

Warum Hacker jetzt auch Fleischfabrikanten und die Polizei angreifen

Verschlüsselungstrojaner gefährden alle Branchen. Die jüngsten Opfer: Colonial Pipeline und der Großschlachter JBS. Nun streiten Experten, welche Gegenmaßnahmen helfen würden.

Von Patrick Beuth
03.06.2021, 07:45 Uhr

Immer wieder Ransomware: Cyberattacken auf kritische Sektoren nehmen zu
16. Juni 2021



Ermittlungen nach Todesfall während Hackerangriff auf Uniklinik

Unbekannte haben vergangene Woche an der Düsseldorfer Uniklinik einen IT-Ausfall ausgelöst. Eine Patientin musste in ein anderes Krankenhaus gebracht werden – und starb.



Ransomware-Erpressungen sind teuer: Das höchste gezahlte Lösegeld, das in der Sophos-Umfrage genannt wurde, betrug 2,65 Millionen Euro.

heise + Das digitale Abo für IT und Technik.

Cyberangriff: TU Berlin rechnet mit monatelangen IT-Einschränkungen

Es wird noch einige Zeit dauern, bis die zentralen IT-Systeme der TU Berlin nach der Ransomware-Attacke wieder laufen. Auch das SAP-Kernsystem ist betroffen.

Lesezeit: 3 Min. In Pocket speichern



Colonial Pipeline über kompromittiertes Passwort gehackt

Der kürzlich gehackte Pipelinebetreiber Colonial äußert sich zu dem Vorgehen der Ransomware-Gruppe Darkside.

7. Juni 2021, 11:24 Uhr, Moritz Tremmel



Bilder der betroffenen Colonial Pipeline

Hacker haben das Computersystem des Landkreises Anhalt-Bitterfeld lahmgelegt, nicht einmal Sozialhilfe kann derzeit angewiesen werden. Lösegeld will Landrat Grabner trotzdem nicht zahlen.



Zwei Drittel der deutschen Unternehmen erleiden Ransomware-Attacken

67 Prozent der Unternehmen in Deutschland waren im Jahr 2020 von Ransomware-Angriffen betroffen. In einem Gastbeitrag schildert Andrew Rose, resident CISO, EMEA bei Proofpoint, die Dimension der Bedrohung und zeigt sechs Schritte zur Vermeidung von Ransomware-Attacken auf.

von Dr. Jakob Jung am 21. Juni 2021, 12:27 Uhr



Umfrage: Ransomware größte Sicherheitsbedrohung für Unternehmen

Deep Instinct stellt den ersten jährlichen "Voice of SecOps"- Bericht vor – mit Umfrage unter führenden IT-Sicherheitsfachleuten in der D-A-CH-Region + Über 54 Prozent sind besorgt, den schnellen Wandel von IT-Technologien nicht mehr bewältigen zu können. + Fast 70 Prozent beklagen, drastische Zunahme von Ransomware im Jahr 2021. + 80 % der Befragten würden eine selbstlernende Cybersicherheitslösung, die kein menschliches Eingreifen erfordert, in ihrer IT-Umgebung als nützlich empfinden. + 99 % der Befragten glauben, dass das Angebot einer Ransomware-Garantie ihre Entscheidung zum Kauf einer bestimmten Sicherheitslösung beeinflussen würde.

Q&A

Henrik Knoblauch
Henrik.Knoblauch@bechtle.com



Daniel Moosbauer
Daniel.Moosbauer@bechtle.com



Cyber Sicherheitslage in Deutschland.

Deutschland · Digital · Sicher · BSI

Die Lage der IT-Sicherheit in Deutschland 2021 im Überblick

RANSOMWARE/DDOS

Deutliche Ausweitung cyber-krimineller Erpressungsmethoden



13 Tage lang konnte ein Universitätsklinikum nach einem Ransomware-Angriff keine Notfall-Patienten aufnehmen.

144 MIO. neue Schadprogramm-Varianten gegenüber 2020: **117,4 MIO.** **+22%**

DURCHSCHNITTLICH	IM HÖCHSTWERT
394.000 neue Schadprogramm-Varianten pro Tag <small>2020: 322.000</small>	553.000 <small>2020: 470.000</small>

40.000 BOT-INFESTIONEN DEUTSCHER SYSTEME
98% aller geprüften Systeme waren durch Schwachstellen in **MS Exchange** verwundbar.

14,8 MIO.

Meldungen übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.



44.000

Mails mit Schadprogrammen wurden in deutschen Regierungsnetzen abgefangen.



