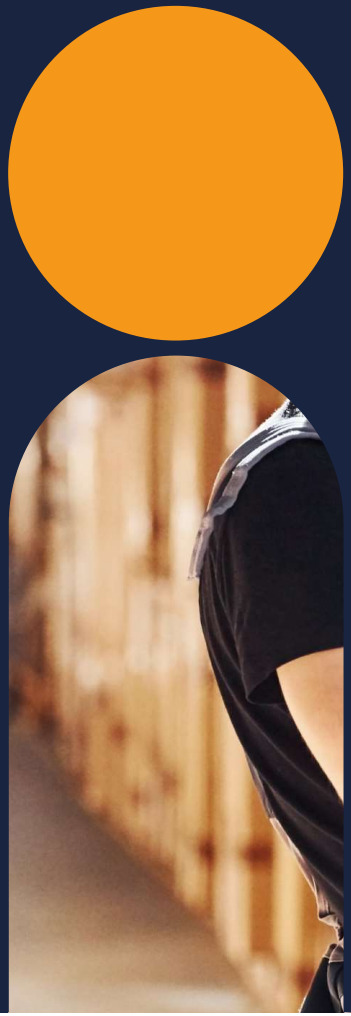
„Cyber Security – wie sieht effektiver und erschwinglicher Schutz aus? Ausblick NIS2"

Cyberresilienz

Marcel van Asperdt



Verschiedene Akteure in der Cyberwelt

Cybervandalismus
- Motiv: ärgern
- Wer: online Gemeinschaften

Cybercriminalität
- Motiv: finanzieler Profit
- Beispiel: organisierte Bande

Staatliche Akteure
- Motiv: Spionage
- Beispiel: APT-gruppen

Erster Schritt in einem Cyberangriff

(Spear)phishing -> Credentials

Schwachstelle angreifen

Neuer Exploit

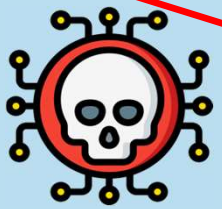
Schwachstelle suchen

Zugriff

Gegenmaßnahmen

MFA implementieren

Patch durchführen



Neuer Exploit

Schwachstelle suchen

Zugriff

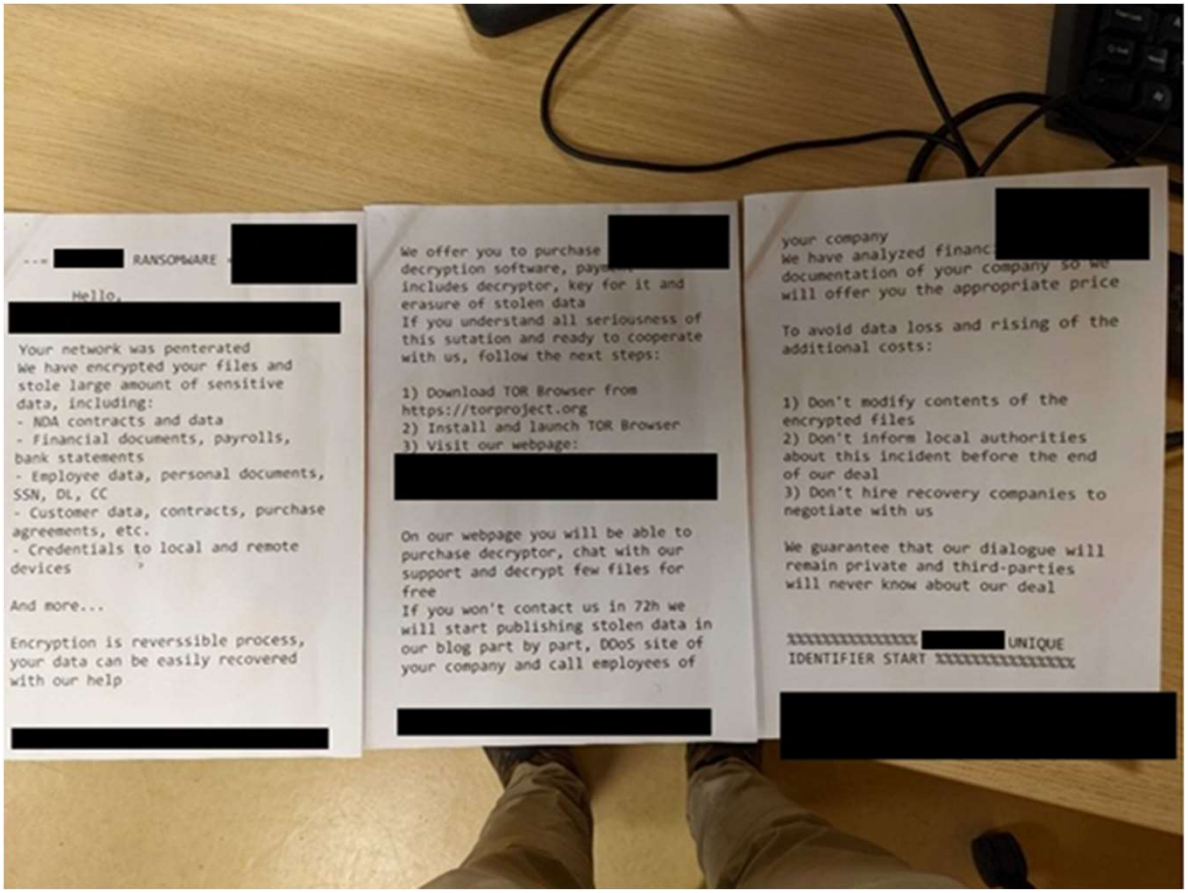
Entwicklungen

Phishing:
- Spearphishing statt Phishing
- MFA ist effektiv aber:
  - SIM swapping
  - Pass-the-cookie

Schwachstelle Angriff:
- Patchen kein Priorität
- Covid -> VPN Schwachstellen (z.B. Citrix, Fortinet)
- Supply-chain Angriff (z.B. Solarwinds Angriff)

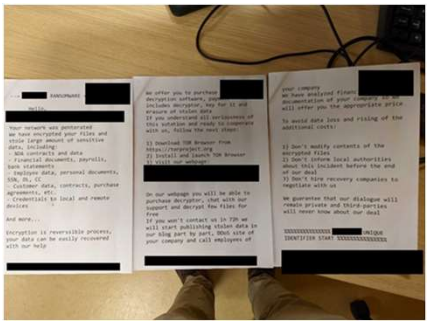
Feststellung:
Früher oder später kommt ein Angreifer rein!

