordinierte Erkennung, Prävention und Reaktion über die gesamte digitale Angriffsfläche und den Lebenszyklus hinweg – einschließlich konvergierter Netzwerke und Sicherheitsfunktionen für Randbereiche, Clouds, Endpunkte und Benutzer.

Fehler Nr. 4: Erweiterung der Konnektivität ohne native Security

Um die wachsende Gerätezahl in Netzwerken und die damit verbundenen Cyber-Bedrohungen in den Griff zu bekommen, implementieren viele Unternehmen zahlreiche isolierte Sicherheitsprodukte, die sich nicht integrieren lassen sowie schwer zu überwachen und zu verwalten sind. Einige Firmen nutzen sogar für den gleichen Anwendungsfall unterschiedliche Hardware-, Software- und As-a-Service-Anbieter. Dies erhöht die Komplexität der Netzwerk-Sicherheit zusätzlich.

Cloudbasierte Anwendungen sind für Unternehmen unerlässlich, um digitale Innovationen umzusetzen. Sie erweitern aber auch das Netzwerk und schaffen neue Netzwerk-Ränder. Unternehmen müssen agil und anpassungsfähig sein, um eine einheitliche Anwendungsverfügbarkeit und Nutzererfahrung zu gewährleisten – unabhängig davon, wo jemand arbeitet. Heutige Netzwerke sind zwar sehr agil, doch auf die meisten Sicherheitslösungen trifft das nicht zu. Daher können in einer adaptiven Cloud-Netzwerkumgebung kritische Ressourcen und Daten ungeschützt bleiben, obwohl die Sicherheitslösungen eigentlich mit dieser Dynamik Schritt halten sollten. Solche Probleme lassen sich nur mit einer Lösung vermeiden, die Security- und Netzwerk-Funktionen in einem einzigen integrierten System konvergiert, das bis zu jedem Randbereich des Netzwerks erweitert werden kann.

Achten Sie bei Bereitstellungsmodellen auf Einheitlichkeit. Sie sollten Hardware-, Software- und As-a-Service-Angebote passend zu Ihrem einzigartigen Sicherheitsprofil kombinieren können. Hohe Verfügbarkeit (HA) durch 5G- und LTE-Technologien sowie die Umstellung auf ein softwaredefiniertes WAN (SD-WAN), um Ressourcen besser zu nutzen und die Gesamtbetriebskosten (TCO) zu senken, sollten ebenfalls in die Bewertung einer Sicherheitslösung einfließen. So stellen Sie sicher, dass Sie digitale Innovationen – z. B. bei der Einführung neuer Angebote – problemlos umsetzen können.

32 %

der IT-Verantwortlichen sehen in „zu vielen manuellen Prozessen“ ein großes Sicherheitsproblem.[3]

Fehler Nr. 5: Keine Berücksichtigung Ihres gesamten Ökosystems

Eine der größten Herausforderungen bei der schnellen Erweiterung des Netzwerk-Randes besteht darin, dass viele notwendige Technologien nicht zusammenarbeiten. Die meisten Cyber-Security-Lösungen „wissen“ nichts voneinander. Diese mangelnde Integration führt zu mehr Komplexität, bremst die Arbeit von Security-Teams aus und macht das Unternehmen anfällig für Angriffe. Erschwerend kommt hinzu, dass digitale Innovationen oft nur vereinzelt ohne eine einheitliche Sicherheitsstrategie oder ein gemeinsames Security-Konzept realisiert werden. In den meisten Unternehmen finden sich daher zahlreiche isolierte Security-Tools für ein bestimmtes Sicherheitsproblem oder Netzwerk-Segment. Dies verringert die Transparenz und die Kontrolle, wodurch Bedrohungen übersehen und Reaktionen ineffektiv werden.

