



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

Cyberresilienz

Marcel van Asperdt



# Verschiedene Akteure in der Cyberwelt

## Cybervandandalismus

Motiv: ärgern

Wer: online Gemeinschaften

## Cybercriminalität

Motiv: finanzieller 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



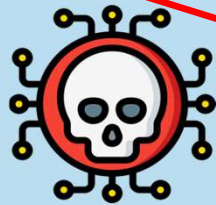
Zugriff

# 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:

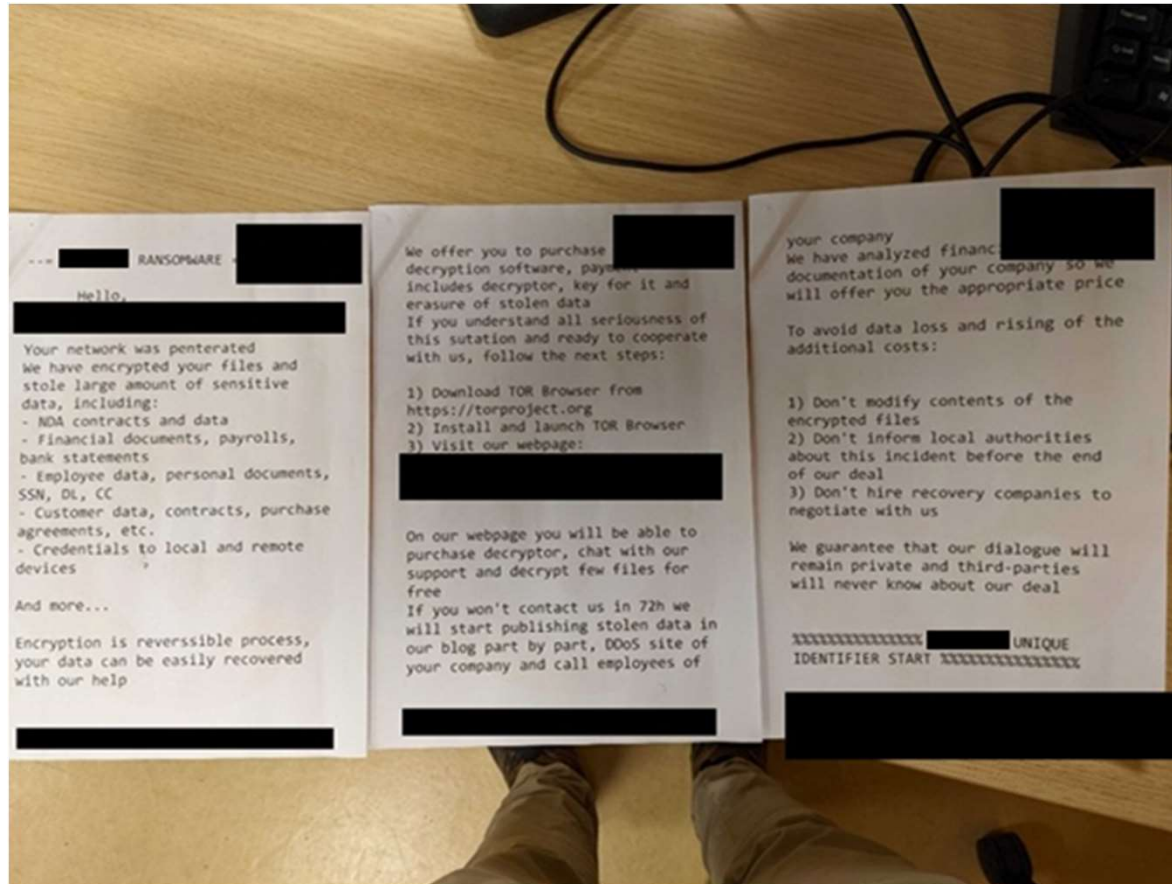
- Patchen kein Priorität
- Covid -> VPN Schwachstellen (z.B. Citrix, Fortinet)
- Supply-chain Angriff (z.B. Solarwinds Angriff)

## Feststellung:

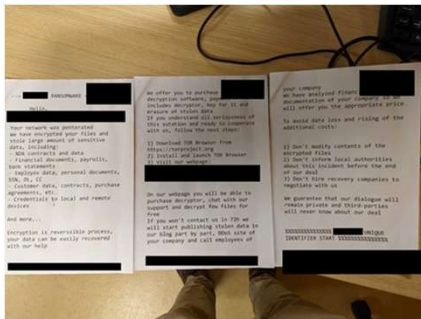
Früher oder später kommt ein Angreifer rein!



# Ransomware – und jetzt?



# 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

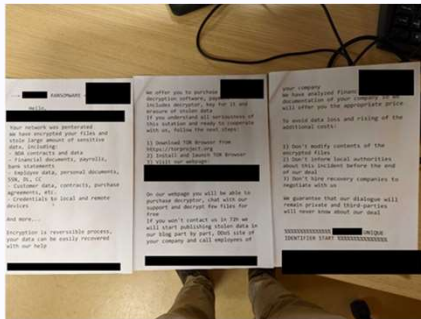
And more...