Ransomware – und jetzt?



Beispiel

Ransomware – und jetzt?



Your network was penetrated

We have encrypted your files and stole large amount of sensitive data, including:

- NDA contracts and data

- Financial documents, payrolls, bank statements

- Employee data, personal documents, SSN, DL, CC

- Customer data, contracts, purchase agreements, etc.

- Credentials to local and remote devices

And more...

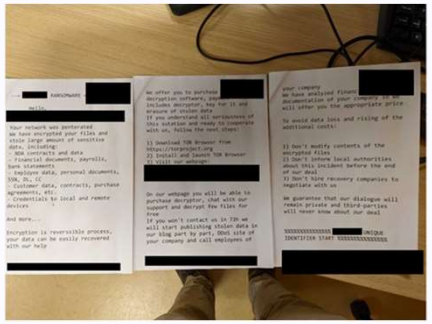
Encryption is reverssible process, your data can be easily recovered with our help

We offer you to purchase special decryption software, payment includes decryptor, key for it and erasure of stolen data

If you understand all seriousness of this situation and ready to cooperate with us, follow the next steps:

Beispiel

Ransomware – und jetzt?



1) Download TOR Browser from
2) Install and launch TOR Browser
3) Visit our webpage: http:XXX

On our webpage you will be able to purchase decryptor, chat with our support and decrypt few files for free

If you won't contact us in 72h we will start publishing stolen data in our blog part by part, DDoS site of your company and call employees of your company

We have analyzed financial documentation of your company so we will offer you the appropriate price

1) Don't modify contents of the encrypted files

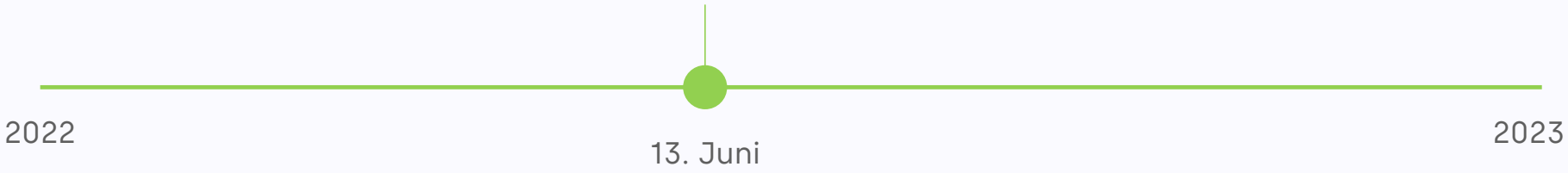
2) Don't inform local authorities about this incident before the end of our deal

3) Don't hire recovery companies to negotiate with us

Beispiel

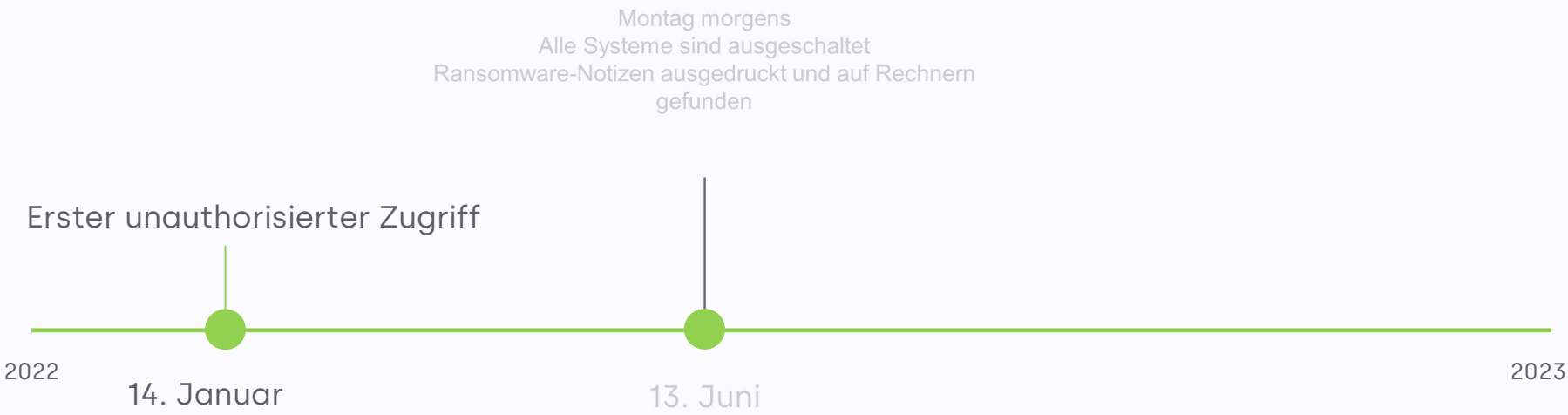
Was ist passiert?

Montag morgens
Alle Systeme sind ausgeschaltet
Ransomware-Notizen ausgedruckt und
auf Rechnern gefunden



Beispiel

Was ist passiert?