74.000

Webseiten wurden wegen enthaltener Schadprogramme durch die Webfilter der Regierungsnetze gesperrt.



100 Zertifizierungen von Produkten, Standorten und Schutzprofilen im Bereich Common Criteria



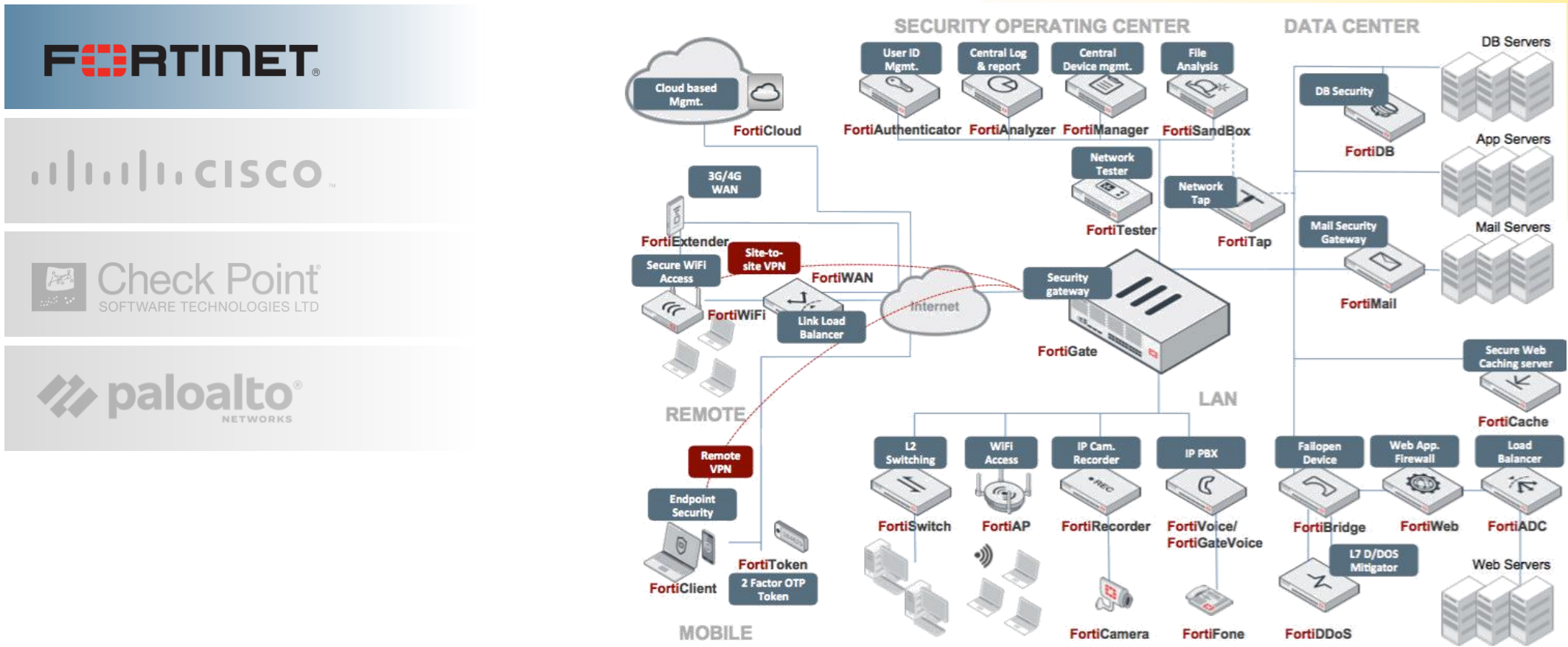
5.100 MITGLIEDER DER ALLIANZ FÜR CYBER-SICHERHEIT