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:

# 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

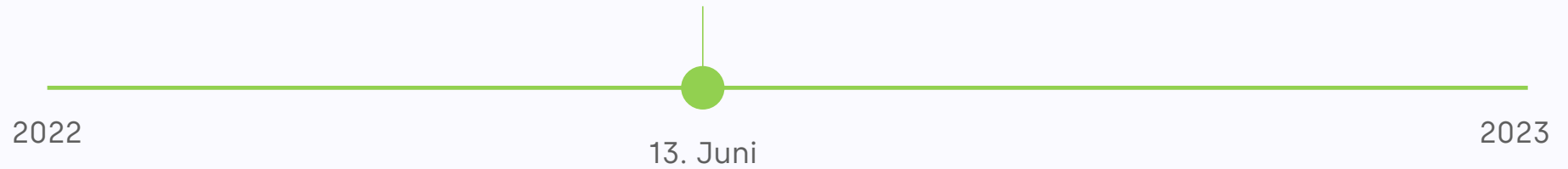
We have analyzed financial documentation of your company so we will offer you the appropriate price

- 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

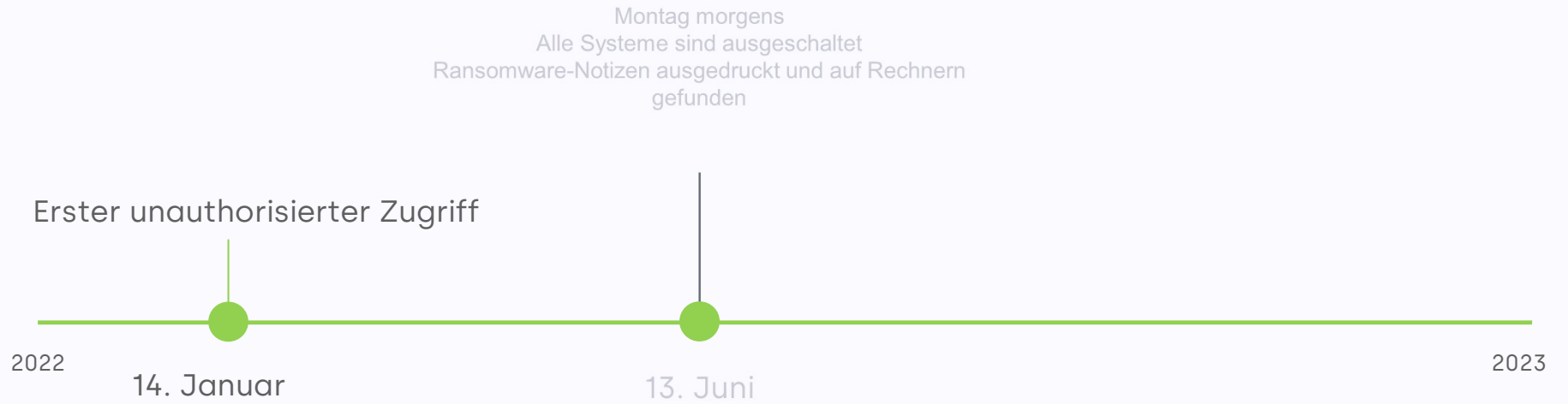


# Was ist passiert?

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



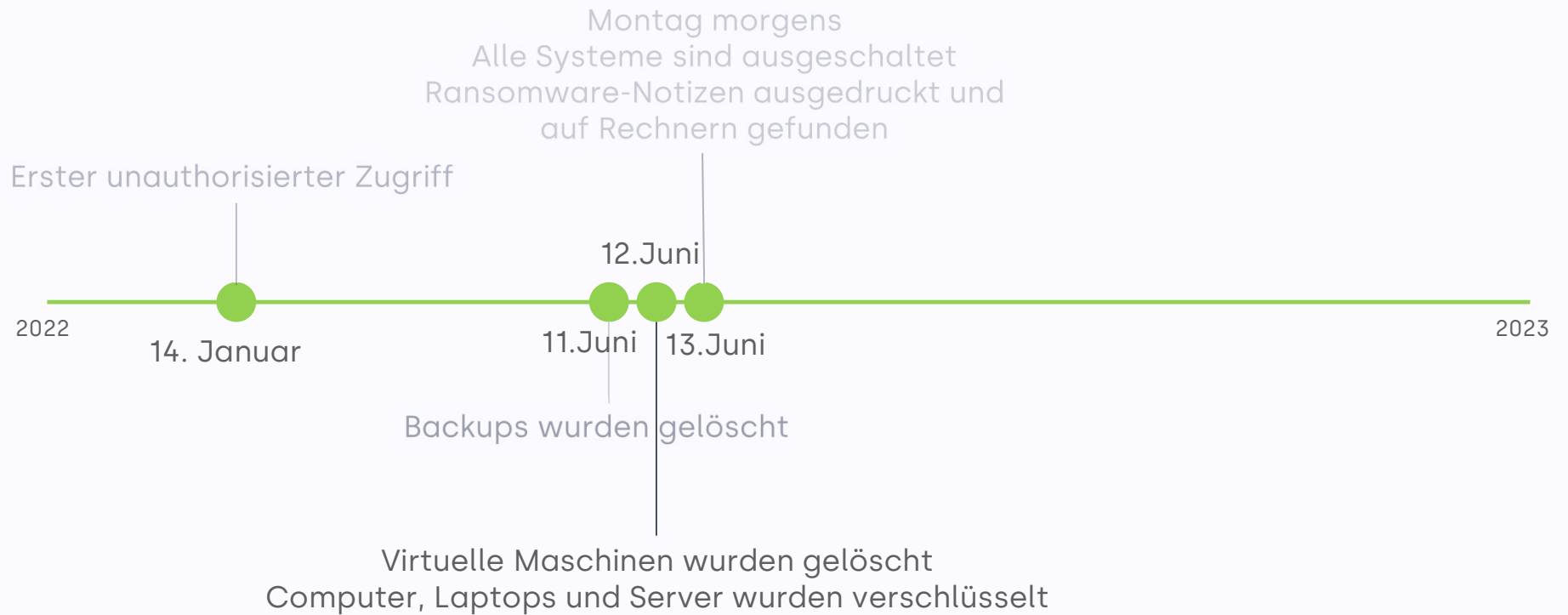
# Was ist passiert?



