Auf den Ernstfall vorbereitet: Krisenresistente IT durch Schwachstellen-Management & Bedrohungserkennung

8. Fachkonferenz „Cybersicherheit“

09.11.2023, Trafo Hub, Braunschweig

GRASS-MERKUR GmbH & Co. KG
Rothwiese 5
30559 Hannover
0511 47 54 14 0
info@grass-merkur.de
www.grass-merkur.de

GRASS MERKUR

HAN-CIX powered by DE CIX

GRASS-MERKUR

DAS UNTERNEHMEN

Das Unternehmen

GRASS-MERKUR

Geschäftsbereich IT

Consulting &
Software-Entwicklung

Sicherheits-Rechenzentrum
(Secure Data Center)

Technologie-Consulting

Strategie-Consulting

Software-Entwicklung

Colocation

Managed Services

Cloud Services

Netzwerk Services

Auf den Ernstfall vorbereitet

SCHWACHSTELLEN-MANAGEMENT UND BEDROHUNGSERKENNUNG

Cyberangriff 1983…

Quelle: https://www.imdb.com/title/tt0086567/

Cyberangriff heute...“auf Bestellung im Internet“

Botnets & Malware › Stampado Ransomware - FUD - CHEAPEST - ONLY $39 - ...

Stampado Ransomware - FUD - CHEAPEST - ONLY $39 - FULL LIFETIME LICENSE

---------- Stampado Ransomware ---------- You always wanted a Ransomware but never wanted to pay hundreds of dollars for it ? - This list is for you! :) ----------
Stampado is a cheap and easy to manage ransomware, developed by me and my team. It...

Sold by The_Rainmaker - 2 sold since *Jul 12, 2016* **Vendor Level 1** **Trust Level 5**

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 39.00

Quelle: https://documents.trendmicro.com/images/TEx/articles/stampado-dark-web-ad.png

Quelle: https://www.zdnet.de/88296267/wannacry-infektionen-koennten-wieder-ansteigen/

Cyberangriff heute...

