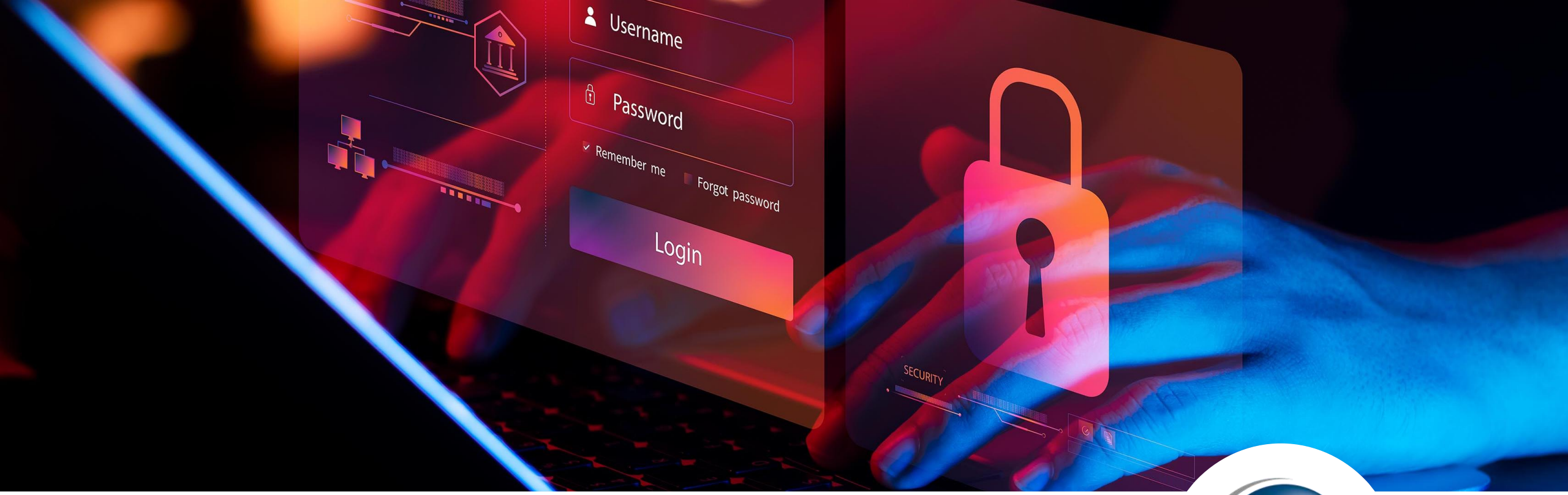


BEI UNS FUNKTIONIERT NUR NOCH DAS TELEFON. CYBERANGRIFF – WAS TUN, WENN ES PASSIERT IST?

