



**DIGITAL
SICHER
NRW**

Kompetenzzentrum für
Cybersicherheit in der Wirtschaft

TÜR ZU IM NETZ: Wie Sie sich vor Cyberangriffen schützen

Düsseldorf, 15.09.2026



Beauftragt vom

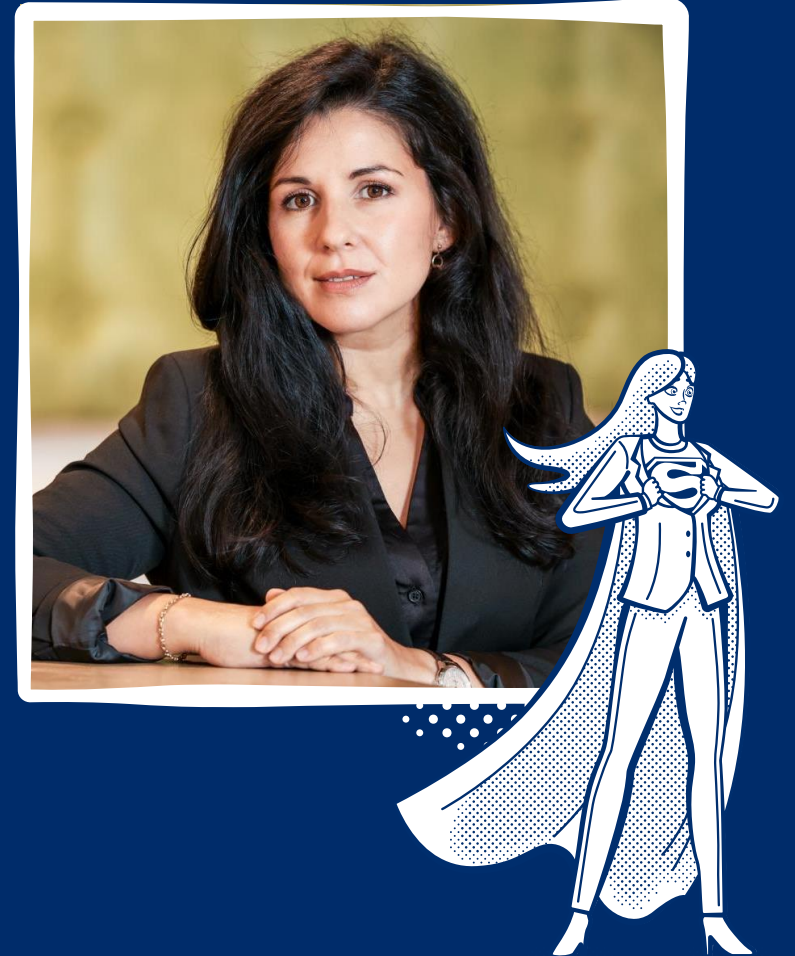
Ministerium für Wirtschaft,
Industrie, Klimaschutz und Energie
des Landes Nordrhein-Westfalen



KURZE VORSTELLUNG

Tatjana Ljucovic

- Master of Science in Internet-Sicherheit
- Mitarbeit in der Forschung im Bereich IT-Sicherheit, insbesondere zu sicheren Kommunikationslösungen für Unternehmen
- 6 Jahre Erfahrung als Security Engineer im Bereich Schadsoftwareanalyse
- Beraterin für digitale Sicherheit bei DIGITAL.SICHER.NRW



Das schauen wir uns heute an:



Welche Schadprogramme gibt es?



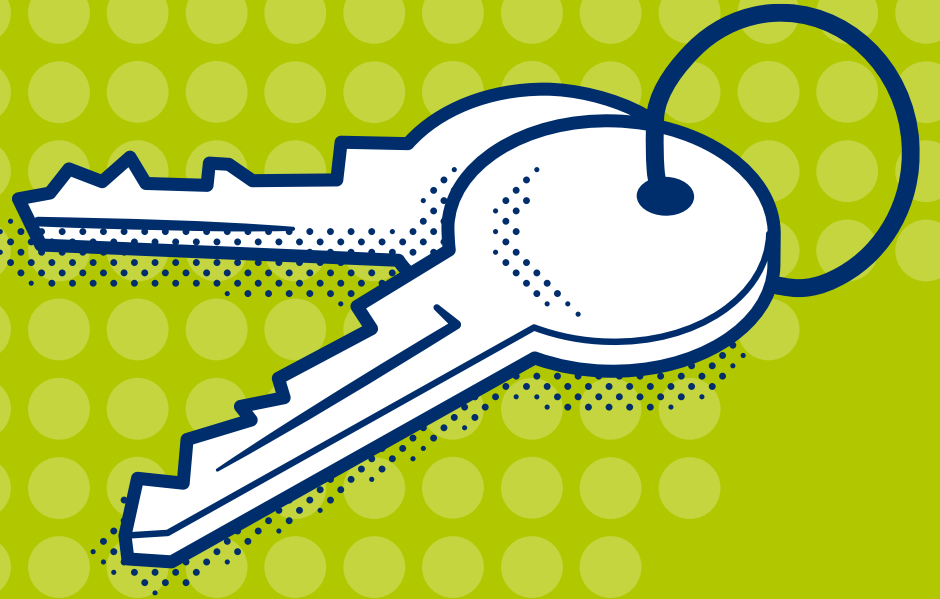
Ransomware (Arten, Gruppierungen, Motivation etc.)



