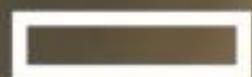


15. BECHTLE IT-FORUM THÜRINGEN

BECHTLE

2024

15. Mai 2024 • STEIGERWALD Stadion ^{Erfurt}



Hewlett Packard
Enterprise



CISCO
Partner



HUAWEI

intel.

Von Angriff bis Verteidigung: Das Bechtle Cyber Defense Center im Kampf gegen Hacker

05.2024 | Patrick Sommer | Bechtle Cyber Defense Technical



Agenda.

- 1** Einleitung.
- 2** Unsere Leistungen.
- 3** Aktuelle Bedrohungslandschaft.
- 4** Schlussfolgerung.
- 5** Q&A.



Einleitung.

Wer bin ich?



Patrick Sommer

IT Solutions Architekt Security

CompTIA+

Netzwerk
Security

ISC2

CISSP

Projektmanagement

Prince2

Hersteller

Sophos
Macmon
Trellix (McAfee)
Crowdstrike
Cybereason
Cisco
Darktrace

Wer bin ich?



Patrick Sommer

IT Solutions Architekt Security

CompTIA+

Netzwerk
Security

ISC2

CISSP

Projektmanagement

Prince2

Hersteller

Sophos
Macmon
Trellix (McAfee)
Crowdstrike
Cybereason
Cisco
Darktrace

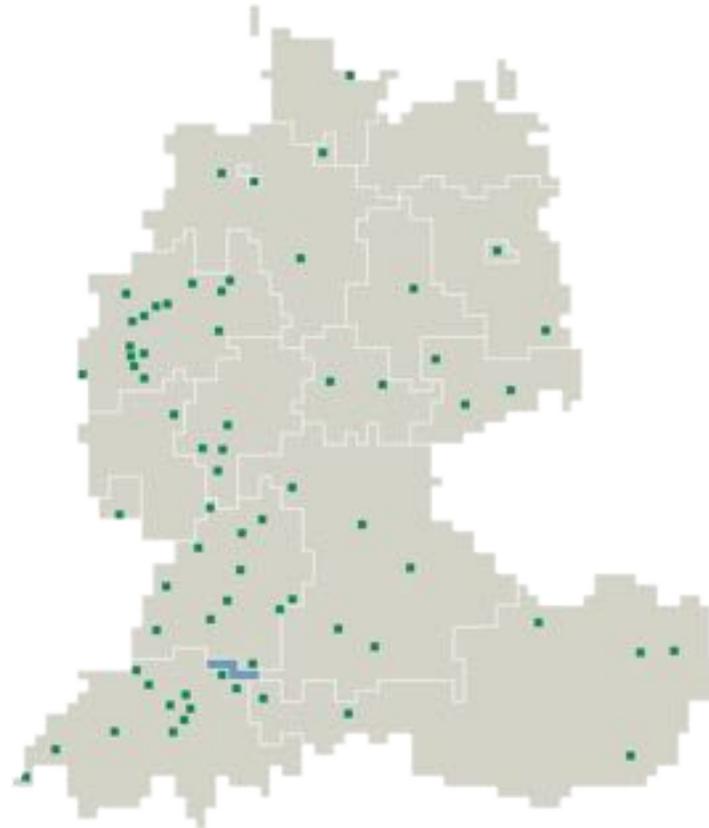
Wer sind wir im CDC?

Cyber Defense Center Plattform

- Wien

Forensic Labors

- Wien
- Dresden
- Chemnitz
- Neckarsulm
- Bodensee
- Dortmund



Cyber Defense Center Personal

- Wien
- Dresden
- Chemnitz
- Neckarsulm
- Bremen
- Hille
- Bielefeld
- Dortmund

Vorgehensweise in der Krisenbewältigung

CYBER NOTFALLKARTE

VERHALTEN BEI IT-SICHERHEITSVORFÄLLEN.