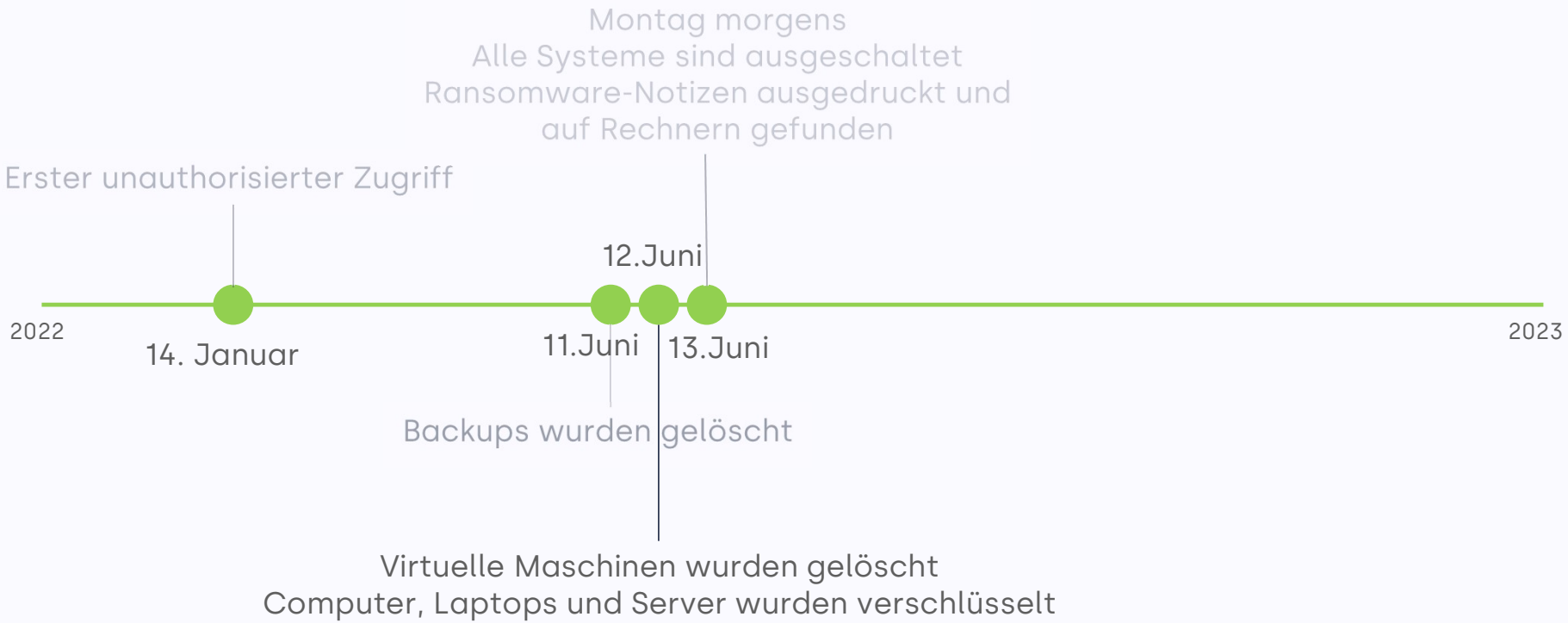


Beispiel

Was ist passiert?

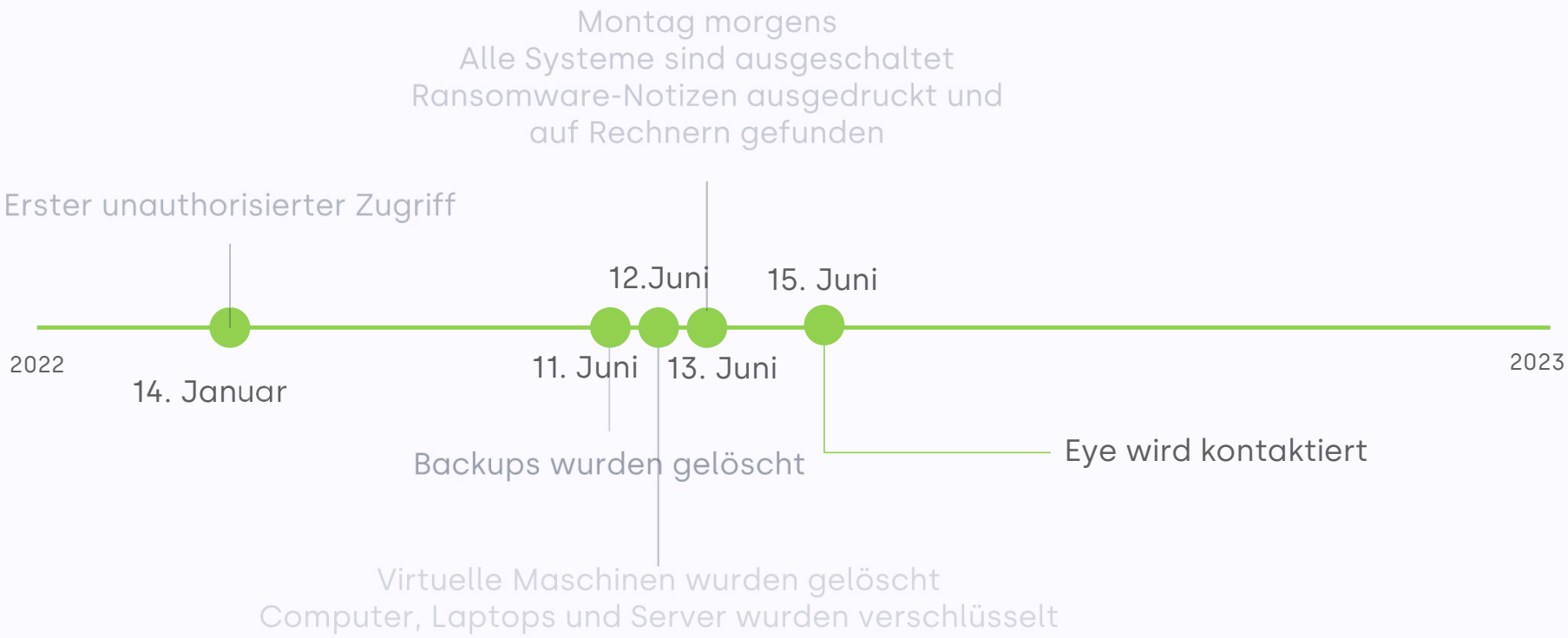
Beispiel

Was ist passiert?



Beispiel

Was ist passiert?