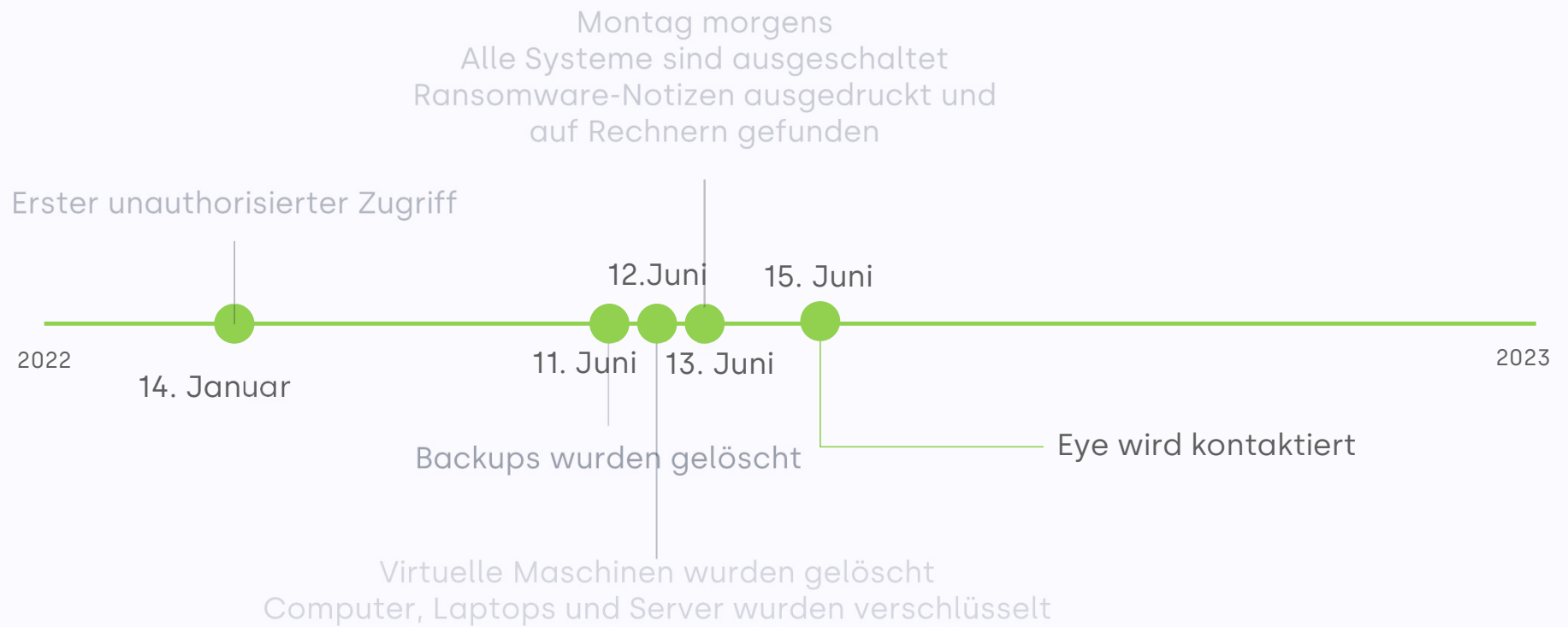
# Was ist passiert?