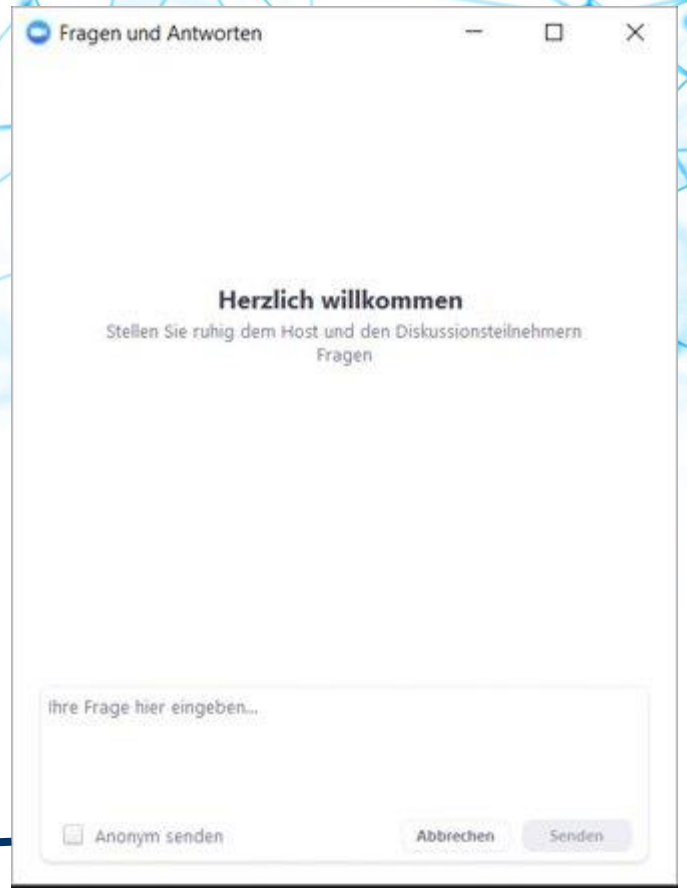
Web-Seminar | 11.01.2024

CompuGroup Medical

Fragen oder Anregungen?

Hand heben und mittels Mikrofon Frage an Präsentator stellen

Fragen hier eingeben



Frage anonym senden

Referenten

Hans-Peter Mohr
Leitung Vertrieb
IT Design & Service

Martin Glönkler
Senior Sales Professional
IT Design & Service

Aktuelle Meldungen

Cyberangriffe mit Ransomware sind nach wie vor die größte Bedrohung

Die Lage der IT-Sicherheit in Deutschland 2023

06.11.2023 · Quelle: Pressemitteilung · 3 min Lesedauer ·

Die Cybersicherheitslage in Deutschland ist weiter angespannt. Das geht aus dem aktuellen Bericht zur Lage der IT-Sicherheit in Deutschland 2023 hervor. Der BSI-Lagebericht verdeutlicht, dass von Angriffen mit Ransomware die derzeit größte Bedrohung ausgeht. Hinzu kommt eine wachsende Professionalisierung auf Täterseite, der eine steigende Anzahl von Sicherheitslücken gegenübersteht.

Cyberangriffe mit Ransomware sind nach Einschätzung des BSI nach wie vor die größte Bedrohung für Wirtschaft und Verwaltung. Sie verursachen einen Großteil der wirtschaftlichen Schäden, die durch Cyberangriffe entstehen.
(© MH - stock.adobe.com)

Die Bedrohungslage im Cyberraum nimmt stetig zu. Das BSI hat für den Bericht „Die Lage der IT-Sicherheit in Deutschland 2023“ im Berichtszeitraum täglich rund 250.000 neue Varianten von Schadprogrammen und 21.000 mit Schadsoftware infizierte Systeme registriert. Hinzu kommen durchschnittlich 70 neue Sicherheitslücken pro Tag, von denen jede zweite als hoch oder kritisch eingestuft wird. Das entspricht einer Steigerung von 24 Prozent gegenüber dem Vorjahr.

Aktuelle Meldungen

Cyberangriff auf Kliniken in Ostwestfalen

Am 24.12. suchte nicht der Weihnachtsmann, sondern ein Erpressungstrojaner Kliniken in Ostwestfalen-Lippe heim. Die gesamte IT stehe still.

Lesezeit: **1 Min.** In Pocket speichern 345

(Bild: Skorzewiak/Shutterstock.com)

25.12.2023 12:57 Uhr | Security

Von Peter Siering

Gezielter Angriff mit Lockbit

Eine erste Prüfung hat ergeben, dass gezielt Daten mit dem Erpressungstrojaner Lockbit 3.0 verschlüsselt worden sind. Es wurde ein Krisenstab eingerichtet, der die Situation analysiert. Die Betreiber betonen, dass Patienten weiter versorgt würden und dass der Betrieb mit leichten technischen Einschränkungen weiterlaufe. Zur Sicherheit habe man die Häuser aber von der Notfallversorgung abgemeldet.