Wie gehen die Angreifenden vor?



Tipps: Schutz vor Ransomware



SCHADPROGRAMME

Schadprogramme



● Virus

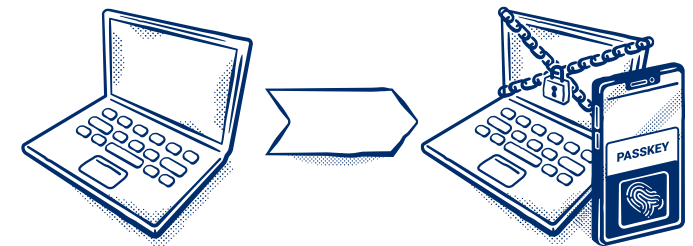
- infiziert Dateien und verbreiten sich durchs Öffnen, Ausführen o.ä.

● Würmer

- verbreiten sich selbständig über das Netzwerk oder Dienste

● Trojaner

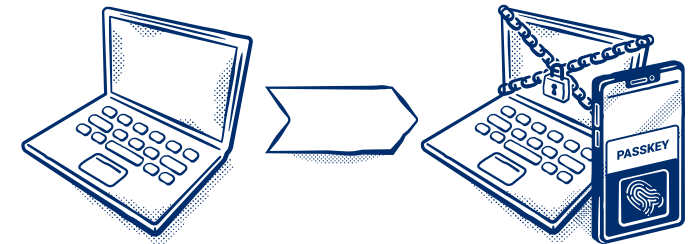
- tarnen sich als legitime Software
- öffnen Hintertüren und ermöglichen z.B. Datenklau oder das Nachladen von weiterer Schadsoftware



Schadprogramme



- **Spyware**
 - zeichnet Eingaben auf oder greift Informationen ab (Keylogger usw.)
- **Remote Access Trojaner (RAT)**
 - ermöglicht den Angreifenden vollständige Fernsteuerung des Systems
- **Rootkits**
 - verstecken sich im System und tarnen andere Schadprogramme vor Sicherheitssoftware
- **Ransomware ...**



RANSOMWARE

Was Ransomware macht



1. Stehlen

- Bevor verschlüsselt wird, wird kopiert.

Die Täter haben Ihre Daten – und drohen mit Veröffentlichung.

2. Verschlüsseln

- Ihre Daten sind noch da – aber unlesbar. Den Schlüssel gibt es gegen Geld.

Zwei Probleme statt einem: „doppelte Erpressung“

„WIR HACKEN JEDEN GmbH“



**WIE KOMMEN DIE
ANGREIFENDEN
AUFS SYSTEM?**

Einfallsvektor NR. 1



90% aller Angriffe beginnen mit einer E-Mail!

Phishing:

- nicht zielgerichtet
- Erbeuten von Informationen oder Verleiten zu einer bestimmten Aktion
- Ausübung von Druck

Spear-Phishing:

- zielgerichtet
- Einzelpersonen oder Gruppen
- geht mit Ausspähung einher
- Wir sind gläserner, als wir denken!

Weiterer Einfallsvektor



- **Exploit:** Werkzeug, um Sicherheitslücken von Software aufzuzeigen
- **kommt auf zwei Arten auf Ihren Computer:**
 - **Drive-by-Exploits:** manipulierte Webseiten oder Werbebanner, dabei wird im Hintergrund eine Sammlung an Exploits heruntergeladen
 - **Exploits in Dateien:** meist über den Anhang von E-Mails oder infizierte Links

Weiterer Einfallsvektor



- **unsichere Zugänge für Remote Desktop Tool** (Fernzugriff auf Computern)
 - **Tools:** TeamViewer, AnyDesk, Remotedesktopprotokoll (RDP)
- Meist ist der Zugang mit einem **schwachen Passwort** versehen und **ohne 2-Faktor-Authentifizierung** geschützt.
- Angreifende versuchen u.a. mit gestohlenen oder erratenen Zugangsdaten einzudringen.

DIE TOP NINE PASSWÖRTER IN DEUTSCHLAND VON 2025

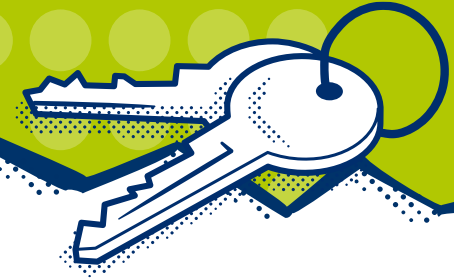
Top Nine deutscher Passwörter 2025:

1. 123456
2. 123456789
3. 565656
4. 12345678
5. hallo123
6. kaffeetasse
7. 1234567
8. passwort
9. lol123



