KHZG-Erfahrungsberichte

Martin Weiß
Senior Sales Engineer Public

SOPHOS

Krankenhauszukunftsgesetz - Fördertatbestände

- 01: Notaufnahme
- 02: Patientenportal
- 03: Pflege- und Behandlungsdokumentation
- 04: Entscheidungsunterstützung
- 05: Medikationsmanagement
- 06: Krankenhausinterner digitaler Leistungsprozess
- 07: Leistungsabstimmung und Cloud-Computingsysteme
- 08: Versorgungsnachweissystem Betten
- 09: Telemedizinische Netzwerke
- 10: IT- und Cybersicherheit
- 11: Anpassung von Patientenzimmern bei Epidemien

Krankenhauszukunftsgesetz (KHZG/KHZF)

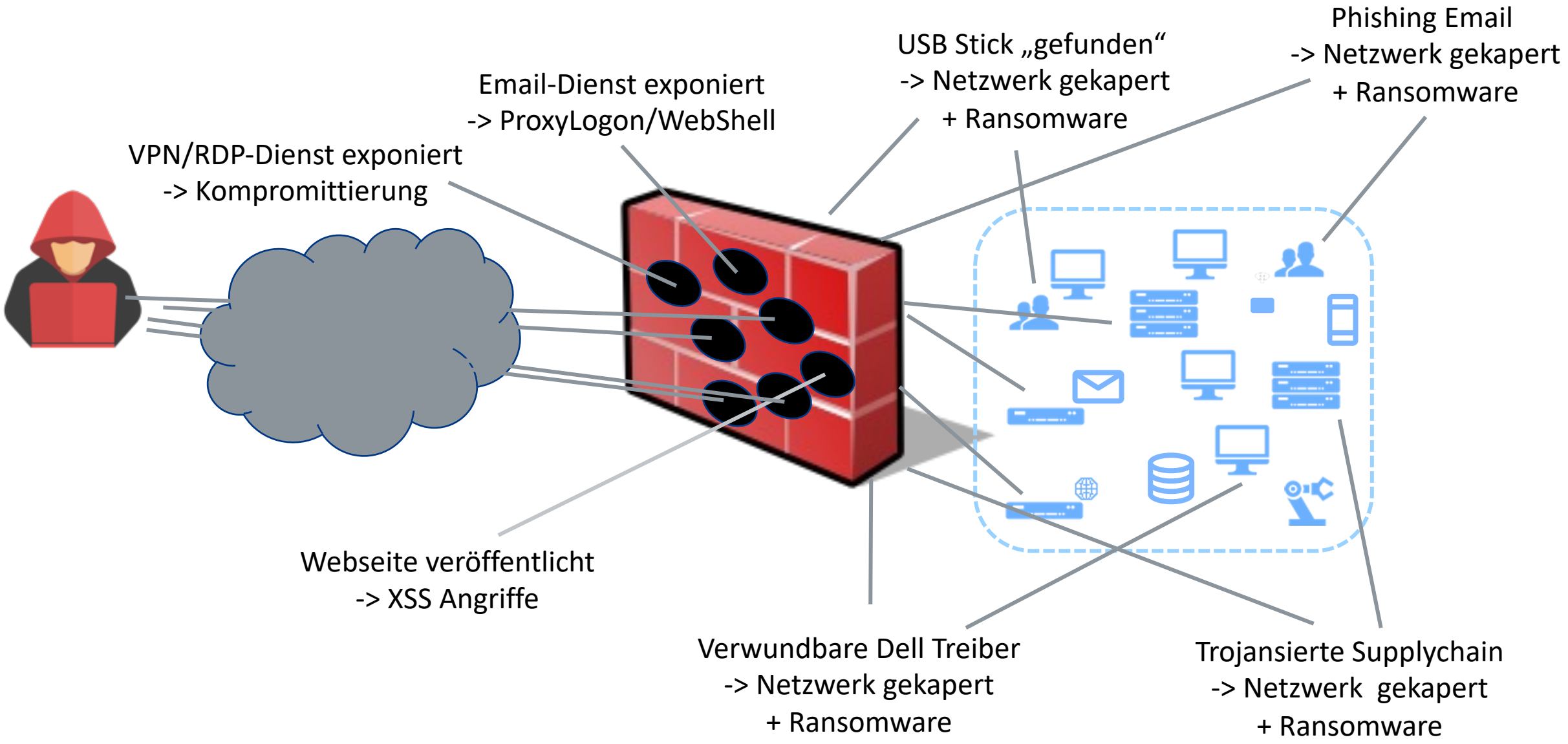
- Maßnahmen müssen Stand der Technik entsprechen
- Schutz von Netzwerken, Zonierung, VPN, IDS/IPS, ZTNA
- Interoperabilität muss gewährleistet sein
- Systeme zur Detektion von Informationssicherheits-Vorfällen (u. a. SOC & MDR) werden explizit gefördert
- Steigerung und Aufrechterhaltung der Awareness gegenüber Informationssicherheits-Vorfällen

