4 wichtige Überlegungen zur Gestaltung der Security-Architektur

Umfassende, integrierte und automatisierte Sicherheit mit der Fortinet Security Fabric

Inhaltsverzeichnis

Zusammenfassung

Initiativen für digitale Innovationen (DI) werden derzeit in vielen Unternehmen in rasantem Tempo umgesetzt. Die Ziele sind klar: schnellere Geschäftsabläufe, Kostensenkungen, Effizienzsteigerung und bessere Kundenerfahrungen. Damit aber digitale Innovationen halten, was sie versprechen, müssen Unternehmen die Komplexität minimieren und ein effektives Risiko-Management praktizieren. Beides lässt sich mit einer Cyber-Security-Plattform erreichen, die Security- und Netzwerk-Teams mit einer Transparenz über alle Umgebungen und einem einfachen Management unterstützt.

Die Fortinet Security Fabric löst diese Herausforderungen mit umfassenden, integrierten und automatisierten Lösungen, die sicherheitsorientierte Netzwerke, einen Zero-Trust-Netzwerkzugang, eine dynamische Cloud-Sicherheit und Sicherheitsprozesse mit künstlicher Intelligenz (KI) ermöglichen. Zur Erweiterung des Fortinet-Angebots gibt es zudem zahlreiche nahtlos integrierbare Drittprodukte, die die Lücken in Security-Architekturen minimieren und gleichzeitig für eine maximale Kapitalrendite (ROI) von Investitionen in die Sicherheit sorgen.

84 % der Security-Manager glauben, dass das Risiko von Cyber-Angriffen steigen wird.[1]

Digitale Innovationen verändern alle Branchen

Weltweit gelten digitale Innovationen (DI) in allen Branchen als Muss für das Geschäftswachstum und die Verbesserung der Kundenerfahrung.[2]

Aus der Sicht der führenden Anbieter von Cloud-Plattformen und Cyber-Security bringen digitale Innovationen zahlreiche Änderungen für Netzwerk-Umgebungen mit sich. Zunehmend mobilere Benutzer greifen von Standorten und mit Endgeräten auf das Netzwerk zu, über die das IT-Team eines Unternehmens oft keine Kontrolle hat. Auch werden direkte Verbindungen zu Public Clouds hergestellt, um wichtige Geschäftsanwendungen wie Office 365 zu verwenden. Die Fülle solcher Benutzergeräte wird noch durch die Masse an IoT-Geräten (Internet der Dinge) übertroffen, die sich überall im Netzwerk befinden – häufig an entfernten, unüberwachten Orten. Hinzu kommen die stark dezentralen Infrastrukturen von Cloud-Anbietern mit entlegenen Standorten, die sich direkt mit der Cloud und Mobilfunknetzen verbinden und so die Rechenzentren von Unternehmen umgehen.

Durch all diese Änderungen ist das herkömmliche Konzept der Bedrohungsabwehr am Netzwerk-Rand zum Scheitern verurteilt und verlangt vom Cloud-Anbieter eine neue, mehrstufige Security-Strategie.

77 % der Security-Experten berichten, dass in ihrem Unternehmen trotz Sicherheitsbedenken Anwendungen oder Infrastrukturen in die Cloud verlagert wurden.[3]

Migration von Anwendungen und Workloads in die Cloud

Fast jedes Unternehmen hat damit begonnen, einige Workloads und Anwendungen in die Cloud zu verlagern – oder plant dies zumindest. Diese Entscheidungen beruhen oft auf dem Wunsch, mit einer flexiblen Cloud-Lösung Kosten zu senken und die betriebliche Effizienz und Skalierbarkeit zu verbessern.

Die Auswahl an Cloud-Modellen ist groß: Unternehmen können z. B. Lösungen wie SaaS (Software-as-a-Service) und PaaS (Platform-as-a-Service) implementieren.