Verhalten bei IT-Sicherheitsvorfällen.
Ruhe bewahren und Notfall melden.

Notfallkontakt intern

Notfallkontakt extern 24x7
Bechtle Security Incident Response Team
+49 7132 / 981 2783
help.sirt@bechtle.com

- Wer meldet?
- Welche Systeme sind betroffen?
- Wann ist das Ereignis eingetreten?
- Was wurde gemacht?
- Was wurde beobachtet?
- Wo befinden sich die Systeme?

Verhaltensregeln bei Cyberangriffen.

DO'S.

- Systeme unverändert lassen
- Netzwerkverbindung trennen
- Notfallkontakte informieren
- Beobachtungen dokumentieren
- Maßnahmen nach Anleitung umsetzen

DONT'S.

- Auf Forderungen reagieren
- PC ausschalten (Beweissicherung)
- Informationen nach außen geben (Presse, Partner, Kunden)

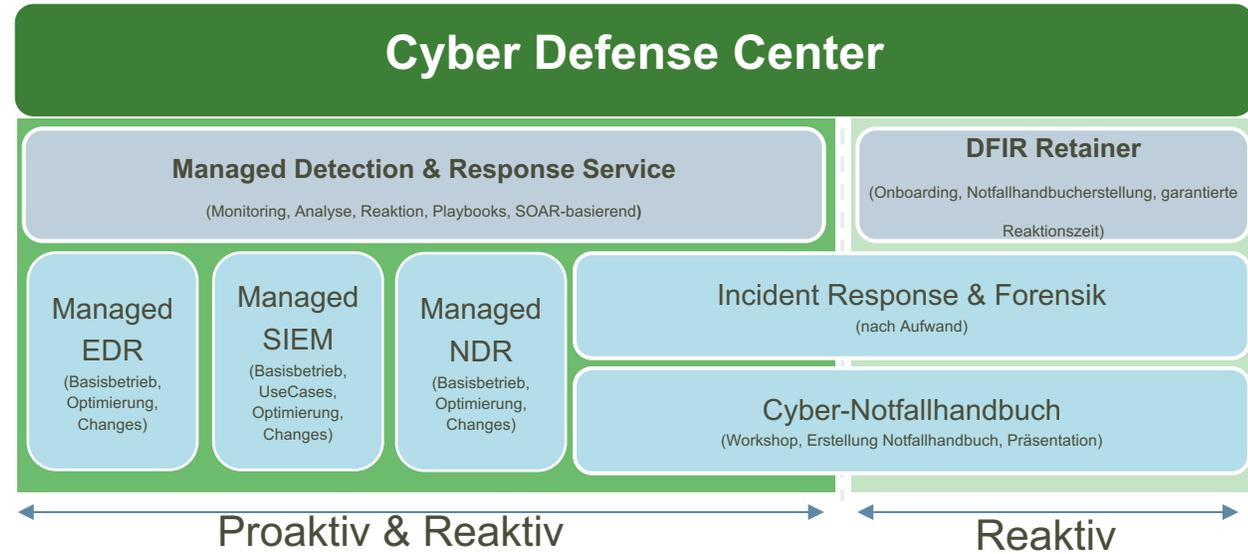
Ohne eine vertragliche Vereinbarung können wir zeitnahe Unterstützung zusagen.

© Bechtle IT/Sec 19.12.2023

Unsere Leistungen.