Optimale Sicherheit für Ihre Organisation

Was nutzen Sie?

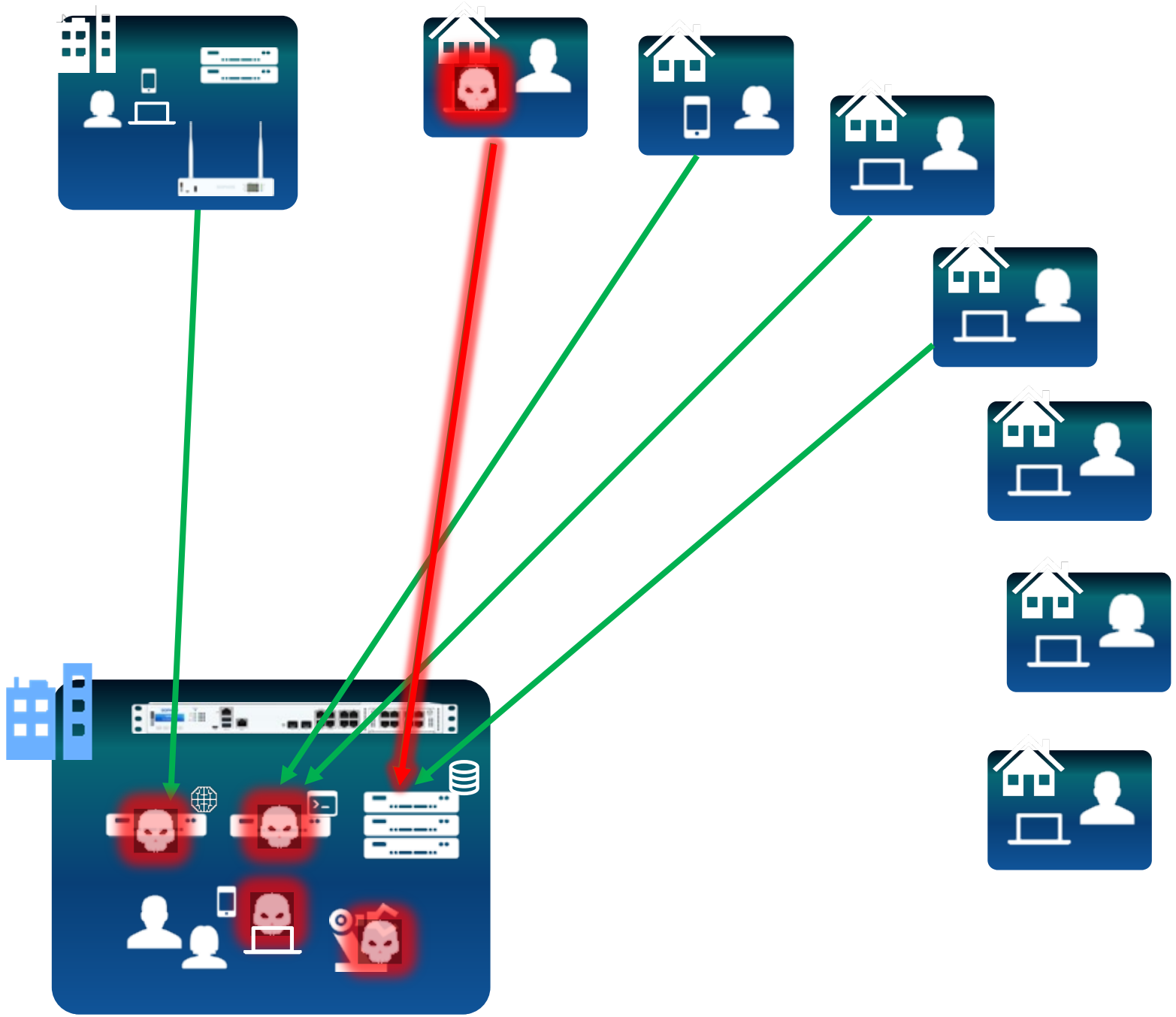
Aktuelle Technik

Realität


Phishing Email
-> Netzwerk gekapert
+ Ransomware
USB Stick „gefunden“
-> Netzwerk gekapert
+ Ransomware
Email-Dienst exponiert
-> ProxyLogon/WebShell
VPN/RDP-Dienst exponiert
-> Kompromittierung
Webseite veröffentlicht
-> XSS Angriffe
Verwundbare Dell Treiber
-> Netzwerk gekapert
+ Ransomware
Trojansierte Supplychain
-> Netzwerk gekapert
+ Ransomware

Problem bei VPN:

*“You’re **ON** the network”*



Ransomware Gruppen greifen gezielt VPN an

ZDNet CLOUD STORAGE IOT MOBILE SICHERHEIT NETZWERKE WHITEPAPE

ZDNet / Sicherheit / Cyberkriminalität

Ransomware attackiert VPN und RDP

Ransomware wird immer gefährlicher. Hacker nutzen vor allem das Remote Desktop Protocol (RDP), und Virtual Private Networks (VPN) als Einfallstore. E-Mail-Phishing verliert dagegen an Bedeutung.

von Dr. Jakob Jung am 24. August 2020 .

INFOPOINT SECURITY IT-Security Events Über Uns Kontakt

News > Remote Access VPNs rücken ins Visier von Ransomware-Angriffen