Viele entscheiden sich für eine Multi-Cloud-Infrastruktur, um nicht an einen Cloud-Anbieter gebunden zu sein und die jeweils am besten geeignete Cloud für Anwendungen und Workloads zu nutzen. Der Nachteil ist jedoch, dass sich Unternehmen mit den Besonderheiten jeder Cloud-Umgebung befassen müssen. Auch erfordert jede Umgebung unterschiedliche Management- und Security-Tools. Das geht nicht nur zu Lasten der Transparenz. Auch muss beim Richtlinien-Management, Reporting und anderen Aufgaben mit mehreren Konsolen gearbeitet werden.

Cloud-Umgebungen sind dynamisch: 74 % der Unternehmen haben eine Anwendung in die Cloud verlagert – und dann wieder On-Premises bereitgestellt.[4]

Fülle an Endgeräten in mehreren Umgebungen

Endgeräte sind mit Abstand die am stärksten gefährdeten Knoten im Netzwerk eines Cloud-Anbieters. Die größeren Anbieter beschäftigen Tausende von Mitarbeitern, von denen jeder mit verschiedenen geschäftlichen und persönlichen Geräten auf Netzwerk-Ressourcen zugreift. Das Sicherstellen einer guten Cyber-Hygiene und aktuellen Endpunkt-Security auf all diesen Geräten ist eine Mammutaufgabe. Doch eine noch größere Herausforderung stellen die unzähligen IoT-Geräte dar: Schon Ende 2019 waren es über 26,66 Milliarden Geräte – und laut Schätzungen von Experten dürfte diese Zahl 2020 auf 31 Milliarden steigen.[5]

IoT-Geräte sind in zahlreichen Geschäftskontexten vorhanden: Sie bieten Einzelhandelskunden und Hotelgästen personalisierte Erlebnisse, verfolgen den Lagerbestand in der Fertigung und Logistik und überwachen Geräte in Fabrikhallen oder Kraftwerken.

IoT-Geräte sind in der Regel robust, energieeffizient und legen den Schwerpunkt auf die Leistung – Security-Funktionen und sichere Kommunikationsprotokolle sind oft nachrangig. Anders als die meisten Geräte im Netzwerk befinden sich IoT-Geräte häufig an entfernten Standorten, im Freien oder in unbesetzten bzw. selten besetzten Einrichtungen (wie Kraftwerken) und übertragen von diesen unsicheren Standorten unablässig kritische, sensible Daten an On-Premises-Rechenzentren und Cloud-Dienste.

84 % der Unternehmen verfolgen eine Multi-Cloud-Strategie.
81 % bezeichnen die Security als große Herausforderung bei der Cloud.[6]

Erweiterte Geschäftspräsenz über verteilte Märkte und Regionen hinweg

Erweitern Unternehmen ihre internationale Präsenz um neue Werke, Niederlassungen und andere dezentrale Standorte, kommt es häufig zu einer eingeschränkten WAN-Bandbreite (Wide Area Network): Zwar steigern SaaS-Anwendungen, Videokonferenzen und VoIP (Voice over IP) die Produktivität und ermöglichen neue Leistungsangebote, tragen jedoch auch zu einem exponentiellen Wachstum des WAN-Traffics bei.

Seit vielen Jahren laufen WAN-Verbindungen über das hochzuverlässige Multiprotocol Label Switching (MPLS). Bei MPLS ist es jedoch schwierig, die Nutzung der WAN-Bandbreite zu optimieren und die Dienstqualität (QoS) bedarfsgerecht und flexibel für verschiedene Anwendungen anzupassen. Daher können durch neue Standorte und Dienste schnell die WAN-Kosten explodieren.

Viele Unternehmen entscheiden sich daher für ein SD-WAN (Software-Defined WAN), das MPLS-, Internet- und sogar Telefonverbindungen effizient bereitstellen kann. Auch läuft bei einem SD-WAN der Traffic dynamisch über die jeweils am besten geeignete Verbindung. Allerdings muss bei softwaredefinierten WANs auch an die Sicherheit gedacht werden. Optimal ist daher ein Secure SD-WAN, das als integrierte Plattform eine Kombination aus Netzwerk- und Sicherheitsfunktionen bietet.