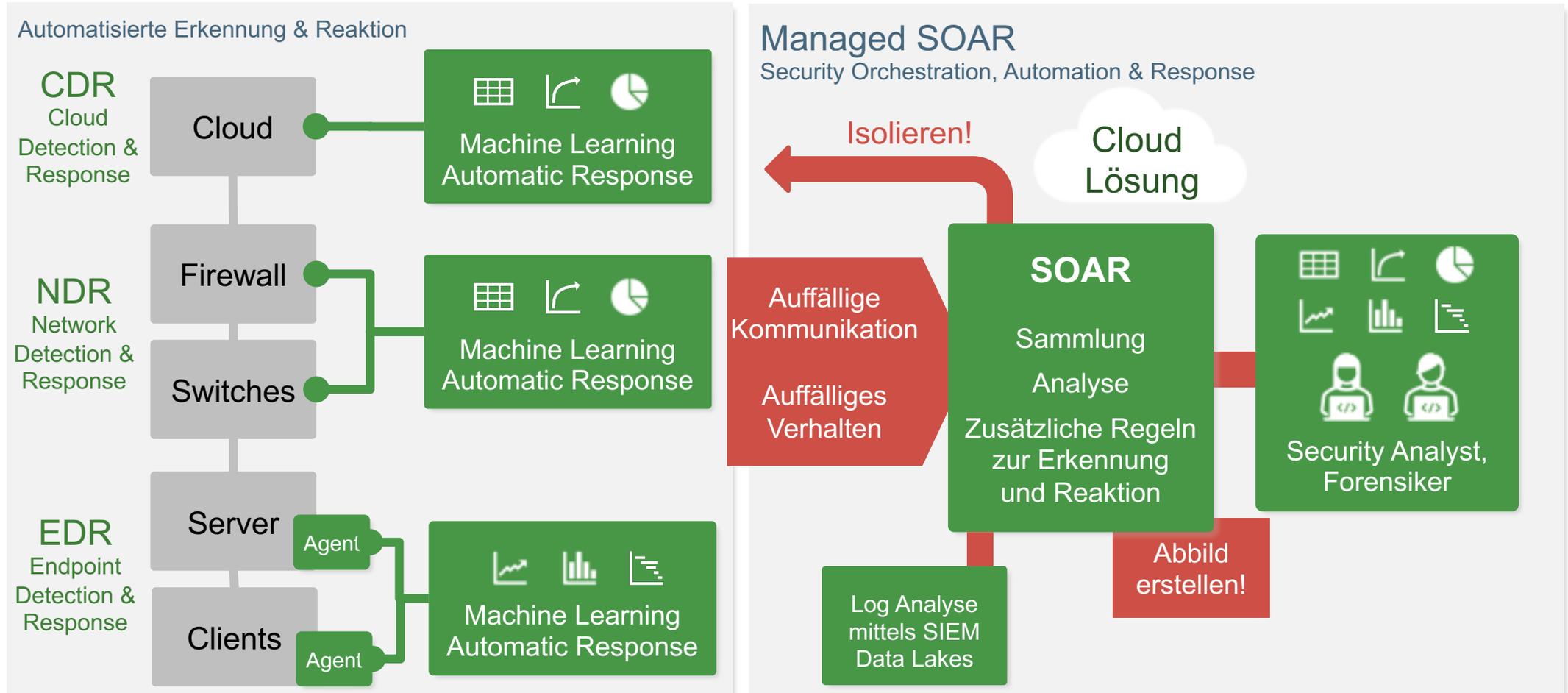
Managed Security Services CDC-Portfolio

- Modular aufgebaut
- Kunden-individuell
- Wächst mit den Anforderungen



Next Generation Cyber Defense

Bechtle SOC Plattform



Incident Response

Wenn dennoch was passiert ist...

- Krisenmanagement, Planung und Koordination erforderlicher Maßnahmen
- Gegebenenfalls Aufbau, Installation und Konfiguration der Analyseplattform
- Sammlung und Sicherung wichtiger Informationen beispielsweise von Windows- (Logs, Events, Images), Firewall-, NDR- oder EDR-Systemen
- Analyse der gesicherten Daten, Forensische Analyse und Verhaltensanalyse des Netzwerkverkehrs sowie der Aktivitäten auf den Endgeräten
- Entwicklung einer Kommunikations- und Response-Matrix
- Einsatz von geprüften Security-Tools
- Entwicklung kurzfristiger und langfristiger Lösungsansätze
- Entfernen von Schadsoftware, Aufzeigen von Sicherheitslücken, Unterstützung bei der
- Behebung entstandener Schäden bis hin zur Beratung bei Neuanschaffungen von Hard- und Softwarelösungen
- Dokumentation der durchgeführten Maßnahmen
- Präsentation und Übermittlung der Ergebnisse