Ransomware

Remote Access VPNs rücken ins Visier von Ransomware-Angriffen

15.01.2020, San Jose | Autor: Herbert Wieler

Sodinokibi-Ransomware nutzt VPN-Verbindung als Schwachstelle für die Attacke auf Travelex

golem.de IT-NEWS FÜR PROFIS HOME TICKER VIDEOS VORGELESEN FORUM

Artikel, News, ... Suchen Golem.de jetzt w

KARRIEREWELT JOBS IT-FACHTRAININGS COACHINGS SPRACHKURSE GEHALTSCHECK | GOLEM-PC PRODUKTVERGLEICH TO

RANSOMWARE

Colonial Pipeline über kompromittiertes Passwort gehackt

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

in Pocket speichern merken 7. Juni 2021, 11:24 Uhr, Moritz Tremmel

(Bild: Reuters)

Die Treibstofftanks der betroffenen Colonial Pipeline

Der Pipeline-Betreiber Colonial wurde über kompromittierte Zugangsdaten gehackt. Laut einem Bericht des Magazins Bloomberg verschaffte sich die Angreifergruppe am 29. April 2021 Zugang zu dem internen Netz von Colonial. Dazu nutzten sie ein VPN-Konto, welches Angestellten den Fernzugriff auf das Netzwerk von Colonial ermöglicht.