Alle **11 Sekunden**
passiert eine Ransomware Attacke weltweit (in 2021)*

21 Tage
Downtime eines Unternehmens nach einem Ransomware-Angriff

570.000 USD ist
die durchschnittlich gezahlte Lösegeldsumme**

Palo Alto 2021 **

80% der zahlenden Opfer
werden erneut angegriffen *

*Prof. Hartmut Pohl,
softCheck, St. Augustin, Nov. 2021

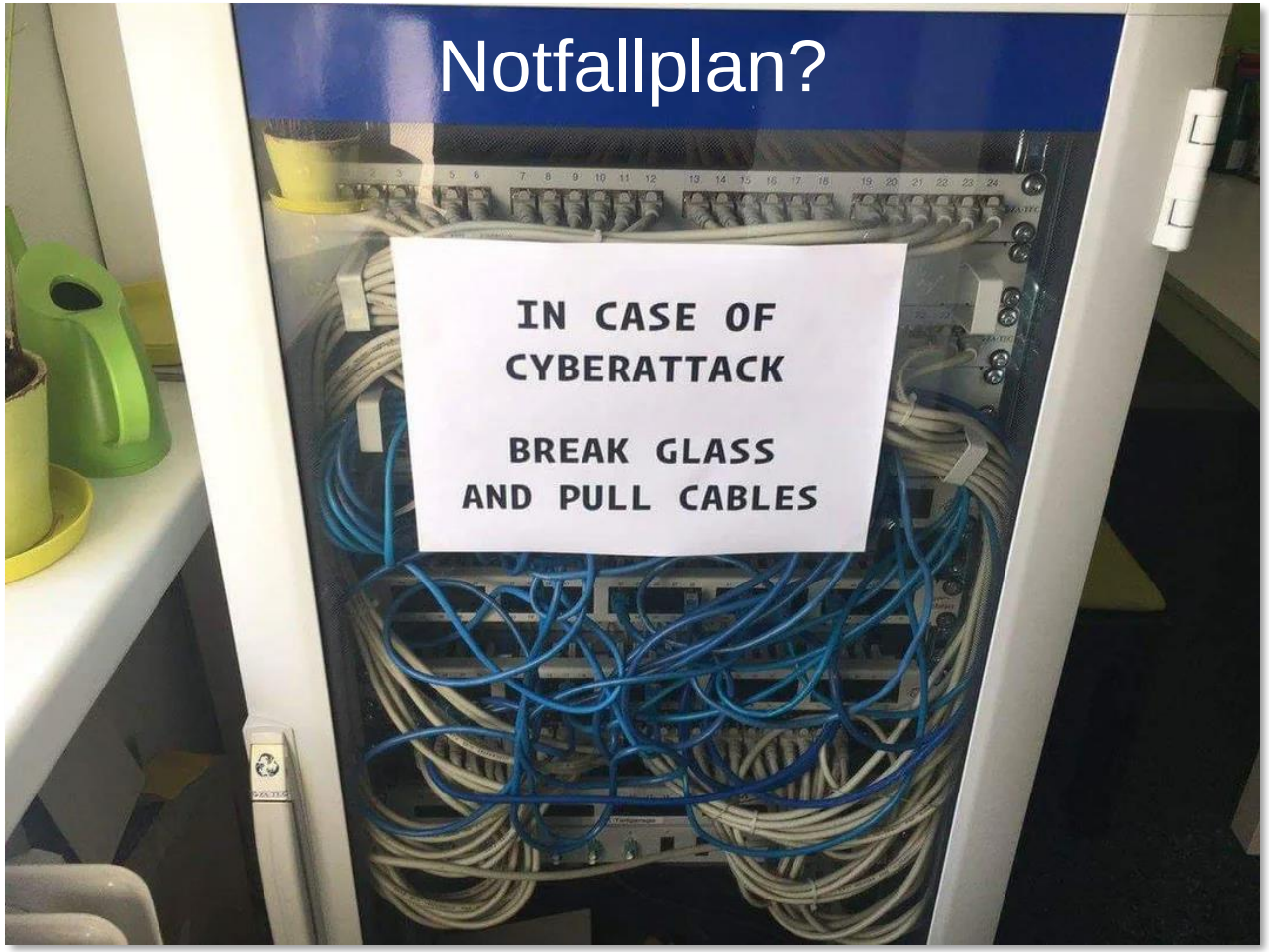
RaaS
Ransomware-as-a-Service als neues Businessmodell – im Monatsabo, als Partnermodell mit Gewinnbeteiligung