Von 2017 bis 2019 stieg die Anzahl der Unternehmen, bei denen es durch ungesicherte IoT-Geräte oder Anwendungen zu Datenpannen kam, um 73 %.[7]

Ein SD-WAN bietet gegenüber MPLS eine höhere Leistung und Sicherheit – zu geringeren Kosten.[8]

Vier Überlegungen zur Gestaltung der Security-Architektur

Viele Unternehmen treiben digitale Innovationen mit Begeisterung voran. Die Folgen für die Netzwerk-Security werden dabei oft übersehen oder heruntergespielt: Fast 80 % der Unternehmen führen neue digitale Innovationen schneller ein, als sie diese vor Cyber-Bedrohungen schützen können.[9]

IT-Verantwortliche sollten bei der Gestaltung von sicheren Architekturen für digitale Innovationen folgende vier Punkte mit Priorität angehen:

1. Genaue Kenntnis der wachsenden Angriffsfläche

Sensible Daten können sich überall befinden – und über unterschiedlichste Verbindungen übertragen werden, über die das Unternehmen keine Kontrolle hat. Da Anwendungen in der Cloud dem Internet ausgesetzt sind, erweitert jede neue Cloud-Instanz die Angriffsfläche des Unternehmens. Gleiches gilt für IoT-Geräte, durch die entfernte, unbesetzte Standorte zum Sicherheitsrisiko werden. In diesen intransparenten Bereichen der Angriffsfläche können illegale Zugriffe wochen- bis monatelang unbemerkt stattfinden und so verheerende Schäden im gesamten Unternehmen anrichten. Da Anwender zwischen Unternehmensstandorten wechseln, sich im öffentlichen Raum bewegen und ins Ausland reisen, wird die Angriffsfläche durch mobile Geräte und benutzereigene Endgeräte unberechenbar. Insbesondere drei Faktoren – die umfassende Migration in die Cloud, die starke Nutzung von Mobility-Lösungen und der breite Einsatz von IoT-Geräten – lassen bei einer Datenpanne die Kosten pro Datensatz schnell auf sechsstellige Beträge klettern.[10]

61 % der CISOs geben an, dass sie bereits in weiten Teilen mit Cloud-, IoT- und mobilen Lösungen arbeiten.[11]

Bis zu 40 % der pro Tag erkannten neuen Malware ist Zero-Day-Schadsoftware oder war zuvor unbekannt.[12]

Diese erweiterte, dynamische Angriffsfläche erodiert den einst klar abgegrenzten Netzwerk-Rand und die damit verbundenen Sicherheitsmaßnahmen. Angreifer können heutzutage viel leichter in Unternehmensnetzwerke eindringen und stoßen im Netzwerk auf nur geringen Widerstand, um ungehindert und unentdeckt bis zum Ziel ihres Angriffs vorzudringen. Wer auf digitale Innovationen setzt, braucht eine mehrstufige Security. Notwendig sind Kontrollen pro Netzwerk-Segment – weil man einfach davon ausgehen muss, dass es früher oder später am Perimeter zu einem erfolgreichen Angriff kommt. Wichtig ist auch ein reglementierter Zugriff auf Netzwerk-Ressourcen, der nur das unbedingt notwendige Maß an Benutzerrechten gewährt und die Vertrauenswürdigkeit eines Benutzers ständig neu bewertet.

DI-Initiativen bedeuten, dass interne Security-Teams einen Schutz für 17 verschiedene Arten von Endpunkten bereitstellen müssen.[13]

2. Vorbereitung auf sich weiterentwickelnde Cyber-Bedrohungen

Die Cyber-Bedrohungslage verschärft sich rasant angesichts von Kriminellen, die alles daran setzen, herkömmliche Abwehrmaßnahmen auszuhebeln: Bis zu 40 % der pro Tag erkannten neuen Malware ist Zero-Day-Schadsoftware oder war zuvor unbekannt.[14] Unabhängig davon, ob dies auf den vermehrten Einsatz von polymorpher Malware oder auf die Verfügbarkeit von Malware-Toolkits zurückgeht – bisher gut funktionierende, signaturbasierte Malware-Erkennungsalgorithmen können den zunehmenden Zero-Day-Malware-Angriffen wenig entgegensetzen. Auch Social Engineering ist bei kriminellen Elementen beliebt, um herkömmliche Sicherheitskonzepte mit statischen Zugriffsrechten in die Knie zu zwingen: Wie Studien zeigen, haben 85 % der Unternehmen im vergangenen Jahr Phishing- oder Social-Engineering-Angriffe erlebt.[15]