Aktuelle Meldungen

Skrupel nur vorgeschoben? Ransomware-Banden attackieren Kliniken

Zwar zürnt der Lockbit-Betreiber öffentlich mit einem Handlanger, ist sich dennoch für Krankenhaus-Erpressung nicht zu schade. Andere bedrohen gar Patienten.

Lesezeit: 3 Min. In Pocket speichern

(Bild: ARMMY PICCA/Shutterstock.com)

09.01.2024 15:36 Uhr | Security

Von Dr. Christopher Kunz

Derweil weisen die Betreiber der Ransomware Lockbit 3.0 die Verantwortung für den Angriff von sich: Ein "Affiliate", also ein selbstständiger Krimineller, der die Software und Infrastruktur der Bande gegen Provision nutzen darf, habe regelwidrig Daten verschlüsselt, teilte der Lockbit-"Kundendienst" den Malware-Spezialisten von VX Underground mit. In nicht zitierfähigem Russisch echauffierte sich der anonyme Cybergangster über den missliebigen Ex-Spießgesellen und wünschte ihm die baldige Verhaftung. Die Regeln für LockBit-Affiliates verbieten das Verschlüsseln medizinischer Daten, wenn sich daraus Lebensgefahr für Patienten ergibt.

Aktuelle Meldungen

Aktuell sind hier **153 betroffene Organisationen** aus NRW und Niedersachsen aufgelistet.

Vom Cyberangriff bzw. der IT-Abschaltung sind ganz oder teilweise betroffen:

in Nordrhein-Westfalen:

- 1 Südwestfalen-IT
- 11 Kreisverwaltungen
- 105 Gemeinden
- 26 Unternehmen, Verbände und andere Organisationen

in Niedersachsen:

- 10 Standesämter (wahrscheinlich sind es mehr)

Zero-Day-Angriffe

Alert!

Sicherheitsupdates Fortinet: Angreifer können Passwörter im Klartext einsehen

Fortinet hat wichtige Sicherheitspatches für FortiOS und FortiProxy veröffentlicht.

Lesezeit: 1 Min. In Pocket speichern 3

(Bild: Tatiana Popova/Shutterstock.com)