Beispiel

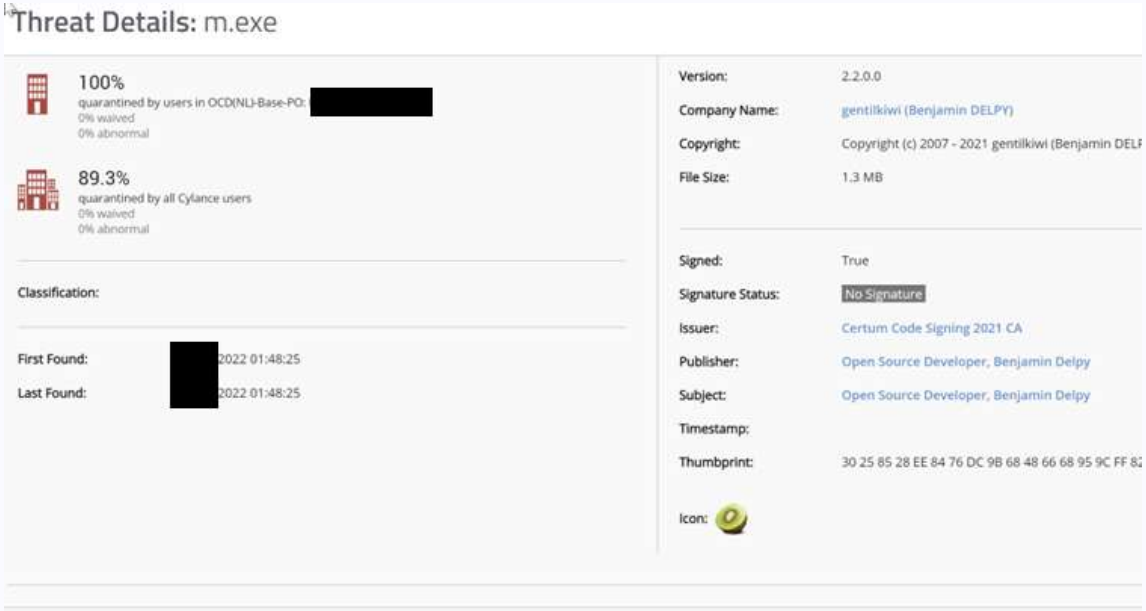
Erstgespräch (Intake Call)

- Auf allen Geräten haben wir sowohl eine Sicherheitslösung (EDR) und einen Anti-Virus installiert.
- Jede Software und alle Geräte haben den neusten Patch
- Unsere Firewall ist aktiv
- Wir haben ein öffentliches und ein privates Netzwerk und beide Netzwerke sind strikt von einander getrennt.

Instagram	**Reality**
	
Burger King Whopper	**Burger King Whopper**

Beispiel

“EDR und Anti-Virus waren installiert”

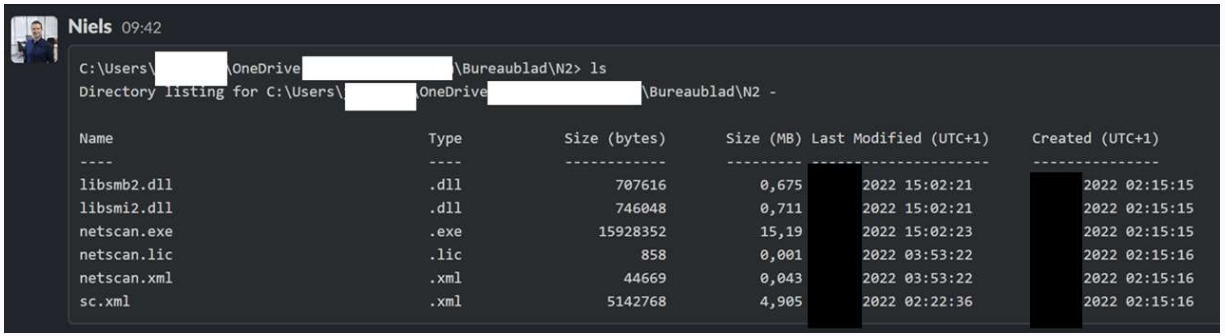


Ransomware wurde blockiert

Beispiel

“EDR und Anti-Virus waren installiert”

Angreifer hat die Ransomware geändert und sie wurde dann zugelassen und installiert



“Alles ist gepatcht”

Es sei denn Systeme sind so alt, dass sie nicht mehr unterstützt werden.

➔ Wenn es keine neuen Patches gibt, sind wir auf dem neusten Stand.

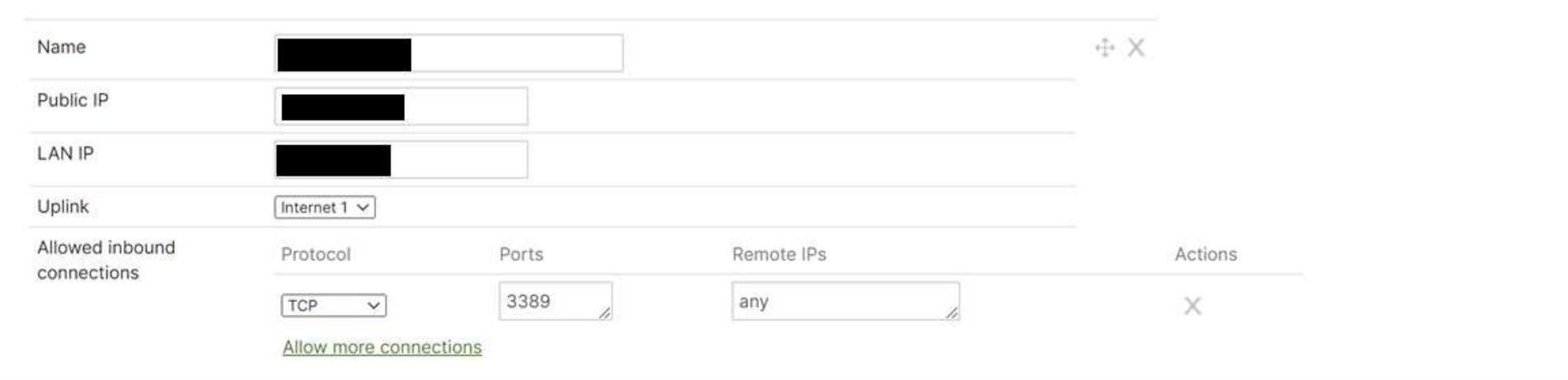
➔ Systeme waren für Angriffe anfällig.

➔ Vor allem ein Server..

