heise Business Services

Ein eBook von

Powered by Gigamon®

IT in the Age of Change

Entwicklung, Management und Sicherheit von Applikationen in Zeiten des Wandels

- **Vom Monolithen zum Microservice**
  Wie sich Software-Entwicklung und Bereitstellung verändern
- **IT-Sicherheit in verteilten Systemen**
  Wenn Anwendungen und Anwender mobil werden
- **Anwendungen intelligent managen und absichern**
  Performance und Sicherheit gewährleisten, Investitionen schützen

Extra

Netzwerke & Sicherheit

Whitepaper: Wenn Netzwerke auf die Zukunft treffen

2020 Cyberthreat Defense Report: die wichtigsten Ergebnisse

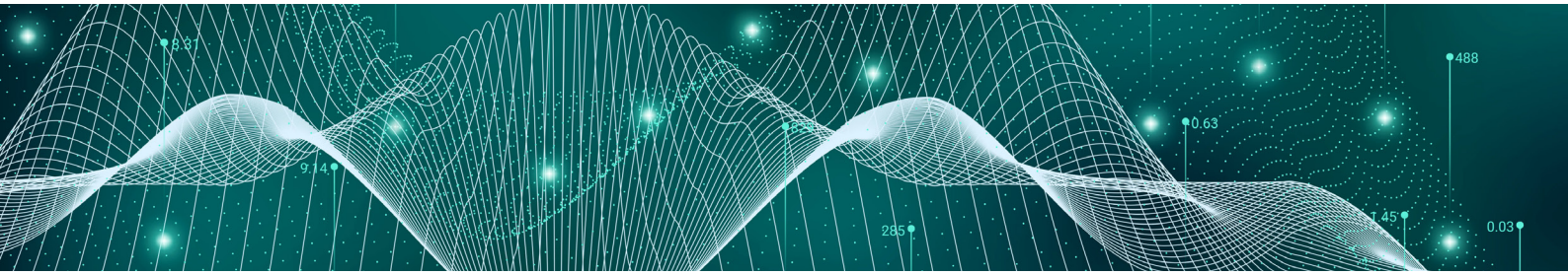


Foto: Inga Ra, BigStock

Editorial

Microservices statt monolithischer Architekturen, Scrum und DevOps statt Wasserfall, Container statt physischer Server – die Art und Weise, wie Anwendungen entwickelt und bereitgestellt werden, hat sich in den vergangenen Jahren grundlegend gewandelt. Aber auch die Nutzung hat sich drastisch verändert. Software-as-a-Service ersetzt zunehmend das Perpetual Licencing, Mitarbeiter greifen immer häufiger aus dem Home-Office oder von unterwegs auf Applikationen zu. Ob sich diese im Firmennetz befinden oder in einer Cloud-Umgebung, darüber machen sie sich in der Regel keine Gedanken – Hauptsache Verfügbarkeit und Performance stimmen.

Administratoren und IT-Sicherheitsverantwortliche stellt diese Entwicklung vor eine ganze Reihe neuer Herausforderungen. Sie müssen nicht nur eine immer größere Zahl von Anwendungen, Plattformen und Infrastrukturen verwalten und absichern, sondern auch mit wachsenden Datenströmen zurechtkommen. Dass diese hauptsächlich über Weitverkehrsstrecken und oft verschlüsselt übertragen werden, macht es nicht einfacher. Die Analyse von Ausfällen und Performance-Problemen gerät zur Detektivarbeit, Sicherheitssysteme sind überlastet oder versagen, weil ihnen zu wenige, zu viele oder die falschen Daten zur Verfügung gestellt werden.

Dieses eBook zeigt Ihnen, wie Sie die genannten Herausforderungen meistern, das Management von Anwendungen erfolgreich gestalten und die richtigen Maßnahmen für die Absicherung einer modernen Applikationslandschaft ergreifen.

Dr. Thomas Hafen
Freier Journalist

Heise Medien GmbH & Co.KG
Abt. Heise Business Services
Hans-Pinsel-Straße 10b
85540 Haar bei München

Registergericht:
Amtsgericht Hannover HRA 26709

Persönlich haftende Gesellschafterin:
Heise Medien Geschäftsführung GmbH

Registergericht:
Amtsgericht Hannover, HRB 60405

Geschäftsführer:
Ansgar Heise, Dr. Alfons Schräder

Verantwortlich für den Inhalt:
Heise Business Services
Thomas Jannot, tj@heise.de

Haftung: Für den Fall, dass Beiträge oder Informationen unzutreffend oder fehlerhaft sind, haftet der Verlag nur beim Nachweis grober Fahrlässigkeit. Für Beiträge, die namentlich gekennzeichnet sind, ist der jeweilige Autor verantwortlich.

Haben Sie Fragen zu diesem eBook oder haben Sie Interesse an einer eigenen Produktion, dann schicken Sie bitte eine E-Mail mit dem Betreff **„HBS-eBook“** an hbs@heise.de

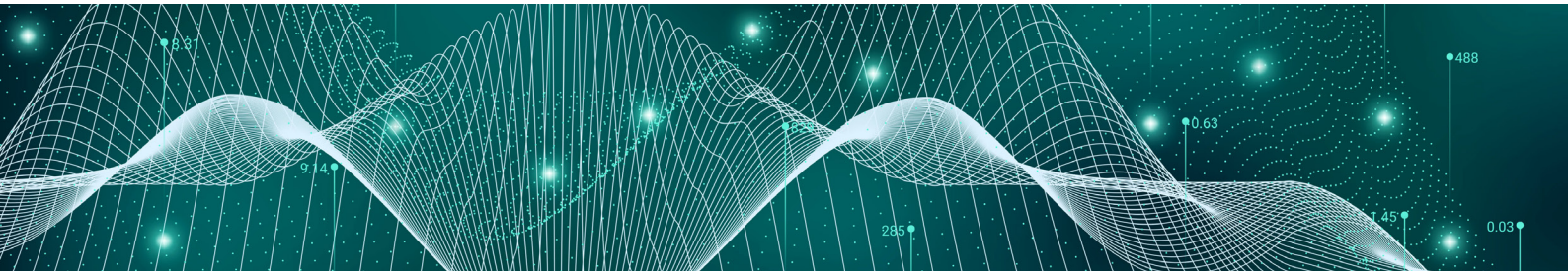


Foto: Inga Ra, BigStock

Inhalt

Vom Monolithen zum Microservice **4**
Das Ende des Wasserfalls 4
Kurze Release-Zyklen dank Scrum und DevOps 5
Robuste Software durch Microservices 6
Cloud und Container auf dem Vormarsch 6
Vom LAN zum WAN 7
Fazit: Herausforderungen für das Applikationsmanagement 8

Sicherheit verteilter Anwendungslandschaften **9**
Zahl erfolgreicher Angriffe steigt 10
Kontinuierliche Überwachung statt Abschottung 11
Security-Trends 2020 12
Fazit: Herausforderungen für die IT-Security 13

Anwendungen intelligent managen und absichern **14**
Weniger Komplexität, mehr Flexibilität durch Inline Bypass 14
Traffic-Filterung schützt Investitionen 15
Effizientes Applikationsmanagement braucht Transparenz 16
SSL-Entschlüsselung ohne Performance-Einbußen 16
Guter Schutz braucht Kontextinformationen 17
Fazit: Neue Zeiten brauchen neue Wege 17

Extra: Netzwerke und Sicherheit **18**
Whitepaper: Wenn Netzwerke auf die Zukunft treffen 18
2020 Cyberthreat Defense Report: die wichtigsten Ergebnisse 31

ÜBER DEN AUTOR

Dr. Thomas Hafen war über 15 Jahre als Redakteur, Moderator und Manager für verschiedene IT-Fachverlage tätig. Seine fachlichen Schwerpunkte liegen in den Bereichen Digitale Transformation, Cloud Computing und Advanced Analytics. Thomas Hafen lebt und arbeitet heute als freier Journalist und Moderator in München.

Foto: ChamilleWhite, BigStock

Major Releases alle fünf, sechs oder sieben Jahre gehören der Vergangenheit an.

Trends in der Software-Entwicklung

Vom Monolithen zum Microservice

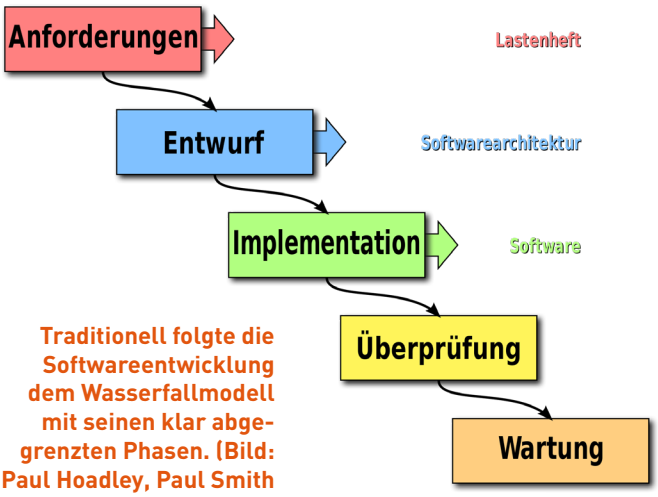
Immer mehr Softwareprodukte sind modular aufgebaut, werden häufig aktualisiert und als Service zur Verfügung gestellt. Diese Entwicklung, aber auch Trends wie DevOps, Continuous Development / Integration und Container erfordern von Unternehmen neue Strategien für die Verwaltung und Absicherung von Applikationen.

Machen wir eine Zeitreise zurück ins Jahr 2001. Mit großem Medienrummel veröffentlichte Microsoft vor fast 20 Jahren „Windows XP“ [1]. Das Betriebssystem blieb für rund ein Jahrzehnt der Standard auf Heim- und Arbeitsrechnern. Selbst 15 Jahre nach Markteinführung nutzten es noch mehr als fünf Prozent der PC-Anwender [2]. Der ungeliebte Nachfolger „Windows Vista“, der sieben Jahre später auf den Markt kam, konnte XP nie wirklich ablösen.

Heute funktioniert die Bereitstellung von Windows fundamental anders. Im „Modern Lifecycle“ [3] veröffentlicht der Hersteller halbjährliche Funktions-Updates für sein aktuelles Betriebssystem Windows 10, die aufeinander aufbauen. Major Releases alle fünf, sechs oder sieben Jahre gehören der Vergangenheit an. Allein schon die Idee, eine Software so lange zu pflegen, ohne daraus nennenswerte Umsätze generieren zu können, lässt Herstellern heute einen Schauer über den Rücken laufen.