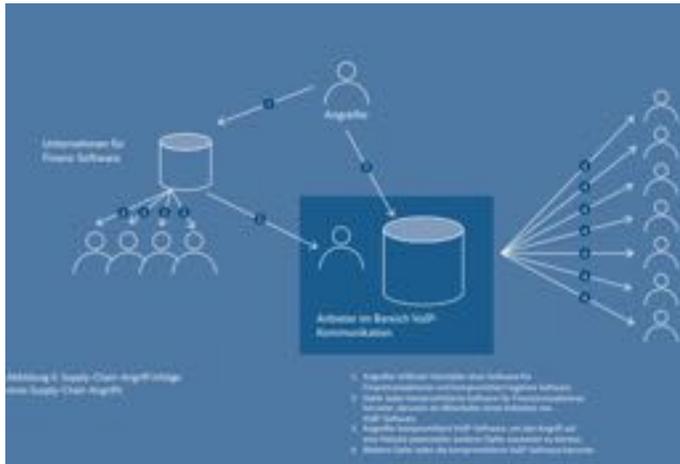
Bechtle Kontaktdaten
Telefonnummer:
+49 7132 981 2783
E-Mail-Adresse:
help.sirt@bechtle.com



**Bundesamt
für Sicherheit in der
Informationstechnik**

Aktuelle Bedrohungslandschaft.

BSI-Lagebericht



Die Lage der IT-Sicherheit in Deutschland 2023

Ransomware

ist weiterhin die größte Bedrohung.

2 Ransomware-Angriffe auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.

68 erfolgreiche Ransomware-Angriffe auf Unternehmen wurden bekannt.

15 davon richteten sich gegen IT-Dienstleister.

Mehr als **2.000** Schwachstellen in Software-Produkten (15 % davon kritisch) wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein Zuwachs von 24 %.