223 Mrd. Euro
Schaden durch Diebstahl von IT-Ausrüstung, Daten, Spionage und Sabotage auf deutsche Unternehmen***

***Bitkom 2021

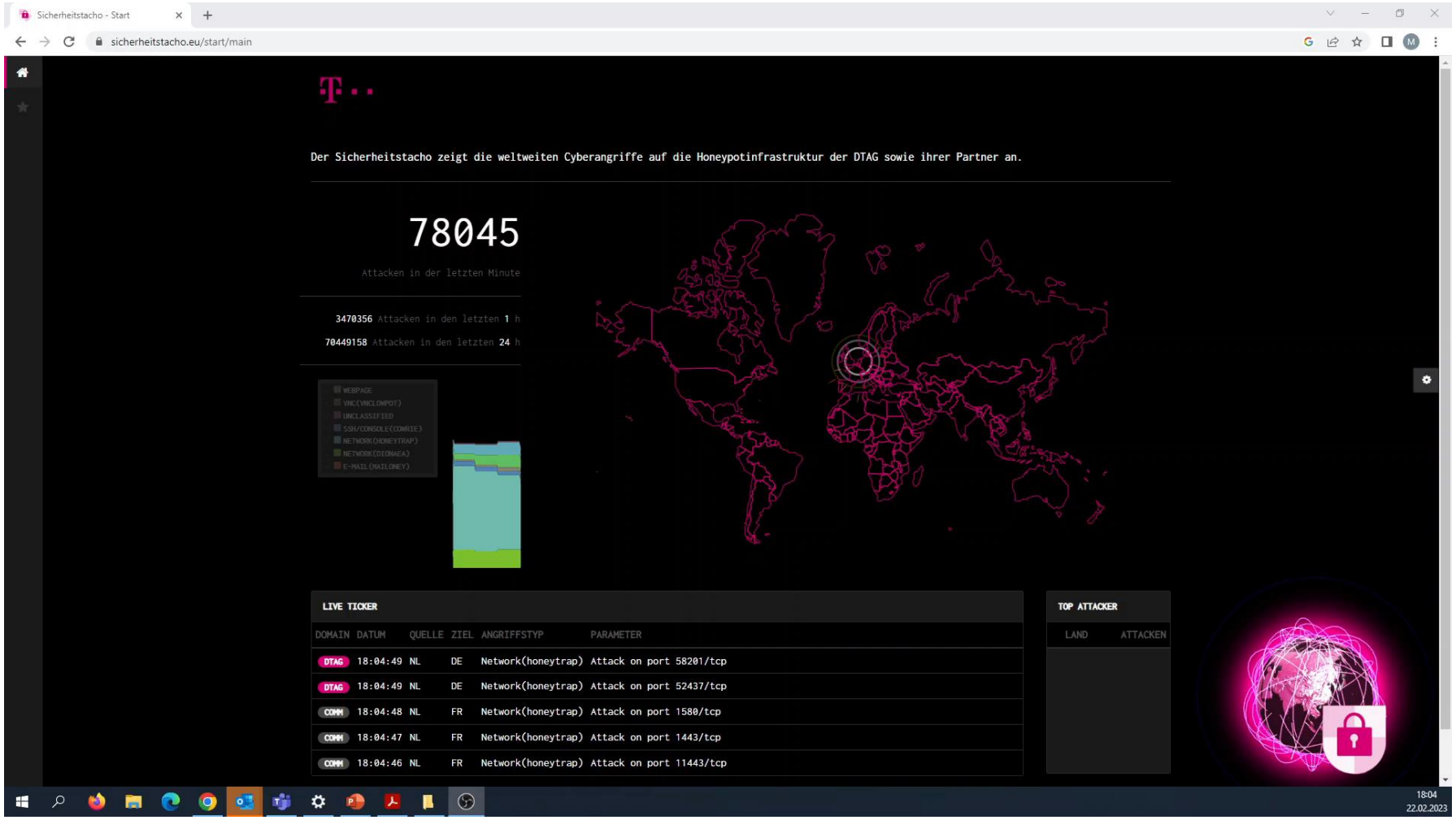
Es besteht Handlungsbedarf…

Quelle: https://www.otto.de/p/v2aox-treppenschutzgitter-2x-personenleitsystem-vip-abgrenzungsstaender-absperrung-absperrband-chrom-v2aox-S0K25069/#variationId=S0K25069W0JR



Quelle: https://twitter.com/PR0GRAMMERHUM0R/status/1660480629161574401

Cyberangriffe – live: Honeypot-Infrastruktur (Bsp. Telekom)



Quelle: https://www.sicherheitstacho.eu/start/main

NIS2-Richtlinie – Verschärfte Sicherheitsanforderungen

- **Risikomanagement:**
  - Identifikation von Cyber-Risiken
  - Bewertung der Auswirkungen von Sicherheitsvorfällen
  - Entwicklung von Risikobewertungen und -managementplänen
- **Sicherheitsrichtlinien und -verfahren:**
  - Erstellung und Implementierung von Sicherheitsrichtlinien
  - Definition von Sicherheitsverfahren und -standards
  - Schulung der Mitarbeiter zu Sicherheitsbest practices
- **Zugangskontrolle:**
  - Verwaltung von Zugriffsrechten und -berechtigungen
  - Implementierung von Identitäts- und Zugriffsmanagement
  - Überwachung und Protokollierung von Zugriffen
- **Incident Response und Management:**
  - Einrichtung eines Incident-Response-Teams
  - Entwicklung von Incident-Response-Plänen
  - Schnelle Reaktion auf Sicherheitsvorfälle und Berichterstattung an Behörden
- **Informationssicherheit:**
  - Verschlüsselung von sensiblen Daten
  - Sicherung von Netzwerken und Systemen
  - Schutz vor Malware und Viren
- **Überwachung und Audit:**
  - Echtzeitüberwachung von Netzwerkaktivitäten
  - Regelmäßige Sicherheitsaudits und -prüfungen
  - Archivierung von Sicherheitsereignisdaten
- **Meldung von Sicherheitsvorfällen:**
  - Pflicht zur Meldung von Sicherheitsvorfällen an nationale Be…
  - Zusammenarbeit mit CERTs (Computer Emergency Response Teams)
- **Zusammenarbeit und Koordination:**
  - Zusammenarbeit mit anderen kritischen Infrastrukturen und Behörden
  - Teilnahme an Informationssicherheitsforen und -gemeinschaften
- **Technische Sicherheitsmaßnahmen:**
  - Netzwerksicherheit (Firewalls, Intrusion Detection/Prevention Systems)
  - Patch-Management und regelmäßige Systemupdates
  - Sicherheitssoftware und -tools
- **Business Continuity und Wiederherstellung:**
  - Entwicklung von Notfall- und Wiederherstellungsplänen
  - Sicherung wichtiger Geschäftsdaten und -prozesse
  - Regelmäßige Durchführung von Notfallübungen