Das Ende des Wasserfalls

Die Geschichte von Windows XP ist typisch für die traditionelle Art und Weise, Betriebssysteme und Applikationen zu entwickeln und auf den Markt zu bringen. Die Softwareentwicklung erfolgte nach dem Wasserfallmodell in klar abgegrenzten, aufeinanderfolgenden Phasen. War eine Applikation „fertig“ und getestet, wurde sie über mehrere Jahre kaum mehr verändert und nur noch in Details aktualisiert.



Traditionell folgte die Softwareentwicklung dem Wasserfallmodell mit seinen klar abgegrenzten Phasen. (Bild: Paul Hoadley, Paul Smith und Shmuel Csaba Otto Traian / CC BY-SA)

1 https://web.archive.org/web/20101213072849/http://www.microsoft.com/presspass/press/2001/aug01/08-24WinXPRTMPR.mspx
2 https://www.heise.de/newsticker/meldung/Zahlen-bitte-Windows-XP-The-Walking-5-Percent-3358461.html
3 https://docs.microsoft.com/de-de/lifecycle/policies/modern

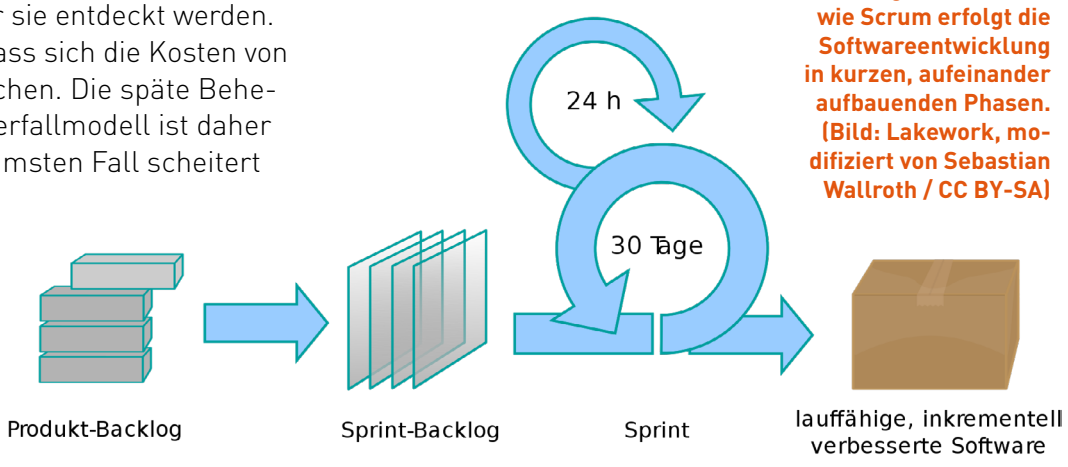
Foto: ChamilleWhite, BigStock

Bei jedem Release-Wechsel gab es deutliche Fortschritte in Funktionalität und Performance gegenüber dem Vorgänger. Oft handelte es sich sogar um völlige Neuentwicklungen, die nur bedingt kompatibel zur bisherigen Version waren. Unternehmen begegneten den Aktualisierungen meist mit Vorsicht, vor allem wenn geschäftskritische Prozesse betroffen waren. Erst nach monatelangen Tests wurden die neuen Releases eingeführt. Teils verzichteten Anwender auch ganz auf eine Aktualisierung, denn diese war meist mit hohen Kosten verbunden. Neue Versionen bedeuteten in der Regel nämlich auch, neue Lizenzen kaufen und neue Wartungsverträge abschließen zu müssen.

Das traditionelle Modell der Softwareentwicklung und -bereitstellung hat aber noch weitere Nachteile. Zwischen der Definition der neuen Features und Funktionen im Lastenheft und dessen Umsetzung vergehen viele Monate oder sogar Jahre. Ändern sich die Markt- und Wettbewerbsbedingungen in dieser Zeit – heute der Normalfall –, ist das Produkt schon veraltet, bevor es auf den Markt kommt. Tests sind im Wasserfallmodell zudem erst nach Abschluss der Entwicklungsarbeit vorgesehen. Fehler werden aber umso teurer, je später sie entdeckt werden. Die Zehnerregel[4] besagt, dass sich die Kosten von Phase zu Phase verzehnfachen. Die späte Behebung von Fehlern im Wasserfallmodell ist daher sehr kostspielig. Im schlimmsten Fall scheitert das gesamte Projekt.

Kurze Release-Zyklen dank Scrum und DevOps

Heute werden Softwareprojekte in der Regel nicht mehr von langer Hand geplant und neue Features vorab in einem Lastenheft definiert. Stattdessen erarbeiten kleine Teams agil und in kurzen Sprints von wenigen Tagen oder Wochen immer wieder eine neue lauffähige Version, die sofort getestet und veröffentlicht wird. Fehler fallen deshalb sehr viel früher auf und lassen sich kostengünstiger beheben. In einer Studie der Hochschule Koblenz[5] gaben 92 Prozent der Befragten an, agile Methoden zu verwenden. 85 Prozent der Teilnehmer sagten, agile Ansätze verbesserten Ergebnisse und Effizienz von Projekten und Entwicklungsprozessen. Laut dem CHAOS-Report[6] der Standish Group scheitern agile Projekte deutlich seltener als nach der Wasserfallmethode durchgeführte. Durch die kurzen Release-Zyklen von wenigen Tagen oder Wochen können Unternehmen außerdem sehr viel schneller auf Marktveränderungen und neue Anforderungen reagieren.



In agilen Ansätzen wie Scrum erfolgt die Softwareentwicklung in kurzen, aufeinander aufbauenden Phasen. (Bild: Lakework, modifiziert von Sebastian Wallroth / CC BY-SA)

4 https://www.sixsigmablackbelt.de/fehlerkosten-10er-regel-zehnerregel-rule-of-ten/

5 https://www.process-and-project.net/studien/studienunterseiten/status-quo-scaled-agile-2020/

6 https://www.standishgroup.com/sample_research_files/CHAOSReport2015-Final.pdf

Foto: ChamilleWhite, BigStock

Immer häufiger erfolgen Aktualisierungen sogar fortlaufend – Continuous Development, Integration und Deployment ist das Modell der Zukunft. Auch die typische organisatorische Trennung in Softwareentwicklung und Softwarebetrieb löst sich auf. Im DevOps-Konzept verantwortet ein Team den kompletten Lebenszyklus einer Anwendung.

Robuste Software durch Microservices

Um diese Geschwindigkeit zu ermöglichen, musste sich auch die Architektur der Software ändern. Bestanden Applikationen traditionell aus großen, in sich geschlossenen Blöcken, sind sie heute zunehmend modular aus kleinen, wiederverwendbaren Komponenten, sogenannten Microservices, aufgebaut. Diese Funktionseinheiten sind unabhängig voneinander und kommunizieren mit anderen Microservices über Standardschnittstellen.

Da Microservices separat voneinander entwickelt werden können, senkt dies den organisatorischen Aufwand in der Softwareentwicklung deutlich. Neue Funktionen oder Leistungsanforderungen lassen sich leicht über zusätzliche Mikroservices realisieren. Laut dem Report „State of Mikroservices 2020[7]", für den fast 700 Entwickler befragt wurden, sind Performance und Skalierbarkeit die wichtigsten Vorteile von Mikroservice-Architekturen. Auch die Auswirkung von Fehlern wird minimiert. Stürzt ein Mikroservices ab, hat das in der Regel keine oder nur geringe Auswirkungen auf das Gesamtsystem.

Cloud und Container auf dem Vormarsch

Auch die Art und Weise, wo und wie Software entwickelt und bereitgestellt wird, hat sich in den vergangenen Jahren drastisch verändert. 80 Prozent der für die DORA-Studie 2019[8] (DevOps Research and Assessment) befragten Entwickler und Administratoren arbeiten primär in der Cloud. Insgesamt wächst der Software-as-a-Service-Markt jährlich um mehr als 13 Prozent und soll bis 2022 einen Wert von mehr als 220 Milliarden US-Dollar erreichen[9].

Sowohl on-premises als auch in der Cloud setzt sich dabei immer mehr die Bereitstellung von Software in Containern durch. Applikationen werden dabei mit allen notwendigen Komponenten in eine lauffähige Umgebung verpackt, die sich schnell starten, zwischen Umgebungen verschieben und auch wieder stoppen lässt. Entwickler müssen sich so über Abhängigkeiten und unterschiedliche Laufzeitumgebungen keine Gedanken mehr machen. Da die Ressourcennutzung streng getrennt ist, hat ein fehlerhafter Container keine negativen Auswirkungen auf das Gesamtsystem. Laut dem Monitoring-Spezialisten Datadog nutzen bereits 25 Prozent der Unternehmen das Containersystem Docker[10], in großen Unternehmen sind es sogar fast 50 Prozent.

7 https://tsh.io/state-of-microservices/

8 https://cloud.google.com/blog/products/devops-sre/the-2019-accelerate-state-of-devops-elite-performance-productivity-and-scaling

9 https://www.prnewswire.com/news-releases/global-software-as-a-service-saas-market-report-2020-market-was-valued-at-134-44-bn-in-2018-and-is-expected-to-grow-to-220-21-bn-at-a-cagr-of-13-1-through-2022--300970629.html

10 https://www.datadoghq.com/docker-adoption/

Foto: ChamilleWhite, BigStock

Vom LAN zum WAN

Nicht zuletzt sind Anwendungen und Anwender mobiler geworden. Applikationen werden aus verschiedensten Quellen zur Verfügung gestellt, sei es aus dem eigenen Rechenzentrum, einer Cloud oder einem App-Store. Mitarbeiter greifen längst nicht mehr nur aus dem Firmenbüro auf Unternehmensressourcen zu, sondern arbeiten aus dem Home-Office oder nutzen unterwegs ihr privates mobiles Endgerät.

Durch diese Entwicklung hat sich der Verkehr aus dem traditionellen Firmen-LAN (Local Area Network) immer mehr ins Weitverkehrsnetz (Wide Area Network, WAN) verlagert, das Unternehmenszentrale und Zweigstellen mit diversen Cloud-Anbietern und Mobilfunk-Providern verbindet. Laut dem Data Center Industry Survey[11] des Uptime Institute wird bis 2021 die Hälfte alle Workloads außerhalb des Firmenrechenzentrums betrieben werden. Das Marktforschungsunternehmen Gartner prognostiziert [12], dass bis 2023 60 Prozent der Unternehmen das Netzwerk als Kernelement ihrer Digitalstrategie betrachten werden.

> Bis 2021 wird die Hälfte alle Workloads außerhalb des Firmenrechenzentrums betrieben.

Foto: a_v_d, BigStock

11 https://uptimeinstitute.com/2019-data-center-industry-survey-results

12 https://www.gartner.com/en/documents/3933946

Foto: ChamilleWhite, BigStock

Fazit: Herausforderungen für das Applikationsmanagement

Für die IT-Verantwortlichen ergibt sich aus diesen Entwicklungen eine ganze Reihe von Herausforderungen:

- Neue Applikationen und Releases lassen sich nicht mehr ausgiebig testen, bevor sie in den Produktivitätseinsatz kommen. Funktionale und nicht-funktionale Tests müssen daher als integraler Bestandteil der Entwicklungs-Pipeline betrachtet und weitgehend automatisiert werden.