VMWare Horizon Server

Es gab zwar eine alternative Lösung, wie man den Server schützen konnte, aber der Systemadministrator hat den Server **falsch konfiguriert.**

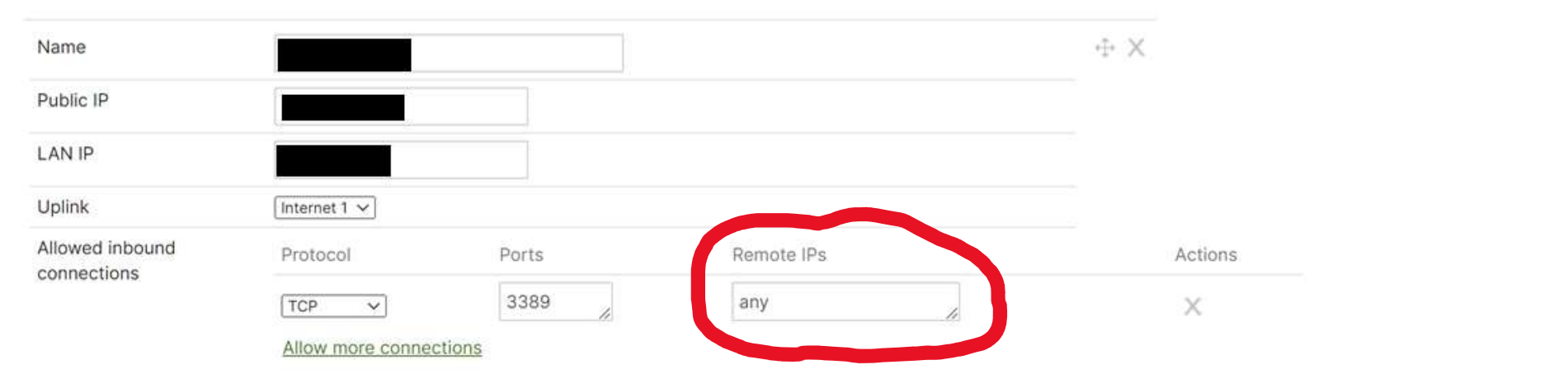
“Unsere Firewall ist aktiv”



Offener Port

➔ Eintritt für den Angreifer

“Unsere Firewall ist aktiv”



Offener Port

➔ Eintritt für den Angreifer

“Netzwerke sind strikt getrennt”

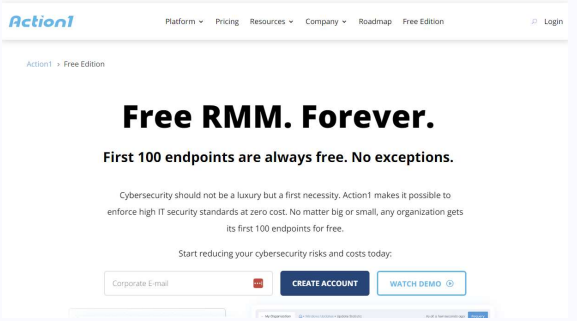
Alle Verbindungen vom öffentlichen Netzwerk erlauben eine Verbindung ins private Netzwerk

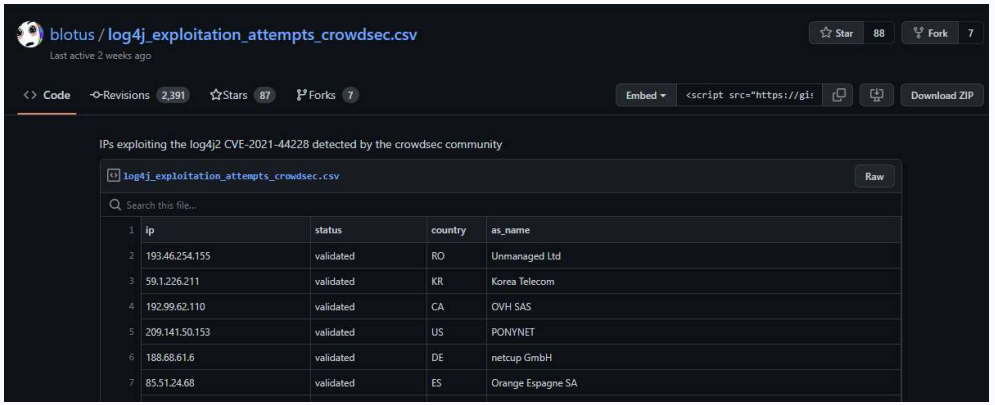
➔ Falsche Konfiguration

Weitere Untersuchungsergebnisse

- Normale Software missbraucht
  RMM-Tool (Remote Monitoring & Management)

- Server verbindet mit einer IP-Addresse, die
  bekannt für Log4j-Angriffe war.