CDC-Lagebericht

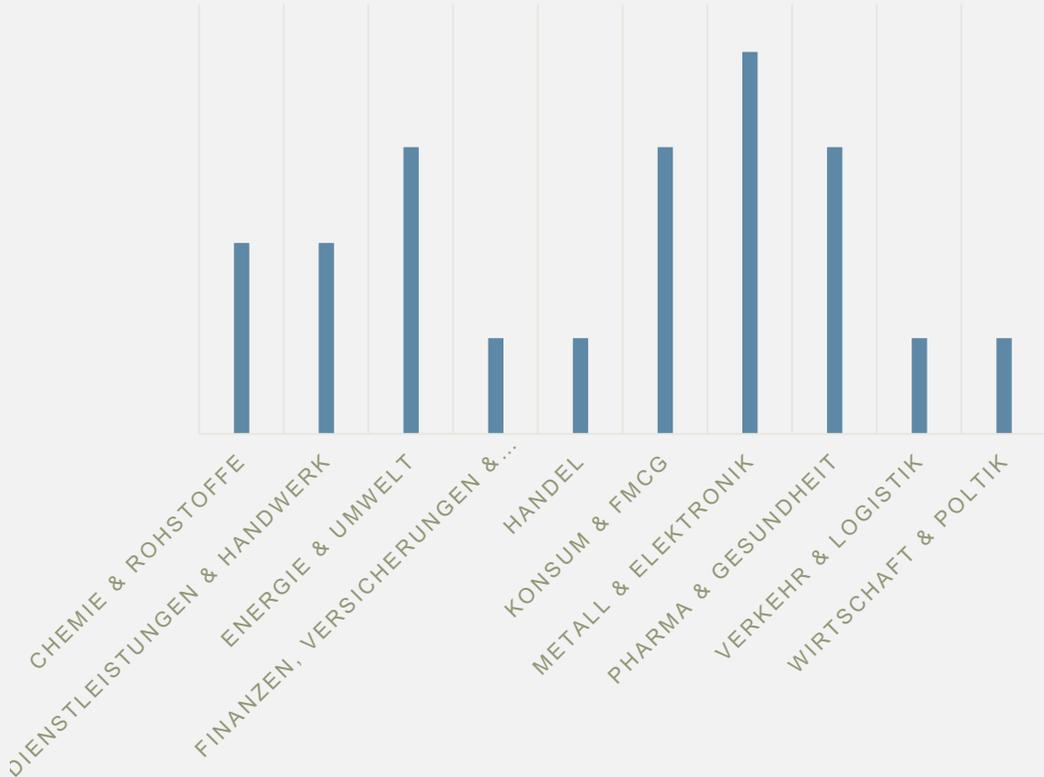
Häufigsten Angriffssektoren

- Exploits/Zero Day Lücken
- Malware/Ransomware
- E-Mail/Phishing
- Insider Bedrohungen/Supply Chain Attacken
- E-Mail/Fraud

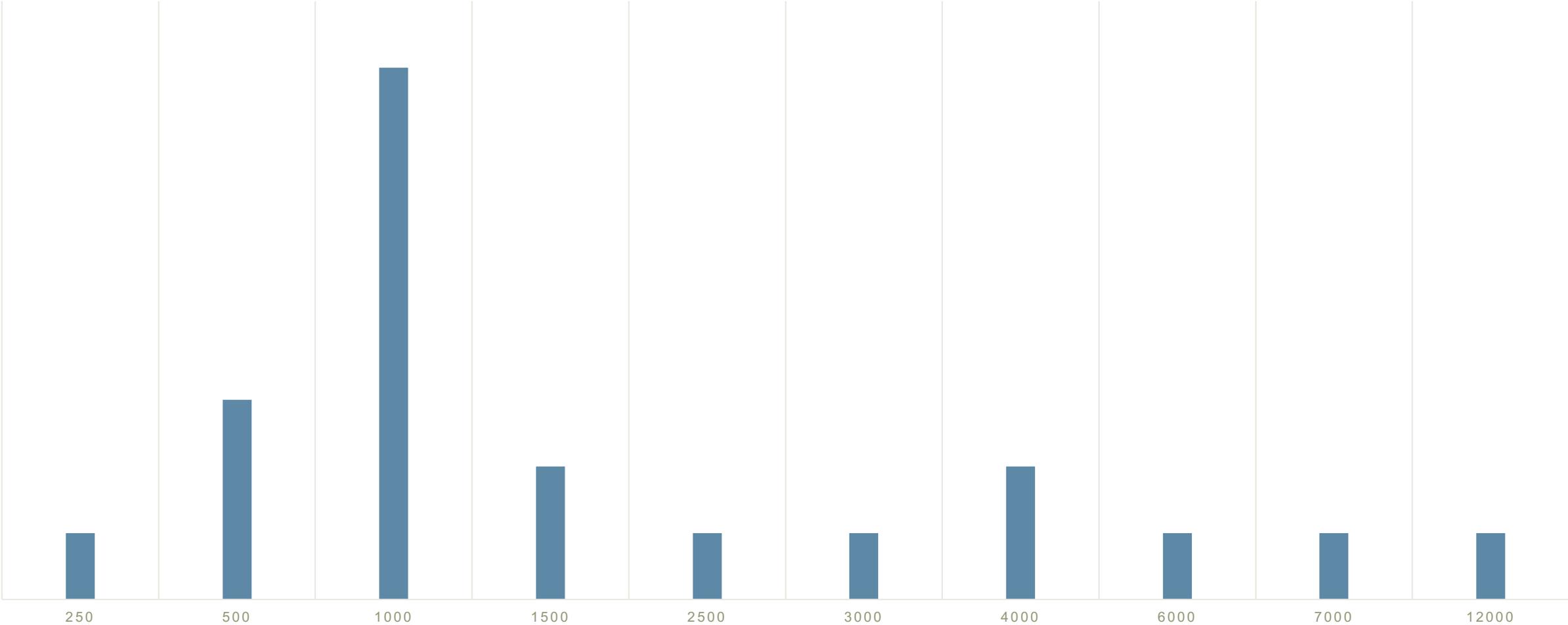
Häufigsten Erkennungstool

- EDR
- Mailsecurity
- SIEM
 - Firewall
 - IDS
- AV-Software
- Vulnerability Management
- NTA

Häufigste Angriffe

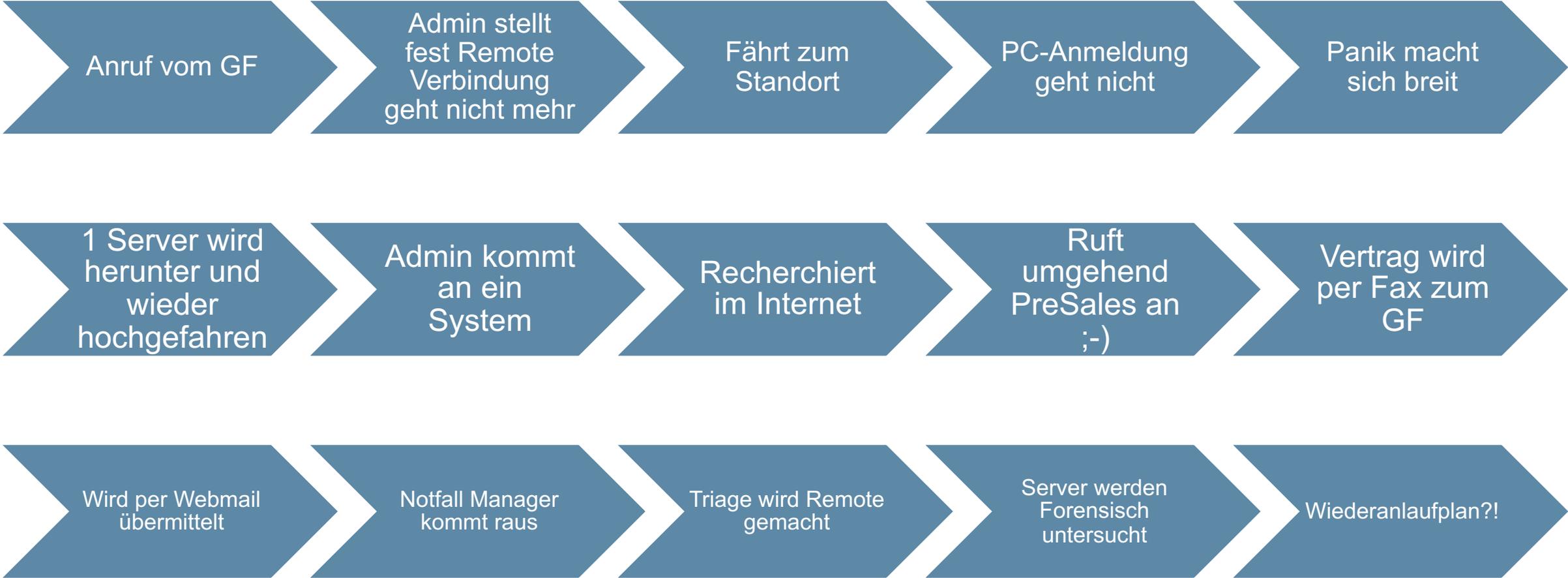


CDC-Lagebericht



CDC - Angriffsbericht

Kunde im September CDC 24*7 Angriffserkennung vorgestellt > Projekt auf 2024/2025 verschoben



IT-Forensik

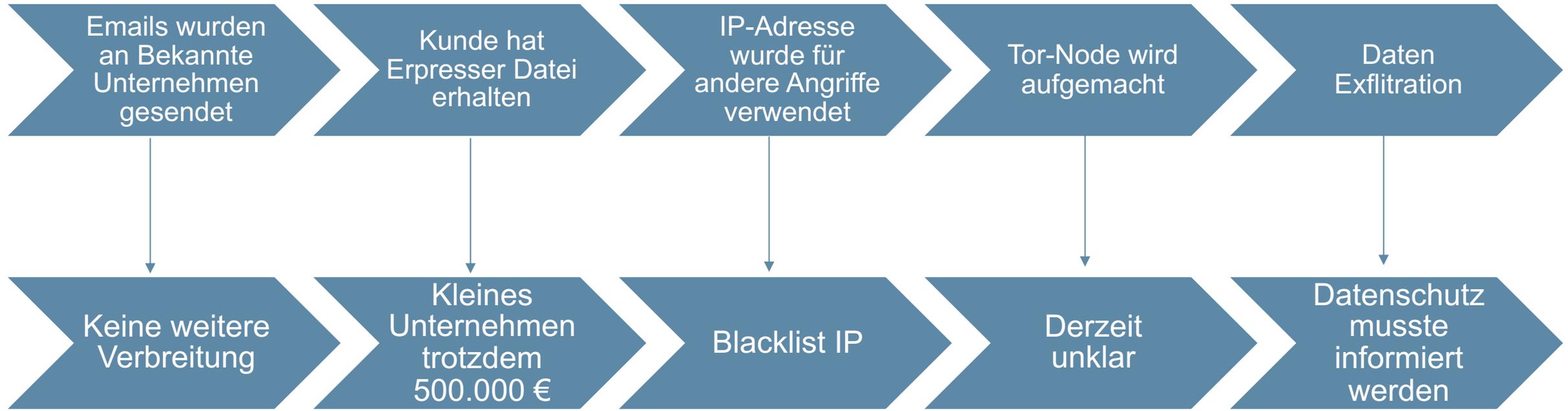
Spurensicherung und ggf. Strafverfolgung

- Forensische Sicherung von Datenträgern
- Unterstützung bei der Ermittlung des Täters
- Aufrechterhaltung der Beweiskette (Chain of Custody)
- Einsatz von bewährten Methoden und Technologien zur forensischen Analyse digitaler Spuren
- Dokumentation der Ergebnisse als forensisches Gutachten



CDC – Bericht danach

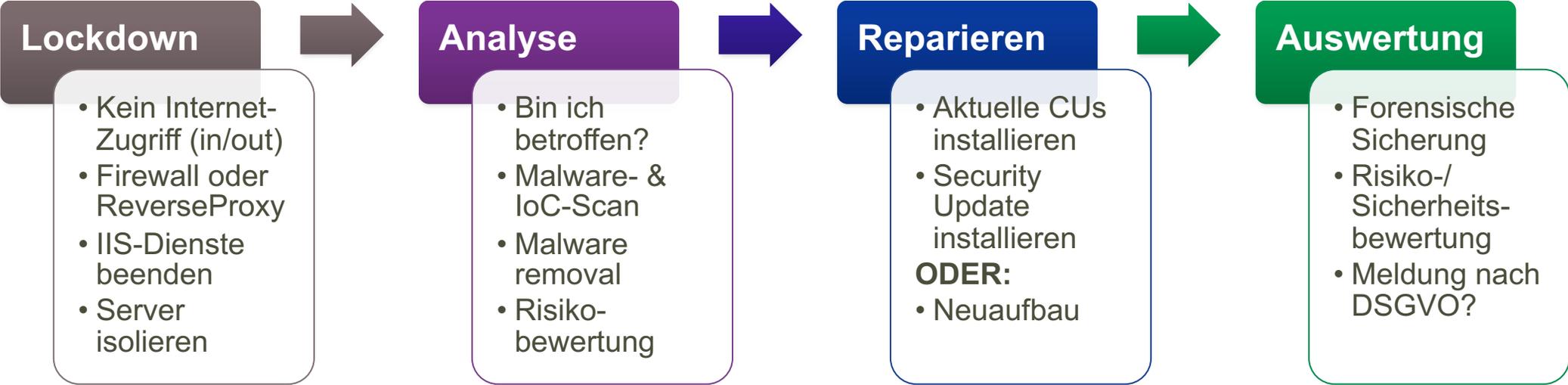
Was war parallel passiert



Schlussfolgerung.

Was ist zu tun wenn es passiert ist ?

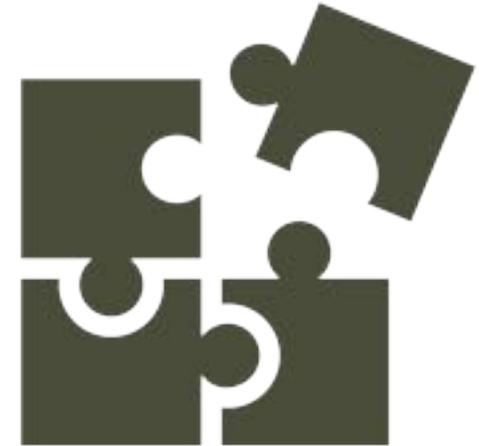
Incident Bearbeitung



Incident Response

Wenn dennoch was passiert ist...

- Krisenmanagement, Planung und Koordination erforderlicher Maßnahmen
- Gegebenenfalls Aufbau, Installation und Konfiguration der Analyseplattform
- Sammlung und Sicherung wichtiger Informationen beispielsweise von Windows- (Logs, Events, Images), Firewall-, NDR- oder EDR-Systemen
- Analyse der gesicherten Daten, Forensische Analyse und Verhaltensanalyse des Netzwerkverkehrs sowie der Aktivitäten auf den Endgeräten
- Entwicklung einer Kommunikations- und Response-Matrix
- Einsatz von geprüften Security-Tools
- Entwicklung kurzfristiger und langfristiger Lösungsansätze
- Entfernen von Schadsoftware, Aufzeigen von Sicherheitslücken, Unterstützung bei der Behebung entstandener Schäden bis hin zur Beratung bei Neuanschaffungen von Hard- und Softwarelösungen
- Dokumentation der durchgeführten Maßnahmen
- Präsentation und Übermittlung der Ergebnisse



Vorgehensweise in der Krisenbewältigung

CYBER NOTFALLKARTE

VERHALTEN BEI IT-SICHERHEITSVORFÄLLEN.

Verhalten bei IT-Sicherheitsvorfällen.

Ruhe bewahren und Notfall melden.

Notfallkontakt intern

Notfallkontakt extern 24x7
 Bechtle Security Incident Response Team
 +49 71 32 7 581 2783
help.sirt@bechtle.com

- 👤 Wer meldet?
- 📄 Welche Systeme sind betroffen?
- 🕒 Wann ist das Ereignis eingetreten?
- 🔧 Was wurde gemacht?
- 👁️ Was wurde beobachtet?
- 📍 Wo befinden sich die Systeme?

Verhaltensregeln bei Cyberangriffen.

DO'S.

- 📌 Systeme unverändert lassen
- 📌 Netzwerkverbindung trennen
- 📌 Notfallkontakte informieren
- 📌 Beobachtungen dokumentieren
- 📌 Maßnahmen nach Anleitung umsetzen

DO NOT'S.

- 📌 Auf Forderungen reagieren
- 📌 PC ausschalten (Datenverlust)
- 📌 Informationen nach außen geben (Presse, Partner, Kunden)

Ohne eine vertragliche Vereinbarung können wir zeitnahe Unterstützung zusagen.

BECHTLE

Q&A.