- Die Anwendungslandschaft in Unternehmen wird heterogen. IT-Administratoren müssen neben traditionellen Applikationen und Mikroservice-Architekturen auch verschiedenste Plattformen und Bereitstellungsmodelle verwalten – von der Legacy-Software auf dem Mainframe bis zur SaaS-Lösung aus einer Public Cloud.

- Administratoren und Sicherheitsverantwortliche müssen immer mehr Anwendungen managen. Allein die Zahl offiziell genehmigter Cloud-Services stieg 2019 laut des Sicherheitsspezialisten McAfee [13] im Jahresvergleich um ein Drittel. Hinzu kommen Cloud-Services und mobile Apps, die Fachanwender ohne Wissen der IT-Abteilung buchen.

- Der Datenverkehr innerhalb und zwischen Applikationen nimmt zu und wird komplexer. Legitimer Traffic lässt sich dadurch nur schwer von unerwünschtem unterscheiden.

- Die Fehlersuche bei Performance-Einbußen wird schwieriger. In einem engen Geflecht aus Services, Applikationen, Infrastrukturen und Netzwerken kann die eigentliche Ursache eines Problems oft nicht oder nur nach einer ausgiebigen Analyse oder langem Herumprobieren identifiziert werden.

- Netze müssen immer mehr Daten in immer kürzerer Zeit transportieren. Der Hersteller Cisco prognostiziert in seinem VNI Forecast[14], dass im Jahr 2023 pro PC und Monat fast 60 Gigabyte (GB) an Daten ausgetauscht werden. Hinzu kommen rund 15 Milliarden IoT-Geräte (Internet of Things), die ebenfalls über das Weitverkehrsnetz kommunizieren.

- Der rasante Ausbau der Netzwerkkapazitäten führt zu hohen Folgeinvestitionen. Bis 2023 soll die durchschnittliche Bandbreite bei drahtgebundenen Breitbandverbindungen 110 Megabit pro Sekunde (Mbit/s) betragen[15]. Monitoring-, Analyse- und Sicherheitssysteme müssen ständig erneuert oder erweitert werden, um diesen Durchsatz bewältigen zu können. ■

13 https://www.mcafee.com/enterprise/de-de/about/newsroom/press-releases/2020/20200128-01.html

14 https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html

15 https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html

Foto: World Image, BigStock

Überwachung statt Abschottung

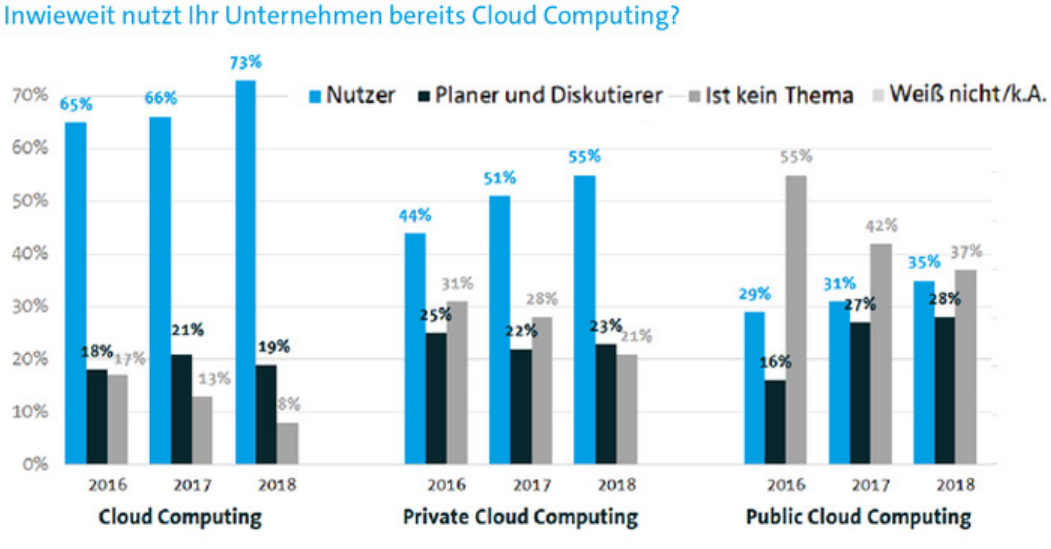
Sicherheit verteilter Anwendungslandschaften

Wenn Anwender und Applikationen mobil werden, vergrößert sich die Angriffsfläche für Cyber-Kriminelle erheblich. Sicherheitsverantwortliche stellt dies vor eine ganze Reihe von Herausforderungen.

In der alten IT-Welt gab es klare Verhältnisse: Applikationen wurden auf Servern in den Rechenzentren betrieben. Anwender griffen von ihren PCs in den Firmenbüros über das interne LAN darauf zu. Für den Schutz von Hard- und Software genügte es, am Perimeter Eindringlinge zu identifizieren und aufzuhalten – auch das zugegebenermaßen schon keine leichte Aufgabe.

Heute befinden sich Applikationen und Anwender dagegen oft außerhalb der schützenden Mauern. Laut einer Umfrage [16] des Bayerischen Forschungsinstituts für Digitale Transformation (bidt) arbeiten aktuell 43 Prozent der deutschen Berufstätigen im Home-Office, 39 Prozent davon mehrmals die Woche. Auch die Cloud-Nutzung befindet sich auf Rekord-

16 https://badw.de/die-akademie/presse/presse mitteilungen/pm-einzelartikel/detail/digitalisierung-durch-corona-verbreitung-und-akzeptanz-von-homeoffice-in-deutschland.html



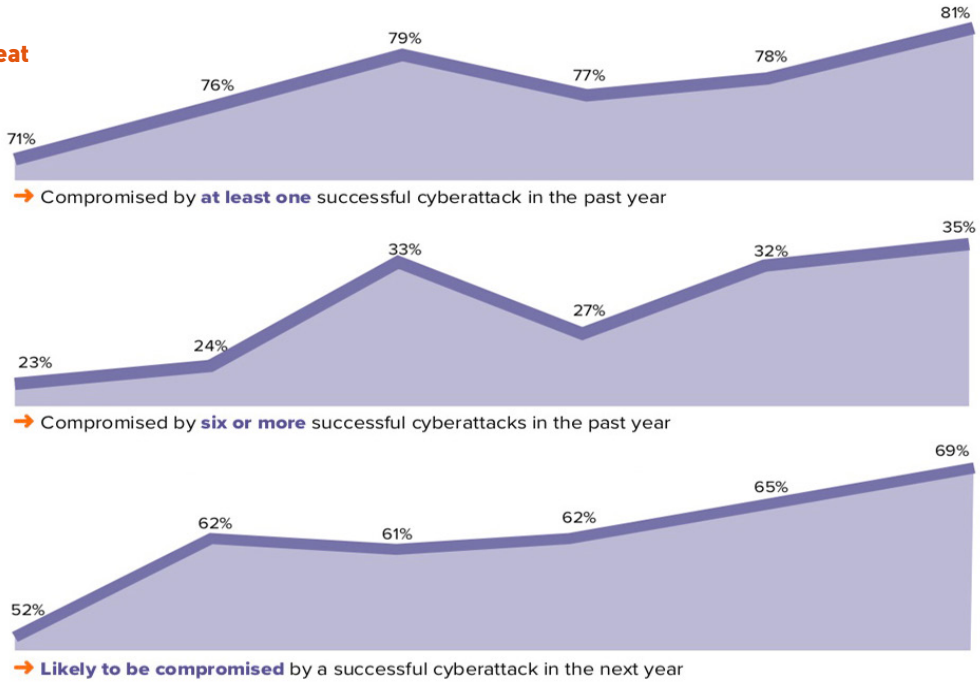
Basis: Alle befragten Unternehmen (2018: n=553 | 2017: n=557 | 2016: n=554) von 100 Prozent abweichende Werte ergeben sich aus Rundungsdifferenzen. Quelle: Bitkom Research

Die Cloud-Nutzung in Deutschland befindet sich auf Rekordniveau. (Bild: Bitkom Research)

KPMG | bitkom research

Foto: World Image, BigStock

Die Zahl erfolgreicher Angriffe steigt. (Bild: Gigamon, Quelle: 2020 Cyberthreat Defense Report)



niveau, wie der jährlich erhobene Cloud Monitor [17] von KPMG und Bitkom Research zeigt. Demnach nutzen drei Viertel der deutschen Unternehmen Cloud Computing, nur noch acht Prozent lehnen das Bereitstellungsmodell Cloud kategorisch ab.

Durch die Mobilität der Mitarbeiter und den Erfolg neuer Bereitstellungsmodelle entsteht eine bunte Mischung aus selbst betriebener Software im eigenen Rechenzentrum, Infrastruktur und Plattformen aus der Cloud sowie Software-as-a-Service. Die Folge ist eine enorme Zunahme des perimeterüberschreitenden WAN-Verkehrs (Wide Area Network), manchmal bis hin zum Verlust der Möglichkeit der Einschätzung drinnen/draußen oder gut/böse. Oft verliert die zentrale IT sogar komplett den Überblick. Ein Fünftel der Unternehmen weiß laut einer Umfrage im Auftrag des Sicherheitsspezialisten McAfee nicht, welche Daten sich in der Cloud befinden. [18]

Zahl erfolgreicher Angriffe steigt

Für Sicherheitsverantwortliche stellt dies eine zunehmende Herausforderung dar. Dem „2020 Cyberthreat Defense Report“ [19] des Marktforschungsunternehmen Cyberedge Group zufolge verzeichneten im vergangenen Jahr erstmals mehr als ein Drittel der befragten IT-Security-Entscheider und -Experten sechs oder mehr erfolgreiche Attacken. Mit fast 70 Prozent erreichte auch der Anteil derer Rekordniveau, die einen erfolgreichen Angriff in den kommenden zwölf Monaten für wahrscheinlich halten. Erpressungstrojaner stellen dabei nach wie vor eines der größten Probleme dar. Fast zwei Drittel berichteten über Ransomware-Attacken, zwei Jahre zuvor war es noch knapp über die Hälfte. Auch die Schäden werden größer: 57 Prozent der Betroffenen bezahlten Lösegeld für ihre Daten, zwölf Prozent mehr als im Vorjahr.