Mit zunehmender Komplexität von Cyber-Bedrohungen sind Datenschutzverletzungen schwerer zu erkennen und zu beheben: Von 2018 bis 2019 stieg die Zeit bis zur Erkennung und Eindämmung einer Datenpanne von 266 auf 279 Tage.[16] Neben der Fähigkeit, einen versuchten Angriff zu entdecken und zu verhindern, müssen Unternehmen auch in der Lage sein, einen erfolgreichen Angriff schnell zu identifizieren, zu stoppen und die Folgen zu beheben. Dass 88 % der Unternehmen nach eigenen Angaben in den letzten 12 Monaten mindestens einen Vorfall erlebten, zeigt, dass alle Unternehmen einem Angriffsrisiko ausgesetzt sind und dass die Cyber-Resilienz von entscheidender Bedeutung ist.[17]

Ein Drittel der Unternehmen erlebte im Vorjahr Verstöße bei geschäftskritischen Daten, für die Bußgelder erhoben werden könnten.[18]

3. Vereinfachen des zunehmend komplexeren IT-Ecosystems durch Automatisierung

Für fast die Hälfte der CIOs ist die zunehmende Komplexität das größte Problem bei der wachsenden Angriffsfläche.[19] Schuld an dieser erhöhten Komplexität sind die vielen isoliert arbeitenden Einzelprodukte, die für unterschiedliche Sicherheitsfunktionen implementiert wurden: In einem durchschnittlichen Unternehmen gibt es mehr als 75 verschiedene Sicherheitslösungen.[20]

Diese fehlende Security-Integration verhindert, dass Unternehmen von den Vorteilen automatisierter Sicherheitsfunktionen profitieren. Tatsächlich geben 30 % der CIOs an, dass die Anzahl der manuellen Prozesse ein zentrales Sicherheitsproblem darstellt.[21] Ohne Security-Automatisierung benötigen CIOs besser qualifizierte Cyber-Sicherheitsexperten, um das Netzwerk zu überwachen und zu sichern.

Viele Unternehmen haben jedoch Schwierigkeiten damit, geeignete Fachkräfte für die Cyber-Sicherheit einzustellen. Schätzungen zufolge sind derzeit über 4 Millionen Cyber-Security-Stellen unbesetzt – Tendenz steigend.[22] Dieser Fachkräftemangel gefährdet das gesamte Unternehmen: 67 % der CIOs geben an, dass sie wegen fehlender Mitarbeiterkenntnisse zur Cyber-Security nicht mit Änderungen Schritt halten können.[23]

Angreifer kennen diese Probleme sehr wohl – und nutzen sie zu ihrem Vorteil aus.

4. Proaktive Vorbereitung auf zunehmende regulatorische Anforderungen

Die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union (EU) und das kalifornische Verbraucherschutzgesetz (CCPA) sind zwei der bekanntesten Datenschutzbestimmungen. Sie sind jedoch bei weitem nicht die einzigen. So gibt es z. B. in einigen US-Bundesstaaten eine Meldepflicht bei Datenschutzverletzungen und viele Länder erlassen zusätzliche Bestimmungen zum Schutz der Privatsphäre von Verbrauchern. Aufgrund des politischen und gesellschaftlichen Drucks dürfte die Zahl der Vorschriften in den nächsten Jahren steigen – und mit ihnen Höhe, Strafmaß und Häufigkeit von Bußgeldzahlungen.

Weiter müssen Unternehmen Industriestandards einhalten, scheitern hieran jedoch häufig. Beispielsweise bestehen weniger als 37 % der Firmen das Compliance-Audit für den PCI-DSS-Standard für Kreditkartenzahlungen.[24] Da PCI DSS bald durch das PCI Software Security Framework (PCI SSF) ersetzt wird, dürften sich die Konformitätsprobleme für diese Unternehmen noch verschärfen.

Die Notwendigkeit der Einhaltung gesetzlicher Vorschriften wirkt sich stark auf den Erfolg der Security-Transformation aus – und zeigt auch, wie Unternehmen in Technologielösungen investieren. Beispielsweise haben 21 % der 71 % der Unternehmen, die cloudbasierte Anwendungen wieder zurück in On-Premises-Rechenzentren verlagerten, dies nur aus einem Grund getan: um gesetzliche Vorschriften zu erfüllen.[25]

Die Fortinet Security Fabric

Die Fortinet Security Fabric wurde speziell für alle vier zuvor beschriebenen Sicherheitsherausforderungen entwickelt. Unternehmen erhalten damit umfassende Transparenz und Kontrolle über die gesamte digitale Angriffsfläche, um Risiken zu minimieren. Da es sich bei der Security Fabric um eine integrierte Lösung handelt, verringert sich auch die Komplexität (es müssen weniger Einzelprodukte unterstützt werden) und Betriebsabläufe werden dank automatisierter Workflows beschleunigt – während gleichzeitig ein produktiver, ausfallsicherer Geschäftsbetrieb aufrechterhalten werden kann.

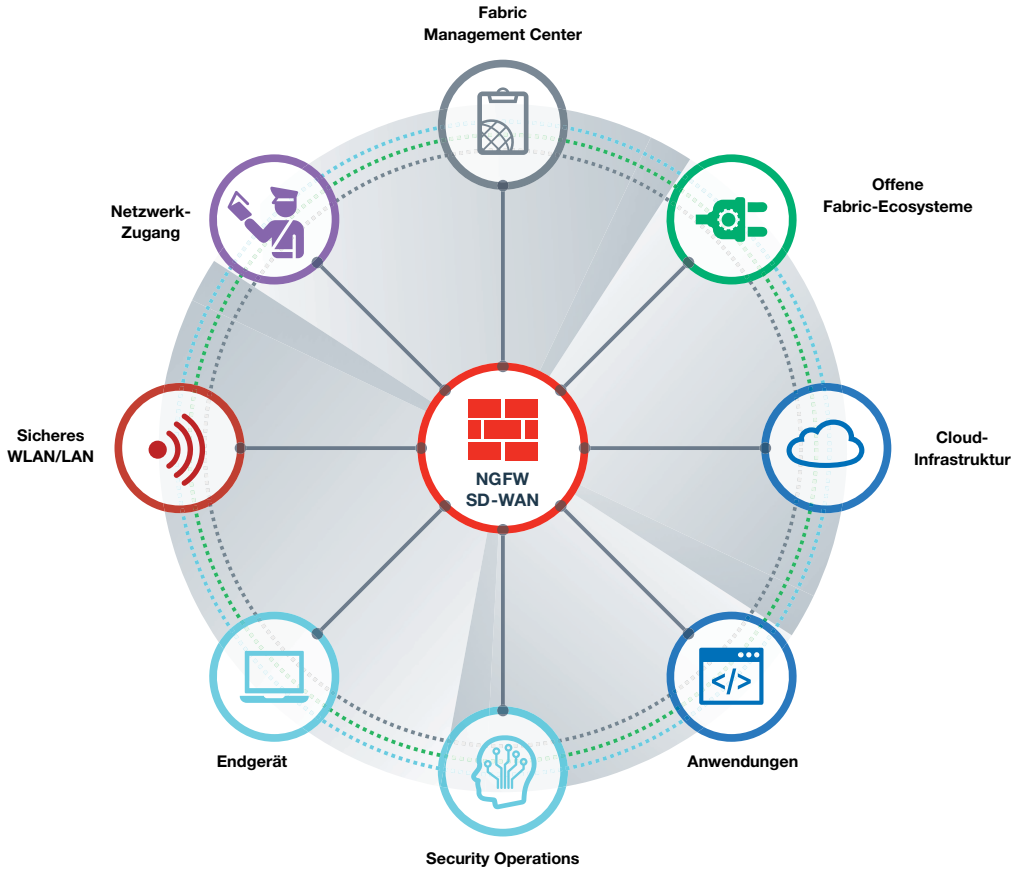

Abbildung 1: Mit der Fortinet Security Fabric können mehrere Security-Technologien nahtlos über alle Umgebungen hinweg zusammenarbeiten – unterstützt von einer einzigen Threat-Intelligence-Quelle und kontrolliert über eine gemeinsame „Schaltzentrale". So werden Security-Lücken im Netzwerk geschlossen und Reaktionen auf Angriffe und Datenschutzverletzungen beschleunigt.

Für fast die Hälfte der CISOs haben eine integrierte Security und bessere Analysen oberste Priorität bei der Technologie-Strategie im Bereich Cyber-Sicherheit.[26]

Mit der Fortinet Security Fabric können Teams Folgendes erreichen:

Umfassende, tiefgehende Transparenz über die Angriffsfläche

Mit einem breitgefächerten Angebot an leistungsstarken, sicherheitsorientierten Netzwerk-Lösungen für Rechenzentren, Filialen und Kleinunternehmen sowie für alle wichtigen Cloud-Plattformen bietet die Fortinet Security Fabric Unternehmen die notwendige Flexibilität, um jedes Netzwerk-Segment zu schützen. Alle Sicherheitskomponenten werden zentral konfiguriert, verwaltet und überwacht. Diese „Security-Schaltzentrale“ löst nicht nur isolierte Bereiche auf, die beim Einsatz punktueller Einzelprodukte zwangsläufig entstehen, sondern reduziert auch den Schulungsaufwand für personell begrenzte IT-Teams. Zudem erleichtert das zentrale Management-System die Zero-Touch-Bereitstellung von Remote-Komponenten, reduziert Außendienst-Einsätze und senkt die Betriebskosten noch stärker.

Integrierte, umfassende Security-Architektur

Da alle Komponenten mit FortiOS das gleiche Netzwerk-Betriebssystem verwenden, sorgt die Fortinet Security Fabric automatisch für einheitliche Konfigurationen, ein konsequentes Richtlinien-Management und eine reibungslose Echtzeit-Kommunikation innerhalb der gesamten Sicherheitsinfrastruktur. Dies minimiert Verzögerungen bei der Bedrohungserkennung und -abwehr, reduziert Sicherheitsrisiken durch Konfigurationsfehler und manuelle Dateneingaben und ermöglicht zeitnahe, korrekte Compliance-Audits. Neben der Integration von Fortinet-Produkten und -Lösungen umfasst die Security Fabric auch vorkonfigurierte APIs (Application Programming Interface) für über 70 Fabric-Ready-Partner, die eine tiefgehende Integration aller Security-Fabric-Elemente sicherstellen.

Externe Tests zeigen: FortiGate NGFWs bieten das beste Preis-Leistungs-Verhältnis beim Überprüfen von verschlüsseltem Datenverkehr. Sie erreichen eine SSL-Leistung von 5,7 Gbit/s und blockieren gleichzeitig 100 % der Umgehungsversuche.[27]

Werden Verstöße schneller erkannt und Reaktionszeiten verkürzt, sinken die Gesamtkosten einer Datenpanne um bis zu 25 %.[28]

Automatisierte operative Abläufe und Reaktionen

Zusätzlich zu ihrer nahtlosen Integration ist die Fortinet Security Fabric marktführend bei der Anwendung von ML-Technologien (Machine Learning), um mit der dynamischen Cyber-Bedrohungslandschaft Schritt zu halten. Ihre Security-Features reichen von intelligenten SOAR-Funktionen (Security Orchestration, Automation und Response), einer proaktiven Bedrohungserkennung, Bedrohungskorrelationen und dem Austausch von Bedrohungsdaten bis hin zur Erforschung und Analyse von Bedrohungen.

Die Security Fabric bietet automatisierte Workflows und Abläufe für den Netzwerk-Betrieb. So lässt sich die Komplexität im gesamten Unternehmen und übergreifend über Abteilungen verringern – On-Premises, in der Cloud und in Filialen.