# Was ist passiert?

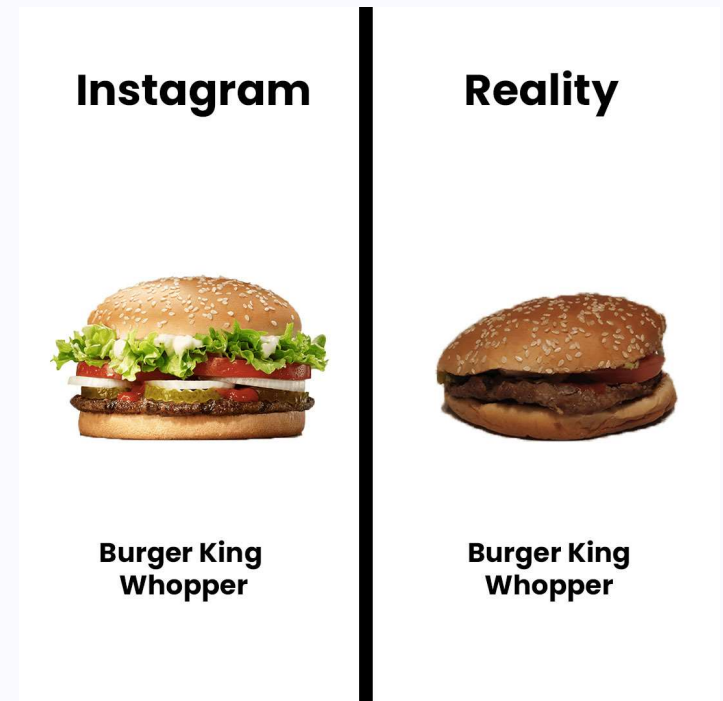


# Was ist passiert?



## 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.



# "EDR und Anti-Virus waren installiert"

Threat Details: m.exe

<b>100%</b> quarantined by users in OCD(NL)-Base-PG: [REDACTED] 0% waived 0% abnormal	<b>Version:</b> 2.2.0.0
<b>89.3%</b> quarantined by all Cylance users 0% waived 0% abnormal	<b>Company Name:</b> gentilkiwi (Benjamin DELPY)
<b>Classification:</b>	<b>Copyright:</b> Copyright (c) 2007 - 2021 gentilkiwi (Benjamin DELPY)
<b>First Found:</b> [REDACTED] 2022 01:48:25	<b>File Size:</b> 1.3 MB
<b>Last Found:</b> [REDACTED] 2022 01:48:25	<b>Signed:</b> True
	<b>Signature Status:</b> No Signature
	<b>Issuer:</b> Certum Code Signing 2021 CA
	<b>Publisher:</b> Open Source Developer, Benjamin Delpy
	<b>Subject:</b> Open Source Developer, Benjamin Delpy
	<b>Timestamp:</b>
	<b>Thumbprint:</b> 30 25 85 28 EE 84 76 DC 9B 68 48 66 68 95 9C FF 82
	<b>Icon:</b>



Ransomware wurde blockiert

## "EDR und Anti-Virus waren installiert"

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



```
Niels 09:42
C:\Users\ [redacted] \OneDrive [redacted] \Bureaublad\N2> ls
Directory listing for C:\Users\ [redacted] \OneDrive [redacted] \Bureaublad\N2 -

```

Name	Type	Size (bytes)	Size (MB)	Last Modified (UTC+1)	Created (UTC+1)
libsmb2.dll	.dll	707616	0,675	2022 15:02:21	2022 02:15:15
libsmi2.dll	.dll	746048	0,711	2022 15:02:21	2022 02:15:15
netscan.exe	.exe	15928352	15,19	2022 15:02:23	2022 02:15:15
netscan.lic	.lic	858	0,001	2022 03:53:22	2022 02:15:16
netscan.xml	.xml	44669	0,043	2022 03:53:22	2022 02:15:16
sc.xml	.xml	5142768	4,905	2022 02:22:36	2022 02:15:16

Multi Module:Mimikatz indicators

Look for obvious indicators that Mimikatz has been used on this machine across all available modules

	Hostname	sourcetype	timestamp_consolidated	activity
1	[redacted]000356	amcache		c:\users\ [redacted] \onedrive [redacted] \bureaublad\m.exe
2	[redacted]000356	amcache		c:\users\ [redacted] \desktop\m.exe

Storage of Cleartext Passwords in LSASS (WDigest)



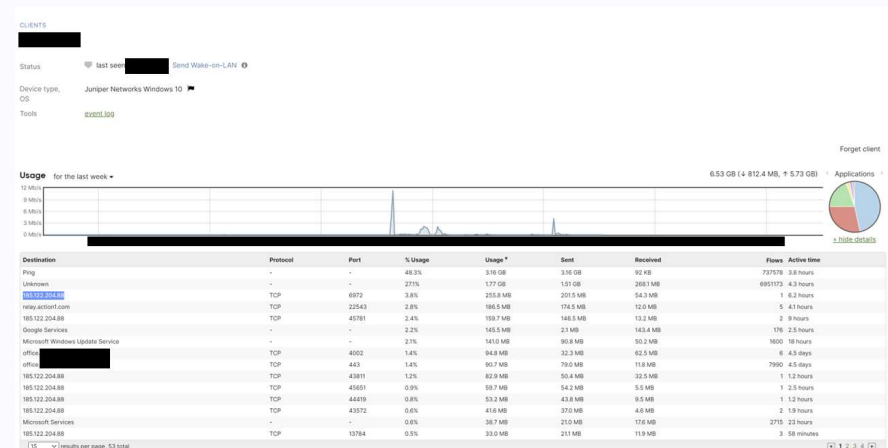
## "Alles ist gepatcht"

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”

Name	<input type="text" value="REDACTED"/>				+ X
Public IP	<input type="text" value="REDACTED"/>				
LAN IP	<input type="text" value="REDACTED"/>				
Uplink	<input type="text" value="Internet 1"/>				
Allowed inbound connections	Protocol	Ports	Remote IPs	Actions	
	<input type="text" value="TCP"/>	<input type="text" value="3389"/>	<input type="text" value="any"/>	X	
<a href="#">Allow more connections</a>					