Umsetzung in nationales Recht bis Oktober 2024

Schwachstellen-Management und netzwerkbasierte Bedrohungserkennung

WIE FUNKTIONIERT EIN SIEM / SOC IN DER PRAXIS?

Funktionsprinzip SIEM & SOC

- **S**ecurity **I**nformation and **E**vent **M**anagement
  - Erkennung von Anomalien
  - Sensoren sammeln Log-Daten
  - Analyse der Daten
- **S**ecurity **O**peration **C**enter
  - Detailuntersuchung durch Spezialisten
  - Empfehlung von Maßnahmen
  - Behandlung und Behebung von Schwachstellen.

SIEM – Security Information and Event Management

- Netzwerkbasierte Bedrohungserkennung
  - Kontinuierliche **Überwachung** von Angriffsvektoren und –mustern
    - z.B. Anmeldeversuche, Ausführen von Scripten, …
  - **Auswertung** von Logfiles durch Regelwerke
    - „Threat Intelligence“, >65.000 Regeln, >50 Kategorien, +50 neue Regeln pro Tag, branchenbekannte Regelsätze (ET* Ruleset)
  - **Erkennung** verdächtiger und bösartiger Aktivitäten (IDS)
  - **Maßnahmen** zur Abwehr (IPS)

*) Emerging Threats Ruleset: Sammlung von Regeldefinitionen, die von der Sicherheitsgemeinschaft gepflegt wird

SOC – Security Operation Center

- Sicherheitsüberwachung
  - **Echtzeit-Erkennung** und -**reaktion** rund um die Uhr
- Managed Detection and Response (MDR)
  - Concierge-Security-Team (CST)
  - Untersuchung von **Sicherheitsvorfällen,** kampagnenbasierte **Jagd nach Bedrohungen** und Anzeichen einer Gefährdung
  - Bereitstellung von **Gegenmaßnahmen** (Triage Team)
- Risikomanagement und Berichterstattung
  - Sicherheitsberichte und **Empfehlungen zur Verbesserung**

Incident Response

FRÜHZEITIGE BEDROHUNGSERKENNUNG

Managed Detection and Response in der Praxis

eMail vom Threat Research Team mit potenzieller Bedrohung und Handlungsempfehlung:

Von: Threat Research Team
Gesendet: 11. April 2023
Betreff: Managed Detection Alert

„…Unser Threat-Research-Team hat eine Liste gefunden, auf der der Name Ihres Unternehmens als eines der Unternehmen aufgeführt ist, von denen Daten erworben werden konnten.

Laut Informationen konnten sie Zugang zu Archiven mit mehr als 172 GB erhalten, wie auf dem Screenshot zu sehen ist. Wir empfehlen eine sofortige Untersuchung im Rahmen des Incident Response (IR) bezüglich dieser Erkenntnis…“

Frühzeitige Reaktion auf Bedrohungen ist möglich

heise online heise+ Jetzt 1 Monat gratis testen

heise online > Security > MOVEit: Ransomware-Gang "Clop" erpresst Unternehmen nach Sicherheitslücke

MOVEit: Ransomware-Gang "Clop" erpresst Unternehmen nach Sicherheitslücke

Ransomware-Gang erpresst Unternehmen wegen Sicherheitslücke in der Datenübertragungssoftware MOVEit. Unter den potenziellen Opfern sind auch prominente Firmen.