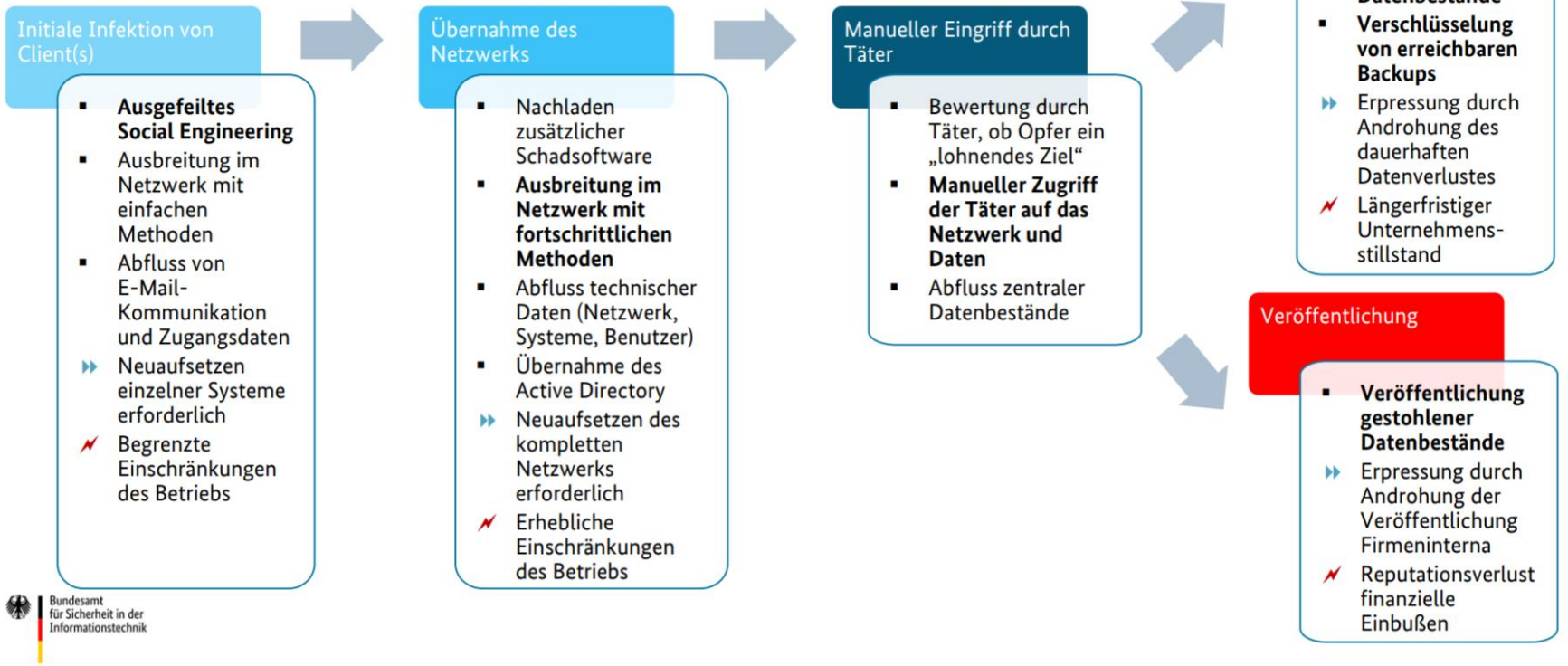
11.10.2023 14:38 Uhr | Security

Von Dennis Schirrmacher

Wie aus dem Sicherheitsbereich der Fortinet-Website hervorgeht, ist nur eine (CVE-2023-41841) der fünf geschlossenen Sicherheitslücken mit dem Bedrohungsgrad „**hoch**“ eingestuft. Aufgrund einer fehlerhaften Authentifizierung können authentifizierte Angreifer an der Web-UI-Komponente ansetzen und Aktionen als Admins ausführen. Wie so ein Angriff vonstatten gehen könnte, ist bislang unklar. Die Entwickler geben an, dass Sicherheitsproblem in den **FortiOS-Versionen 7.0.12**, **7.2.5** und **7.4.0** gelöst zu haben.