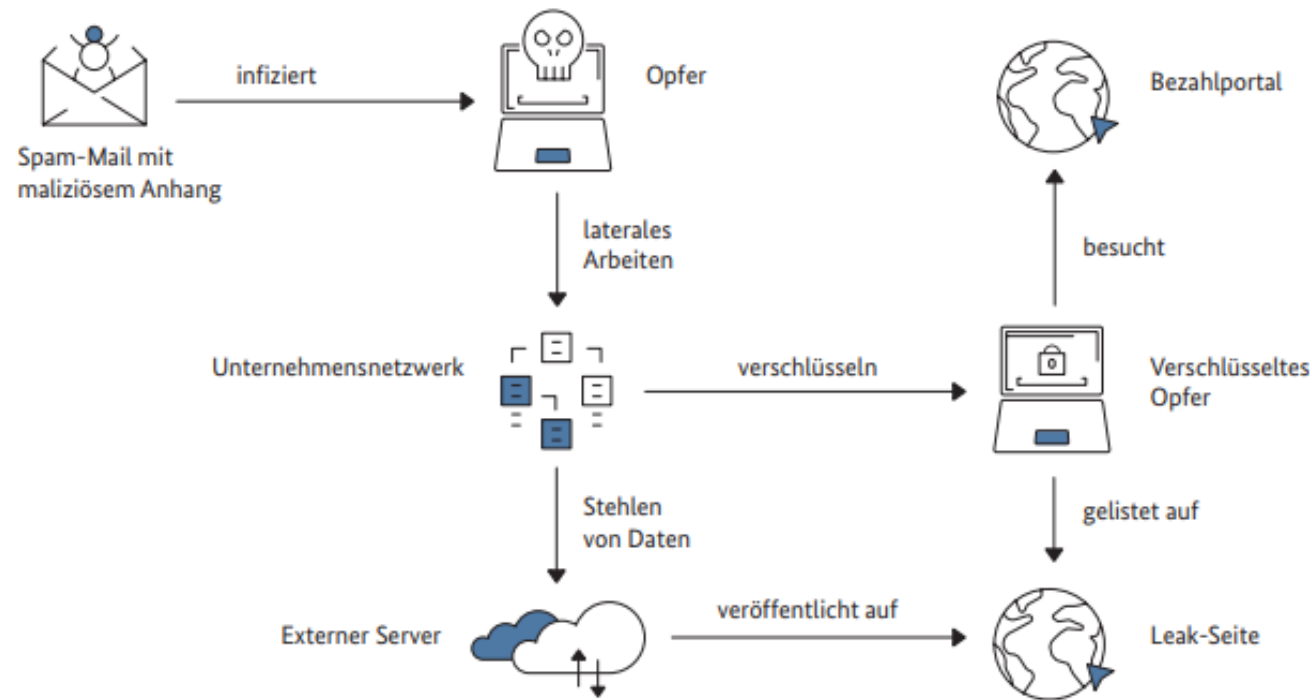
TATHERGANG

Der Ablauf



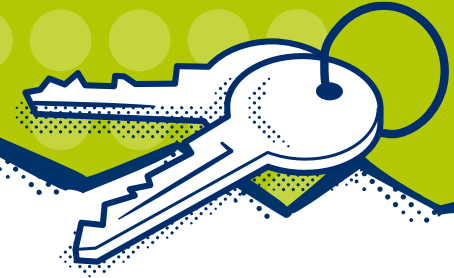
Beispielhafter Angriffsablauf

Abbildung 3:
Beispielhafter Ablauf eines Ransomware-Angriffs mit Lösegeld-
und Schweigegelderpressung (schematische Darstellung)
Quelle: BSI



Quelle:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=8

Der Ablauf



Beispielhafter Angriffsablauf

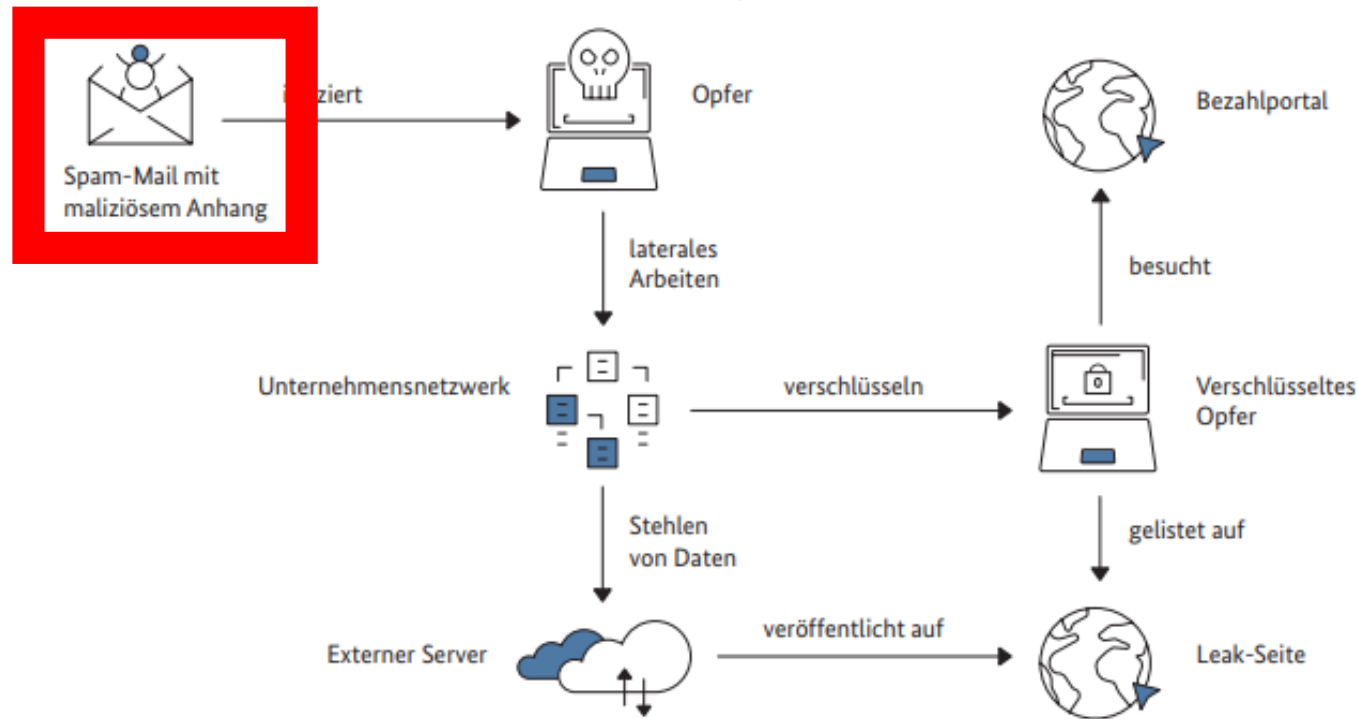
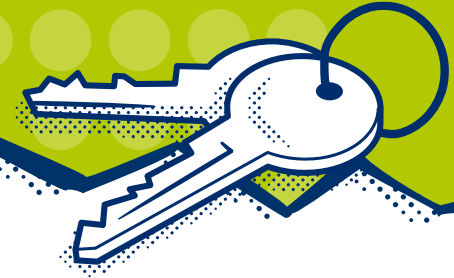