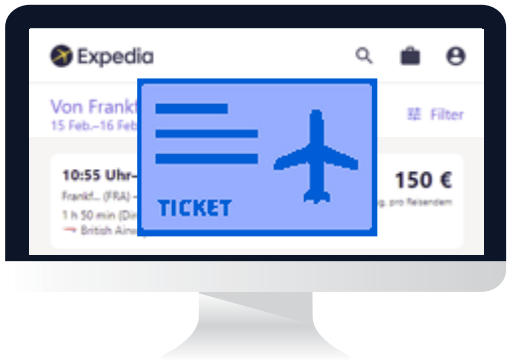
ANZEIGE Google Anz Diese Werbung b Warum sehe ich dies

SOPHOS

Zero Trust Network Access

Sophos ZTNA

Flughafen-Sicherheit heute



Ticketkauf mit Kreditkarte

Überprüfung:

- Ist das Ticket gültig?
- Ist der Pass gültig?
- Stimmt der Name überein?

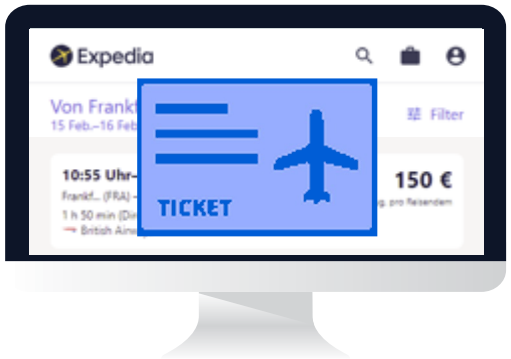
Überprüfung:

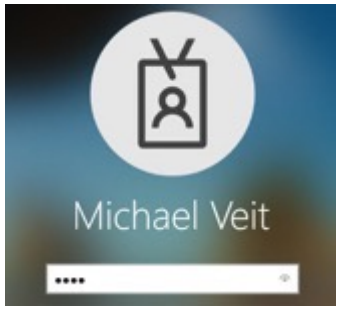
- Waffen, Sprengstoff?
- Darf die Person in ein Flugzeug?

Überprüfung:

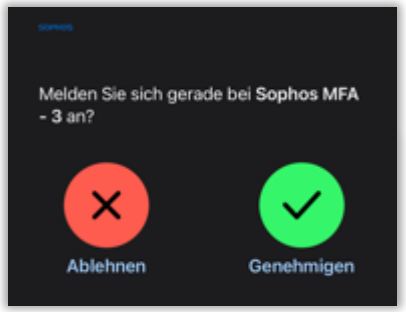
- Ist das Ticket gültig?
- Ist der Pass gültig?
- Darf die Person in dieses Flugzeug?