Vorgehen der Angreifer

Fortschrittliche Angriffe – Vorgehen der Angreifer

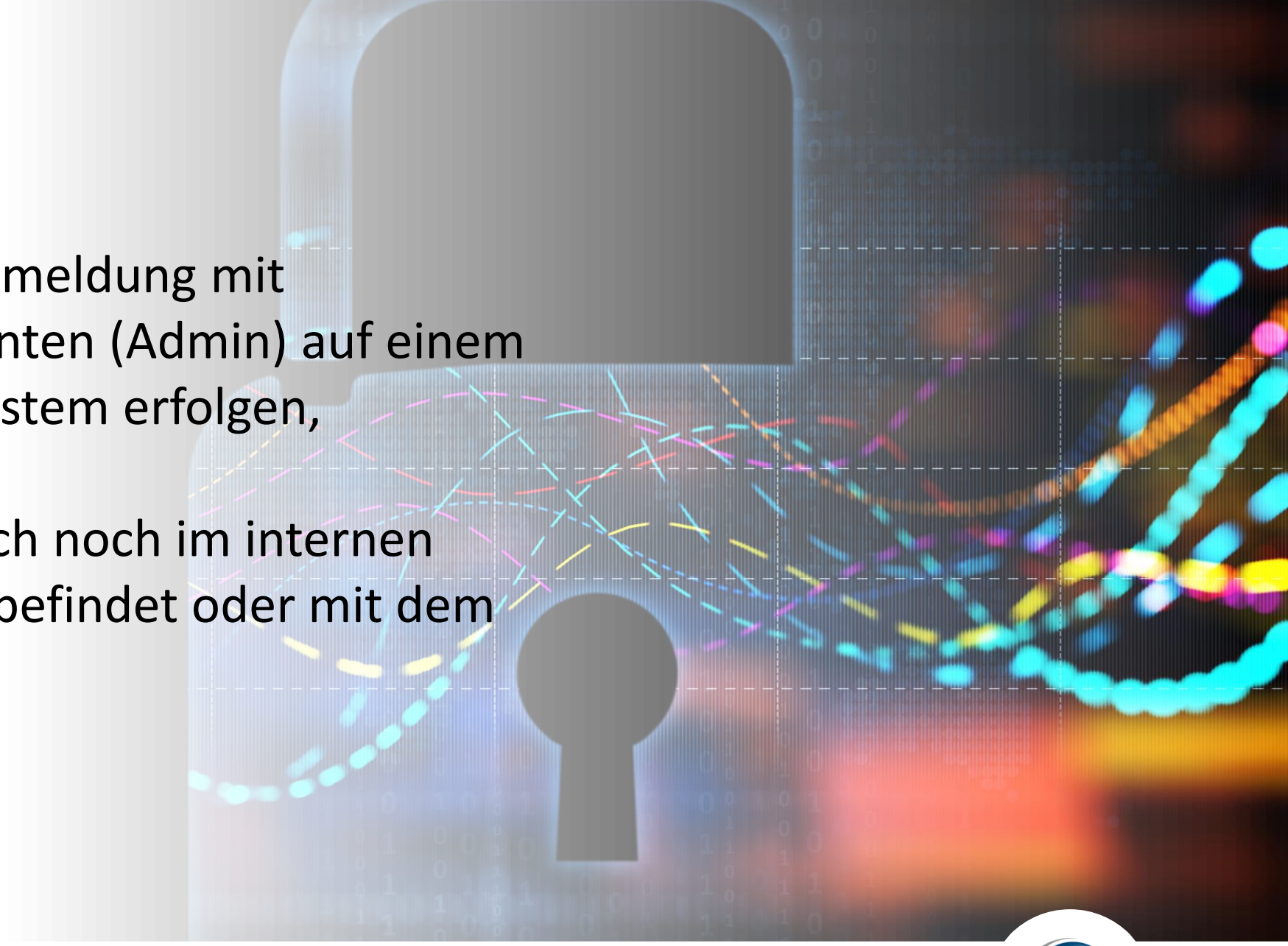


Bundesamt für Sicherheit in der Informationstechnik

An was ist alles zu denken.

Tritt der IT-Vorfall so oder so ähnlich ein und an was ist alles zu denken?

Oberste Regel



Keinesfalls darf eine Anmeldung mit privilegierten Nutzerkonten (Admin) auf einem potenziell infizierten System erfolgen,

während das System sich noch im internen produktiven Netzwerk befindet oder mit dem Internet verbunden ist!

Organisatorische Maßnahmen

- IT-Vorfall - Bewältigung als Projekt
- Krisenstab einrichten
- Kommunikation nach außen und innen
- Kurzfristige Wiederherstellung der Arbeitsfähigkeit
- Meldepflichten beachten
- Externe Unterstützung einholen
- Lösegeld bezahlen ??
- Nacharbeiten und Ausarbeiten eines
  - Information Sicherheits-Management-System (ISMS)
  - Business Continuity Management (BCM)

Technische Maßnahmen

- Ruhig bleiben und geplant handeln
- Wo beginnen
  - Potentielle infizierte Systeme vom Netz trennen
  - Ermitteln um welches Schadprogramm es sich handelt
  - Forensische Beweissicherung
  - Umgang mit Logdaten
- Systeme neu aufsetzen oder Restore aus Backup

Org. Maßnahmen: Vorfalls-Bewältigung als Projekt

Phase 1: Analyse
- Identifikation betroffener Systeme
- Analyse der Schadprogramme
- Schadensfeststellung

Phase 2: Übergangsbetrieb
- Verhinderung weiterer Infektion und Verschlüsselung
- Blockierung der Täterzugänge
- Intensives Monitoring des Netzes

Phase 3: Bereinigung
- Konzeption / Umsetzung / Neustart
- Weitere Sicherheitsmaßnahmen (neues Sicherheitskonzept)

Org. Maßnahmen: Krisenstab einrichten

Leitungsebene
als Leiter des Krisenstabes (nach Möglichkeit jedoch nicht „den Kopf“ der Institution).