Abbildung 3:
Beispielhafter Ablauf eines Ransomware-Angriffs mit Lösegeld-
und Schweigegelderpressung (schematische Darstellung)
Quelle: BSI

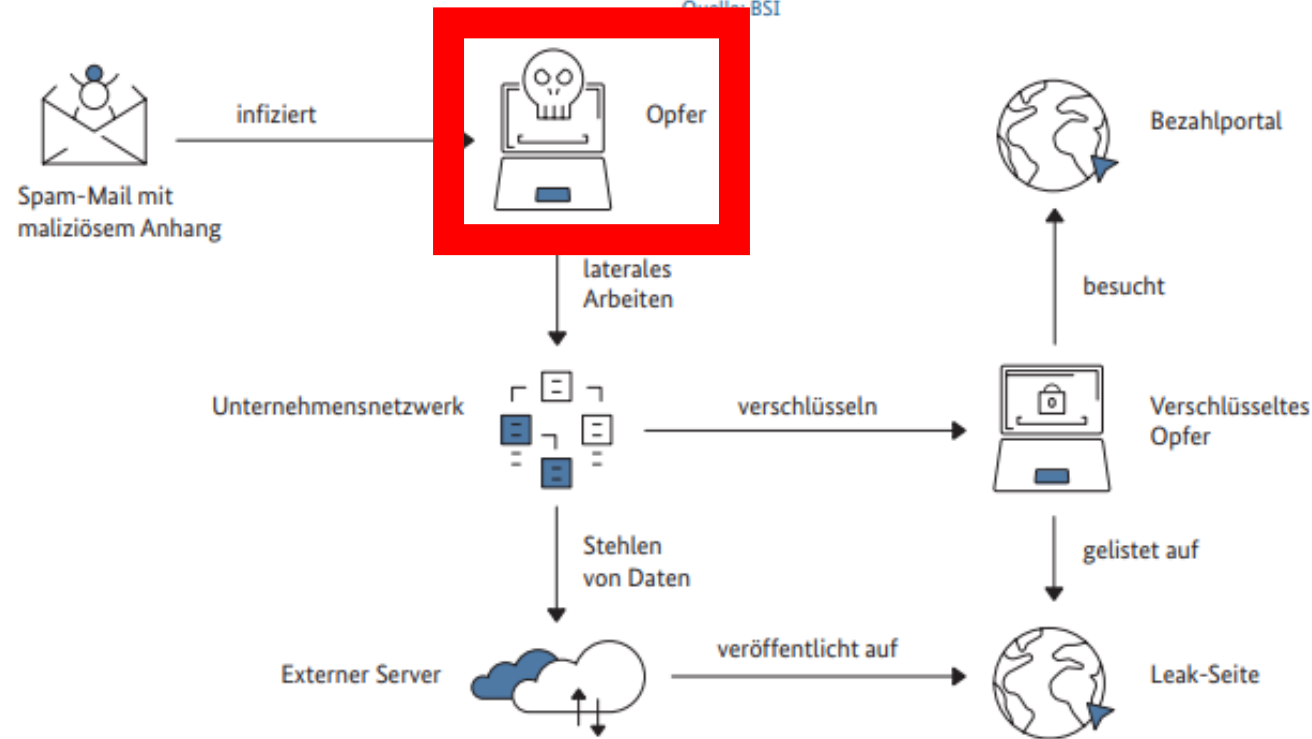
Quelle:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=8

Der Ablauf



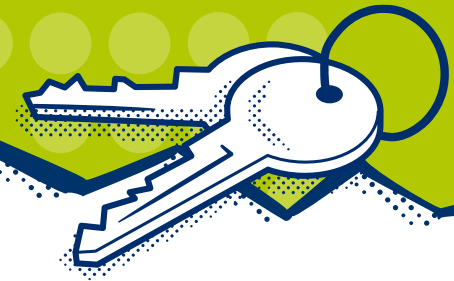
Beispielhafter Angriffsablauf

Abbildung 3:
Beispielhafter Ablauf eines Ransomware-Angriffs mit Lösegeld-
und Schweigegelderpressung (schematische Darstellung)
Quelle: BSI