Offener Port

➔ Eintritt für den Angreifer

# “Unsere Firewall ist aktiv”

Name	<input type="text" value="REDACTED"/>			<span>+</span> <span>X</span>
Public IP	<input type="text" value="REDACTED"/>			
LAN IP	<input type="text" value="REDACTED"/>			
Uplink	<input type="text" value="Internet 1"/>			
Allowed inbound connections	Protocol	Ports	Remote IPs	Actions
	<input type="text" value="TCP"/>	<input type="text" value="3389"/>	<input type="text" value="any"/>	<span>X</span>
<a href="#">Allow more connections</a>				

Offener Port

➔ Eintritt für den Angreifer

## “Netzwerke sind strikt getrennt”

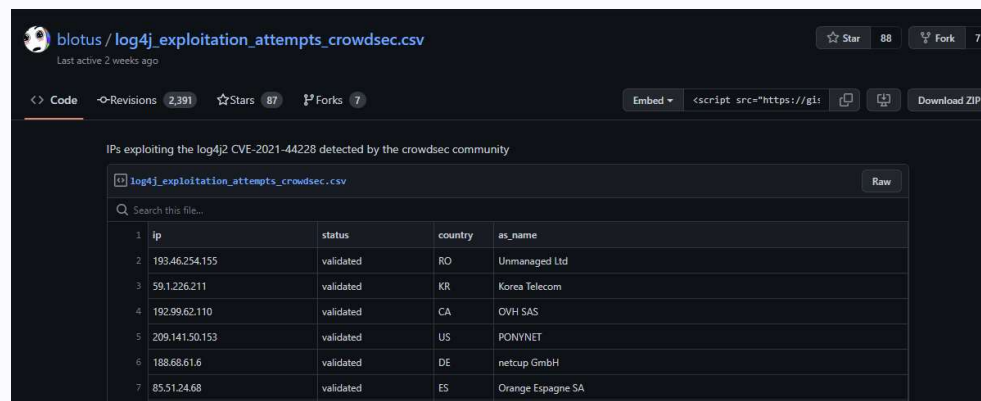
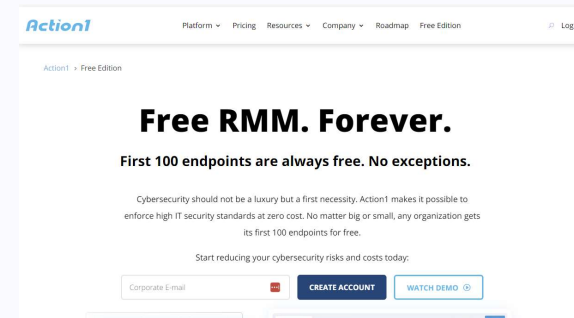
156	<u>✓ Allow</u>	VODAFONE-P Public <u>permit s</u> <u>hould be deny</u>	Any	Public_Netwerk_Compleet
-----	----------------	---	-----	-------------------------

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-Adresse, die bekannt für Log4j-Angriffe war.



blotus / log4j\_exploitation\_attempts\_crowdsec.csv

Last active 2 weeks ago

Code Revisions (2,391) Stars (87) Forks (7)

Embed <script src="https://gi: ... Download ZIP

IPs exploiting the log4j2 CVE-2021-44228 detected by the crowdsec community

ip	status	country	as_name
193.46.254.155	validated	RO	Unmanaged Ltd
59.1.226.211	validated	KR	Korea Telecom
192.99.62.110	validated	CA	OVH SAS
209.141.50.153	validated	US	PONYPNET
188.68.61.6	validated	DE	netcup GmbH
85.51.24.68	validated	ES	Orange Espagne SA

# Verhandlung mit den Angreifern

```
..... /sign_out
-----
You
> Hello, we found a note saying we should connect here, what are the next
steps ?

We
> Hello. You've reached an Akira support chat. Currently, we are preparing
the list of data we took from your network. For now you have to know that
dealing with us is the best possible way to settle this quick and cheap.
Keep in touch and be patient with us. We will reach out to you soon.

Do you have a permission to conduct a negotiation on behalf of your
organization? Once we get a response you will be provided with all the
details.

You
> Hello, yes I am and in contact with rest of our management

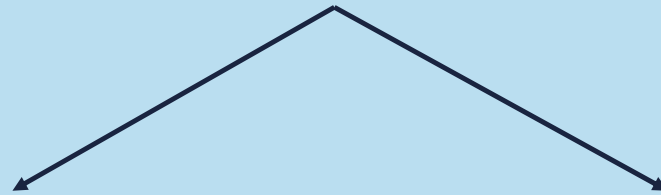
Enter text...

[ submit ] [ +file ]
```