Flughafen-Sicherheit heute – ZTNA Zugriff



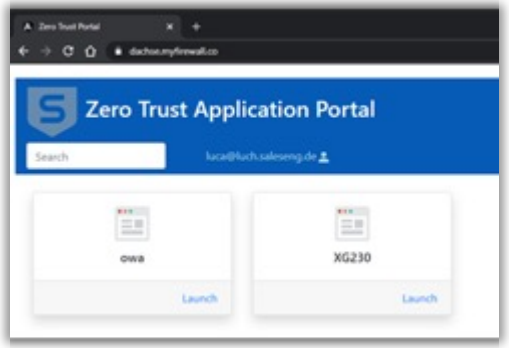


Windows-Anmeldung
mit User/Passwort



MFA Bestätigung
auf Smartphone

Intercept X überprüft,
ob der Computer OK ist



Zugriff nur auf für den User
freigeschaltete Anwendungen

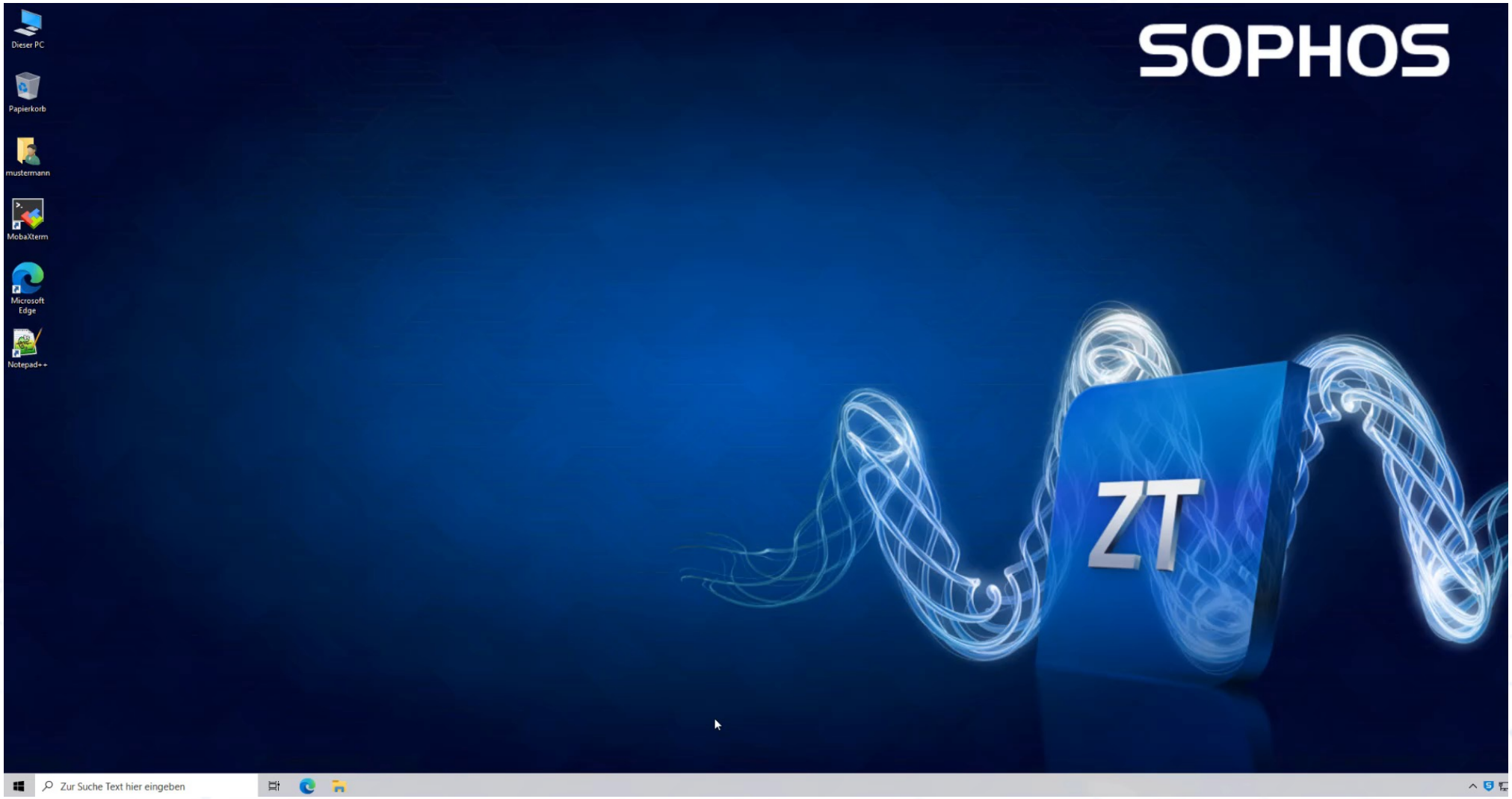
SOPHOS

ZTNA Ressourcen

- Direkter Tunnel vom Client zur Applikation
- Port Range oder direkter Port
- Verkehr von Client zur Applikation wird nicht verändert

https://youtu.be/l5irgKiJ0Hc

Demo Video


Dieser PC
Papierkorb
mustermann
MobaXterm
Microsoft Edge
Notepad++
SOPHOS
ZT
Zur Suche Text hier eingeben