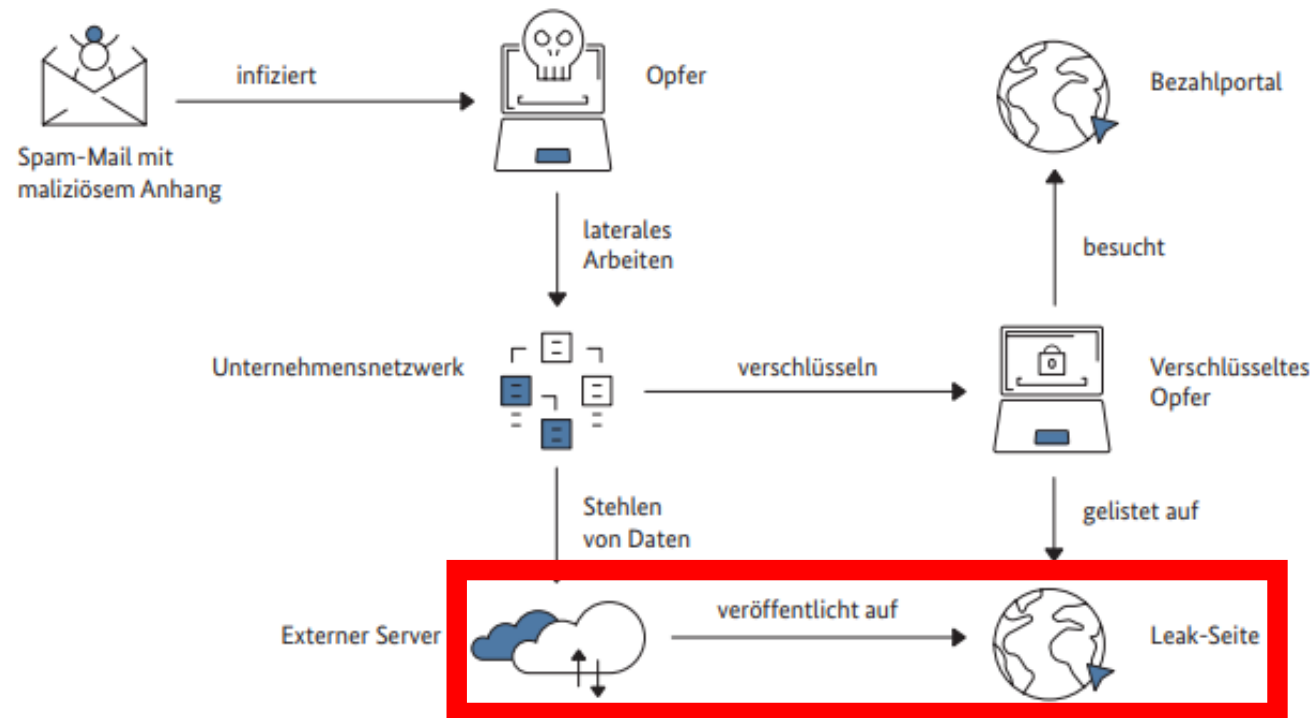
Quelle:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=8

Der Ablauf



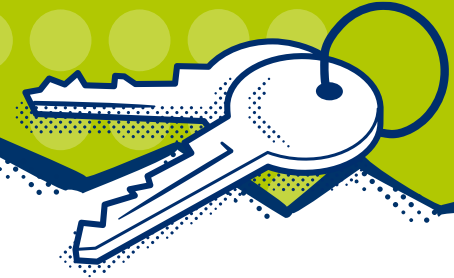
Beispielhafter Angriffsablauf

Abbildung 3:
Beispielhafter Ablauf eines Ransomware-Angriffs mit Lösegeld-
und Schweigegelderpressung (schematische Darstellung)
Quelle: BSI



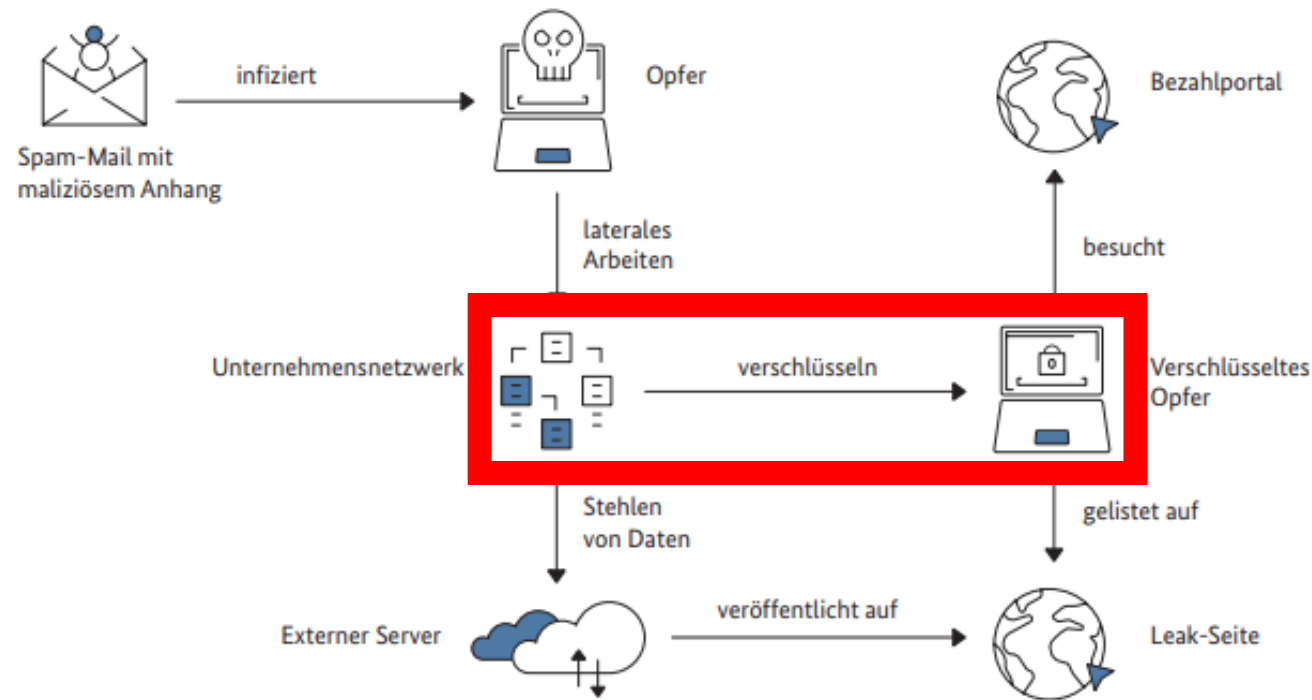
Quelle:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=8