IT-Leitung:
Als technischen Sachverstand für den Krisenstab, um operative Kräfte für die Arbeit freizuhalten.

Juristen:
Fragen zu Haftung, Strafanzeige, weitere rechtliche Aspekte.

Presse- und Öffentlichkeitsarbeit:
eine angemessene Krisenkommunikation nach innen und außen bewahrt die Reputation des Unternehmens, schützt Geschäftsbeziehungen und motiviert die Mitarbeiterinnen und Mitarbeiter

Datenschutzbeauftragte:
sowie für datenschutzrechtliche Fragen das „was wird wie“ protokoliert und aufgezeichnet.

Personal- / Betriebsrat.
Wegen Zugriff auf Logdaten sowie personalrelevante Fragen wie Überstunden.

Org. Maßnahmen: Kommunikation

Die interne und externe Kommunikation bei schweren IT-Sicherheitsvorfällen ist eines der wichtigsten Maßnahmen

- Überlassen Sie die Kommunikation den Spezialisten!
- Stellen Sie die notwendige Kommunikationsinfrastruktur bereit!
  - VOIP Telefone funktionieren eventuell nicht mehr!
- Interne Kommunikation vor externer Kommunikation!
- Bündeln Sie den Informationsfluss und nutzen Sie FAQs!
- Für „blame, name, shame“ und „bashing“ ist in der Krise kein Platz!
- Sagen Sie öffentlich sowie gegenüber ihren MitarbeiterInnen jederzeit die Wahrheit!

Org. Maßnahmen: Schadensanalyse

Für Schadenbewältigung bedarf es einer genauen Schadensanalyse

- Erstellen Sie eine Übersicht der vorhandenen Daten
  - Nicht betroffen Systeme,
  - Backups
  - externe Datenquellen
- Aufklärung der Schadensursache
- Beseitigung der Schwachstellen die für den Sicherheitsvorfall die Ursache war.

Org. Maßnahmen: Meldepflichten

Denken Sie an etwaige Meldepflichten etwa nach DSGVO, BSIG und anderen Gesetzen gegenüber Regulatoren.
Beachten Sie außerdem etwaige Verpflichtungen aus vertraglichen Vereinbarungen.

- Bei DSGVO-Verstößen wie dem Abfluss personenbezogener Daten
  - Haben innerhalb von 72 Stunden bei der Landesdaten-schutzbeauftragten zu erfolgen.

- Bei EMOTET Vorfällen sind Kunden und Partner zu informieren
  - Eventuell wurden hier EMAILs mit Schadcode versendet.

- Cyber-Versicherung: Informieren Sie diese frühzeitig. Häufig gibt Ihnen diese Vorgaben, was Sie tun können.

Org. Maßnahmen: externe Unterstützung

Wenden Sie sich frühzeitig an externe Experten, wenn Sie sich überfordert fühlen.

- IT-Sicherheitsdienstleister „Partner Ihres Vertrauens CGM ITD&S“
  - Hilfe bei dem Bereinigen von Systemen und des ADs
  - Es muss das Einfallstor gefunden werden
- Polizei
  - Zentrale Ansprechstelle Cybercrime, ZACs
- Bundesamt für Sicherheit in der Informationstechnik
  - Vermittlung von (Forensik-)Experten
  - Besprechung von Maßnahmen

Org. Maßnahmen: Lösegeld bezahlen?