Lesezeit: 2 Min. In Pocket speichern 9

(Bild: Pixels Hunter/Shutterstock.com)

07.06.2023 10:31 Uhr

Von Marie-Claire Koch

Erpresser-eMail an betroffene Unternehmen

DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.

STEP 2 - EMAIL OUR TEAM UNLOCK@SUP-BOX.COM OR UNLOCK@SUPPORT-MULT.COM

STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

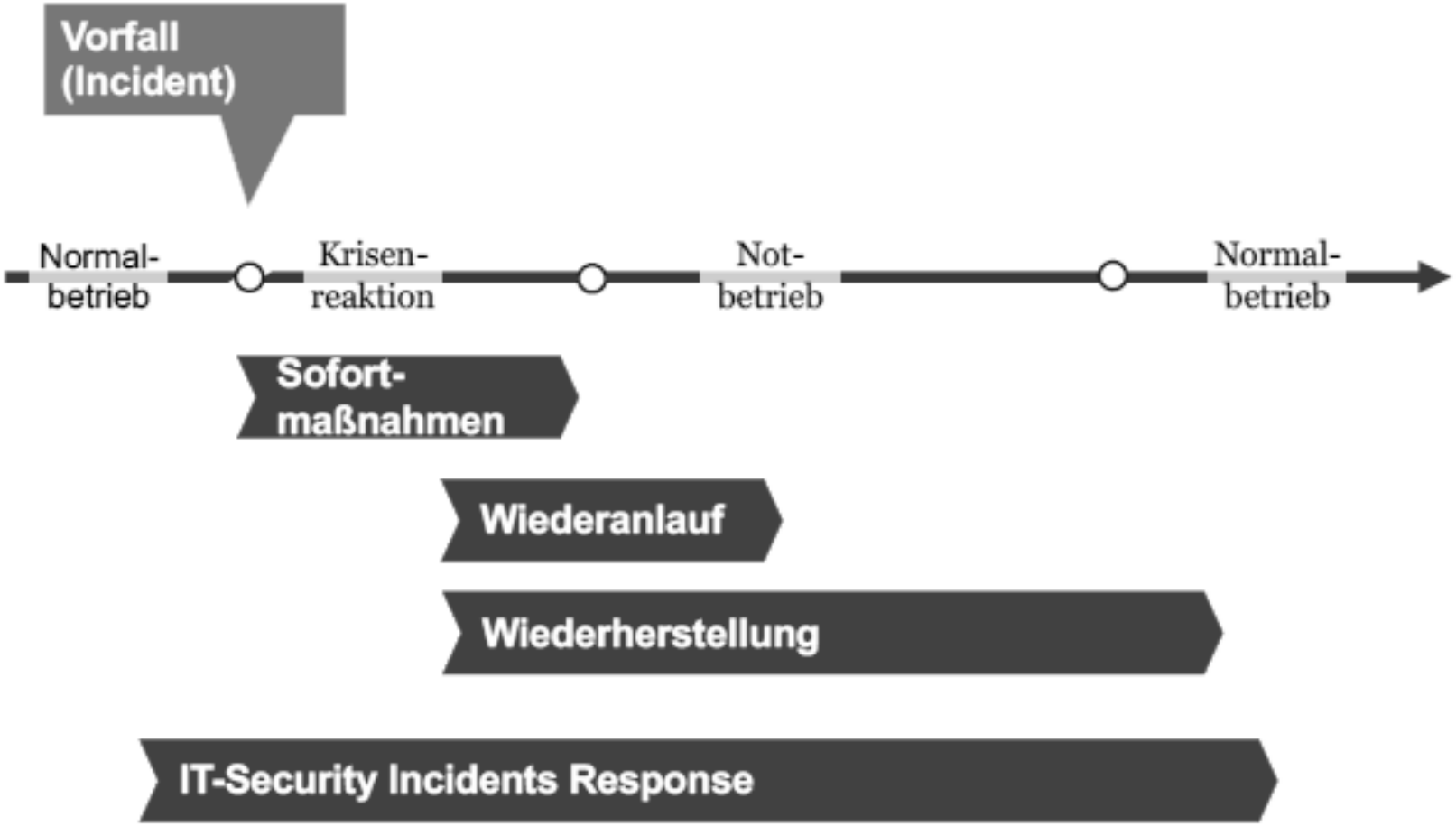
STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE

STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU

STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE

STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING

Krisenreaktion – Incident Response bei einem Angriff



RACI-Matrix: eindeutige Aufgabenverteilung im Krisenfall

	R Responsible	A Accountable	C Consulted	I Informed
	„Verantwortlich“	„Rechenschafts-pflichtig“	„Zu konsultieren“	„Zu informieren“
Beschreibung	• **Bearbeiter** • Für die Durchführung verantwortlich	• **Zustimmer** • Muss der Durchführung zustimmen	• **Berater** • Kann bei der Durchführung hinzugezogen werden	• **Beteiligter** • Kann über die Durchführung informiert werden
Beispiel im Projektmanagement	Projektmanager	Lenkungsausschuss	Projektmitarbeiter	Stakeholder

RACI-Matrix: Incident Response im Krisenfall

Beispiel	Gesamt-koordination	Medien und Kommunikation	Interne Kommunikation	Kunden-kommunikation	Technische Unterstützung	-Verbindung zur Regeulierungs-behörde	Äufzeichnungen und Records erstellen	Abschluss-Dokumentation erstellen
CIO / CSO	A	I	A / R	I	I	I		
Incident Management Team Koordinator	0R	C	C		A / R	I	A / R	A / R
Security Operations Leiter	I				A / R	I	R	C / I
Leiter Medien- und Öffentlichkeitsarbeit		A / R	I	A / R				I
SIEM und SOC Team	I				C	C	C / I	C / R

Auf den Ernstfall vorbereitet….

IMPLEMENTIERUNG EINES SIEM & SOC

Beispiele für SIEM / SOC Services

Managed Detection and Response

Erkennung und Abwehr komplexer Bedrohungen

Rund-um-die-Uhr-Überwachung für Netzwerk und Endgeräte

Cloud Detection and Response

Bedrohungser-kennung für Cloud-Umgebungen

identifiziert und verhindert Bedrohungen über IaaS- und SaaS-Ressourcen hinweg.

Managed Risk

Kontinuierliches Vulnerability- und Risiko-Management

Durch Experten begleitete Schwachstellen-Analyse

Managed Security Awareness

Bereiten Sie Ihre Mitarbeitenden darauf vor, Social-Engineering-Angriffe zu erkennen und zu neutralisieren.

Beispiel eines Sicherheitsberichts

ID	Abweichung	Status	Auswirkung auf Geschäftsbetrieb	Risiko	Nachweis / Quelle	Maßnahmen zur Fehlerbehebung
1	Operating System (OS) hat Laufzeitende erreicht (End of Life (EOL)	Risiko	Hoch	Das Betriebssystem (BS) auf dem entfernten Host hat das Ende seines Lebenszyklus (EOL) erreicht und sollte nicht mehr verwendet werden.	Host IP: …..	Aktualisieren Sie das Betriebssystem auf dem entfernten Host auf eine Version, die vom Hersteller noch unterstützt wird und Sicherheitsupdates erhält.
2	Offener Port	Risiko	Hoch	Offenes Eingangstor zum internen Netzwerk, auch wenn dieser sich in der DMZ befindet	Host IP …..	Den SSH-Port nicht der ganzen Welt freigeben. Dem Root-Benutzer nicht erlauben, ein SSH-Terminal zu verwenden. Zwingen Sie alle Benutzer, sich mit einem SSH-Schlüsselpaar anzumelden, und deaktivieren Sie dann die Passwortauthentifizierung.
3	Apache …… Mehrere Sicherheitslücken	Risiko	Mittel	Apache ….. Ist anfällig für Sicherheitslücken	Host IP ……	Es wurde keine Lösung vom Anbieter bereitgestellt. Allgemeine Lösungsoptionen sind ein Upgrade auf eine neuere Version, das Deaktivieren entsprechender Funktionen, das Entfernen des Produkts oder das Ersetzen des Produkts durch ein anderes. Es liegen folgende Sicherheitslücken vor: - CVE-2018-8032: Cross-Site Scripting (XSS) im Standard-Servlet/Services - CVE-2019-0227: Serverseitige Request-Fälschung (SSRF)