- 2020: 4.400
- 2019: 3.700
- 2018: 2.700

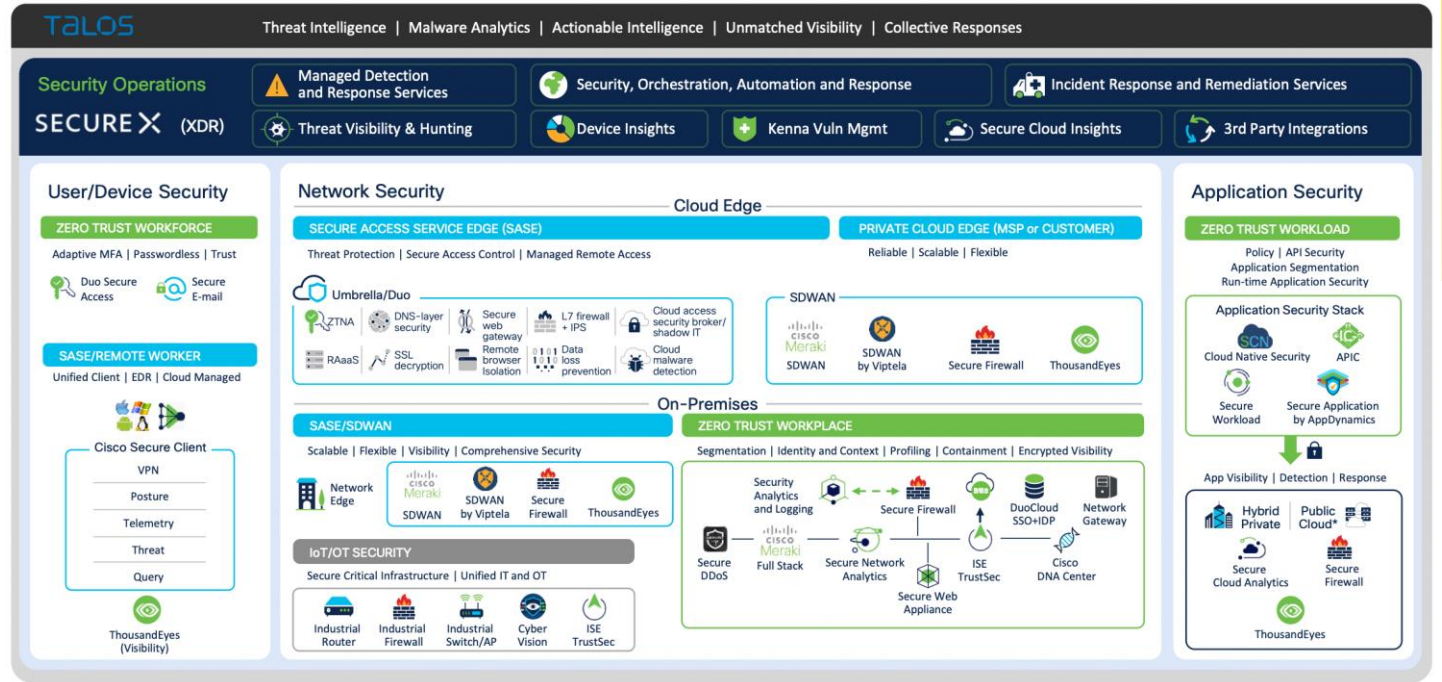
< 10% waren nach Warnungen von BSI und Microsoft immer noch durch Schwachstellen in **MS Exchange** verwundbar.

Deutschland **Digital·Sicher·BSI**

Full-Stack Security (Möglichkeiten)



Full-Stack Security.



Full-Stack Security.



CloudGuard SECURE THE CLOUD

CloudGuard Posture Management Posture Management and Visibility	CloudGuard Intelligence Network Traffic Analysis
CloudGuard Workload Runtime Workload Protection	CloudGuard Network Cloud Access Control, Prevention
CloudGuard AppSec Web & API Protection	

Quantum SECURE THE NETWORK

Quantum Security Gateway Perimeter & Data Center	Quantum Maestro Hyperscale	Quantum SMB Branch & SMB
Quantum Rugged ICS Security	Quantum IoT Protect IoT Security	
<ul style="list-style-type: none"> Access Control Multi-Layered Security Advanced Threat Prevention Data Protection 	<ul style="list-style-type: none"> Access Control Multi-Layered Security Advanced Threat Prevention Wi-Fi, DSL, 3G/4G/LTE 	

Check Point INFINITY

INFINITY-VISION
CONSOLIDATED MANAGEMENT & SECURITY OPERATIONS

INFINITY PORTAL
Management & Unified Visibility

INFINITY-VISION SOC
Security Operations & XDR

R31
Security Platform

Quantum Smart-1 Cloud
Management

THREATCLOUD
Threat Intelligence

Harmony SECURE USERS & ACCESS

REMOTE ACCESS

- Harmony Connect
 - Corporate Access
 - Internet Access

EMAIL & OFFICE

- Harmony Email & Office
 - Account Takeover Protection
 - Data Loss Prevention
 - Threat Prevention
 - Zero Phishing

ENDPOINT & MOBILE

Harmony Endpoint	Harmony Browse	Harmony Mobile
<ul style="list-style-type: none"> Threat Prevention Anti-Ransomware Forensics Secure Media Access Control 	<ul style="list-style-type: none"> Zero Day Browser Protection Threat Prevention Zero Phishing 	<ul style="list-style-type: none"> App Protection Network Protection Device Protection