FORTINET

Next Generation Endpoint Security: Welche Verbesserungen sind notwendig?

Wie IT-Infrastrukturleiter Endpunkte schützen und die betriebliche Effizienz optimieren können

Inhaltsverzeichnis

FORTINET

Zusammenfassung

Endpunkte sind nach wie vor eines der beliebtesten Ziele von Cyber-Angriffen. Kompromittierte Laptops, Smartphones oder IoT-Geräte (Internet der Dinge) können zur lateralen Verbreitung von Bedrohungen im Netzwerk beitragen, andere Endpunkte im Unternehmen infizieren und Angreifern Zugriff auf kritische Ressourcen ermöglichen. Das schwächt nicht nur die Sicherheit, sondern hält auch Mitarbeiter von wichtigen Aufgaben wie der Verbesserung der Netzwerk-Leistung und der Optimierung von Betriebsabläufen ab.

Um diesen Herausforderungen zu begegnen, benötigen IT-Infrastrukturleiter integrierte Netzwerk- und Security-Lösungen, die Endpunkte schützen, betriebliche Folgen einer wachsenden Angriffsfläche minimieren und Skalierungen unterstützen. Durch das enge Ineinandergreifen von Endpunkt- und Netzwerk-Security lassen sich wichtige Verbesserungen für einen ganzheitlichen Schutz des Unternehmens realisieren – von einer risikobasierten Transparenz über alle Endgeräte, richtlinienbasierten Zugriffskontrollen und gemeinsam genutzten Echtzeit-Bedrohungsinformationen bis hin zu automatisierten Security-Reaktionen und -Workflows.

Nur 26 % der führenden Technologie-Unternehmen geben an, auf Cyber-Angriffe „gut vorbereitet“ zu sein.[1]

Einleitung: IT-Infrastrukturleiter und der Endpunkt-Schutz

Das exponentielle Wachstum bei Endbenutzer-Geräten erweitert die Endpunkt-Angriffsfläche in rasantem Tempo, was durch die zunehmende Verbreitung vernetzter Geräte wie IoT-Sensoren, Wearables, Steuerungstechnik (ICS) und autonome Fahrzeuge noch verstärkt wird. Infolgedessen steigt die Zahl der erfolgreichen Cyber-Angriffe unablässig: Allein in den letzten 12 Monaten kam es in der Hälfte der Unternehmen zu mindestens einem Sicherheitsvorfall, der durch ein Endgerät verursacht wurde.[2] Die meisten Unternehmen erwarten, dass IT-Infrastrukturleiter solche Probleme lösen – von denen fast drei Viertel (73 %) direkt für die Endpoint Security zuständig sind.[3]

Abgesehen von den Bedrohungen selbst gibt es schwerwiegende Probleme bei der Netzwerk- und Endpunkt-Security, die meistens voneinander getrennt sind und nicht miteinander kommunizieren können. Eine Integration verschiedener Sicherheitskomponenten ist jedoch mit herkömmlichen Ansätzen für den Netzwerk- und Endpunkt-Schutz nicht möglich. IT-Infrastrukturleiter müssen deshalb diese isolierten Strukturen auflösen und durch eine Security-Architektur ersetzen, die Netzwerk- und Sicherheitselemente – und auch Endpunkte – in eine intelligente Security-Plattform integriert. Diese Transformation erfordert vier grundlegende Verbesserungen: höhere Risiko-Transparenz, dynamische Zugriffskontrollen, gemeinsam genutzte Bedrohungsinformationen und automatisierte Security-Workflows.

56 %

der IT-Infrastrukturleiter müssen über die Hälfte ihrer Zeit in die Cyber-Security investieren.[4]

1. Anforderung: Höhere Risiko-Transparenz

Transparenz ist eine wichtige Voraussetzung für eine effektive Endpunkt-Security. Schließlich kann man nur schützen, was man sehen kann. Infrastruktur-Teams müssen den Endpunkt-Status inner- und außerhalb des Unternehmensnetzwerks genau identifizieren können, wie z. B. ungepatchte Schwachstellen, veraltete Software, potenziell unerwünschte Anwendungen, riskante Verhaltensweisen oder Richtlinienverstöße. Die risikobasierte Transparenz hängt von einem klaren Verständnis der Gefährdungen durch Endpunkte ab und muss auch Benutzeridentitäten, Schutzstatus und Sicherheitsereignisse abdecken.

