Verfasst für

riverbed

Die Vereinigung von Netzwerk- und Sicherheitsbetrieb

April 2021 EMA Whitepaper
Von Shamus McGillicuddy

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Kurzzusammenfassung

Wenn Netzwerk- und Sicherheitsbetriebsteams zusammenarbeiten, ist das gut fürs Geschäft. Forschungsergebnisse von EMA belegen, dass viele Unternehmen diese Art der Zusammenarbeit verfolgen und manchmal sogar beide Teams vollständig zusammenlegen. Dadurch können Risiken reduziert, Kosten gespart und die Produktivität gesteigert werden. Außerdem kann die IT-Organisation schneller auf geschäftliche Anforderungen reagieren. In diesem Whitepaper erfahren Sie, wie Sie diese Art der Zusammenarbeit umsetzen und welche Fallstricke es gibt.

Netzwerkbetriebsteams von Unternehmen schließen sich mit der IT-Sicherheit zusammen

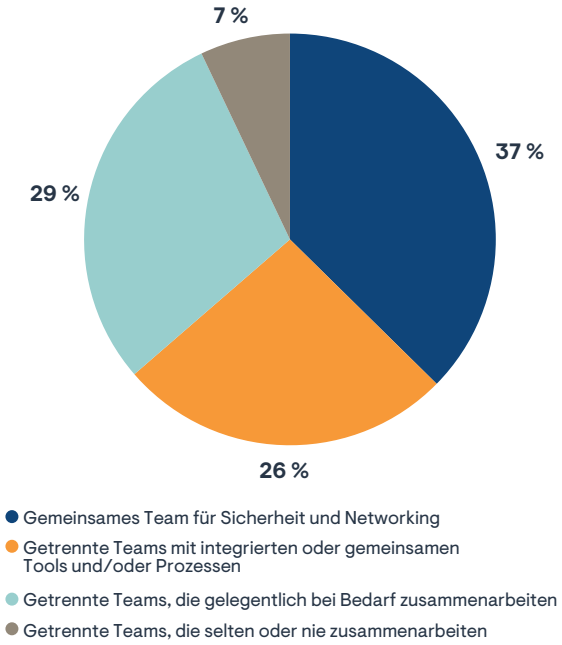
Netzwerkmanager kommen heutzutage nicht am Thema Sicherheit vorbei. Sie ist beispielsweise ein zentraler Faktor bei komplexen IT-Serviceproblemen und Ausfällen, die eine domänenübergreifende Fehlerbehebung erfordern. Laut den Forschungsergebnissen von Enterprise Management Associates (EMA) sind Sicherheitssysteme (Geräteausfälle und mangelhafte Richtlinien) die dritthäufigste Ursache komplexer Probleme, während Sicherheitsvorfälle (Angriffe und Datenschutzverletzungen) die vierthäufigste Ursache sind. (Die häufigste Ursache ist die Netzwerkinfrastruktur und die zweithäufigste Ursache sind Endkundensysteme und Benutzerfehler).[1] Umfassende Kenntnisse zum Thema Sicherheit sind immer sinnvoll, aber insbesondere für Netzwerkteams von Bedeutung, da diese oft als Erstes für Dienstprobleme verantwortlich gemacht werden und sie so beweisen können, dass der Fehler nicht bei ihnen liegt.

Sicherheit ist für das Netzwerkmanagement unerlässlich. Netzwerksicherheit nimmt seit mehr als zehn Jahren den ersten Platz bei Netzwerktechnologieinitiativen ein, die die Prioritäten im Bereich Netzwerkmanagement beeinflussen. Dies hat sich auch 2020 nicht geändert. Auf die Frage von EMA, welche Konzepte bei der Messung des Erfolgs im Netzwerkbetrieb an Bedeutung gewannen, wurde die Reduzierung von Sicherheitsrisiken häufiger von Netzwerkmanagern genannt als die Bereiche Servicequalität, verbesserte Netzwerktransparenz und Anwendungs-Performance.