Der Ablauf



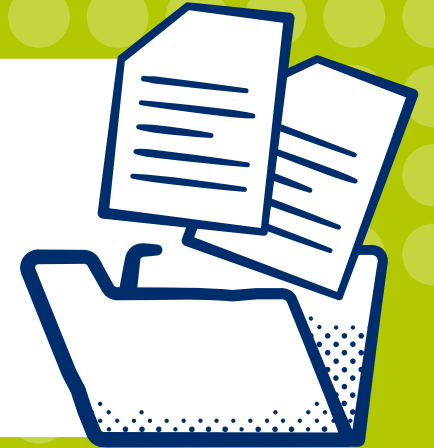
Beispielhafter Angriffsablauf

Abbildung 3:
Beispielhafter Ablauf eines Ransomware-Angriffs mit Lösegeld-
und Schweigegelderpressung (schematische Darstellung)
Quelle: BSI



Quelle:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=8

WOHIN GEHEN DIE DATEN?



Surface Web, Deep Web, Darknet



Surface Web

- Alles, was Suchmaschinen finden

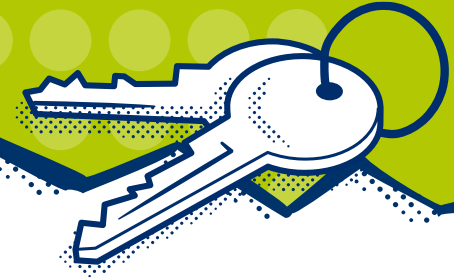
Deep Web

- Alles, wofür Sie ein Passwort brauchen: Online-Banking, Intranet, Postfach.
Alltäglich und legal.

Darknet

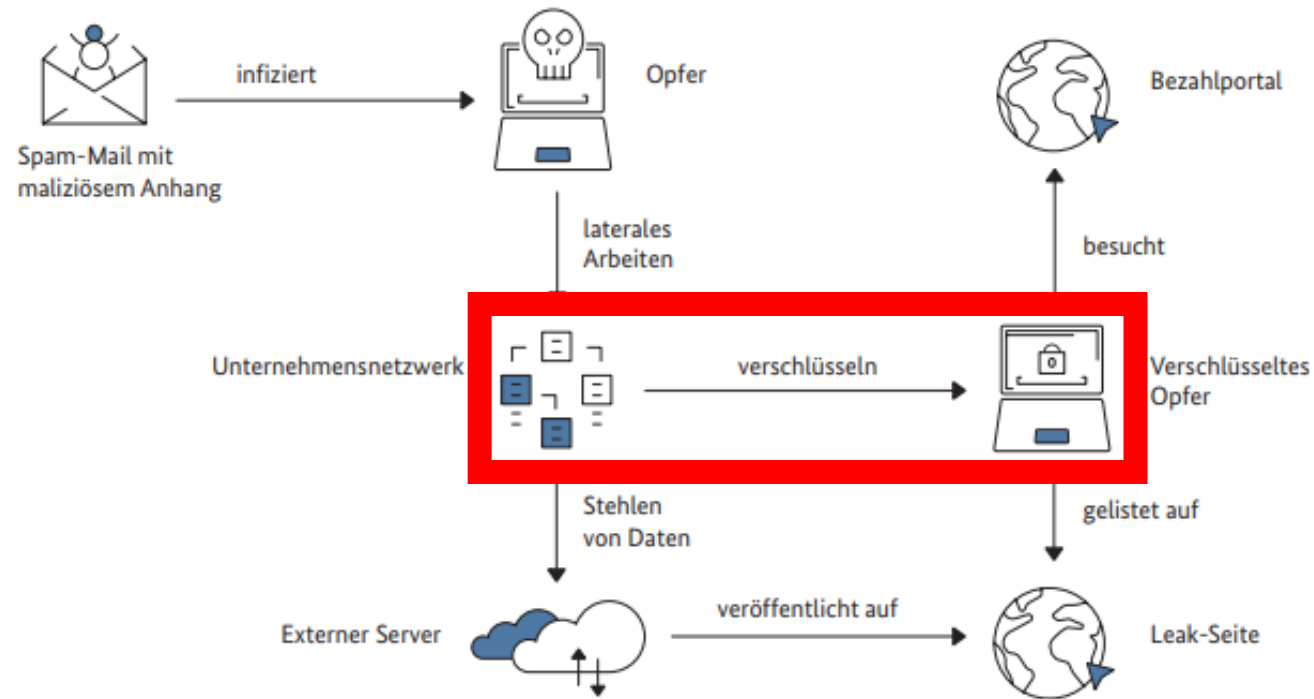
- Nur mit spezieller Software erreichbar. In keinem Suchindex.
Weder Seite noch Besucher sind identifizierbar.