17 https://www.bitkom.org/Presse/Presseinformation/Cloud-Nutzung-auf-Rekordniveau-bei-Unternehmen

18 https://www.mcafee.com/enterprise/de-de/about/news-room/press-releases/2020/20200128-01.html

19 https://cyber-edge.com/cdr/

Foto: World Image, BigStock

Aber es gibt auch gute Nachrichten: Die von der Cyberegde Group befragten IT-Experten verzeichneten in allen erfassten Kategorien eine leichte Verbesserung des Sicherheitsniveaus. Auf einer Skala von 1 (= sehr schlecht abgesichert) bis 5 (= sehr gut abgesichert) verbesserte sich der Mittelwert um 0,23 Punkte auf 4,05. Besonders groß war die Verbesserung bei mobilen Endgeräten (+0,30), Laptops (+0,29) und Programmierschnittstellen (API, +0,26). Auch die Finanznot scheint ein Ende zu haben. 85 Prozent der Befragten verzeichneten eine Erhöhung ihres IT-Security-Budgets.

Kontinuierliche Überwachung statt Abschottung

Um verteilte Nutzer, Applikationen und Ressourcen zu schützen und Bedrohungen frühzeitig zu erkennen, müssen IT-Organisationen heute weniger auf die Abwehr von Angriffen am Perimeter und mehr auf eine kontinuierliche Überwachung und Analyse des Traffics setzen. Diese Früherkennung macht derzeit aber noch Schwierigkeiten. Gefragt nach den größten Hindernissen für einen besseren Schutz nannten die Teilnehmer an der Cyberthreat-Studie neben personellen Problemen vor allem die Datenflut und die mangelnde Automatisierung der Bedrohungserkennung und -bekämpfung. Security-Tools lieferten nach Aussage der Befragten außerdem zu wenig Kontextinformationen, um Alarme sinnvoll bewerten zu können. Dies wiederum trifft die Sicherheitsverantwortlichen doppelt, da „nicht automatisierte" Gegenmaßnahmen eine noch höhere Belastung der ohnehin knappen Ressource „qualifiziertes Personal" darstellen.

Auch die zunehmende Nutzung der Cloud macht den IT-Sicherheitsverantwortlichen Sorgen. An erster Stelle der Herausforderungen steht der Verlust von Daten und geistigem Eigentum, gefolgt von mangelhaften Sicherheitsvorkehrungen der Cloud-Provider und Verstößen gegen Gesetze und regulatorische Vorgaben. Die Autoren weisen außerdem auf eine weitere massive Sicherheitslücke hin: Nur in etwas über einem Drittel der befragten Unternehmen entschlüsseln und analysieren Security-Systeme den verschlüsselten HTTPS-Internetverkehr. Da Angreifer gerne Malware oder Command-and-Control-Befehle in den SSL/TLS-Verkehr einbetten und somit erfolgreich verstecken, stellt dies ein erhebliches Sicherheitsrisiko dar.

An erster Stelle der Herausforderungen steht der Verlust von Daten und geistigem Eigentum, gefolgt von mangelhaften Sicherheitsvorkehrungen der Cloud-Provider und Verstößen gegen Gesetze und regulatorische Vorgaben.

Foto: World Image, BigStock

Security-Trends 2020

Das auf IT-Security spezialisierte Beratungsunternehmen TAG Cyber [20] gibt bereits seit 2017 jährlich eine Übersicht über die 50 wichtigsten Cyber-Security-Handlungsfelder (Cyber Security Controls) heraus, die in der Art eines „Periodensystems" den sechs Kategorien „Enterprise", „Netzwerk", „Endpunkt", „Governance", „Daten" und „Industrie" zugeordnet werden. Hier einige der wichtigsten Erkenntnisse aus dem aktuellen Report [21]:

- Die Sicherheit von Cloud-Diensten verbessert sich durch die zunehmende Verbreitung und Effizienz von Cloud-Access-Security-Broker-Lösungen (CASB), Mikrosegmentierung und Cloud-Verschlüsselung.
- Mobilität wird mehr und mehr zum Alltag. Das Management und die Absicherung mobiler Endgeräte dürfen daher nicht mehr separat betrachtet werden, sondern müssen integraler Bestandteil der Enterprise-Security werden.
- Unternehmen verlassen sich immer weniger auf Maßnahmen der Perimetersicherheit. Lösungen wie Data Leakage Prevention (DLP), Intrusion-Detection / Prevention-Systeme (IDS / IPS) und Firewalls müssen daher in der Lage sein, Daten, Applikationen und Endgeräte unabhängig von deren physischer Lokalisierung zu schützen.
- Agile Ansätze, DevOps- und Continuous Development / Integration beschleunigen die Softwareentwicklung, tägliche Aktualisierungen sind keine Seltenheit mehr. Die IT-Sicherheit kann hier nur durch eine zunehmende Automatisierung Schritt halten. Das gilt sowohl für die Integration von Security-Tests in die Applikationsentwicklung als auch für das Management und die Aktualisierung von Web Application Firewalls (WAF), Web-Fraud-Prevention-Lösungen (WFP), der Abwehr von Distributed-Denial-of-Service-Attacken (DDOS) und anderen Security Controls.
- Die Bedeutung künstlicher Intelligenz – insbesondere von Deep Learning – für die Mustererkennung in Angriffen nimmt zu. Einsatzgebiete für selbstlernende Algorithmen sind beispielsweise WAF und WFP, Authentifizierung und Security-Information-and-Event-Management-Systeme (SIEM).

20 https://www.tag-cyber.com/
21 https://www.tag-cyber.com/analysis/annuals

Foto: World Image, BigStock

Fazit: Herausforderungen für die IT-Security

Für IT-Sicherheitsverantwortliche ergeben sich aus diesen Trends unter anderem folgende Herausforderungen:

- Immer mehr Daten müssen in immer kürzerer Zeit immer genauer analysiert werden. Sicherheitslösungen wie ATP (Advanced Threat Protection), WAF, E-Mail-Security, SIEM und andere auf Verhaltensanalysen basierende Systeme werden dabei häufig entweder komplett außen vor gelassen oder mit Daten überschwemmt, die für sie gar nicht relevant sind – beides hat einen negativen Einfluss auf die Sicherheit.
- Das Analysieren und Filtern führt entweder zu Performance-Verlusten oder muss durch überdimensionierte und damit eigentlich zu teure Systeme abgefangen werden.
- Soll für erhöhte Sicherheit auch der SSL-Verkehr entschlüsselt werden, sind weitere Investitionen nötig, da diese Aufgabe sehr ressourcenhungrig ist und sich ebenfalls negativ auf die Performance von Sicherheitssystemen auswirkt. ■

Foto: blackboard, BigStock

Mehr Effizienz, weniger Komplexität

Anwendungen intelligent managen und absichern

Um die Herausforderungen heutiger Anwendungs- und Nutzerlandschaften zu meistern, ohne dass Kosten und Managementaufwand explodieren, sind intelligente Systeme notwendig, die sich nahtlos in das Netzwerk integrieren lassen.

Hybride und Multi-Cloud-Umgebungen, unterschiedliche Bereitstellungsmodelle für IT-Ressourcen und Applikationen, zunehmend mobile Nutzer sowie die Vielzahl an Endgeräten haben die Komplexität von IT-Umgebungen drastisch erhöht. Für Administratoren und Sicherheitsverantwortliche wird es daher immer schwieriger, Ursache und Wirkung zu erkennen, unerwünschten Verkehr vom legitimen zu unterscheiden und Eindringlinge rasch zu identifizieren. In einem ersten Schritt gilt es daher, die Komplexität wieder zu reduzieren, indem das Management der Infrastruktur von der physikalischen Hardware abstrahiert wird, wie dies beispielsweise im Software-Defined Networking (SDN) geschieht. Switches und andere Netzwerkgeräte bilden dabei die sogenannte Data Plane, die für das physikalische Routing der Pakete verantwortlich ist. Das Management erfolgt logisch getrennt davon in der Control Plane, die softwarebasiert auf einem Server realisiert wird. Hardware muss so nicht mehr manuell konfiguriert werden, neue Routen, aber auch neue Funktionen können zentral und ohne physikalischen Zugriff ausgerollt werden.

Weniger Komplexität, mehr Flexibilität durch Inline Bypass

Ähnliche Vorteile bringen Inline-Bypass-Systeme, wie sie Gigamon in den Plattformen HC1, HC2 und HC3 bietet. Einmal im Netzwerk integriert, lassen sich Monitoring- und Security-Systeme logisch in die Leitung einschleifen, ohne dass physisch Änderungen vorgenommen werden müssten. Das reduziert die Komplexität deutlich und erhöht die Flexibilität. Der Anwender kann außerdem entscheiden, welcher Verkehr von welchem Gerät analysiert wird. Durch die gezielte Verkehrslenkung lassen sich Performance-Einbußen zuverlässig verhindern.

Die Segmentierung des Verkehrs schont auch die Investitionsbudgets. Wenn Systeme wie Web Application Firewalls (WAF) oder E-Mail-Security nur noch die für sie relevanten Daten verarbeiten müssen, lassen sie sich kleiner dimensionieren und müssen seltener erweitert oder ersetzt werden. Auch die Auflösung des Perimeters ist für eine solche logische Traffic-Steuerung kein Problem, denn

> Für viele Sicherheitssysteme ist nur ein Bruchteil des Internetverkehrs von Bedeutung.

Foto: blackboard, BigStock

das Routing kann unabhängig von der tatsächlich physischen Richtung erfolgen. So lässt sich etwa definieren, dass jedes Paket zunächst auf das Intrusion-Detection / Prevention-System (IDS/IPS) trifft, unabhängig davon, ob es von außen in das Firmennetzwerk gelangt oder im eigenen LAN erzeugt wurde.