Solche Probleme lassen sich gemeinsam mit Partnern, Bedrohungsforschern und Anbietern angehen, die sich auf Threat Intelligence (Bedrohungsinformationen) spezialisiert haben. Einrichtungen wie die FortiGuard Labs arbeiten mit der internationalen Intelligence-Community zusammen, um Best Practices auszutauschen und die Ausbreitung von Angriffen zu verhindern. Diese engagierte Community trägt entscheidend zur Erkennung von Millionen Bedrohungen und zum Schutz von Unternehmen bei – z. B. mit weltweiten Fabric-Implementierungen oder Partnern, die einen zweiten „Patienten Null“ durch der Community bereits bekannte Bedrohungen verhindern. Dank dieser Zusammenarbeit lassen sich Transparenz, Erkennung und koordinierte Reaktionen erfolgreich vereinheitlichen.

Wählen Sie eine Lösung, die sich problemlos in Ihre vorhandene Umgebung integrieren lässt. Damit erhalten Sie einen einheitlichen Schutz mit nativer Erkennung und Reaktion sowie ein umfassendes Ökosystem, das die erweiterte Angriffsfläche sichert. Eine moderne Security-Lösung sollte zudem über APIs (programmierbare Schnittstellen für Anwendungen), Konnektoren und DevOps-Automatisierungstools und -Skripte in unterschiedlichste Drittlösungen integrierbar sein.

Eine offene API-Architektur ermöglicht die Kommunikation und Synchronisation zwischen verschiedenen Geräten. Kundenspezifische Konnektoren bieten eine bessere Integration und Interoperabilität und sorgen für eine Echtzeitkommunikation und automatische Updates im gesamten Ökosystem. Eine Bibliothek mit DevOps-Tools und -Skripten gewährleistet eine schnelle, anpassbare Bereitstellung und Verwaltung und skaliert die Funktionalität schlanker Security-Teams. Mit einer derart integrierten Sicherheitsarchitektur erhalten Sie einen einheitlichen Schutz, der alle Netzwerk-Ränder sichert – unabhängig davon, wo sie sich befinden.

35 % der IT-Verantwortlichen verlassen sich auf nichtintegrierte Security-Architekturen.[4]

Fazit

In Zeiten, in denen Veränderung die einzige Konstante ist und vorhandene Umgebungen schnell mit neuen Innovationen erweitert werden, sind Einfachheit und Anpassungsfähigkeit entscheidend. Da Netzwerke immer komplexer und heterogener werden, benötigen Unternehmen eine breite, integrierte und automatisierte Sicherheitsplattform. Nur so lässt sich die Erkennung und Verhinderung von Angriffen sowie die Reaktion auf Vorfälle vereinfachen und optimieren. Die Vorteile liegen dabei auf der Hand: Das Unternehmen erhält volle Transparenz, kann Sicherheitslücken schließen und Komplexität verringern, während Security-Abläufe und Reaktionen auf Vorfälle beschleunigt werden.

Eine erfolgreiche digitale Erfahrung bietet vertrauenswürdige, leistungsstarke Verbindungen zwischen Benutzern, Geräten und Anwendungen in unterschiedlichsten Umgebungen und Cloud-Konfigurationen – auch weltweit. Allein die Konsolidierung isolierter Bereiche ist jedoch nicht genug: Notwendig ist eine Koordinierung, Vereinheitlichung und Konvergenz von Netzwerk und Security gemeinsam mit Partnern. Unser Tipp: Vermeiden Sie die hier beschriebenen fünf Fehler bei der Bewertung Ihrer nächsten Sicherheitsinvestition, um erfolgreich Sicherheitslücken zu schließen, isolierte Systeme zu vereinheitlichen und Reaktionszeiten zu verkürzen.

[1] „RightScale 2019 State of the Cloud Report from Flexera“. Flexera und RightScale, 27. Februar 2019.

[2] Nick Galov: „Cloud Adoption Statistics for 2021“. Hosting Tribunal, 19. Januar 2021.

[3] „The IT Infrastructure Leader and Cybersecurity: A Report on Current Priorities and Challenges“. Fortinet, 18. August 2019.

[4] Ebd.

www.fortinet.com/de

5-vermeidbare-Fehler-E-Book_DE

914666-0-0-DE