Der Ablauf



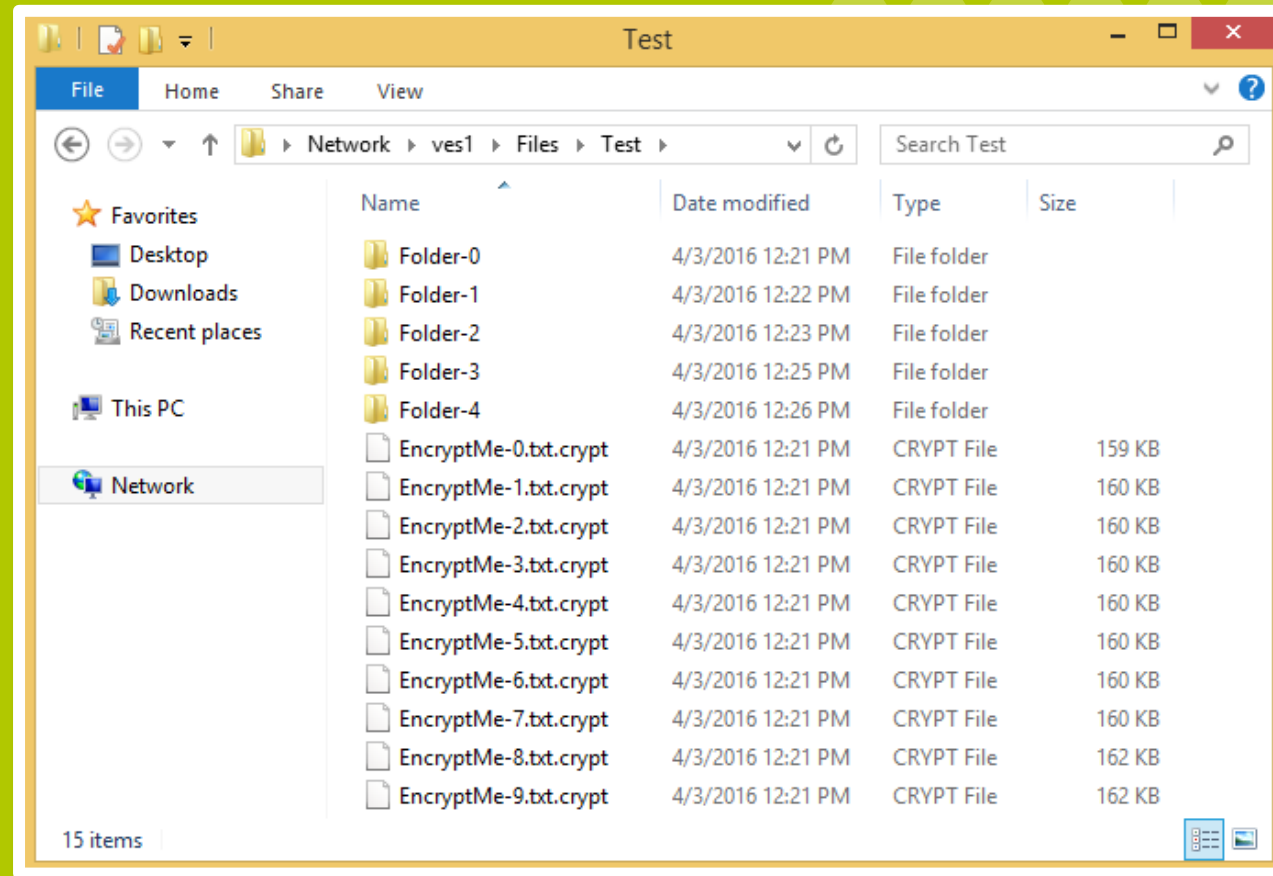
Beispielhafter Angriffsablauf

Abbildung 3:
Beispielhafter Ablauf eines Ransomware-Angriffs mit Lösegeld-
und Schweigegelderpressung (schematische Darstellung)
Quelle: BSI