IT-Infrastrukturleiter sollten daher eine Endpoint-Security-Lösung wählen, die Telemetrie-Daten in Echtzeit mit anderen Security-Tools wie Firewalls, Sandboxes und Web-Filtern austauscht und ein nahtloses Ineinandergreifen von Security-Workflows und Bedrohungsabwehr bietet. Fehlen jedoch die richtigen Integrationspunkte, bedeutet das für IT-Teams einen enormen Zeitaufwand. Vermeiden lässt sich dies mit einer Next Generation Endpoint Security, die mit zentralen Management-Tools einen sofortigen Überblick über den aktuellen Sicherheitsstatus liefert.

8,19 MIO. USD

betragen die durchschnittlichen Gesamtkosten einer Datenschutzverletzung in den USA.[5]

2. Anforderung: Moderne Zugriffskontrollen

Ist die Risiko-Transparenz gegeben, benötigen IT-Infrastrukturleiter eine granularere, dynamischere Netzwerk-Zugriffskontrolle. Die Endpunkt-Security sollte Richtlinien und Kontrollen auf allen Geräten durchsetzen und vor Angriffen schützen, die von Endgeräten ausgehen können. Dabei muss sichergestellt werden, dass Endpunkte alle Compliance- und Sicherheitsstandards erfüllen, bevor ein Zugang zum Netzwerk gewährt wird. Auch sollte der Endpunkt-Schutz unerwünschte und gefährdete Endpunkte analysieren und in Quarantäne setzen können.

Ein wichtiger Teil dieses Prozesses ist das Gruppieren von Endgeräten in absichtsbasierte Segmente, um eine dynamische Zugriffskontrolle zu erhalten. Dies erfordert optimierte Implementierungs- und Management-Funktionen – einschließlich Compliance-Aktivitäten und Reporting –, da ohnehin schon überlastete Infrastruktur-Teams solche Aufgaben nicht manuell erledigen können.

67 %

der führenden Technologie-Unternehmen sehen im Fachkräftemangel die Ursache für ihre schlechte Anpassung an neue Entwicklungen.[6]

3. Anforderung: Gemeinsam genutzte Bedrohungsinformationen

Je gezielter und virulenter Angriffe werden, desto kürzer wird das Zeitfenster für eine effektive Incident Response. Schneller funktioniert die Abwehr, wenn Bedrohungsinformationen sofort ausgetauscht werden. Dafür müssen Endpoint- und Netzwerk-Security-Tools umfassend integriert sein. Fängt dann eine Netzwerk-Komponente eine neue Bedrohung ab, sendet sie die Informationen automatisch sofort an andere Endpunkte und Sicherheitslösungen im gesamten Unternehmen.

Durch den Informationsaustausch in Echtzeit erhalten Infrastruktur-Teams ein vollständiges, genaues Bild des aktuellen Netzwerk-Sicherheitsprofils. Der Endpunkt-Schutz vergleicht Ereignisse beim Work-Traffic mit Threat-Intelligence-Feeds, um Warnungen zu überprüfen, Bedrohungen zu erkennen und potenzielle Kompromittierungen zu entdecken. Eine tiefe Integration trägt dazu bei, die „Spreu vom Weizen“ zu trennen und Fehlalarme zu minimieren. Auch wird so ein versehentliches Übersehen von Warnungen verhindert und Teams können sich ein genaueres Bild vom aktuellen Netzwerk-Sicherheitsprofil machen.

Um die Mitarbeiterproduktivität zu maximieren, sollten IT-Infrastrukturleiter die Endpoint-Security ggf. zusätzlich durch einen Security Rating Service stärken. Solche Dienste werden als Abonnement angeboten und bieten hilfreiche Tools, um das eigene Sicherheitsprofil mit Marktbegleitern und anerkannten Standards zu vergleichen. Manchmal sind auch detaillierte Anleitungen und Checklisten verfügbar, um das Sicherheitsprofil systematisch zu verbessern und Fortschrittsberichte für das leitende Management zu erstellen.