Von \$150.000 auf  
\$10.000  
runtergehandelt

## Wesentliche Erkenntnisse



Viele menschliche  
Fehler

Technologie alleine  
reicht nicht aus

## Wesentliche Erkenntnisse

Viele menschliche  
Fehler

Technologie alleine  
reicht nicht aus

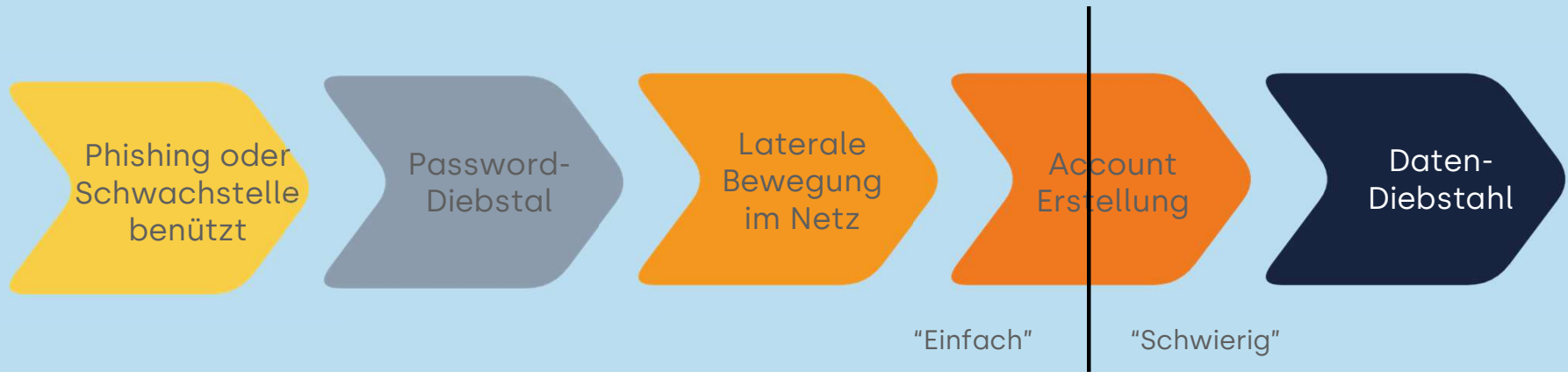


## “Assume Breach”

*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

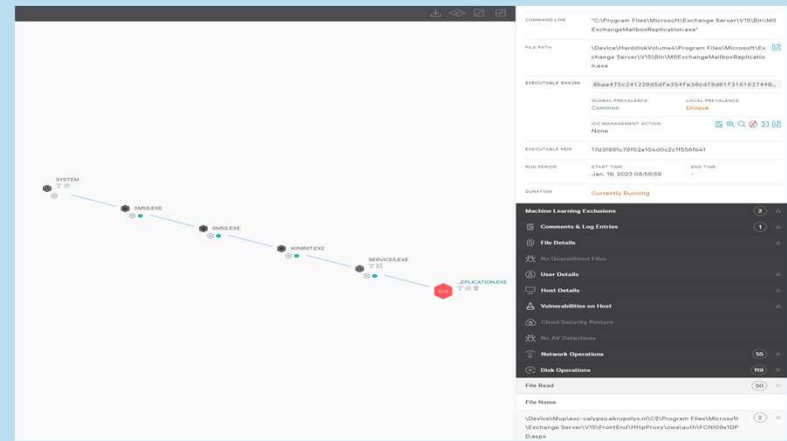




# Analyse & Root Cause

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|NlriYmZZ.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

Processes and Services

Process Executions

File Name: \* Command Line: \* Excluded File Name(s): NONE Excluded Command Line(s): NONE Exclude Common Processes:

Time (UTC)	Host Name	User Name	File Name	PID	Process ID	Command Line
2023-01-24 15:37:00	EXC-CALYPSO		bfeToolWin8.exe	5452	24270088799	"bfeToolWin8.exe"
2023-01-24 15:35:32	EXC-CALYPSO		netsh.exe	15092	24268834837	"netsh" interface tcp show global
2023-01-24 15:35:29	EXC-CALYPSO		nslookup.exe	22684	24267333515	"C:\Windows\system32\nslookup.exe" -typeA EXC-CALYPSO.Akroon1ys.nl. 10.0.0.4
2023-01-24 15:34:47	EXC-CALYPSO		wlprvse.exe	22684	24267091387	C:\Windows\system32\wbem\wlprvse.exe -secured -Embedding
2023-01-24 15:33:16	EXC-CALYPSO		wlprvse.exe	15336	24265919863	C:\Windows\system32\wbem\wlprvse.exe -secured -Embedding
2023-01-24 15:33:11	EXC-CALYPSO		rellog.exe	19484	24263517141	"rellog.exe" "C:\Program Files\Microsoft\Exchange Server\V15\Logging\Diagnosics\PerformanceLogsToBeProcessed\Exchange\Diagnosics\PerformanceLog_01241620_blg" -f
2023-01-24 15:30:32	EXC-CALYPSO		netsh.exe	15216	24262486887	"netsh" interface tcp show global
2023-01-24 15:28:45	EXC-CALYPSO		wlprvse.exe	19976	24261261059	C:\Windows\system32\wbem\wlprvse.exe -Embedding
2023-01-24 15:28:43	EXC-CALYPSO		wlprvse.exe	4784	24260531039	C:\Windows\system32\wbem\wlprvse.exe -secured -Embedding
2023-01-24 15:28:15	EXC-CALYPSO		wlprvse.exe	15768	24258831837	C:\Windows\system32\wbem\wlprvse.exe -secured -Embedding

```
Time | Event
-----|-----
1/24/23 | { [-]
11:40:15.179 AM | Agent IP: 40.68.207.130
| CallStackModuleNames:
| 0000000000000000000000011010000001<-1>\Device\HarddiskVolume4\Windows\System32\ntdll.dll+0xa7344:0x1cf000:0x633688f6\[\
| [HEAP:45;RWX-;REFLECTIVE:server.dll:0x1c1bcbcc00]+0x1c1bcbccfe6
| CallStackModuleNamesVersion_decimal: 8
| ComputerName: EXC-CALYPSO
| ConfigBuild: 1007.3.0016303.10
| ConfigStateHash_decimal: 1953016244
| ContextProcessId_decimal: 23645389876
| ContextThreadId_decimal: 7512180280892
| ContextTimeStamp_decimal: 1674560414.988
| EffectiveTransmissionClass_decimal: 2
| Entitlements_decimal: 15
| LocalAddressIP4: 10.0.0.6
| MAC: 00-22-48-7F-25-61
| MemoryRegionProtection_decimal: 64
| MemoryRegionStart_decimal: 1931606753280
| ProcessExecuteFlags_decimal: 0
| ProductType: 3
| ReflectiveDllName: server.dll
| ReflectivePeEntryRva_decimal: 87808
| ReflectivePeTimestamp_decimal: 1639090350
| StackBase_decimal: 0
| StackLimit_decimal: 0
| SuspectAddress_decimal: 1931606806502
| SuspectStackFlag_decimal: 3329
| TargetThreadId_decimal: 7514474150680
| ThreadStartAddress_decimal: 1931606806848
| TreeId_decimal: 12887374259
| aid: 544f6c48e12f437aa89e3933a7b26b2e
| aip: 40.68.207.130
| cid: 4f441b8d3f6d4865822aff6ff8a1b67b
| company: NFR - EYE Control
| eid: 999
| esize: 507
| event_err: false
| event_platform: Win
| event_simpleName: CreateThreadReflectiveDll
| event_version: 12
| eventtype: Eam
| host: localhost:8088
| id: 74733955-ce3a-4d73-bc37-2cd56e98fde9
| index: main
| name: CreateThreadReflectiveDllV12
| source: main
| sourcetype: CreateThreadReflectiveDllV12-v02
| tid: 12676880
| timestamp: 1674560415179
| }
```

# Beispiel für Erkennung – Wiederherstellung

Der Angreifer von der Maschine werfen (aktive Reaktion)


- Prozess des Angreifers beenden
- Veränderte Dateien entfernen
- Falls nötig: Isolieren

Server patchen

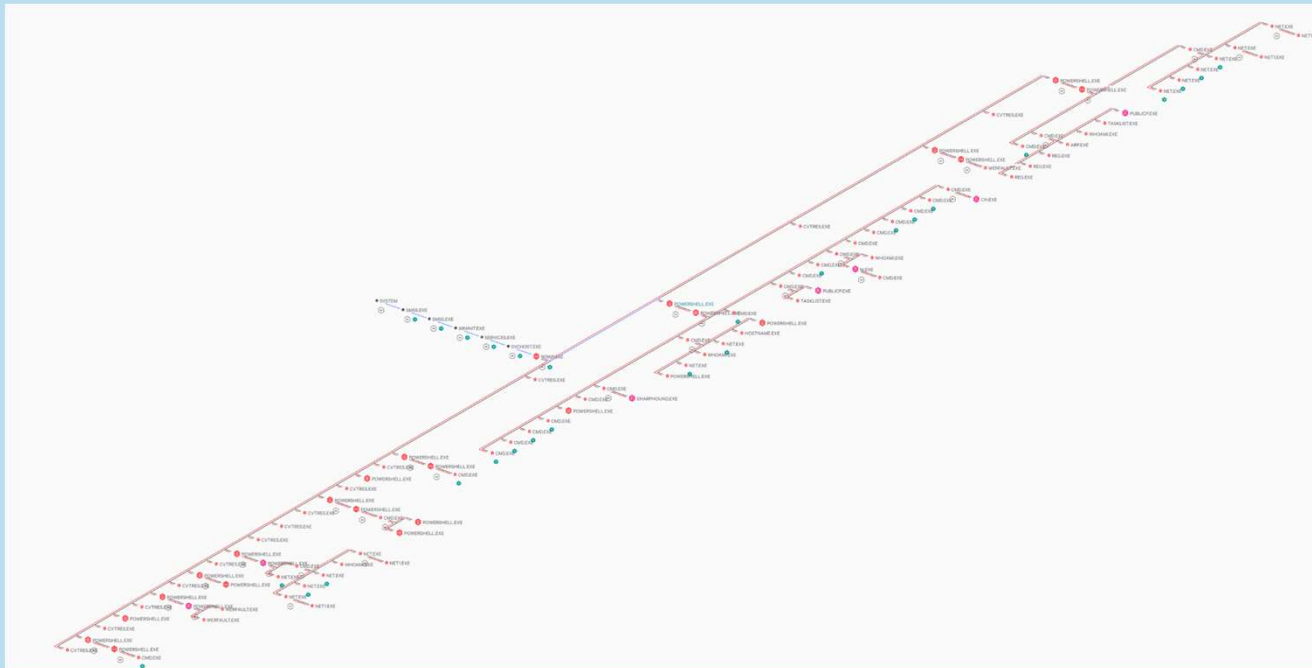
Process Name	PID	Time	Value 1	Value 2	Path
ApplicationFrameHost	19284	1/23/2023 5:00:05	18,956	0.23	C:\Windows\system32\ApplicationFrameHost.exe
cmd	3388	1/23/2023 1:36:06 PM	2,844	0.02	C:\Windows\SYSTEM32\cmd.exe
cmd	9752	1/23/2023 1:25:16 PM	2,844	0.00	C:\Windows\SYSTEM32\cmd.exe
cmd	13716	1/23/2023 10:57:26 AM	2,992	0.03	C:\Windows\system32\cmd.exe
cmd	14492	1/23/2023 1:51:41 PM	2,844	0.02	C:\Windows\SYSTEM32\cmd.exe
cmd	14640	1/23/2023 1:52:19 PM	2,840	0.02	C:\Windows\SYSTEM32\cmd.exe
cmd	15664	1/23/2023 5:42:36 PM	3,016	0.06	C:\Windows\system32\cmd.exe
cmd	17392	1/23/2023 3:17:06 PM	3,136	0.13	C:\Windows\system32\cmd.exe
cmd	23500	1/23/2023 5:09:48 PM	2,976	0.03	C:\Windows\system32\cmd.exe
ComplianceAuditService	4520	1/19/2023 8:56:58 AM	192,696	23.20	C:\Program Files\Microsoft\Exchange Server\V15\Bin\ComplianceAuditService.exe
conhost	2668	1/23/2023 11:00:21 AM	5,520	0.02	C:\Windows\system32\conhost.exe
conhost	3460	1/23/2023 1:52:19 PM	6.148	3.97	C:\Windows\system32\conhost.exe