- Grundsätzlich wird empfohlen nicht zu bezahlen
  - und nicht auf die Erpressung einzugehen.
- Falls doch Lösegeld bezahlt wurde
  - ersetzt dies nicht die Neuinstallation der kompromittierten Systeme.
- Die Hintertür könnte noch vorhanden sein,
  - ein erneuter Angriff ist möglich.

Tech. Maßnahmen: Vorgehen

Das Vorgehen bei einem schweren IT-Sicherheitsvorfall ist häufig vom Einzelfall abhängig.

- Wie lange können die Systeme offline bleiben?
- Wobei handelt es sich bei diesem Vorfall (Ransomware, Wirtschaftsspionage)?
- Ist eine Sicherung der Spuren für eine Anzeige gewünscht?
- Wie ist die Bedrohungslage für Ihre Institution?

Tech. Maßnahmen: Wo beginnen

Bei Systeme, die **noch** in Betrieb sind gilt die oberste Regel:

Keinesfalls darf eine Anmeldung mit privilegierten Nutzerkonten (Administrator) auf einem potenziell infizierten System erfolgen, während es sich noch im produktiven Netzwerk befindet!

- Validierung aller (Admin-)Accounts
  - Sind alle Admin Accounts legitim?
- Auf betroffenen Systemen auf neue RDP-Freigaben prüfen
- Gibt es weitere Auffälligkeiten an den Systemen?

Tech. Maßnahmen: Forensische Beweissicherung

Wird eine forensische Beweissicherung angestrebt ist das System hart auszuschalten, da bei Shutdown des Betriebssystems Logs bereinigt und eventuell unwiderruflich verändert werden.

Bei der Erstellung eines Festplattenimages ist darauf zu achten, dass ein richtiges forensisches Image, d.h. eine 1:1 Sektorkopie, erstellt wird. Marktübliche Festplatten-Backupprogramme können solche forensischen Images in der Regel nicht erstellen.

Bei virtuellen Systemen reicht es aus, das Verzeichnis der Virtualisierungssoftware zu sichern. Wenn die virtuelle Maschine suspendiert wird, befindet sich im Virtualisierungsverzeichnis zudem ein Dump des Arbeitsspeichers.
Dies kann bei der Auswertung der flüchtigen Daten helfen!

Tech. Maßnahmen: Umgang mit Logdaten

Bei einem Angriff ist die Auswertung von Logdaten eines der wichtigsten Mittel, um das Ausmaß des Angriffs und/oder Datenabfluss aufklären zu können.

- Die Logs des HTTP-Proxy, um HTTP-Datenverkehr zu Command & Control Servern
- Logs des E-Mail Servers
- Firewall-Logs / VPN Zugänge / RDP Zugänge
- Active-Directory / LDAP-Logs
- Telemetriedaten* von Cybersicherheits Schutzsoftware mit XDR Funktionen (keine Standard Antiviren Software auf Pattern Basis)

* Funktionen z.B. bei SOPHOS XDR „Extended Detection and Response“ oder MDR Cybersecurity as a Service 24/7/365

Tech. Maßnahmen: Bereinigen

Das BSI empfiehlt grundsätzlich die infizierten Systeme als vollständig kompromittiert zu betrachten und neu aufzusetzen.

- Alle Systeme vom Netz nehmen
  z.B. über abschalten der Netzwerk Ports.
- Die Systeme neu aufsetzen.
- Admin/Serviceaccounts ändern und Admin Konten überwachen.
- Überprüfen ob unbekannte Adminaccounts bestehen.
- Mögliche Infektionswege schließen.
- Langfristig sollte das AD neu aufgesetzt werden.
- Der Krisenstab definiert die Reihenfolge der Wiederherstellung.

Tech. Maßnahmen: Bereinigen II

Das BSI empfiehlt grundsätzlich die infizierten Systeme als vollständig kompromittiert zu betrachten und neu aufzusetzen.