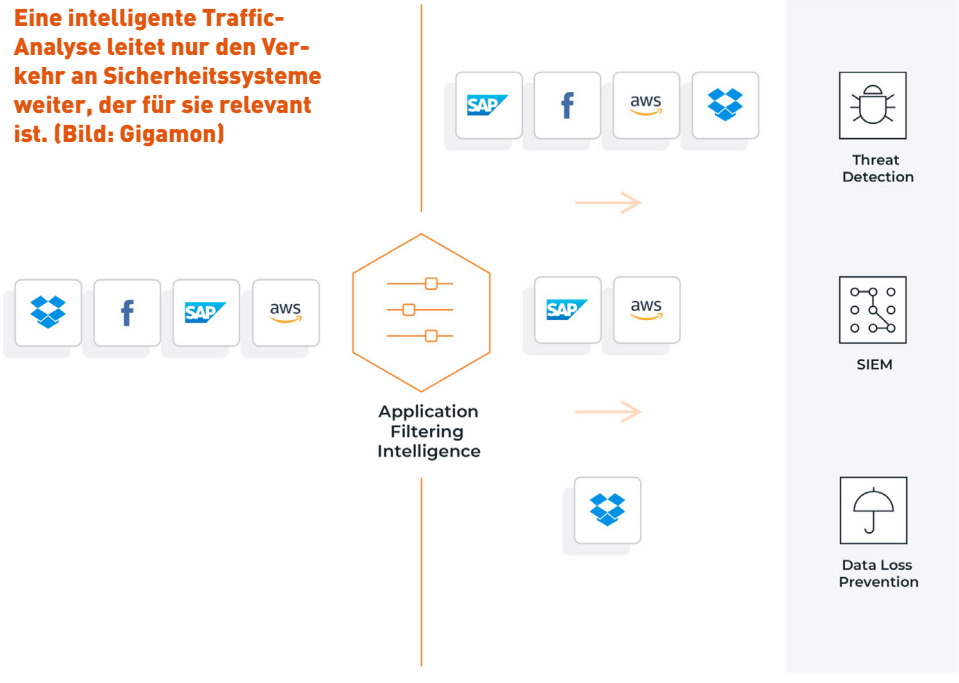
Traffic-Filterung schützt Investitionen

Der massive Anstieg der Datenmengen sowie der schnelle Ausbau von Breitbandanschlüssen und Netzwerkkapazitäten ziehen erhebliche Folgekosten nach sich. Wenn etwa eine Netzwerkinfrastruktur von 10-Gigabit-Ethernet auf 40-Gigabit-Ethernet aufgerüstet wird, müssen auch leistungsfähigere Sicherheitslösungen angeschafft werden, damit diese Systeme nicht zum Bottleneck werden und die Performance ausbremsen.

Für viele Sicherheitssysteme wie WAF, ATP (Advanced Threat Protection) oder E-Mail-Security ist aber nur ein Bruchteil des Internetverkehrs tatsächlich von Bedeutung. Mit einer entsprechenden Filterung der Daten lassen sich Einsparpotenziale realisieren und Performance-Probleme beheben. Traffic-Filter verlängern daher die Einsatzdauer des bestehenden Equipments, auch wenn durch Netzwerk-Upgrades oder das Wachstum des Datenaufkommens die Anforderungen steigen.

Die Gigamon Application Filtering Intelligence [22] (AFI) erkennt beispielsweise tendeziell risikoarmen Datenverkehr wie Video-Streams, der von Netzwerk- und Sicherheits-Tools nicht beziehungsweise nur einer generellen Sicherheitsbehandlung unterworfen werden muss, und leitet ihn um teure Spezialwerkzeuge herum. So können sich Sicherheitsverantwortliche auf den risikoreichen Datenverkehr konzentrieren und diese Pakete an die richtigen Sicherheitstools senden.

Eine intelligente Traffic-Analyse leitet nur den Verkehr an Sicherheitssysteme weiter, der für sie relevant ist. (Bild: Gigamon)



22 https://www.gigamon.com/de/products/optimize-traffic/application-intelligence/application-filtering-intelligence.html

Foto: blackboard, BigStock

Effizientes Applikationsmanagement braucht Transparenz

Um Applikationen effizient managen und absichern zu können, müssen IT-Verantwortliche wissen, was sich in ihrem Netzwerk abspielt. Hierbei ist es essentiell, dass nicht nur das verwendete Protokoll (in den meisten Fällen HTTPS), sondern die tatsächliche Anwendung (etwa Facebook oder Netflix) erkannt wird. Sie benötigen daher Lösungen, die Anwendungen automatisch identifizieren und einordnen können.

Gigamon AFI etwa klassifiziert Anwendungen auf der Grundlage verschiedener Attribute rund um das Verkehrsverhalten. Auf diese Weise lässt sich der Datenverkehr von über 3.000 Standardsoftwareapplikationen sowie von benutzerdefinierten Anwendungen genau identifizieren und filtern. AFI erkennt die Applikationen unabhängig von Kapselung, Port-Nummer oder Verschlüsselung, auch ohne diese aufbrechen zu müssen.

SSL-Entschlüsselung ohne Performance-Einbußen

Nahezu der gesamte Internetverkehr wird heute verschlüsselt übertragen. Laut dem Google-Transparenzbericht [23] verwenden 96 der Top-100-Websites standardmäßig HTTPS. Aber auch Cyber-Kriminelle vertrauen auf das Protokoll, um Malware einzuschleusen oder die Kommunikation mit einem Command-and-Control-Server zu tarnen. Dennoch entschlüsselt nur etwa ein Drittel der Unternehmen SSL/TLS-Verkehr (siehe dazu auch den Beitrag „Sicherheit verteilter Anwendungslandschaften“).

Dies hat vor allem Performance-Gründe. Firewalls, IPS und andere Sicherheitssysteme sind zwar durchaus in der Lage, HTTPS-Verkehr zu entschlüsseln, diese Aufgabe ist aber sehr ressourcenhungrig und belastet die CPU. Unternehmen müssen dann einen geringeren Durchsatz in Kauf nehmen oder in neue leistungsfähigere Systeme investieren. Da jede Lösung den Verkehr separat wieder aufs Neue entschlüsselt, kommen so erhebliche Mehrkosten zusammen.

Mit der GigaSMART-Lösung [24] ist SSL-Entschlüsselung nicht auf bestimmte Geräte oder Ports beschränkt. Jedweder Datenverkehr, der auf der Visibility Platform empfangen wird, kann entschlüsselt und jedem beliebigen angeschlossen Gerät zur Verfügung gestellt werden. Ein höherer Durchsatz lässt sich einfach durch Hinzufügen weiterer GigaSMART-Module erreichen. So kann das System mit steigenden Anforderungen an die SSL-Verarbeitung wachsen, ohne dass eine Vielzahl von Geräten ausgetauscht oder erweitert werden müsste.

Da der SSL-Verkehr sensible Benutzerdaten enthalten kann, achtet Gigamon besonders auf den Datenschutz. Nachdem die Pakete entschlüsselt wurden, können diese segmentiert werden, um private Nutzerdaten zu entfernen. Alternativ können sensible Felder maskiert werden. In beiden Fällen werden private Daten von den Überwachungswerkzeugen weder gespeichert noch gelesen oder analysiert. Dies erleichtert die Einhaltung der gesetzlichen und manchmal komplizierten und unübersichtlichen Vorschriften und vereinfacht den Prüfungsprozess erheblich.

23 https://transparencyreport.google.com/https/overview?hl=de

24 https://www.gigamon.com/de/products/optimize-traffic/traffic-intelligence/gigasmart/ssl-tls-decryption.html

Foto: blackboard, BigStock

Guter Schutz braucht Kontextinformationen

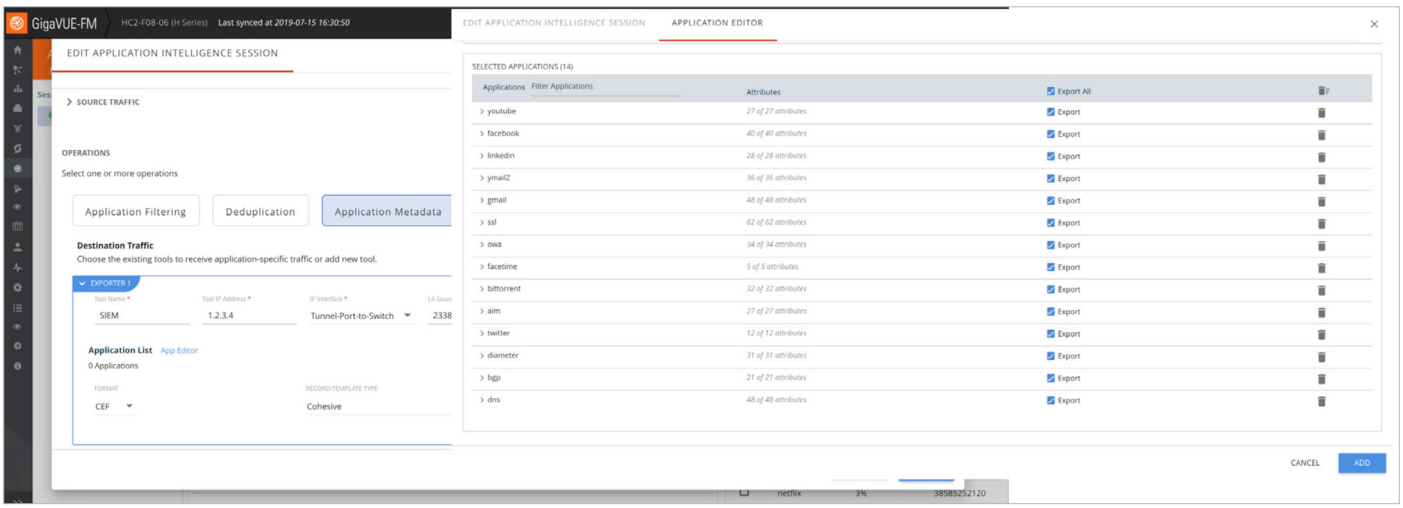
SIEM-Systeme (Security Information and Event Management) sind umso effizienter, je mehr Daten sie analysieren können. Leider steigen durch volumenbasierte Lizenzmodelle auch die Kosten, wenn zusätzliche Datenquellen erschlossen werden. Dabei sind bis zu 90 Prozent der Informationen für eine Sicherheitsanalyse kaum relevant. Intelligente Systeme können die Spreu vom Weizen trennen. Sie stellen den SIEM-Lösungen nur die relevanten Metadaten zur Verfügung, die etwa für eine Verhaltensanalyse völlig ausreichend sind. So lässt sich mit kleineren, preisgünstigeren SIEM-Systemen erheblich mehr Traffic untersuchen und absichern.

Die Gigamon Application Metadata Intelligence [25] (AMI) kann beispielsweise kontextbezogene Informationen auf Basis der OSI-Schichten vier bis sieben bereitstellen. Netzwerk- und Sicherheits-Tools stehen dabei mehr als 7.000 Metadatenattribute zur Verfügung, die Aufschluss über die Leistung der Anwendung, das Kundenerlebnis und die Sicherheit geben.

Fazit: Neue Zeiten brauchen neue Wege

Komplexe verteilte IT-Landschaften, eine steigende Zahl von Applikationen und Endgeräten sowie die Explosion des Datenverkehrs machen herkömmliche Konzepte des Managements und der Absicherung von IT-Infrastrukturen teuer und träge und somit oft unwirksam. Administratoren und Sicherheitsverantwortliche suchen daher beständig nach neuen Wegen, IT-Verwaltung und IT-Sicherheit zu verbessern, ohne dass Kosten und Komplexität aus dem Ruder laufen. Mit intelligenten Werkzeugen wie der Gigamon-Plattform kommen sie diesem Ziel ein gutes Stück näher. Die intelligente Traffic-Steuerung und -Analyse trennt den logischen vom physischen Netzverkehr, gibt endlich wieder Durchblick im Dschungel der Applikationen und versorgt jedes Analyse- und Sicherheitssystem mit genau den Informationen, die es für seine Arbeit benötigt. ■

Über das Dashboard kann der Anwender genau definieren, welche Metadaten exportiert werden sollen. (Bild: Gigamon)



25 https://www.gigamon.com/products/optimize-traffic/application-intelligence/application-metadata.html

Wenn Netzwerke auf die neue Zukunft treffen

Ein Homeoffice-Modell, grenzenlose Sicherheit und schrumpfende Budgets. So kommen Sie damit zurecht.