# Beispiel falls nicht direkt eingegriffen wurde

Falls nichts unternommen wird:  
113 Alerts

 **Critical**  
+112 others

TACTIC & TECHNIQUE  
Credential Access via OS Credentia...



## 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

### Beaufsichtigung (durch BSI)

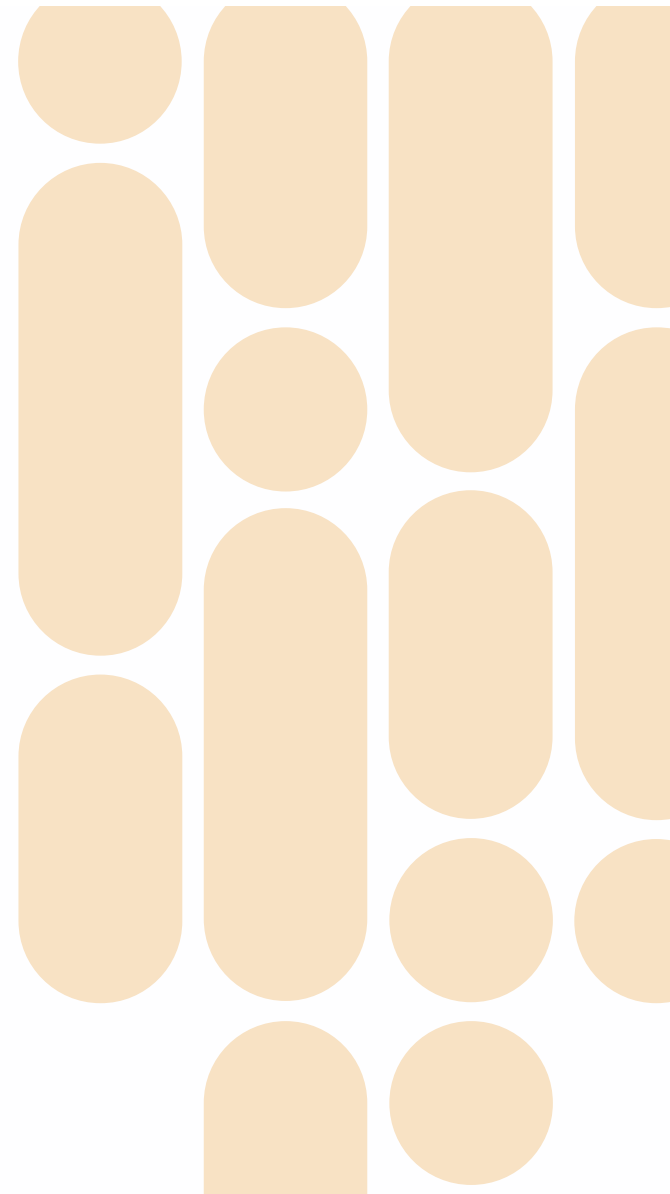
- Proaktiv für besonders wichtige Einrichtungen, reaktiv für wichtige Einrichtungen
- BSI kann nachforschen (auch lokal)
- BSI kann Fristen zur Beseitigung von Mängeln setzen
- BSI kann Nichteinhaltung veröffentlichen
- Das BSI kann die Verwaltung aussetzen (oder aussetzen lassen)
- Verwaltungsgeld bei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



[marcel.van.asperdt@eyesecurity.de](mailto:marcel.van.asperdt@eyesecurity.de)

[eyesecurity.de](https://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.