Risiken im Griff, Chancen verfolgen

Digitale Innovationen (DI) eröffnen Unternehmen neue Effizienz- und Kosteneinsparungen sowie eine Verbesserung der Kundenerfahrung. DI-Initiativen erweitern und verändern jedoch auch die Angriffsfläche des Unternehmens und bieten damit den Nährboden für neue Cyber-Bedrohungen und Angriffsformen.

Für Unternehmen, die zu den Vorreitern bei digitalen Innovationen zählen wollen, ist es von größter Bedeutung, Risiken zu identifizieren, zu akzeptieren und richtig zu handhaben. Die Fortinet Security Fabric bietet die Basis dafür. Sie vereinheitlicht Security-Lösungen über eine zentrale Konsole, macht die wachsende digitale Angriffsfläche sichtbar, integriert einen KI-gesteuerten Schutz vor Datenschutzverletzungen und automatisiert Betriebsabläufe, Orchestrierung und Reaktionen. Zusammenfassend lässt sich sagen, dass sie es Unternehmen ermöglicht, mit digitalen Innovationen einen neuen Mehrwert zu schaffen, ohne die Sicherheit im Tausch für Agilität, Leistung und einfache Bedienung zu beeinträchtigen.

[1] Nick Lansing: „Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources“. Forbes und Fortinet, 2019.

[2] „The CIO and Cybersecurity: A Report on Current Priorities and Challenges“. Fortinet, 23. Mai 2019.

[3] Jeff Wilson: „The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments“. IHS Markit, 2019.

[4] Ebd.

[5] Gilad David Maayan: „The IoT Rundown For 2020: Stats, Risks, and Solutions“. Security Today, 13. Januar 2020.

[6] „Rightscale 2019 State of the Cloud Report“. Flexera, 2019.

[7] Larry Ponemon: „Third-party IoT risk: companies don’t know what they don’t know“. ponemonsullivanreport.com, abgerufen am 4. Februar 2020.

[8] Nirav Shah: „SD-WAN vs. MPLS: Why SD-WAN is a Better Choice in 2019“. Fortinet, 9. September 2019.

[9] Kelly Bissell et al.: „The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study“. Accenture Security und Ponemon Institute, 2019.

[10] „2019 Cost of a Data Breach Report“. IBM Security und Ponemon Institute, 2019.

[11] „The CIO and Cybersecurity: A Report on Current Priorities and Challenges“. Fortinet, 23. Mai 2019.

[12] Laut internen Daten der FortiGuard Labs.

[13] „6 Obstacles to Effective Endpoint Security: Disaggregation Thwarts Visibility and Management for IT Infrastructure Leaders“. Fortinet, 8. September 2019.

[14] Laut internen Daten der FortiGuard Labs.

[15] Kelly Bissell et al.: „The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study“. Accenture Security und Ponemon Institute, 2019.

[16] „2019 Cost of a Data Breach Report“. IBM Security und Ponemon Institute, 2019.

[17] Basierend auf Daten einer internen Fortinet-Studie.

[18] Laut Daten aus einer internen Fortinet-Studie.

[19] „The CIO and Cybersecurity: A Report on Current Priorities and Challenges“. Fortinet, 23. Mai 2019.

[20] Kacy Zurkus: „Defense in depth: Stop spending, start consolidating“. CSO, 14. März 2016.

[21] „The CIO and Cybersecurity: A Report on Current Priorities and Challenges“. Fortinet, 23. Mai 2019.

[22] „Strategies for Building and Growing Strong Cybersecurity Teams: $(ISC)^2$ Cybersecurity Workforce Study, 2019“. $(ISC)^2$, 2019.

[23] „CIO Survey 2019: A Changing Perspective“. Harvey Nash und KPMG, 2019.

[24] „2019 Payment Security Report“. Verizon, 2019.

[25] Jeff Wilson: „The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments“. IHS Markit, 2019.

[26] „Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources“. Forbes und Fortinet, 2019.

[27] „Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests“. Fortinet, Januar 2020.

[28] „2019 Cost of a Data Breach Report“. IBM Security und Ponemon Institute, 2019.

www.fortinet.com/de

664959-0-0-DE

31. August 2020, 8:47 Uhr