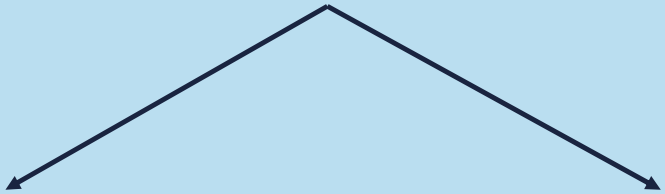


Verhandlung mit den Angreifern

Von $150.000 auf $10.000 runtergehandelt

Beispiel

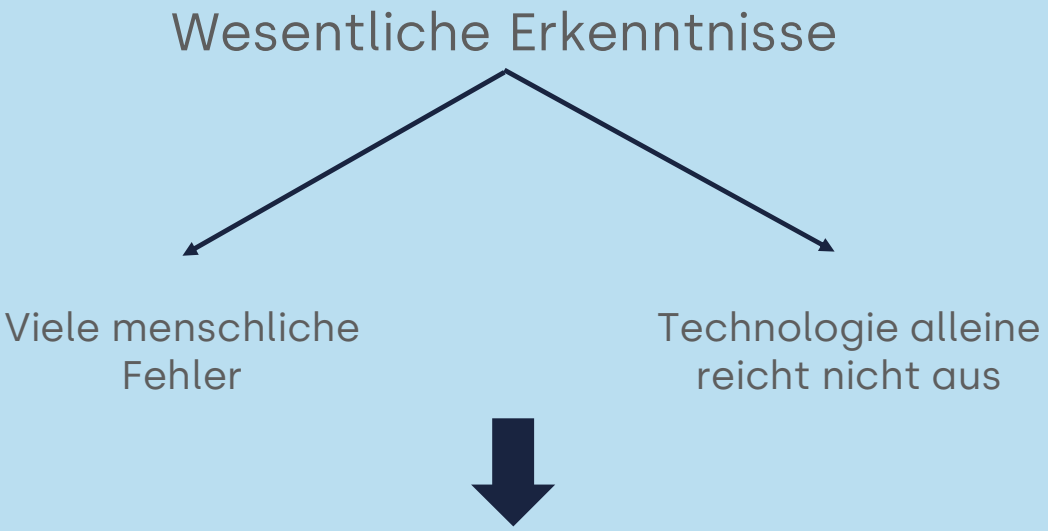
Wesentliche Erkenntnisse



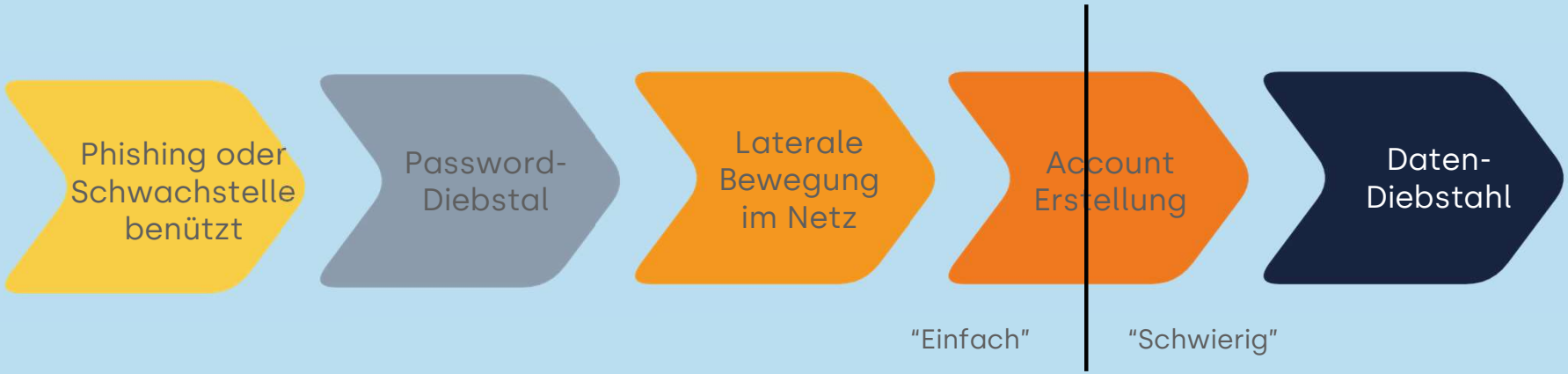
Viele menschliche Fehler

Technologie alleine reicht nicht aus

eye.


Wesentliche Erkenntnisse
Viele menschliche Fehler
Technologie alleine reicht nicht aus
“Assume Breach”
Gehen Sie von einem Sicherheitsvorfall aus

Angriffsablauf Prozess



Wie schnell geht das?

Schwierig zu erkennen nachdem einen Account erstellt ist.

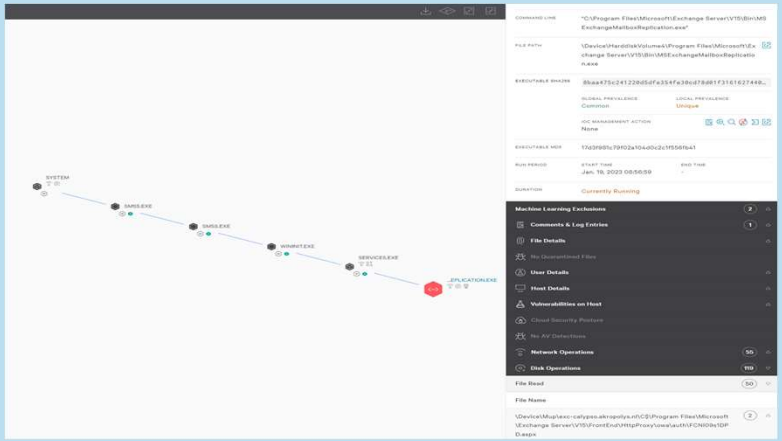
Wie können wir die Auswirkung des Angriffs beschränken?

Unsere Lösung

Entwicklungsprinzipien:
- ‘1 fits all’ Lösung
- Einfach zu installieren und administrieren
- Active Incident Response Dienstleistung 24/7

Drei Datenpunkten:
1. EDR
2. Cloud: Office365 und Google Workspace
3. Angriffsoberfläche Management

Analyse & Root Cause



Bewerten Sie den Alarm:
Was hält den EDR für seltsam?
“Der Exchange-Server hat eine Datei erstellt,
die oft bösartig ist”

Welche Datei wurde erstellt

|Device|HarddiskVolume4|Program Files|Microsoft
|Exchange Server|V15|Bin|MSExchangeMailboxReplication.exe