Gigamon®

Einleitung

Die Welt hat sich gerade verändert. Innerhalb kürzester Zeit haben unvorhergesehene globale Ereignisse zu gewaltigen Veränderungen in unserem Arbeits- und Alltagsleben geführt.

In Bezug auf den Netzwerkbetrieb und der Informationssicherheit müssen neu verteilte Belegschaften sowie digitale Prozesse mit einem abnehmenden Budget zurechtkommen. Die Netzwerkinfrastruktur und -Tools sind bei den meisten Organisationen darauf ausgelegt, vorwiegend im Büro tätige Mitarbeiter/-innen zu unterstützen. Von einem Tag auf den anderen musste die IT umgerüstet werden, um zwei- bis dreimal mehr Mitarbeiter/-innen remote zu unterstützen, als je eingeplant waren. Hinzu kommt, dass die Sicherheit besonders gewährleistet sein muss, da sich der Netzwerkverkehr von innen nach außen verlagert hat. Die schnellen Änderungen an den Netzwerken und den Tools werfen neue Bedenken hinsichtlich Sicherheit, Belastbarkeit und Performance auf. Auch die Anwendungen, auf die wir angewiesen sind – ob als individuelle Lösungen, als Standardpaket oder webbasiert –, werden an bisher ungeahnte Belastungsgrenzen gebracht.

Überblick

Dieses Whitepaper befasst sich mit den wichtigsten Herausforderungen in der IT, denen sich Organisationen jetzt und in der neuen Zukunft stellen müssen:

+ **HEUTE**

  Es ist unerlässlich, die Sicherheit und Kontinuität des Betriebs in dieser neuen, von innen nach außen gerichteten Umgebung zu gewährleisten und gleichzeitig die Netzwerkressourcen umzugruppieren, um das höchstmögliche Niveau im Kundenerlebnis wie auch der internen Benutzererfahrung aufrechtzuerhalten.

+ **DIE NEUE ZUKUNFT**

  Angesichts der allgegenwärtigen Unsicherheit im Hinblick auf die Kapitalmärkte, weltweite Lieferketten, die Regierungspolitik und die Verbraucherstimmung müssen Organisationen flexibel sein, um schnell und kosteneffizient auf neue und unvorhergesehene Herausforderungen und Chancen zu reagieren.

Wir möchten mit Ihnen unsere Erkenntnisse darüber teilen, wie sich Organisationen in diesen unbekannten Gewässern am besten zurechtfinden können – basierend darauf, was wir bei unseren Kunden aus führenden Organisationen aller Branchen beobachten können.

Telefonica gewann eine höhere Sichtbarkeit über das gesamte Netzwerk hinweg und ging bereits auf Probleme ein, währenddessen sie Änderungen am Netzwerk vornahmen. Während des Bereitstellungsprozesses half Gigamon bei der Fehlerbehebung eines Performanceproblems der DNS-Cache-Server-Farm und löste es per Fernzugriff, um einen möglichen Serviceausfall zu vermeiden und auf diese Weise die Leistung des gesamten DNS-Systems von Telefonica zu optimieren. Laut einer Studie der Enterprise Strategy Group (ESG) hilft das den Kunden von Telefonica, Ausfallzeiten um 30-50 Prozent zu reduzieren.

Telefonica Sichtbarkeit während des Übergangs verschaffen.

Heute

Die IT wird dazu aufgefordert, zusätzliche Kapazitäten und Services schneller bereitzustellen als je zuvor und diese neuen Kapazitäten dabei ebenso mit drei entscheidenden Anforderungen in Einklang zu bringen:

Ein neues Homeoffice-Modell

Bestimmte Aspekte der Infrastruktur und der Anwendungen stehen vor Herausforderungen bei der Skalierung – und das in einem wahrscheinlich noch nie dagewesenem Ausmaß. Durch den plötzlichen und schnellen Wechsel hin zum Homeoffice bleibt den IT-Teams nur wenig Zeit, ihre Remote-Access-Infrastruktur für die Mitarbeiter/-innen zu skalieren. Da sie sich darum bemühen, Kapazitäten zur Remote-Arbeit schnell online zu schalten, indem sie ältere oder die bestehende Infrastruktur umfunktionieren, können in den neuen Netzwerksegmenten und der -infrastruktur Probleme wie Ausfälle und Engpässe auftreten. Es ist von entscheidender Bedeutung, solche Probleme schnell aufzudecken. Doch angesichts der ohnehin knappen Ressourcen werden diese Aufgaben zu einer wirklich großen Herausforderung.

Neben der Unterstützung interner Nutzer wird die IT auch zunehmend mit der Nutzung externer Apps konfrontiert. Kunden kommunizieren mit Unternehmen jetzt hauptsächlich über mobile Apps oder online.
Unsere Kunden aus der Finanzdienstleistungs-, Gesundheits-, Unterhaltungs- und Einzelhandels-branche verzeichnen einen deutlichen Anstieg der Nutzer und der Nutzungsfrequenz ihrer Consumer-Apps. Da neue Anwendungscontainer, Microservices und virtuelle Maschinen schnell aufgestellt werden, um der plötzlichen Zunahme der Nutzernachfrage gerecht zu werden, laufen IT- und Infrastrukturteams Gefahr, von schnell arbeitenden DevOps- und Anwendungsteams überholt zu werden. Dieses Ungleichgewicht in der Anpassung kann schwerwiegende Folgen haben. Während die Kapazität für Applikationen möglicherweise ansteigt, könnte die Infrastrukturkapazität hinterherhinken. So könnten Probleme mit der Netzwerkbandbreite und der Benutzererfahrung entstehen; der Zugriff sowie die Nutzung von Anwendungen und Daten könnten möglicherweise nicht ausreichend auf Bedrohungen hin überwacht werden.

Grenzenlose Sicherheit über das Netzwerk hinaus

Jede zusätzliche Aktivität von Netzwerknutzern in neuen Netzwerksegmenten kann zu einer potenziellen Quelle für Bedrohungen wie Datenlecks oder Ransomware werden. „Bad Actors“ nutzen die vorherrschende Paranoia und Unsicherheit schnell aus, um die Systeme der Nutzer zu kompromittieren. Diese Bedrohungen nutzen Dropper, die dann dazu verwendet werden, zusätzliche Malware auf die Systeme der Nutzer herunterzuladen, um Zugangsdaten zu kompromittieren, was letztlich zu Ransomware-Angriffen und potenzieller Datenexfiltration führt. (Beispiele dafür finden Sie hier[1] und hier[2].)

Da Mitarbeiter im Homeoffice ihr Heimnetzwerk und/oder ihre privaten Geräte für die Arbeit nutzen, besteht die große Herausforderung darin, dass auf Daten nicht mehr von innerhalb des Netzwerks sondern von außerhalb zugegriffen wird. Und dabei kann man sich nie sicher sein, ob jeder Arbeitnehmer auch tatsächlich die empfohlenen Sicherheitsprotokolle befolgt. Selbst die vorgeschriebene Nutzung von VPN-Verbindungen löst das Problem nicht unbedingt, insbesondere dann nicht, wenn die Endpunkte nicht kürzlich gepatcht wurden. Beispielsweise gibt es Berichte zu Schwachstellen bei verschiedenen VPN- und Firewall-Herstellern, die es Varianten des Botnet-Typs Mirai ermöglichen, die Kontrolle zu übernehmen[3]. Beim Bestreben, Kapazitäten zu erhöhen, müssen Unternehmen bei älterer Ausrüstung sicherstellen, dass diese auch tatsächlich für ihre Zwecke geeignet sind und sowohl gepatcht als auch gesichert werden können.

Arbeiten mit gekürzten Budgets

Da viele Sektoren der Wirtschaft herunterfahren, treffen Organisationen Vorkehrungen für eine mögliche Rezession. Gerade die Reise-, Unterhaltungs- und Dienstleistungsbranchen sind stark betroffen. Aufgrund der sich daraus ergebenden Auswirkungen auf die gesamte Wirtschaft planen Organisationen Budgetkürzungen, Einstellungsstopps und Ausgabeneinschränkungen. IT- und Anwendungsteams spüren diese Auswirkungen besonders stark, da sie ihre gekürzten Ressourcen dennoch erweitern müssen – mit weniger mehr erreichen, war noch nie so dringend wie heute.

[1] https://www.forbes.com/sites/thomasbrewster/2020/03/18/coronavirus-scam-alert-covid-19-map-malware-can-spy-on-you-through-your-android-microphone-and-camera/#37bf4a0a75fd

[2] https://www.businessinsider.com/hackers-are-using-fake-coronavirus-maps-to-give-people-malware-2020-3

[3] https://krebsonsecurity.com/2020/03/zxyel-flaw-powers-new-mirai-iot-botnet-strain/

Die Neue Zukunft

Bleiben Sie fokussiert, während Sie Ihre Optionen bewerten

Während die Wirtschaft den Schock der letzten Wochen noch verdaut, bereiten sich viele Organisationen bereits auf eine mögliche Rezession vor. Die globalen Lieferketten wurden zunächst in Asien unterbrochen. Diese Auswirkungen werden nun durch die dramatischen Veränderungen in der europäischen und der US-amerikanischen Wirtschaft verstärkt und verschärfen sich somit. Diese Veränderungen wirken sich dramatisch auf die Reise-, Gastgewerbe-, Einzelhandels-, Unterhaltungs- und Dienstleistungsbranchen aus. Auch bei Unternehmen, die nicht direkt von erzwungenen Schließungen betroffen sind, führen die allgemeinen Auswirkungen auf die Wirtschaft dazu, dass fast alle IT-Organisationen ihre Ausgabenprioritäten und Budgets überprüfen.

Geschäftsbereiche und IT-Organisationen der Unternehmen bewerten auf Basis der aktuellen Unsicherheiten ihre Prioritäten: Wie lange wird die Krise dauern? Welche zusätzliche Netzwerkbandbreite, Anwendungen und Dienste müssen hinzugefügt werden? Wie sollen sie mit den Herausforderungen und, in manchen Fällen, mit den Chancen dieser Krise umgehen? Wird sich das Homeoffice möglicherweise dauerhaft in ihren Organisation etablieren?