Beispiel

Ganzheitlicher „4-P-Ansatz“

- **People**
  - Sensibilisieren Sie alle beteiligten Personen
- **Process**
  - Überprüfen Sie Prozesse (Risikomanagement, …)
- **Products**
  - Überprüfen Sie das Sicherheitsniveau eingesetzter Produkte
- **Partner**
  - Erfüllen auch Partner (und Lieferanten) die Ihre Sicherheitsanforderungen? (Stichwort: Lieferkette)

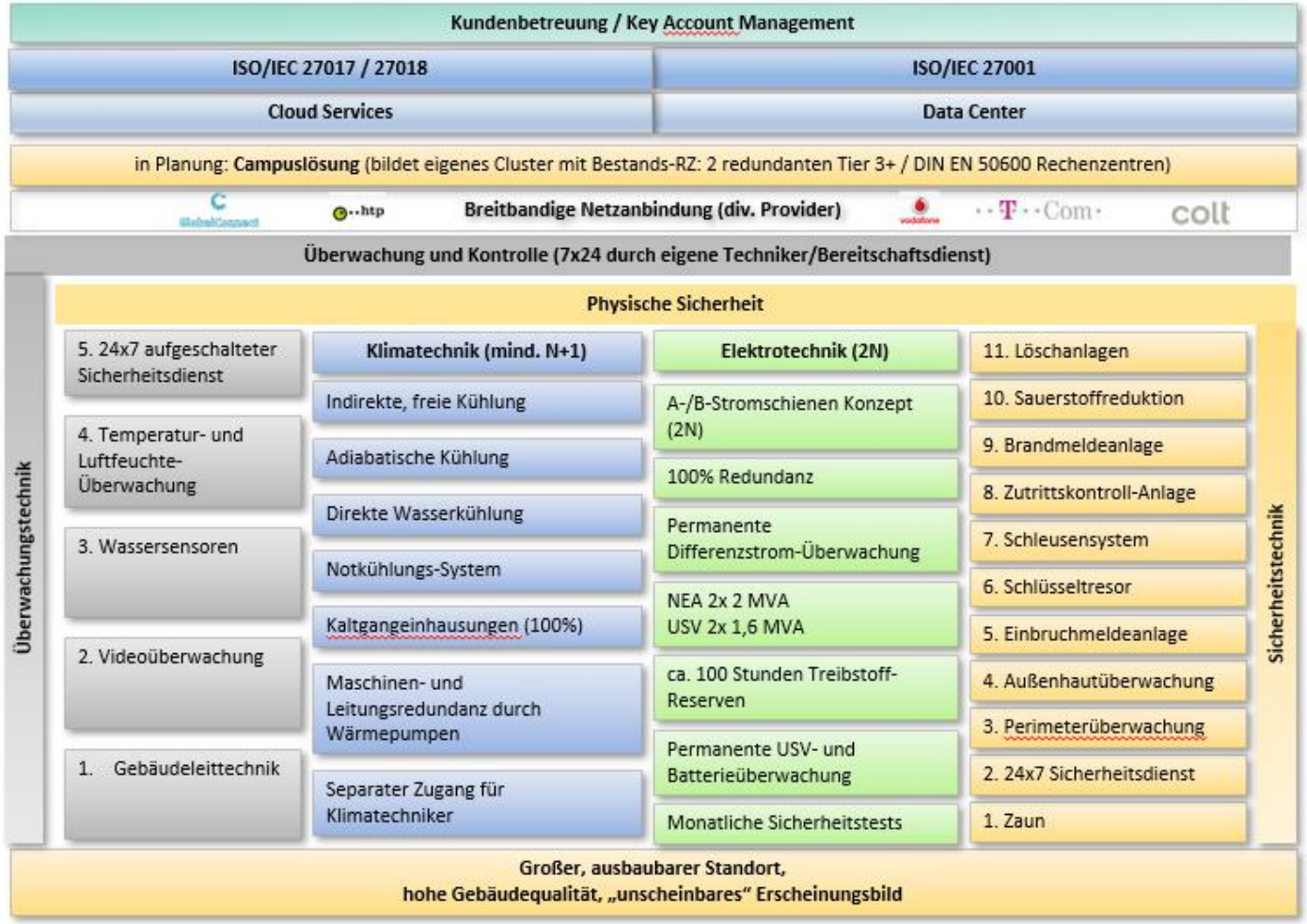
Cybersecurity – SIEM & SOC

Aktueller Status in vielen Unternehmen	Leistungen einer guten SIEM/SOC Lösung	Warum jetzt?
Reduziertes und nicht speziell für **Security-Anforderungen** geschultes Personal Verbesserung der Abwehrstrategien und der unternehmensweiten IT-Security – insbesondere der Schutz des geistigen Eigentums ist gewünscht **24x7x365-Überwachung** mit aktuellen Möglichkeiten oft nicht gegeben Ein strategischer **Partner** zur Entlastung wird gesucht Hoher **Imageverlust** und unschätzbare Störungen des Betriebes bei einem möglichen Befall	**Concierge Ansatz:** Ein dediziertes deutsch- und englischsprachiges Team für strategische Beratung (regelmäßige Statusbesprechungen, Unterstützung bei internen und externen Revisionen) wird Ihnen zugewiesen **SLA**: Anomalien werden 24x7x365 in weniger als 30 Minuten an Kunden eskaliert (niedrigster SLA der Industrie) **Breiteste Visibilität:** Integriert sich mit bestehenden Security-Tools und -Produkten im Rechenzentrum, auf den Endgeräten und den etwaigen Cloud-Diensten **Eindämmung von Bedrohungen:** Infizierte Geräte werden unverzüglich isoliert, um eine Verbreitung von Schadsoftware oder Datenklau zu stoppen/verhindern **Schwarmintelligenz:** Perrmanente Weiterentwicklung und Verbesserung durch Schwarmintelligenz	Jeder Tag ungeschützten 24x7-Betrieb ist ein **risikobehafteter** Tag. Es ist kaum die Frage ob, sondern die Frage wann ein Kunde eine schwere oder