Technical Deep Dive

- Installation von A bis Z
- PoC innerhalb von 30 Minuten möglich
- Ohne Änderungen von Konfiguration auf Firewall oder ähnlichem

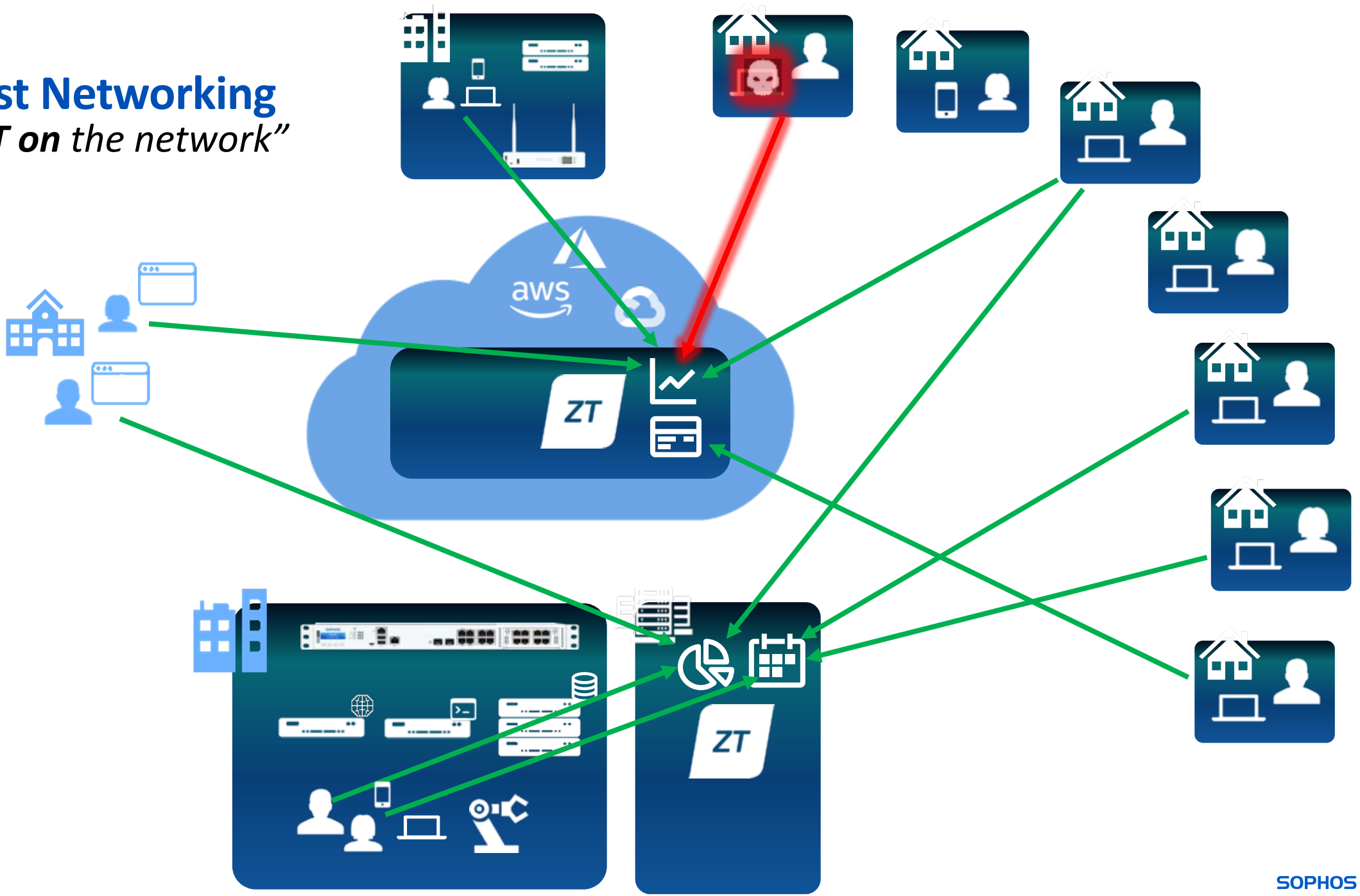
https://youtu.be/fPtmJcslPxo

ZTNA statt Remote Access VPN?