- Achtung: „Image Backups“ können mit Schadcode wie EMOTET bereits belastet sein.
- Wenn Möglich RDP, SSH, Teamviewer, etc. blockieren und Verbindungsversuche mitloggen und analysieren.
- Einen Service wie „**Sophos Rapid Response**“ oder ähnliches für 45 Tage aktivieren.

Tech. Maßnahmen: SOPHOS RAPID RESPONSE Service

Blitzschnelle Reaktion auf aktive Bedrohungen:
„Sophos Rapid Response“ bietet Soforthilfe durch ein Expertenteam.

- Dedizierter Ansprechpartner
- 24/7 Monitoring und Reaktion für 45 Tage um Ihren Schutz zu optimieren
- Schnelles erkennen, eindämmen und beseitigen aktiver Bedrohungen
- Entfernen von Angreifern aus Ihrer Umgebung
- Forensische Analyse des IT-Vorfalls erstellen, soweit möglich
- Empfehlung von Präventiv-Maßnahmen in Echtzeit
- Bedrohungs-Bericht nach dem Vorfall
- Festpreis-Modell ohne versteckte Kosten (nach Benutzer und Server)

Präventivmaßnahmen „die Top 10“

Aufgrund der immer weitergehenden Professionalisierung von Angriffen ist es keine Frage ob, sondern nur wann Ihre Organisation von einem größeren Sicherheitsvorfall betroffen sein wird!

- Neueste Techniken für AV-Scanner in Cybersicherheit einsetzten, Pattern Scan war mal
- MFA oder Zero-Trust für alle externen Zugänge ist ein „must have“
- Erstellen Sie Notfallkonzepte
- Sind Recovery Time Objective (RTO) und Recovery Point Objective (RPO) Werte bekannt
- Sensibilisieren Sie Ihre Mitarbeiter regelmäßig auf Umgang mit Mail/Internet
- Proben Sie den Ernstfall
- Aktuelle Software einsetzten und diese akribisch auf Stand halten
- 3-2-1-Backup-Methode: drei Kopien, zwei verschiedenen Medien, andere Ort, immutable
- Regelmäßige “externe“ IT-Risikobewertungen, um Betriebsblindheit vorzubeugen

Links zum Thema

Cybersicherheitslage
https://www.connect-professional.de/markt/cybersicherheitslage-in-deutschland-angespannt-bis-kritisch.327889.html

BSI Die Lage der IT-Sicherheit in Deutschland 2023
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=129410

BSI Ich habe einen Vorfall
https://www.bsi.bund.de/dok/13983460

Bei KRITIS Häusern
https://www.bsi.bund.de/dok/schwachstellen-KRITIS

Zentrale Ansprechstellen Cybercrime der Polizeien für Wirtschaftsunternehmen
https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html

IT Grundschutz
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/Zip_Datei_Edition_2023.html

BSI Umsetzungs- und Notfallmanagement
https://www.bsi.bund.de/dok/6600630

IT D&S kann im Vorfeld helfen – IT-Security Audit

IT-Sicherheit über alle Ebenen hinweg

Jede Organisation/Klinik hat einen unterschiedlichen IT-Sicherheitsbedarf. Unabhängig von individuellen Anforderungen ist eines klar: Einzelne Security-Komponenten reichen heute für einen zuverlässigen Schutz nicht mehr aus. Gefragt sind vielmehr unterschiedliche perfekt ineinandergreifende Sicherheitsebenen und -maßnahmen.

CGM CompuGroup Medical

IT NOTFALL:
WAS IST ZU TUN – WENN ES PASSIERT IST….

CGM Clinical Deutschland GmbH
Unixstraße 1
88436 Oberessendorf

+49 7355 799 610
Hans-Peter.Mohr@cgm.com

+49 7355 799 642
Martin.Gloenkler@cgm.com

CGM CompuGroup Medical