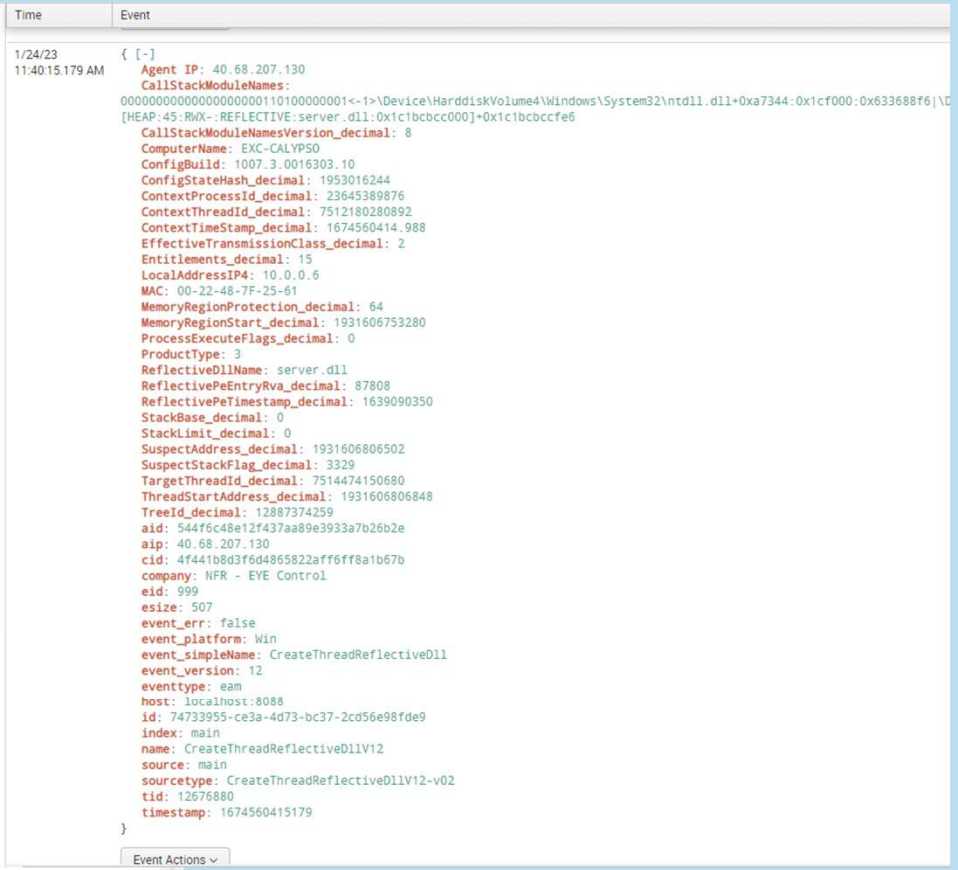
|Device|Mup|exc-calypso.akropolys.nl|C$|Program Files|Microsoft
|Exchange Server|V15|FrontEnd|HttpProxy|owa|auth|NIriYmZZ.aspx

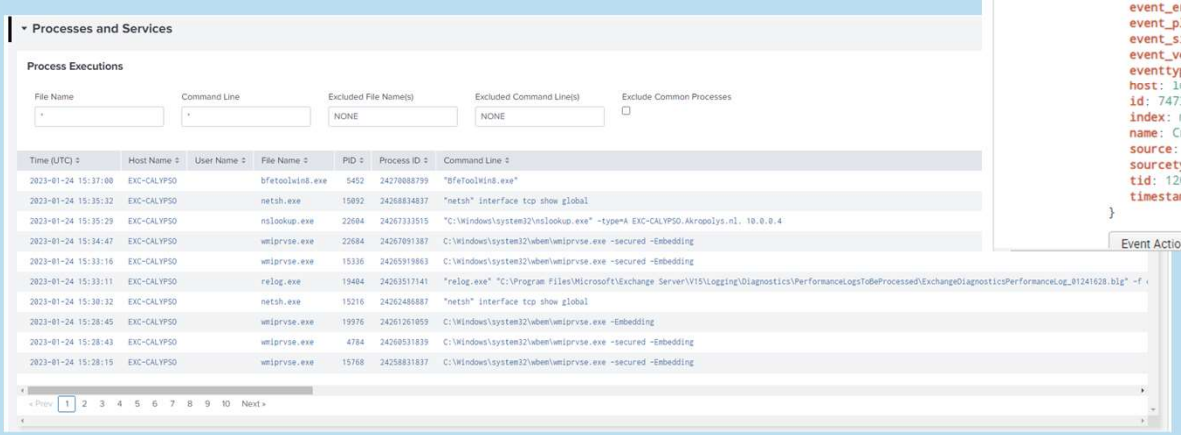
.. Und 44 weitere Dateien

Analyse & Root Cause

Suche nach verdächtigen
- Ausgehende Verbindungen
- Merkwürdige Prozesse
- Ausgeführte Dateien
- Und viele weitere Indikatoren

Beweise deuten auf anfälligen Server

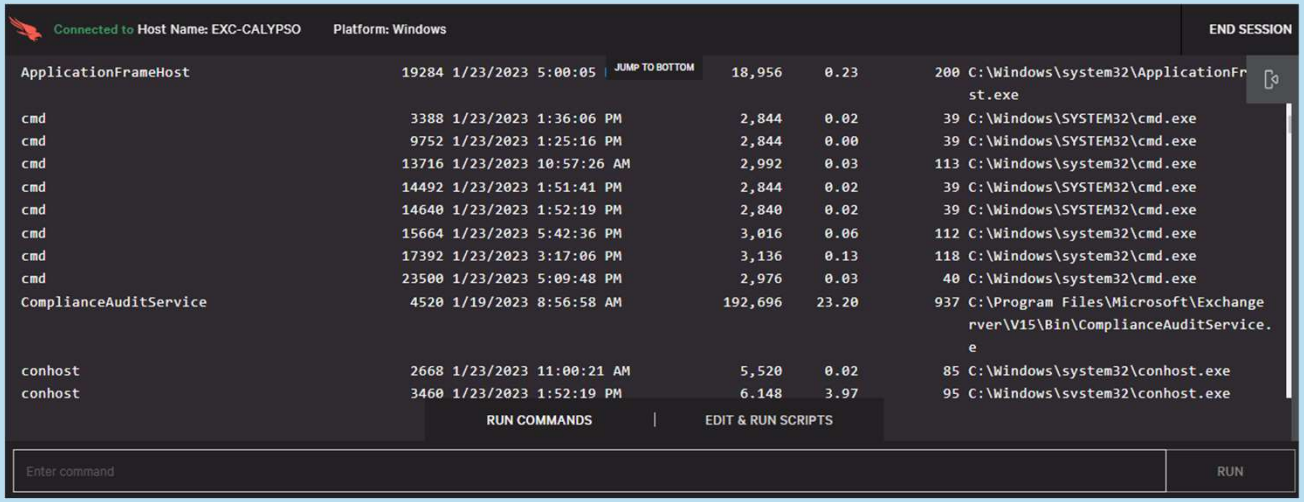




Beispiel für Erkennung – Wiederherstellung

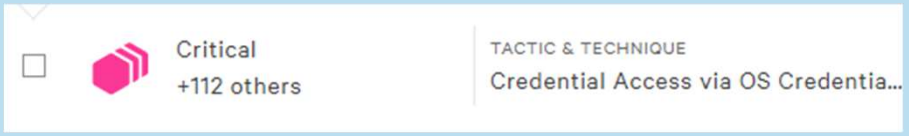
Der Angreifer von der Maschine werfen (aktive Reaktion)
- Prozess des Angreifers beenden
- Veränderte Dateien entfernen
- Falls nötig: Isolieren