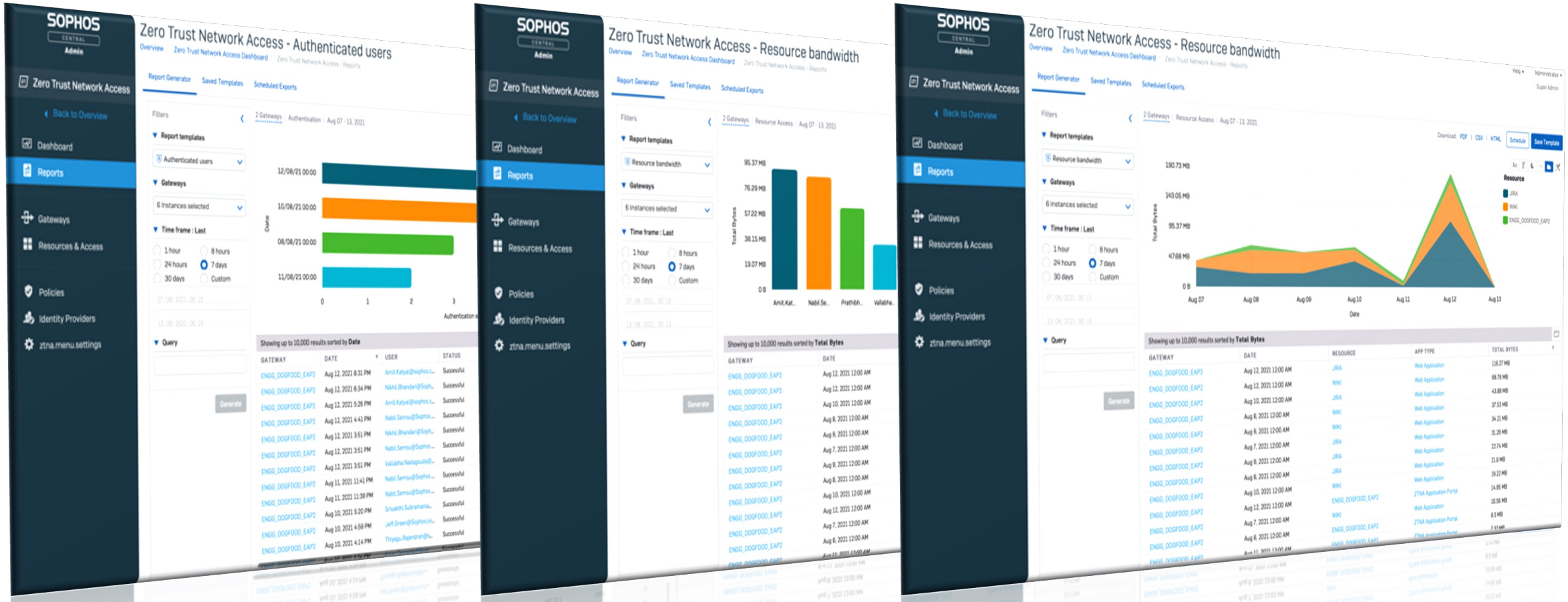
- Schutz vor Ransomware im Home Office und unterwegs
- Höhere Sicherheit – kein direkter Netzwerkzugriff mehr
- Agilität – schnell und einfach Zugriff für Mitarbeiter und Dienstleister
- Compliance – Sichtbarkeit, wer was darf und wer was gemacht hat
- Unterstützt den Weg in die Cloud