206 Tage

dauert es im Durchschnitt, bis eine Datenpanne bemerkt wird – 5 % länger als im Vorjahr.[7]

4. Anforderung: Automatisierte Security-Workflows

Die Automatisierung wichtiger Security-Workflows stellt eine wesentliche Verbesserung dar. IT-Infrastrukturleiter können so einen wirksamen Endpunkt-Schutz realisieren und zugleich personell begrenzte Teams entlasten. Das gesamte Sicherheitsprofil des Unternehmens profitiert von einer automatisierten Endpoint-Security mit Schwachstellen-Management, Bedrohungserkennung und -abwehr sowie einer verlässlichen Regelkonformität von Endpunkten. Im Folgenden sind die wichtigsten Funktionen aufgeführt, die für eine solche Endpoint-Security-Lösung notwendig sind:

Schwachstellen-Management: Hiermit lässt sich viel automatisieren, z. B. das Patching der Software und Betriebssysteme auf Endgeräten oder die Behebung kleinerer Sicherheitsprobleme, ohne dass das IT-Team eingreifen muss. Solche Funktionen tragen zum Schließen grundlegender Verteidigungslücken im Endpunkt-Sicherheitsprofil bei und entlasten zugleich das Infrastruktur-Team von manuellen Routine-Aufgaben.

Automatisierung der Incident Response: Eine automatisierte Reaktion auf Sicherheitsvorfälle und deren Eindämmung verkürzt die erfolgreiche Bedrohungsabwehr, da der Security-Workflow kein Eingreifen eines Mitarbeiters erfordert. Die Endpoint-Security sollte verdächtige oder gefährdete Endpunkte automatisch in Quarantäne setzen, um die Ausbreitung von Infektionen auf andere Geräte sowie die seitliche Bewegung von Bedrohungen im Unternehmen zu verhindern. Dies trägt auch zur Minimierung menschlicher Fehler bei und erleichtert die Endgeräte-Compliance angesichts immer strengerer Datenschutzstandards und Branchenvorschriften.

Offene API-Architektur: Die Automatisierungsfunktionen einer Endpoint-Security-Lösung sollten eng mit der gesamten Netzwerk-Sicherheitsarchitektur zusammenarbeiten. Deshalb sollte der Endpunkt-Schutz auf einer offenen API-Architektur basieren und mit Sicherheitsprodukten von Drittanbietern kompatibel sein. Das erweitert die Security-Integration und trägt zur Maximierung bisheriger Investitionen in andere Antivirus-Lösungen und Sicherheitsprodukte bei.

„Mit einer globalen Armee vernetzter Geräte und einer Angriffsfläche, die jeden Partner und Anbieter im Ökosystem des Unternehmens umfasst, sind Bedrohungsakteure klar im Vorteil.“[8]

Zusammenfassung: Worauf Sie achten sollten

Die rasant wachsende Angriffsfläche – bedingt durch die steigende Anzahl an Netzwerk-Endpunkten – erschwert den Schutz vor Cyber-Angriffen, während das Endpunkt-Management immer mehr Zeit des IT-Teams in Anspruch nimmt.

Schuld daran ist oft mangelnde Transparenz über alle Endpunkte sowie eine fehlende zentrale Schwachstellenverwaltung. IT-Infrastrukturleiter brauchen daher einen Next-Generation-Ansatz für die Endpunkt-Sicherheit, der weder zu höheren Kosten noch zu zeitlichem Mehraufwand führt. Vielmehr muss die Endpoint-Security die Isolierung zwischen Endpunkten sowie zwischen Endpunkten und Netzwerk beseitigen. Nur dann können Bedrohungs- und Telemetriedaten in Echtzeit genutzt und zahlreiche Abläufe automatisiert werden – von Compliance-Audits und Berichten bis hin zu Patching- und Incident-Response-Workflows.

[1] Anna Frazzetto, et al.: „A Changing Perspective: CIO Survey 2019“. Harvey Nash/KPMG, 2019.

[2] Lee Neely: „Endpoint Protection and Response: A SANS Survey“. SANS Institute, 12. Juni 2018.

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

[4] Ebd.

[5] „Cost of a Data Breach Report 2019“. IBM Security und Ponemon Institute, April 2019.

[6] Anna Frazzetto, et al.: „A Changing Perspective: CIO Survey 2019“. Harvey Nash/KPMG, 2019.

[7] „Cost of a Data Breach Report 2019“. IBM Security und Ponemon Institute, April 2019.

[8] „The Post-Digital Era is Upon Us: Are You Ready for What's Next?“. Accenture, 2019.

www.fortinet.com/de

446935-A-0-DE

19. Februar 2021, 11:07 Uhr