Ein Weg, um viele dieser Herausforderungen zu meistern, liegt darin, die Information-in-Motion eines Netzwerks für die Anwendungs-, Benutzer- und Geräteerkennung, für die Fehlerbehebung, Anwendungsperformance, das Monitoring der Benutzererfahrung sowie die Security zu nutzen. Netzwerkdaten sind die „Single Source of Truth“ (SSOT) für die wahre Performance und Sicherheit Ihres Netzwerks. Sind diese Daten zuverlässig und aktuell, müssen die Teams nicht ständig die Log-Level auf Servern ändern, Anwendungsentwickler daran erinnern, Applikationen zu instrumentieren oder neue Anwendungen zum Monitoring hinzuzufügen.

Um sicherzustellen, dass diese Daten zuverlässig genug sind, um sie als SSOT zu klassifizieren, ist es zwingend erforderlich, dass diese Information-in-Motion aus physischen, Cloud- und virtuellen Umgebungen, Anwendungssystemen, Log Files und anderen Datenquellen enthalten. Zu den Best Practices zählt die Verwendung eines „Wire Once“-Modells, bei dem alle Information-in-Motion sofort für Security- und Performance-Monitoring-Tools verfügbar sind, wenn neue Netzwerksegmente online geschaltet werden. Der Zugriff auf Netzwerkdaten sollte schnell, mit minimalen Eingriffen und mit wenig bis gar keiner Abhängigkeit von Anwendungen, DevOps und anderen Teams erfolgen.

Under Armour benötigte vollständige Sichtbarkeit in die Performance und Security ihrer digitalen Anwendungen. Diese Zuverlässigkeit war der Schlüssel, um die Kundenerwartungen im Hinblick auf Benutzererfahrung und -vertrauen zu erfüllen. Laut eines ESG-Berichts ermöglichte Gigamon eine um 75 Prozent höhere Sichtbarkeit in den Netzwerkverkehr.

„Durch die vollständige Sichtbarkeit der Performance und Sicherheit unserer digitalen Anwendungen können wir die Erwartungen unserer Kunden in Bezug auf Benutzererfahrung sowie das Vertrauen, auf das unsere Kunden bestehen, einlösen."

Under Armor dabei unterstützen, seine Kunden zu schützen.

Bleiben Sie fokussiert, während Sie Ihre Optionen bewerten

Auch wenn der Ausgang der aktuellen Krise unklar bleibt, möchten wir Ihnen unsere Empfehlungen ans Herz legen, wie Sie Ihre Organisation darauf vorbereiten können, um erfolgreich aus der Krise hervorzugehen.

BENUTZERERFAHRUNG VON ANWENDUNGEN.

Mehr denn je zeigt sich, dass digitale Anwendungen für Unternehmen von entscheidender Bedeutung sind, um die bestmögliche Kunden- und Benutzererfahrung sicherzustellen. Das war noch nie so wichtig wie heute.

Um das zu erreichen, ist es wichtig, Tools einzusetzen, die nicht nur die Nutzung der Anwendung und der Benutzererfahrung monitoren und visualisieren, sondern auch in der Lage sind, auf Basis der Performance und des Verhaltens dieser Anwendungen Maßnahmen zu ergreifen.

Beispielsweise kann ein Anstieg des Traffics durch Videokonferenzen aufgrund der intensiven Nutzung von Anwendungen wie Cisco WebEx, GoToMeeting, Skype und Zoom sehr schnell Out-of-Band-Security-Tools wie Intrusion Detection überlasten. IT-Teams müssen schnell visualisieren können, welche Anwendungen den Anstieg des Traffics verursachen, entscheiden, ob und in welchem Umfang dieser Traffic analysiert werden soll, und daraufhin sicheren oder risikoarmen Traffic herausfiltern, um die Bandbreite für andere Anwendungen aufrecht zu erhalten.

GRENZENLOSE NETZWERKSICHERHEIT.

Vor dem Hintergrund immer häufigerer und raffinierterer Cyber-Angriffe hat die COVID-19-Pandemie eine neue Welle von Bad Actors angespült, die sich zunutze machen wollen, dass InfoSec-Teams häufig überlastet sind und dass Nutzer lokal und global nach Informationen über das Virus suchen. Aus diesem Grund war es noch nie so wichtig wie heute, über die richtigen Sicherheits-Tools und reichhaltige Netzwerkdaten zu verfügen. Beispiele für verschiedene Tools, die sowohl kurz- als auch langfristig unterstützen können:

+GEFAHRENERKENNUNG UND -BEKÄMPFUNG

Durch die verstärkte Nutzung von Homeoffice, das auf schnell wachsenden VPN-Architekturen basiert, steigen sowohl die Angriffsfläche als auch die Schwachstellen. Organisationen müssen daher zwingend über leistungsfähige Tools verfügen, um neue Bedrohungen zu erkennen und darauf zu reagieren. Beispielsweise bieten auf Ingress/Egress-Verbindungen und auf VPN-Konzentratoren ausgelegte Tools einen gezielten Ansatz zur Minderung potenzieller Risiken.

+ZENTRALISIERTE TRAFFIC-ENTSCHLÜSSELUNG

Während viele Tools verschlüsselten Datenverkehr entschlüsseln können, ist der Einsatz einer zentralisierten Lösung zur Entschlüsselung und Überprüfung des verschlüsselten Datenverkehrs für viele Organisationen oft die effizienteste Lösung. Durch die Zentralisierung der TLS-Entschlüsselungsfunktionen kann der Datenverkehr einmal entschlüsselt und überprüft werden, bevor er erneut verschlüsselt und über mehrere Tools verteilt wird. Es kann wichtig sein, verschlüsselten Datenverkehr von und zu Anwendungen untersuchen zu können, um zu erkennen, ob der Anwendungs- und Datenzugriff legitim oder illegitim ist. Da die Applikationskapazität dynamisch zunimmt, werden bestehende Anwendungen schnell neu konzipiert und neue Anwendungen hochgefahren.

+NUTZEN SIE METADATEN, UM DIE SIEM-EFFIZIENZ ZU STEIGERN

Nutzen Organisationen Lösungen wie Splunk oder andere SIEMs für das aktive Security-Monitoring, kann die Einspeisung von System- und Anwendungsmetadaten in diese Lösungen eine leistungsfähige Methode sein, um die Compliance zu gewährleisten und gleichzeitig neue Anwendungen und Kapazitäten online zu bringen. Organisationen sollten immer versuchen sicherzustellen, dass nur präzise und relevante Metadaten an diese Tools gesendet werden, um den ihnen bereitgestellten Kontext zu maximieren und gleichzeitig die Datenmenge, die an sie gesendet wird, zu minimieren. Das gilt besonders bei SIEM-Tools, die auf Basis des Volumens der verarbeiteten oder gespeicherten Daten Kosten abrechnen.

+ZERO TRUST

Viele Organisationen befanden sich bereits in der Lern-, Planungs- oder Implementierungsphase einer Zero-Trust-Initiative. Die aktuelle Krise könnte der Wendepunkt zur Beschleunigung dieser Initiativen sein. Der Grundgedanke von Zero Trust besteht darin, das implizite Vertrauen, das mit dem Zugriffsort verbunden ist, zu beseitigen und die defensiven Perimeter einer Organisation vom Rand des Netzwerks zu den Assets zu verlagern, die das Netzwerk nutzen. Dazu zählen Nutzer, Geräte, Daten und Anwendungen.

Ob als Folge der COVID-19-Krise oder aufgrund einer geplanten Umstrukturierung des Geschäftsmodells: Die Arbeitswelt verändert sich hin zu einem flexiblen Modell, bei dem man egal von wo und egal wann arbeiten kann. Daher macht der Weg hin zu einer Zero-Trust-Architektur einfach Sinn. Es ist entscheidend für eine umfassende Zero-Trust-Lösung, dass alle Information-in-Motion im Netzwerk sichtbar sind.

Häufig wird Zero Trust als eine Reise beschrieben, die umfangreich geplant werden muss, um sie erfolgreich umzusetzen. Viele Organisationen haben diese Reise zu spät geplant oder zu spät begonnen. Angesichts der COVID-19-Pandemie und der damit verbundenen Neuorientierung, war es noch nie so wichtig wie jetzt, die Sicherheitsinfrastruktur zu rationalisieren und zu vereinheitlichen.

KOSTENEINSPARUNGEN DURCH DIE OPTIMIERUNG DER INVESTITIONEN IN TOOLS.

Die meisten Organisationen haben bereits umfangreich in Netzwerk- und Sicherheitstools investiert, die sie zur Verwaltung und Sicherung ihrer Netzwerke und Anwendungen nutzen. Da sich der Datenverkehr von LAN auf WAN verlagert, ist es entscheidend, dass der Datenfluss zu diesen Tools keine Tool-Überlastung, blinde Flecken bei der Sichtbarkeit oder andere Probleme durch den zunehmenden Traffic verursacht.

Um die Effizienz – und den ROI – der Tools eines Unternehmens zu maximieren, muss der Netzwerkverkehr von physischen, virtuellen und Cloud-Umgebungen optimiert werden, noch bevor dieser an die Tools weitergeleitet wird. Geschieht dies nicht, kann das zu einer Überlastung von Tools, zu erzwungenen manuellen Eingriffen der Teams in sonst automatisierte Prozesse sowie zu Problemen mit der Netzwerk-Verfügbarkeit, -Zuverlässigkeit und -Sicherheit führen.

Das US-amerikanische Gesundheitsministerium rüstete sein Netzwerk auf 10 Gbit/s auf, aber viele ihrer Security-Tools verfügten nur über Netzwerkschnittstellen mit 1 Gbit/s. Dank Gigamon konnten auch die älteren Tools mit dem Datenverkehr aus dem schnelleren Netzwerk arbeiten. Laut einer ESG Studie kann Gigamon Hardware und Tools in der richtigen Größe liefern, was zu Einsparungen von 40-50 Prozent führt.

Schnelligkeit und Kosteneinsparungen für das US-Gesundheitsministerium.

Abschließende Gedanken

Die Summe der aktuellen globalen Ereignisse hat unsere Realität über Nacht verändert. NetOps und InfoSec-Teams müssen mit massiven Beeinträchtigungen umgehen können, da die Nutzer im Homeoffice sind und sich auf eine ungewisse Zukunft vorbereiten. In dieser Situation sind Sichtbarkeit und Flexibilität der Infrastruktur zu wichtigen Erfolgsfaktoren für Organisationen geworden, um bestmöglich auf diese Herausforderungen zu reagieren.

Über Gigamon

Gigamon ist das erste Unternehmen, das eine einheitliche Netzwerksichtbarkeit und -analyse aller Information-in-Motion von Rohpaketen bis zu Apps über physische, virtuelle und Cloud-Infrastrukten hinweg bietet. Wir aggregieren, verarbeiten und analysieren Netzwerk-Traffic, um kritische Performance- und Sicherheitsanforderungen zu erfüllen, einschließlich einer schnellen Gefahrenerkennung und -bekämpfung – sodass Sie digitale Innovationen vorantreiben können.