Zero Trust Networking

*"You're **NOT on** the network"*



Detailliertes Compliance Reporting



Anwendungen | Status | Datentransfer | Bandbreite | Benutzer

SOPHOS

Systeme zur Angriffserkennung (SzA) - Whitepaper

Systeme zur Angriffserkennung (SzA)

Diese Sophos-Lösungen unterstützen Sie beim Erfüllen der BSI-Anforderung

Nach einer Neuerung im deutschen BSI-Gesetz (BSIG) und im Energiewirtschaftsgesetz (EnWG) müssen Betreiber Kritischer Infrastrukturen sowie Betreiber von Energieversorgungsnetzen in Deutschland gegenüber dem BSI so genannte Systeme zur Angriffserkennung (SzA) vorweisen können. Dieses Dokument bietet eine Übersicht, wie Sophos-Lösungen bei der Umsetzung der Anforderung unterstützen können.

Prio	Anforderungen und Maßnahmen	Unterstützung durch Sophos	Sophos-Lösungen	Service-Leistung durch Sophos	Anmerkungen
Grundsätzliche Anforderungen					
MUSS	Die notwendigen technischen, organisatorischen und personellen Rahmenbedingungen MÜSSEN geschaffen werden.	✓	alle	MDR	Die technischen Sophos-Lösungen sowie der Sophos MDR-Service können in die Strukturen und Abläufe der Organisation eingebunden werden.
MUSS	Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten MÜSSEN fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden.	✓	alle	MDR	Die Sophos X-Ops und Sophos Labs liefern den Sophos-Lösungen sowie dem Sophos MDR-Team kontinuierlich Informationen über aktuelle Angriffsszenarien.
MUSS	Alle zur effektiven Angriffserkennung erforderliche Hard- und Software MUSS durchgängig auf einem aktuellen Stand gehalten werden.	✓	alle	MDR	Sophos-Lösungen ermöglichen ein automatisiertes Aktualisieren der Hard- und Software-Komponenten.
MUSS	Die Signaturen von Detektionssystemen MÜSSEN immer aktuell sein.	✓	alle		Die Aktualisierung der Signaturen von Detektionstechnologien in Sophos-Lösungen erfolgt automatisch.
MUSS	Alle relevanten Systeme MÜSSEN so konfiguriert sein, dass Versuche, bekannte Schwachstellen auszunutzen, erkannt werden können, sofern keine schwerwiegenden Gründe dagegensprechen.	✓	alle	MDR, Professional Services	Auf Endpoints und im Netzwerk werden Angriffe erkannt und gestoppt, die versuchen, Schwachstellen auszunutzen. Die Konfiguration sowie deren Überprüfung kann durch Sophos Professional Services und Sophos MDR unterstützt werden.

SOPHOS

Die nächsten Schritte

Entscheidungsvorlage für IT-Leiter und Geschäftsführer

Jetzt downloaden

Podcast

Cybersecurity für kritische Infrastrukturen – was KRITIS-Unternehmen aus gesetzlicher Sicht beachten müssen mit Rechtsanwalt Andreas Daum, LL.M. (LSE) von Noerr Partnerschaftsgesellschaft mbB.

Zum Podcast

IT-Sicherheitsgesetz und Kritis

Das neue IT-Sicherheitsgesetz 2.0 betrifft nicht nur KRITIS-Betreiber in Deutschland, sondern auch deren Lieferanten in anderen Ländern. Weitere Informationen erhalten Sie auf unserer Webseite.

sophos.de/it-sicherheitsgesetz

Kontakt

Wenn Sie Fragen haben oder Unterstützung benötigen, ist Ihr Sophos-Ansprechpartner gerne für Sie da und hilft Ihnen weiter.

gesundheitswesen@sophos.de

SOPHOS