zumindest den Betrieb störende Attacke erfährt **Vorsorge ist besser als Nachsorge**. Die kumulierten Kosten der Schadensbehebung und der Wiederanfahrt des IT-Betriebes nach einem signifikanten Störfall sind um Faktoren höher, als die Vorsorgeaufwände durch Einführung eines SOC Die Einführung eines managed SOC ermöglicht, direkt **Cyberrisiken zu erkennen** und diesen binnen Minuten zu begegnen. Attacken werden abgewehrt und Schäden abgewendet. Darüber hinaus wird das Angriffsmuster analysiert und zukünftige Angriffsmöglichkeiten gleichen Musters Ausgeschlossen

Tipps für die praktische Umsetzung

Sofort-Maßnahmen	Kurzfristige Maßnahmen	Mittelfristige Maßnahmen
• Software auf Aktualität prüfen • Bekannte Schwachstellen beheben • Schulungen planen • Implementierung eines SIEM / SOC	• Incident Response Plan entwickeln • Backup-Daten auslagern • Business Impact Analyse erstellen • Notfallpläne entwickeln • Partner zur Umsetzung hinzuziehen	• Etablierung strategischer Prozesse (ISMS, …) für einen stabilen IT-Betrieb • Automatische Bedrohungserkennung einrichten

Beispiel für ein Leistungsspektrum eines RZ-Dienstleisters



Handlungsempfehlungen

- „Wissen, was läuft“: Kennen Sie Ihre IT-Umgebung
- Prozesse etablieren
  - Risikomanagement, Notfall-Szenarien, ISMS, Wiederherstellungspläne, Backup (immutable)
- Mit zuverlässigen Dienstleistern zusammenarbeiten für
  - SIEM / SOC Lösungen
  - Colocation, Cloud-Services, Managed-Services
  - Sichere Netzanbindungen (Blackholing, DDoS-Protection, …)
  - GRASS-MERKUR bietet passende Lösungen

Ihr Kontakt bei GRASS-MERKUR

Dipl.-Kfm.

MARKUS DIETZ

Leiter Business Development und Vertrieb

GRASS-MERKUR GmbH & Co. KG

Rothwiese 5 - 30559 Hannover

Tel. +49 511 47 54 14 – 13 Fax +49 511 47 54 14 – 33

Mobil + 49 178 7866 400

markus.dietz@grass-merkur.de

www.grass-merkur.de