Daher ist es nicht überraschend, dass Netzwerkmanagementteams engeren Kontakt mit Sicherheitsteams suchen, um die Zusammenarbeit auszuweiten und die allgemeine Transparenz und Reaktionsfähigkeit zu verbessern. Tatsächlich gaben 89 % der Netzwerkmanager an, dass sie den Zusammenarbeitsumfang in den Sicherheitsteams ihrer Unternehmen in den letzten zwei Jahren im Vergleich zu 2018 um 42 % gesteigert haben. Dieser Fokus auf Zusammenarbeit führt zu einer veränderten Organisation. 37 % der Unternehmen gaben an, dass sie ihre Netzwerkmanagement- und Sicherheitsteams vollständig zusammengeführt und mit gemeinsamen Tools und Prozessen ausgestattet haben. 26 % behalten die Trennung ihrer Netzwerk- und Sicherheitsteams bei, bieten aber integrierte Tools und Prozesse an, um die Zusammenarbeit zu vereinfachen.

[1] Die in diesem Whitepaper genannten Daten stammen aus der EMA-Studie „Network Management Megatrends 2020: Enterprises Embrace NetSecOps, the Internet of Things, and Streaming Telemetry“, April 2020.

Abbildung 1. Wie Netzwerkmanagement- und Informationssicherheitsteams heute zusammenarbeiten



Diese Zusammenarbeit hat weitreichende Folgen. Unternehmen nutzen sie, um Sicherheit zu einem elementaren Bestandteil ihrer Netzwerke zu machen. Laut Netzwerkmanagern ist der wichtigste Aspekt der Zusammenarbeit mit dem Sicherheitsteam die Verbesserung der Netzwerk-Performance, gefolgt von der Reduzierung von Risiken und der Beschleunigung der Erkennung und Behebung von Sicherheitsvorfällen.

Toolstrategien für die Zusammenarbeit mit der IT-Sicherheit

Das Netzwerkmanagementteam muss eine Toolstrategie entwickeln, um erfolgreich mit dem Sicherheitsteam zusammenarbeiten zu können. EMA empfiehlt einen integrierten Ansatz. Das Netzwerkteam sollte herausfinden, wie sich bestehende Toolkits erweitern lassen. Nicht empfehlenswert ist hingegen die Einführung eines neuen Einzeltools, das nur begrenzte Integrationsmöglichkeiten in bestehende Workflows und Netzwerkdatensätzen bietet und neuen Installations-, Wartungs- und Schulungsaufwand mit sich bringt. Netzwerkmanager profitieren von einem Sicherheitsüberwachungs- und Managementtool, das Datensätze für bestehende Netzwerkbetriebstools freigeben kann und integrierte Ansichten der Netzwerk-Performance und Sicherheitsüberwachung bietet.

EMA empfiehlt diesen Ansatz unter anderem, da Toolkits für das Netzwerkmanagement bereits überlastet und fragmentiert sind. Eine hohe Anzahl von Managementtools erhöht die Komplexität und den Verwaltungsaufwand und kann sich negativ auf die allgemeine Produktivität auswirken. Unternehmen geben jedes Jahr an, dass sie die Anzahl der genutzten Tools verringern möchten, aber EMA konnte bis zum Jahr 2020 keinen Fortschritt in diesem Bereich feststellen. Zwar wurden im Vergleich zu 2018 tatsächlich weniger Tools verwendet, jedoch zeigten die Studienergebnisse von 2020, dass 64 % der Netzwerkbetriebsteams weiterhin vier bis zehn Tools für die Überwachung und Fehlerbehebung in ihren Netzwerken einsetzen. 17 % nutzen sogar elf oder mehr Tools.

Viele Tools bedeuten aber nicht unbedingt, dass das Netzwerkbetriebsteam weniger effektiv arbeitet. Oft sind sie sogar notwendig. Viele Unternehmen benötigen eine große Anzahl von Tools, da sie umfassende, komplexe Netzwerke managen, deren Betrieb von Natur aus schwierig ist. Unternehmen mit elf oder mehr Netzwerkmanagementtools geben mit höherer Wahrscheinlichkeit (54 %) an, dass ihr Netzwerkbetrieb erfolgreich ist, im Vergleich zu 28 % bei Unternehmen mit einem bis drei Tools und 29 % bei Unternehmen mit vier bis fünf Tools. Trotzdem empfiehlt EMA, die Tools weitmöglichst zu konsolidieren und zu integrieren.

Netzwerkmanagementtools für die Zusammenarbeit mit Sicherheitsteams

EMA hat drei Arten von Netzwerkmanagementtools identifiziert, die wichtig für die Zusammenarbeit mit Sicherheitsteams sind. Das erste ist die Überwachung der Netzwerkinfrastruktur, bei der Gerätekennzahlen über SNMP, Geräte-APIs und mehr erfasst werden können. Außerdem können ungewöhnliche Aktivitäten auf Netzwerkgeräten ermittelt werden, wie etwa die Auslastung von Schnittstellen bei Angriffen. In Unternehmen, in denen das Netzwerk- und Sicherheitsteam eine Einheit bilden, ist die Überwachung der Netzwerkinfrastruktur ein zentraler Faktor für die Zusammenarbeit. In Unternehmen, in denen diese Teams nur bei Bedarf zusammenarbeiten, spielt sie laut EMA eine eher untergeordnete Rolle.

Das zweitwichtigste Tool für die Sicherheitszusammenarbeit ist die Netzwerkautomatisierung/-orchestrierung. Mithilfe von Netzwerkautomatisierungstools können Unternehmen bei Sicherheitsvorfällen schnelle Änderungen am Netzwerk vornehmen. Außerdem können sie eingesetzt werden, um Änderungsrichtlinien durchzusetzen, die verhindern, dass es durch unerwünschte Änderungen am Netzwerk zu Schwachstellen kommt.

Das drittwichtigste Tool für die Sicherheitszusammenarbeit ist die Überwachung des Netzwerk-Flows, zum Beispiel NetFlow, sFlow und IPFIX. Die Flow-Überwachung ermöglicht einen umfassenden Überblick über Netzwerk-Traffic-Muster und -Aktivitäten. Eine fortschrittliche Flow-Analyse kann verdächtige Verhaltensmuster und das typische Verhalten bekannter Bedrohungen offenlegen.

Sicherheitsfunktionen von Netzwerkmanagementtools für einfache NetSecOps-Zusammenarbeit

Die Forschungsergebnisse von EMA belegen, dass die meisten Netzwerkteams (97 %) daran interessiert sind, die Sicherheitsfunktionen zu nutzen, die von ihren Netzwerkmanagementanbietern bereitgestellt werden, um die Zusammenarbeit zu verbessern. 30 % gaben sogar an, dass diese für die Zusammenarbeit mit dem Sicherheitsteam unerlässlich sind. Hierbei sind unter anderem Sicherheitstransparenz, Sicherheitsfunktionen oder dedizierte Produkte gefragt.

Sicherheitsfunktionen von Netzwerkmanagementtools können eine entscheidende Rolle bei der NetSecOps-Zusammenarbeit spielen. Unternehmen sollten jedoch darauf achten, dass die Sicherheitsfunktionen in die Daten und Workflows in ihren Netzwerkmanagementtools integriert werden können – auch dann, wenn sie auf separate Sicherheitsprodukte von diesem Netzwerkmanagementanbieter setzen.

EMA hat Personen, die auf Sicherheitsfunktionen bei ihren Netzwerkmanagementlösungen Wert legen, befragt, wo sie diese Funktionen einsetzen möchten. Die häufigste Antwort war das Rechenzentrum (47 %), gefolgt von Cloud-Workloads (43 %) und IoT-Geräten (39 %). Weitere Einsatzzwecke umfassen SaaS-Anwendungen (31 %) und Remote-Standorte/Außenstellenbüros und Benutzergeräte/BYOD mit jeweils 28 %.

Vorteile und Herausforderungen des gemeinsamen Netzwerk- und Sicherheitsmanagements

Für Unternehmen kann es sehr vorteilhaft sein, wenn ihre Netzwerk- und Sicherheitsmanagementteams zusammenarbeiten. Eine erfolgreiche Zusammenarbeit ist jedoch kein Selbstläufer. EMA hat die vier häufigsten Herausforderungen bei der Zusammenarbeit ermittelt. Die größte Herausforderung ist laut 31 % der Netzwerkmanager, dass Netzwerk- und Sicherheitsteams unterschiedliche Ziele verfolgen. Dies liegt daran, dass die Netzwerk- und Sicherheitsteams nicht per se zusammenarbeiten und oft gegensätzliche Interessen haben. Das Netzwerkteam konzentriert sich auf Konnektivität, indem es Mitarbeitern, Partnern und Kunden Zugriff auf Anwendungen, Daten und Dienste gewährt. Das Sicherheitsteam möchte Daten schützen und die Konnektivität von Anwendungen begrenzen. Daher ist es wichtig, die Herausforderungen zu beachten, die in IT-Organisationen auftreten, wenn diese beiden Teams zusammenarbeiten. Erfolgreiche Zusammenarbeit erfordert engagierte Führungskräfte. Wenn keines der Teams über geeignete Führungskräfte verfügt, müssen sie sich für Unterstützung und Vorgaben an die IT-Führungskräfte wenden.

Häufige Herausforderungen für die erfolgreiche Zusammenarbeit von Netzwerk- und Sicherheitsteams

1. Widersprüchliche Ziele
2. Teamspezifische Kompetenzlücken
3. Konflikte beim Teilen und der Eigentümerschaft von Daten
4. Datenqualität und -relevanz

Ein weiteres Problem sind teamspezifische Kompetenzlücken (29 %). Es kommt oft vor, dass Mitarbeiter eines Teams nicht über die Fertigkeiten und Erfahrungen zur Nutzung der Technologien, Tools und Prozesse verfügen, die für die Mitarbeiter des anderen Teams unerlässlich sind. Dies ist besonders bei spezifischen IT-Teams der Fall. Erfolgreiche Netzwerkbetriebsteams sind seltener von teamspezifischen Kompetenzlücken betroffen (21 %). Eine weitere Herausforderung ist laut 29 % der Befragten, dass Tools nicht für die Zusammenarbeit ausgelegt sind. Um dieses Problem zu beheben, müssen Netzwerkmanagementtools Workflows und Funktionen anbieten, die die Zusammenarbeit erleichtern und sicherheitsbezogene Einblicke bieten.

27 % der Befragten gaben an, dass es beim Teilen von Daten sowie der Frage der Eigentümerschaft von Daten zu Konflikten kommt. Einzelne Teams legen großen Wert auf den Schutz der Daten, die sie aus dem Netzwerk abrufen, was sowohl den Sicherheits- als auch Netzwerkbereich des Unternehmens betrifft. EMA empfiehlt, dass IT-Führungskräfte dieses Thema angehen, indem sie einen Plan für die Zusammenarbeit erstellen. Weitere 27 % geben an, dass es zu größeren Problemen mit der Datenqualität kommt, wenn Daten zwischen Netzwerk- und Sicherheitsteams ausgetauscht werden. Um veraltete oder uneinheitliche Daten zu vermeiden, sollten Netzwerk- und Sicherheitsteams einen Weg finden, ihre Daten sowie Analysetools weitmöglichst zu vereinheitlichen.

Die Vorteile der Zusammenarbeit von Netzwerk- und Sicherheitsteams

Wenn Netzwerk- und Sicherheitsmanagementteams Tools gemeinsam nutzen, Daten kombinieren und zusammenarbeiten, können Unternehmen in vielerlei Hinsicht profitieren. EMA hat die fünf wichtigsten Gründe für diese Art der Zusammenarbeit ermittelt. Erstens sind 39 % der IT-Organisationen der Meinung, dass die Zusammenarbeit von Netzwerk- und Sicherheitsteams zu einer verbesserten Netzwerk-Performance führt. Unternehmen, in denen Netzwerk- und Sicherheitsteams dauerhaft zusammenarbeiten, zeigen mit höherer Wahrscheinlichkeit eine bessere Netzwerk-Performance (48 %).

Ein zweiter wichtiger Grund für die Zusammenarbeit ist die Risikoreduzierung (34 %). Mit den richtigen Prozessen und Toolintegrationen können IT-Organisationen die Netzwerktransparenz verbessern und die allgemeine Netzwerkintegrität erhöhen. Netzwerkmanager, die mit Sicherheitsmanagern zusammenarbeiten, machen seltener Fehler in den Bereichen Netzwerkdesign, -konfiguration und -anpassung, die Schwachstellen zur Folge haben könnten. Außerdem führen Sicherheitsteams seltener Sicherheitskontrollen ein, die den Zustand und die Performance des Netzwerks verschlechtern könnten.

Drittens gaben 32 % der IT-Organisationen an, dass sie eine beschleunigte Erkennung und Behebung von Sicherheitsvorfällen erwarten. Die Zusammenarbeit kann ihre Fähigkeit verbessern, Sicherheitsprobleme zu identifizieren und zu lösen. Optimierte Workflows sorgen außerdem dafür, dass technische Fachkräfte weniger Zeit für die Behebung von Vorfällen aufwenden müssen. Stattdessen können sie sich auf strategische Aufgaben konzentrieren. Auf diese Weise können viele IT-Organisationen die Betriebskosten optimieren (27 %).

Die wichtigsten Gründe für die Zusammenarbeit im Bereich Netzwerk- und Sicherheitsmanagement

1. Höhere Netzwerk-Performance
2. Reduzierung von Sicherheitsrisiken
3. Schnellere Erkennung und Behebung von Sicherheitsvorfällen
4. Optimierung der Betriebskosten

EMA-Perspektive

Die Zusammenarbeit mit dem Sicherheitsteam wird für Netzwerkmanager nicht immer einfach sein. Hindernisse, die mit der Technik und unterschiedlichen Zielsetzung verbunden sind, müssen überwunden werden, aber die Vorteile sprechen für sich. Die Forschungsergebnisse von EMA liefern überzeugende Belege, dass Unternehmen diese Art der Zusammenarbeit nicht nur für sich entdeckt haben, sondern dass Netzwerkbetriebsteams bereits heute enger mit Informationssicherheitsteams zusammenarbeiten, als dies noch vor einigen Jahren der Fall war. Die Zusammenarbeit beginnt mit einfachen Gesprächen und wird nach und nach auf technische Prüfungen der Prozesse und Technologien ausgeweitet, die jedes Team anwendet, um seine Aufgaben im Unternehmen zu erfüllen. Dabei muss jedes Team Kompromisse eingehen und unter Umständen Verantwortung an das andere Team abgeben.

Tools werden eine große Rolle spielen. Netzwerk- und Sicherheitsteams müssen herausfinden, wie sie ihre Management- und Überwachungssysteme, Datensätze und Workflows teilen und integrieren können. Tools, die diese Anforderungen von Beginn an erfüllen, werden sich als besonders wertvoll erweisen. Sicherheitsfunktionen von Netzwerkmanagement-Tools sind ein möglicher Best-Practice-Ansatz für die NetSecOps-Zusammenarbeit.

Über Riverbed

Riverbed ermöglicht es Unternehmen, die Leistung ihrer Netzwerke und Anwendungen zu maximieren und transparent abzubilden, sodass sie ihre Investitionen in digitale Lösungen und die Cloud voll ausschöpfen können. Die Riverbed Network and Application Performance Platform erlaubt es Unternehmen, die Leistung jedes Netzwerks für jede Anwendung zu visualisieren, zu optimieren, zu korrigieren, zu beschleunigen und sicherzustellen. Die Plattform verfolgt hinsichtlich Performance und Transparenz einen ganzheitlichen Ansatz – mit erstklassiger WAN-Optimierung, Netzwerk-Performance-Management (NPM), Anwendungsbeschleunigung (einschließlich Office 365, SaaS, Client- und Cloud-Beschleunigung) und SD-WAN für Unternehmen aller Größenordnungen. Zu den über 30.000 Kunden von Riverbed gehören 99 % der Fortune 100. Weitere Informationen auf https://www.riverbed.com/de/.

Über Enterprise Management Associates, Inc.

Enterprise Management Associates (EMA) wurde 1996 gegründet und ist ein führendes Branchenanalystenunternehmen, das tiefe Einblicke in das gesamte Spektrum der IT- und Datenmanagement-Technologien bietet. Die Analysten von EMA nutzen eine einzigartige Kombination aus praktischer Erfahrung, Einblicken in die Best Practices der Branche und fundierten Kenntnissen über aktuelle und geplante Anbieterlösungen, um die Kunden von EMA beim Erreichen ihrer Ziele zu unterstützen. Erfahren Sie mehr über EMA-Research, -Analyse und -Beratungsdienste für Anwender aus dem Unternehmensbereich, IT-Fachleute und IT-Anbieter unter **www.enterprisemanagement.com** Sie können der EMA auch auf **Twitter** oder **LinkedIn** folgen.

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 **www.enterprisemanagement.com**

4080.033121