Gigamon hat bereits über 75 Technologiepatente erhalten und erfreut sich einer in der Branche führenden Kundenzufriedenheit mit mehr als 3.000 Unternehmen darunter mehr als 80 der Fortune 100.

Für weitere Information und wie Gigamon Ihnen helfen kann, besuchen Sie www.gigamon.com/de/

Wir laden Sie ein, unserer Online Community, insbesondere unserer Homeoffice Collaboration Group beizutreten, wo Sie sich zu Ihren Sorgen, Überlegungen und Ideen mit den Kolleginnen und Kollegen aus Ihrer Branche sowie mit Gigamon Experten austauschen können.

Gigamon®

Internationaler Hauptsitz
3300 Olcott Street, Santa Clara, CA 95054, USA
+1 (408) 831-4000 | www.gigamon.com

2020 Cyberthreat Defense Report

Executive Briefing

PLATIN-SPONSOR

Gigamon®

Demografische Daten zur Umfrage

- Antworten von 1.200 qualifizierten Entscheidern und Experten im Bereich IT-Sicherheit
- Ausschließlich Mitarbeiter von Organisationen mit mehr als 500 Beschäftigten
- Organisationen aus 17 Ländern in Nordamerika, Europa, Asien-Pazifik, Nahost, Lateinamerika und Afrika
- Organisationen aus 19 Branchen

„[Organisationen] müssen wesentlich besser darin werden, große Informationsmengen zu sammeln und zu analysieren, um Anomalien festzustellen … Glücklicherweise reagieren die Anbieter darauf, dass der Markt nach besseren Tools für die Datensammlung, Datenanalyse und Prozessautomatisierung verlangt."
– 2020 CDR

Der siebte jährliche Cyberthreat Defense Report der CyberEdge Group gibt detailliert Aufschluss darüber, wie IT-Sicherheitsexperten Cyberbedrohungen wahrnehmen und wie sie diese bekämpfen möchten. Dieser Bericht basiert auf einer Umfrage, die im November 2019 unter 1.200 Entscheidungsträgern und Experten im Bereich IT-Sicherheit durchgeführt wurde. Er bietet zahlreiche Einblicke, die IT-Sicherheitsteams ein besseres Verständnis für ihre Wahrnehmungen, Prioritäten und Sicherheitssysteme im Vergleich zu denen anderer Wettbewerber vermitteln.

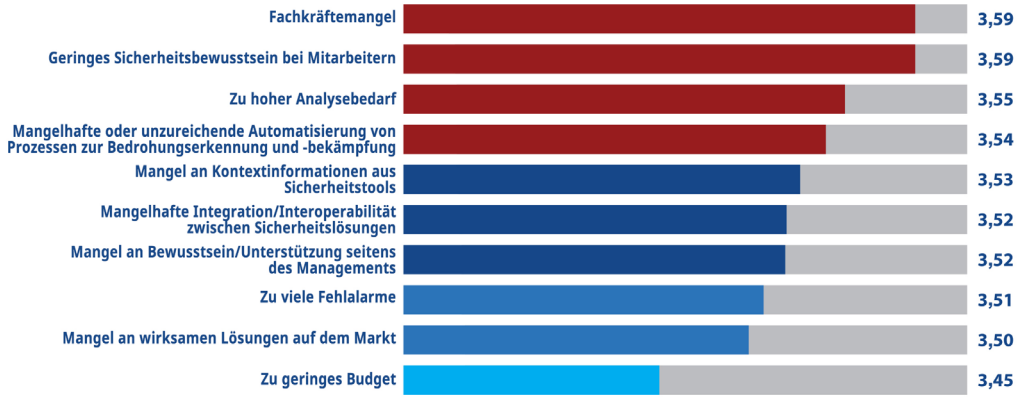
Wesentliche Erkenntnisse

- **Keine Zeit zum Ausruhen.** 81 % der Organisationen – so viele wie noch nie – waren im letzten Jahr mindestens einmal Opfer eines erfolgreichen Cyberangriffs. 35 % waren sechsmal oder häufiger betroffen, und 69 % rechnen in diesem Jahr mit einem Cyberangriff.
- **Vielfältige Bedrohungen.** Eine breite Vielfalt von Cyberbedrohungen, allen voran Malware-, Phishing-, Ransomware-, Account-Takeover- und Denial-of-Service-Angriffe, bereitet IT-Teams Sorgen.
- **Hilfe benötigt.** Die überwältigende Mehrheit (85 %) der Organisationen leidet unter einem Fachkräftemangel im Bereich IT-Sicherheit, und die Lücke ist mit Ausnahme eines einzigen Tätigkeitsfelds noch größer geworden.
- **Pläne für Netzwerksicherheit.** Für 2020 ist die Anschaffung diverser Netzwerksicherheitstechnologien geplant, darunter Network Behavior Analysis (NBA), SSL/TLS-Entschlüsselung und Schutz vor Denial of Service (DoS)/Distributed Denial of Service (DDoS).
- **Zu wenig Entschlüsselung.** Überraschenderweise werden nur 34 % des SSL/TLS-verschlüsselten Web-Traffics zu Prüfungszwecken entschlüsselt.

Herausforderungen beim Sammeln und Analysieren von Sicherheitsdaten

Die beiden größten Hindernisse bei der Umsetzung wirksamer Abwehrmaßnahmen gegen Cyberbedrohungen haben mit dem Faktor Mensch zu tun: Fachkräftemangel und geringes Sicherheitsbewusstsein bei Mitarbeitern. Dahinter folgen jedoch vier wesentliche Herausforderungen, die mit der Sammlung und Analyse riesiger Mengen an im gesamten Unternehmen verteilten Sicherheitsdaten zusammenhängen: zu hoher Analysebedarf, unzureichende Automatisierung von Prozessen zur Bedrohungserkennung und -bekämpfung, Mangel an Kontextinformationen, mangelhafte Integration zwischen Sicherheitslösungen. CyberEdge geht davon aus, dass Unternehmen diese Herausforderungen im kommenden Jahr angehen werden.

Einflussfaktoren, die wirksame Abwehrmaßnahmen gegen Cyberbedrohungen verhindern (Skala von 1 bis 5, höchster Einfluss = 5)

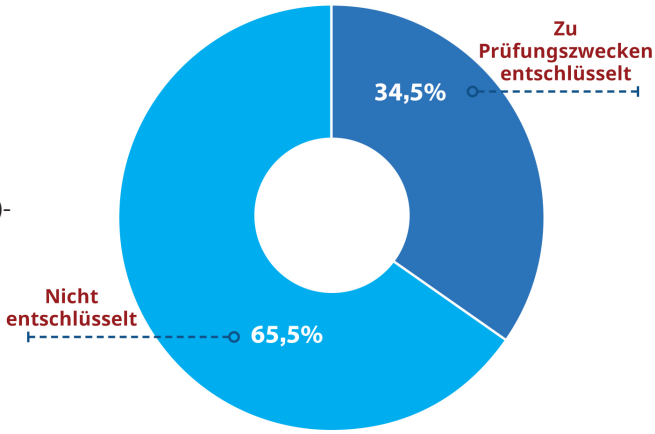


Ein Bericht der CyberEdge Group

Verschlüsselter Web-Traffic ist nach wie vor ein Problem

Zurzeit verfügen 56 % der Organisationen über eine Technologie zur SSL/TLS-Entschlüsselung, doch nur 35 % des SSL/TLS-Traffics wird tatsächlich zu Prüfungszwecken entschlüsselt. Angesichts des Umstands, dass Bedrohungsakteure Malware sowie Befehls- und Kontrollnachrichten in verschlüsseltem Web-Traffic verbergen, ist der tote Winkel viel zu groß. Verursacht wird das Entschlüsselungsdefizit durch IT-Teams, die die Entschlüsselung in Web-Gateways und Geräten deaktivieren, die bei der Entschlüsselung ineffizient sind, sowie durch SPAN(Switched Port Analyzer)-Verbindungen, die Traffic an Sicherheitstools leiten, wenn die Switches überlastet sind. Wir rechnen damit, dass der Anteil des entschlüsselten und geprüften SSL/TLS-Traffics in den kommenden Jahren zunehmen wird, da Organisationen verstärkt Technologien zur effizienteren Sammlung und Entschlüsselung des Netzwerkverkehrs einführen.

Anteil des zu Prüfungszwecken entschlüsselten SSL/TLS-Web-Traffics



Sicherheitsanalysen sind im Kommen

Laut der letztjährigen Umfrage waren erweiterte Sicherheitsanalysen in 41 % der Organisationen installiert. In diesem Jahr waren es bereits 57 %. Es kommt äußerst selten vor, dass so viele Organisationen (16 %) innerhalb von nur einem Jahr eine Sicherheitstechnologie einführen. Dieser Anstieg ist darauf zurückzuführen, dass Sicherheitsanalysen als nützlich (oder gar unverzichtbar) empfunden werden, da IT-Sicherheitsteams auf diese Weise große Datenmengen durchsuchen und schnell auf Bedrohungen reagieren können. Am häufigsten wird diese Technologie genutzt, um Insider-Bedrohungen zu erkennen, Vorfälle zu untersuchen, den Netzwerkverkehr in Bezug auf mögliche Anomalien zu analysieren, gehackte Konten zu ermitteln, Daten-Exfiltration zu erkennen und Cyberbedrohungen aufzuspüren.

So werden Produkte zur Sicherheitsanalyse in meiner Organisation eingesetzt

Kostenloses Exemplar

Ein kostenloses Exemplar des gesamten 2020 Cyberthreat Defense Report finden Sie hier: www.gigamon.com/cdr2020.

Über Gigamon

Gigamon ist das erste Unternehmen, das in einer einzigen Plattform Netzwerktransparenz und -analysen für den gesamten Datenverkehr – von Rohpaketen bis hin zu Apps – über physische, virtuelle und Cloud-Netzwerke bietet. Wir aggregieren, transformieren und analysieren den Netzwerkverkehr, um kritische Leistungs- und Sicherheitsanforderungen zu erfüllen, einschließlich einer schnellen Bedrohungserkennung und -bekämpfung. So kann Ihre Organisation digitale Innovationen vorantreiben. Kurz gesagt: Mit uns sind Sie schnell, stets sicher und innovativ.

CYBEREDGE GROUP

Über die CyberEdge Group

CyberEdge Group ist ein preisgekröntes Forschungs-, Marketing- und Verlagsunternehmen, das die Informationsbedürfnisse von Dienstleistern und Anbietern im Bereich der Informationssicherheit erfüllt. Unsere kompetenten Berater verschaffen unseren Kunden den Vorsprung, den sie benötigen, um ihre Umsätze zu steigern, andere Wettbewerber hinter sich zu lassen und die Verkaufszyklen zu verkürzen. Weitere Informationen finden Sie auf unserer Website www.cyber-edge.com.