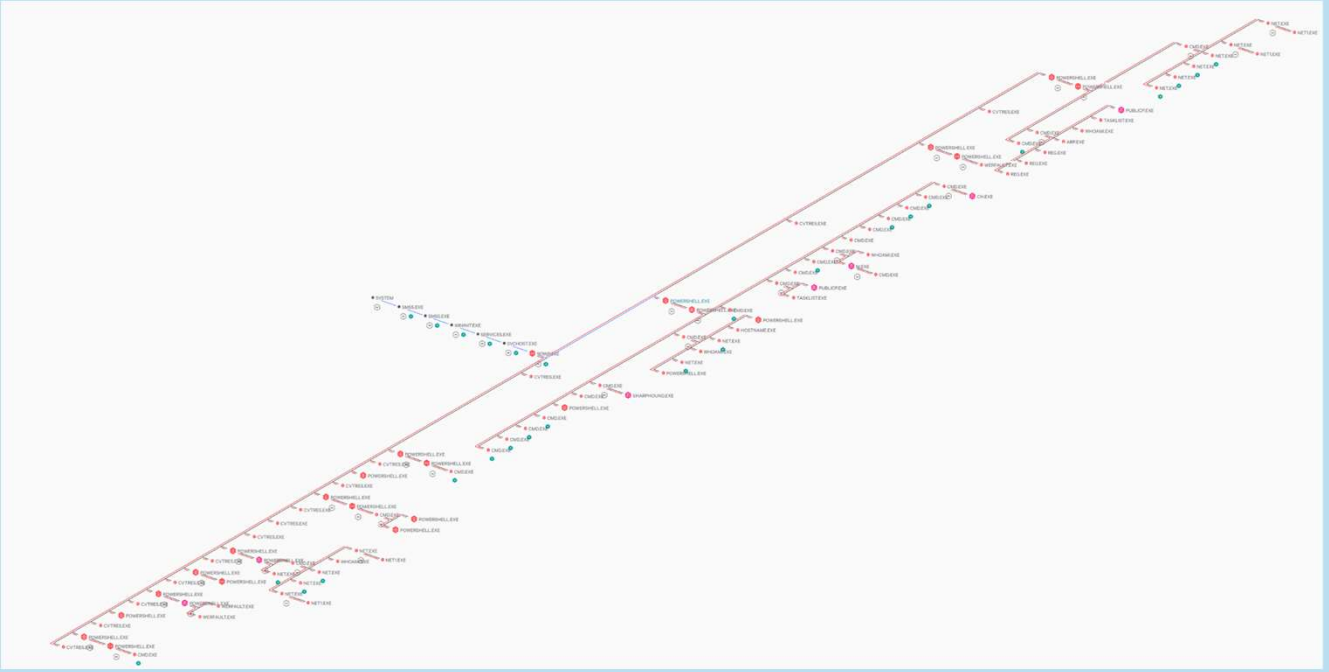
Server patchen



Beispiel falls nicht direkt eingegriffen wurde

Falls nichts unternommen wird:
113 Alerts





EU NIS2

Nachfolger EU NIS1

Mehr Einheitlichkeit bei der Sicherheit der Netze von Organisationen innerhalb der EU.

Wichtige Daten:

17. Oktober 2024 -> Inkrafttreten

17. Januar 2025 -> Ende der Registrierungsfrist

(Kontaktdaten, öffentliche IP-Adresse, Branche)

Entwurf für das Gesetzes zur Umsetzung der NIS-2-Richtlinie (19. Juli 2024)

Besonders wichtige Einrichtungen

Mehr als 250 Beschäftigte oder mehr als 50 Millionen Euro Jahresumsatz.

Energie	Verkehr	Finanzwesen
Gesundheit	Wasser	IT-Infrastruktur
IT-Dienste	Öff. Verwaltung	Weltraum

Wichtige Einrichtungen

Mehr als 50 Beschäftigte oder mehr als 10 Millionen Euro Jahresumsatz.

Energie	Verkehr	Finanzwesen	Gesundheit
Post & Kurier	Abfallwirtschaft	Chemie	Lebensmittel
Wasser	IT-Infrastruktur	IT-Dienste	Öff. Verwaltung
Weltraum	Produktion	Online Dienste	Forschung

Es ist wichtig, die europäische Definition der genannten Sektoren zu konsultieren, um zu prüfen, ob ein Unternehmen darunter fällt.

Sorgfaltspflicht

- Sicherheitsmaßnahmen auf Grundlage des Risikomanagements
- Auf Vorfälle vorbereiten
- Mitarbeiter und Vorstand schulen -> alle 3 Jahre
- Lieferkette einbeziehen (falls sie Zugang zum Netz und zum Informationssystem haben)

Meldungspflicht (an BSI)

- Bei Vorfällen erste Meldung innerhalb von 24 Stunden
- Folgemeldung innerhalb von 72 Stunden
- Abschlussbericht nach einem Monat

eye

Beaufsichtigung (durch BSI)

- Proaktiv für besonders wichtige Einrichtungen, reaktiv für wichtige Einrichtungen
- BSI kann nachforschen (auch lokal)
- BSI kann Fristen zur Beseitigung von Mängeln setzen
- BSI kann Nichteinhaltung veröffentlichen
- Das BSI kann die Verwaltung aussetzen (oder aussetzen lassen)
- Verwaltungsgeld bei Nichteinhaltung Max 100.000
- Die Geldbuße kann bis zu einem vom Umsatz abhängigen Betrag steigen

marcel.van.asperdt@eyesecurity.de

eyesecurity.de

0151 21934825

Maßnahmen die gefordert werden:

- Risikoanalyse und Sicherheit für Informationssysteme;
- Bewältigung von Sicherheitsvorfällen;
- Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;
- Sicherheit der Lieferkette;
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management von Schwachstellen;
- Bewertung der Wirksamkeit von Risikomanagementmaßnahmen;
- grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen;
- Konzepte und Verfahren für den Einsatz von Kryptografie;
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation.