Gemeinsam stärker

Sechs gute Gründe, Netzwerk- und Sicherheitsdienste vom selben Anbieter zu beziehen

verizon business

Netzwerk + Sicherheit

Die geschäftlichen und technischen Vorteile einer einheitlichen Beschaffung und Verwaltung

David Bailey
Global Solutions Executive

Seit mehr als zwei Jahrzehnten hilft David Bailey globalen Unternehmen und öffentlichen Einrichtungen, die passende Infrastruktur und Sicherheit für ihre digitalen Anforderungen aufzubauen. Sein Fokus reicht von kabelgebundenen und drahtlosen IoT-Netzen bis hin zu agilen, leistungsfähigen Architekturen für KI-Anwendungen.

Da Cyberbedrohungen ständig weiterentwickelt und Netzwerkinfrastrukturen immer komplexer werden, sollten Unternehmen Silos aufbrechen und eine stärkere Integration von Cybersicherheits- und Netzwerkfunktionen anstreben. Dadurch entstehen robustere, sicherere und effizientere Systeme, die sie beim Erreichen ihrer Geschäfteziele und Schutz kritischer Assets unterstützen. Das rasante Wachstum von KI-Workloads und deren enormer Datenbedarf steigern die Dringlichkeit dieser Initiativen zusätzlich.

Verizon ist nicht nur ein renommierter Tier-1-Netzwerkanbieter, der eines der weltgrößten IP-Netzwerke betreibt, sondern auch ein führender Anbieter von Cybersicherheits-Diensten. Diese umfassen unter anderem Beratung, Threat Intelligence, Incident Response, Compliance-Audits und Forensik. Darüber hinaus erstellen wir jährlich einen detaillierten datengestützten Bericht über die neuesten Sicherheitsverletzungen, den Verizon Data Breach Investigations Report (DBIR) – nun in der 18. Auflage. Diese Erfahrung verschafft uns wertvolle Einblicke und eine einzigartige Perspektive, die in die Entwicklung, Verwaltung und Sicherung unserer Infrastruktur einfließen.

Wir sind der festen Überzeugung, dass Netzwerke und Sicherheit eng miteinander verbunden sind und einheitlich gemanagt werden sollten – und tun dies für unser globales Backbone, unsere Breitband- und Telefonienetzwerke für Verbraucher und für die Tausenden von WANs, die wir für global agierende Unternehmen verwalten. Dieses Whitepaper beleuchtet die Vorteile der gemeinsamen Beschaffung und Verwaltung von Cybersicherheits- und Netzwerkdiensten.

1 Stärkere Abwehr

Wenn Cybersicherheit und Netzwerke getrennt verwaltet werden, arbeiten die zuständigen Teams oft nicht eng genug zusammen, um Lücken in der Kommunikation und Strategie zu vermeiden. Das kann zu uneinheitlichen Konfigurationen und damit zu Schwachstellen führen.

> Wenn Sicherheits- und Netzwerkteams nicht eng zusammenarbeiten, können blinde Flecken und Kommunikationsprobleme entstehen, die die Bedrohungsabwehr und Incident Response beeinträchtigen.

Die Zusammenführung beider Bereiche erleichtert die kontinuierliche Überwachung und Bedrohungserkennung nahezu in Echtzeit über sämtliche Netzwerkebenen hinweg, die Konfiguration von Geräten wie Routern und Switches und die unternehmensweite Durchsetzung einheitlicher Richtlinien. So können die Teams potenzielle Bedrohungen proaktiv angehen und somit das Risiko einer Sicherheitsverletzung minimieren und Schwachstellen schnell identifizieren und ausmerzen.

- **Optimiertes Betriebsmodell**
  Dieser einheitliche Ansatz stärkt die Cyberresilienz und senkt gleichzeitig die Kosten – dank eines effizienteren Betriebsmodells mit weniger Doppelarbeit, schlankeren Teams, geringerem Kommunikationsaufwand sowie vereinfachten Systemen und Lizenzen. Er kann sogar dazu beitragen, den Aufwand für die Integration oder Verknüpfung mehrerer Technologiesilos zu reduzieren.

- **Minimierung von Ausfallzeiten und Drittparteienrisiken**
  Diese Verbesserungen können sogar dazu führen, dass das Service Desk Mitarbeiterprobleme effektiver bearbeiten kann, sodass Teams effizienter und produktiver arbeiten können. Sie können auch beim Aufdecken von Lücken und Problemen in internen oder Partnerprozessen helfen, die von Angreifern ausgenutzt wurden, um sich Zugriff zu einem Netzwerk zu verschaffen.

- **Effektivere Sicherheitskontrollen**
  Ein einheitliches Management kann auch die Erkennung von Schwachstellen erleichtern, denn wenn eine Infrastruktur in Silos unterteilt ist, besteht die Gefahr, dass einzelne Bereiche – und deren Schwachstellen – übersehen werden. Je schneller und zuverlässiger Schwachstellen erkannt und behoben werden, desto weniger Chancen haben Angreifer, in die Umgebung einzudringen.

- **Effektivere Nutzung von Daten und Threat Intelligence**
  Threat Intelligence ist eine kritische Komponente jeder Cybersicherheits-Strategie. Eine gemeinsame Verwaltung von Sicherheit und Netzwerken ermöglicht eine effektivere Nutzung dieser Bedrohungsdaten: Integrierte Lösungen können sowohl den Netzwerkverkehr als auch Sicherheitsereignisse nahezu in Echtzeit auf Gefahrenindikatoren analysieren und somit Angriffen vorbeugen.

2 Bessere (Kosten)effizienz

Eine getrennte Beschaffung und Verwaltung von Cybersicherheits- und Netzwerkfunktionen führt oft zu Ineffizienz und unnötigen Kosten. Ein einheitlicher Ansatz hingegen bietet folgende Vorteile:

- **Reduzierte Kosten**
  Eine gemeinsame Verwaltung kann die Budgetierung und Finanzplanung vereinfachen, einen besseren Überblick über Technologieausgaben bieten und Kosten einsparen.

- **Effizienterer Mitarbeitereinsatz**
  Das Aufbrechen von Silostrukturen kann Personalengpässe abmildern. Die für die Verwaltung von Cybersicherheit und Netzwerken erforderlichen Kenntnisse überschneiden sich häufig. Ein integrierter Ansatz ermöglicht die Bereitstellung effektiverer Trainingsprogramme, die beide Bereiche abdecken. Mitarbeiter, die sowohl Netzwerk- als auch Sicherheitsaufgaben übernehmen können, lassen sich außerdem vielfältiger einsetzen und sind besonders wertvoll, wenn Kunden weltweit und rund um die Uhr betreut werden müssen. Unternehmen, die ihren Fachkräften die Chance geben, ihre Kenntnisse und ihren Verantwortungsbereich zu erweitern, können gleichzeitig oft die Mitarbeiterzufriedenheit und -bindung stärken.

3 Sichere Einbindung von Multi-Cloud-Umgebungen und beschleunigte digitale Transformation

Cloudbasierte Services spielen bei den meisten Transformationsinitiativen eine kritische Rolle. Eine erfolgreiche Migration von Anwendungen in die Cloud erfordert eine robuste, integrierte Netzwerk- und Sicherheitsstrategie. Unternehmen mit einer ausgereiften Cloud-Strategie benötigen oft Multi-Cloud- oder sogar Hybrid-Cloud-Infrastrukturen. Ein einheitlicher Netzwerk- und Sicherheitsansatz hilft ihnen, diese komplexeren Umgebungen effektiver zu verwalten:

- **Effektivere Verwaltung von Multi-Cloud-Umgebungen**
  Durch die Verbindung von Cloud-Infrastrukturen mit intelligenten Netzwerken erhalten Teams einen besseren Überblick über Workloads, Leistung und Nutzungsmuster. Das vereinfacht die Verwaltung und hilft ihnen, Probleme schneller zu identifizieren und beheben.

- **Konsistente Durchsetzung von Sicherheitsrichtlinien – lokal und in der Cloud**
  Mit einheitlichen Kontrollen kann sichergestellt werden, dass bei der Datenübertragung, -verarbeitung und -speicherung überall dieselben Compliance- und Sicherheitsvorgaben eingehalten werden, was zudem die Wahrscheinlichkeit von Fehlkonfigurationen und Sicherheitslücken reduziert.

- **Einfachere Verwaltung von Hybrid- und Multi-Cloud-Umgebungen**
  Mit integrierten Lösungen können IT-Teams Dienste und Richtlinien über eine zentrale Konsole koordinieren, anstatt viele isolierte Systeme einzeln verwalten zu müssen. Das strafft den Betrieb und fördert Automatisierung, Effizienz und Flexibilität.

4 Mehr Skalierbarkeit und Flexibilität

Unternehmen müssen sich an immer neue Kundenanforderungen und Technologien anpassen. Wenn ihnen das nicht gelingt, laufen sie Gefahr, hinter Mitbewerbern zurückzubleiben, wichtige Geschäftschancen zu verpassen und letztendlich Marktanteile zu verlieren.

- **Lückenlose, ununterbrochene Sicherheit, selbst bei Netzwerkänderungen**
  Mit einem integrierten Cybersicherheits-Ansatz können Unternehmen schneller auf Sicherheitsvorfälle reagieren. Wenn Unternehmen wachsen oder neue Geschäftsmodelle einführen, sorgt eine einheitliche Netzwerk- und Sicherheitsstrategie dafür, dass die Abwehr stark bleibt – selbst wenn sich die Infrastruktur verändert.
- **Vermeidung doppelter Arbeit und Technologie-Investitionen**
  Voneinander isolierte Teams investieren möglicherweise in verschiedene Tools oder Services, obwohl eine einzelne Lösung kosteneffizienter und einfacher zu verwalten wäre. Integrierte Teams arbeiten effektiver zusammen und benötigen daher weniger Zeit und Ressourcen, um neue Services bereitzustellen oder Probleme zu beheben.

5 Schnellere Abwehr und weniger Ausfallzeiten

Eine einheitliche Cybersicherheits- und Netzwerkstrategie ermöglicht eine robustere, koordiniertere Reaktion auf Sicherheitsverstöße.

- **Schadensbegrenzung bei Sicherheitsvorfällen**
  Durch die gemeinsame Verwaltung können Unternehmen Incident-Response-Prozesse klarer ausrichten, die teamübergreifende Zusammenarbeit verbessern, Reaktionszeiten verkürzen und bei Angriffen potenzielle Schäden eingrenzen.
- **Schnellere Erkennung und Isolierung von Bedrohungen**
  Einheitliche Services unterstützen eine proaktivere Sicherheitsstrategie, zum Beispiel durch eine kontinuierliche Überwachung des Netzwerks auf Schwachstellen und Bedrohungen. Dies stärkt das Sicherheitsniveau und reduziert die Wahrscheinlichkeit von Betriebsausfällen.
- **Automatisierte, beschleunigte Incident Response**
  Ein integrierter Ansatz ermöglicht die Implementierung automatisierter Abwehrmaßnahmen, wodurch sich letztendlich auch die Eindämmungs- und Behebungszeiten verkürzen lassen. Zu den weiteren Vorteilen einer einheitlichen Verwaltung zählt eine effektivere Analyse nach einem Verstoß. So können Unternehmen aus Vorfällen lernen und ihr Sicherheitsniveau gezielt verbessern.

6 Einfachere Compliance und Berichterstellung

Beim Thema Compliance denken Sie vielleicht an Branchen wie das Finanz- oder Gesundheitswesen, doch inzwischen unterliegen die meisten Unternehmen strengen Datenschutzregelungen. Jedes Unternehmen, das Kartenzahlungen akzeptiert oder personenbezogene Daten (PII) nutzt, muss vermutlich ein Mindestmaß an Cybersicherheitsregeln einhalten und dies belegen können. Das kann zeitaufwendig und kostspielig sein und wird oft durch die Komplexität der IT-Umgebung erschwert.

- **Mehr Konsistenz bei Sicherheitskontrollen**
  Eine einheitliche Cybersicherheits- und Netzwerkstrategie kann die Erfüllung dieser Anforderungen erleichtern, da Sicherheitskontrollen und Netzwerkkonfigurationen konsistent angewendet und dokumentiert werden können.

> Automatisierte Reporting-Tools sind oft effektiver, wenn Cybersicherheit und Netzwerke gemeinsam verwaltet werden.

- **Klare Verantwortung**
  Einheitliches Management bedeutet auch, dass klar ist, wer für die Compliance verantwortlich ist. Dies erleichtert die Protokollierung und Berichterstellung zur Einhaltung gesetzlicher Vorgaben wie:
  - Datenschutz-Grundverordnung (DSGVO)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Payment Card Industry (PCI) Data Security Standard (DSS)
  - California Consumer Privacy Act (CCPA)

Internetzugang für Unternehmen: Leitfaden zur Anbieterauswahl

In diesem Whitepaper aus derselben Reihe erfahren Sie, worauf Sie bei der Anbieterwahl achten sollten, um die maximale Leistung und besten Ergebnisse für Ihr Unternehmen zu erzielen, und warum das besonders wichtig ist, wenn Sie latenzsensible Anwendungen wie KI-Apps nutzen.

Lesedauer: 15 Minuten

Was spricht für Verizon?

Ganz einfach: Wir sind das Netzwerk. Unsere Millionen Kilometer Glasfaserkabel bilden das Backbone eines Großteils des Internets. Daher können wir deutlich mehr Transparenz, Leistung und Zuverlässigkeit bieten als die meisten anderen Anbieter.

Doch wir bieten nicht nur Konnektivität. Wir beschäftigen eines der weltweit größten und erfahrensten Teams aus Sicherheitsexperten, die sich bestens mit Threat Intelligence, Incident Response, digitaler Forensik, Compliance und vielem mehr auskennen. Sie führen jedes Jahr über 1.000 Projekte in den Bereichen Governance, Risiko und Compliance durch.

Wir sind eben richtige Daten- und Sicherheits-Nerds. Wir haben für unsere jährlichen Data Breach Investigations Reports (DBIR) bereits über eine halbe Million Sicherheitsvorfälle analysiert (542.678, um genau zu sein) – teils aus unseren eigenen Untersuchungen und teils von über 60 Strafverfolgungsbehörden und Sicherheitsunternehmen aus aller Welt, die an diesem Bericht mitwirken. Außerdem ver- und bearbeiten wir jedes Jahr Billionen Sicherheitsvorfälle aus unseren eigenen und den Netzwerken unserer Kunden. Dadurch stehen uns enorme Datenmengen für unsere KI-Prognosen zur Verfügung.

Selbstverständlich sind nicht nur Zahlen und Statistiken wichtig; denn was uns wirklich auszeichnet, sind unser Netzwerk und unser Team. Wenn es darum geht, Ihr Unternehmen zu vernetzen, Ihre Infrastruktur zu schützen und die bestmögliche Leistung aus Ihren Anwendungen herauszuholen, sind Sie bei Verizon in den besten Händen.

Vertrauen Sie also auf die Experten.

>23 Bio.
In einem typischen Jahr werten wir über 23 Billionen Cyberereignisse aus.

>550.000
Wir verwalten über eine halbe Million Netzwerk-, Hosting- und Sicherheitsgeräte.

>1.000
Wir führen jedes Jahr über 1.000 Projekte in den Bereichen Governance, Risiko und Compliance durch.

Gespräch vereinbaren

Von IoT über Echtzeitanalysen bis hin zu KI – Verizon unterstützt Sie dabei, Technologien optimal einzusetzen, um Ihre Prozesse zu überwachen, zu verwalten und kontinuierlich zu verbessern. Wenn Sie nach der Lektüre dieses Whitepapers noch Fragen haben, erreichen Sie uns unter: verizon.com/business/de-de/contact-us

Ressourcen rund um smarte Netzwerkbeschaffung

Dieses Whitepaper ist Teil einer Reihe, die sich mit den wachsenden Anforderungen an Unternehmensnetzwerke beschäftigt – und mit den entscheidenden Fragen, die Unternehmen bei der Beschaffung stellen sollten, um sicherzustellen, dass die gewählten Lösungen wirklich unternehmenstauglich sind und sowohl aktuelle als auch zukünftige Anforderungen erfüllen.

Eine neue Daten-Ära

Daten **IoT** **KI**

In diesem Whitepaper beleuchten wir einige der wichtigsten Faktoren, die das explosionsartige Wachstum der in Unternehmen anfallenden Daten vorantreiben – und welche Auswirkungen das auf die Netzwerkplanung hat.
verizon.com/business/resources/articles/iot-genai-data-explosion.pdf

Internetzugang: Leitfaden zur Anbieterwahl

Leistung

Beim Kauf von Netzwerklösungen müssen viele Entscheidungen getroffen werden. Ein Verständnis der drei Internet-Tiers ist entscheidend, um alle Optionen umfassend beurteilen zu können. Dieses Whitepaper zeigt, wie sich die einzelnen Tiers auf Netzwerkleistung und Sicherheit auswirken.
verizon.com/business/resources/de-de/articles/tier-1-isp-enterprise-connectivity.pdf

Network Peering

Cloud **Leistung** **Zuverlässigkeit**

Peering ist ein wesentlicher Faktor für die Netzwerkleistung und nimmt dadurch direkten Einfluss auf die Leistung von Unternehmensanwendungen, insbesondere Cloud-Diensten. Dennoch wird es im Beschaffungsprozess kaum je thematisiert. Dieses kurze Whitepaper zeigt, warum Peering so wichtig ist.
verizon.com/business/resources/de-de/articles/network-peering.pdf

Tappen Sie im Dunkeln, was die Leistung betrifft?

Daten **Leistung** **Verwaltbarkeit**

Lesen Sie in diesem Whitepaper, wie sich die Entscheidung, physische (Underlay) und logische (Overlay) Netzwerke getrennt zu beschaffen, auf Netzwerkleistung, Transparenz und Verwaltbarkeit auswirken kann.
verizon.com/business/resources/de-de/articles/overlay-underlay-network-procurement.pdf

Gemeinsam stärker

Sicherheit **Leistung** **Verwaltbarkeit**

Cyberangriffe werden immer zahlreicher und komplexer. Dieses kurze Whitepaper gibt sechs Argumente dafür, dass eine engere Verzahnung von Cybersicherheit und Netzwerkbetrieb sinnvoll ist, um den Schutz zu stärken und Aufwand sowie Kosten zu senken.
verizon.com/business/resources/de-de/articles/unified-network-security-services.pdf

Turbo für Ihre KI-Anwendungen

KI **Leistung**

KI hat das Potenzial, die bedeutendste technologische Umwälzung seit der Einführung des Internets vor etwa drei Jahrzehnten auszulösen. In diesem Whitepaper erfahren Sie, warum die Leistungsfähigkeit des Netzwerks für KI-Anwendungen eine zentrale Rolle spielt und wie sie hilft, die erwarteten Vorteile tatsächlich zu realisieren.
verizon.com/business/resources/de-de/articles/network-infrastructure-ai-platforms.pdf

verizon business