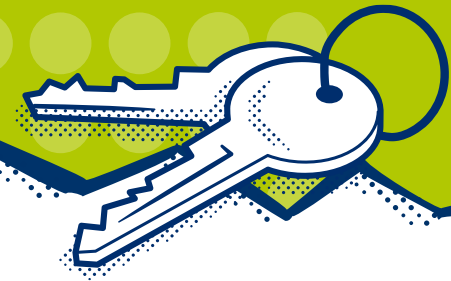


Quelle:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=8

Verschlüsselte Dateien

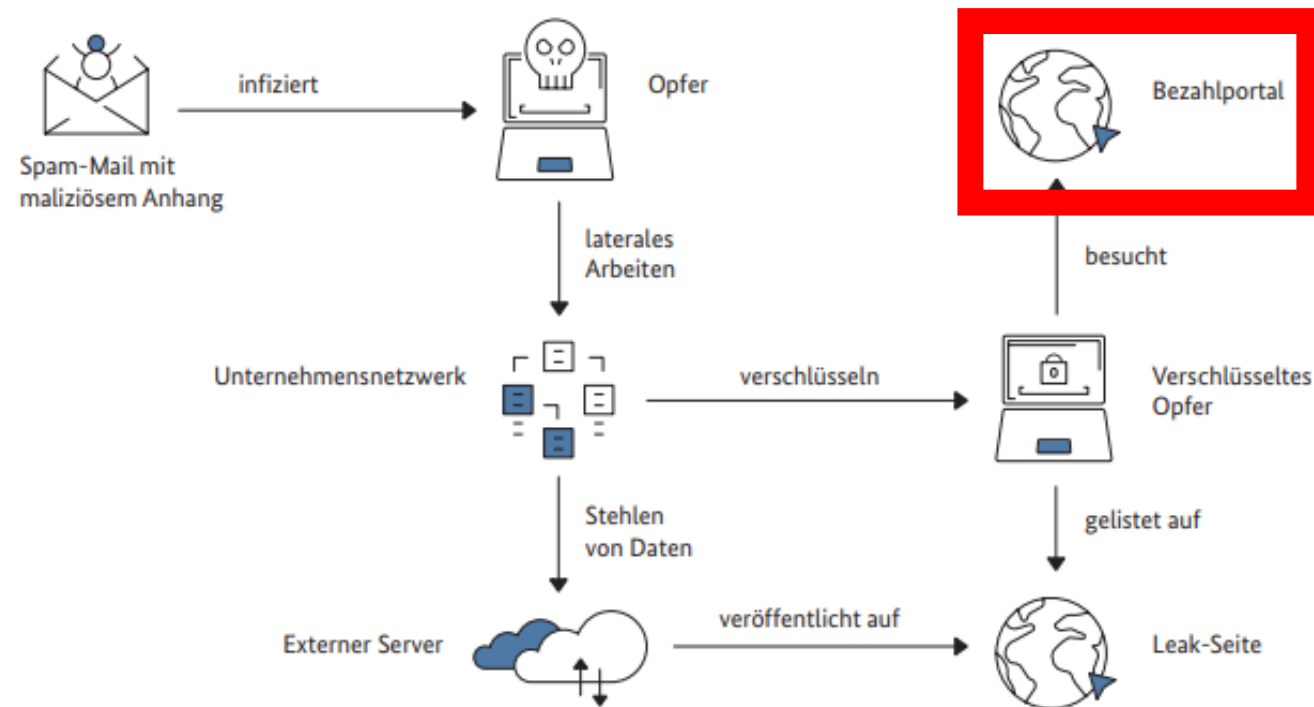


Der Ablauf



Beispielhafter Angriffsablauf

Abbildung 3:
Beispielhafter Ablauf eines Ransomware-Angriffs mit Lösegeld-
und Schweigegelderpressung (schematische Darstellung)
Quelle: BSI



Was macht die Polizei?

Emotet Takedown

2021



Operation Endgame

2022 - heute



Operation Checkmate

2025 - heute



Was macht die Polizei?



HOME

NEWS

SEASONS

SUSPECTS

PARTNERS

CONTACT



EU MOST WANTED



**GALOCKIN, Maksim
Sergeevich**



**KISELEV, Dmitrii
Sergeevich**



**KHALITOV, Danil
Raisowitsch**



**KONIUKHOV, Konstantin
Pavlovich**



**KOVALEV, Vitalii
Nikolaevich**

Quelle:
<https://www.operation-endgame.com/suspects/>

Betroffene Unternehmen in NRW 2025 (Auszug)

Hersteller Sanitär & Armaturen	Düsseldorf	21.01.2025	5.000	Autohandel/Automotiv	Bottrop	10.03.2025	70
Chemieindustrie	Leverkusen	24.01.2025	18.000	Gesundheits- und Sozialwesen	Mönchengladbach	17.03.2025	900
E-Commerce & Handel	Bonn	30.01.2025	70	Dienstleistungen & Zertifizierung für das Gesundheitswesen	Köln	28.03.2025	1.773
Großhandel von Ersatzteilen	Euskirchen	11.02.2025	150	Rüstungsunternehmen	Düsseldorf	04.04.2025	42.000
Dachverband	Leichlingen	17.02.2025	10	Transport & Logistik	Düsseldorf	25.04.2025	80
IT-Dienstleister	Velbert	21.02.2025	2-10	Interessenvertretung	Bochum	22.07.2025	10-50
Kühltransporte & Logistiklösungen	Versmold	24.02.2025	201-500	Verkehr & Logistik Luftfahrt	Münster	20.09.2025	150
Maschinenbau	Bad Salzuflen	27.02.2025	170	Wissenschaft & Forschung	Bonn	21.09.2025	50
IT- und Software Dienstleistungen	Bochum	05.03.2025	15	Immobilienwirtschaft	Lüdenscheid	26.09.2025	9
Materialverarbeitung im Bereich Automotiv	Plettenberg	05.03.2025	600	Energie- und Wasserversorgung	Detmold	18.11.2025	180
Energie- und Wasserversorgung	Schwerte	05.03.2025	140	Groß- und Einzelhandel	Wuppertal	03.12.2025	150

Anzahl der Mitarbeitenden / Betriebsgröße

Branche / Tätigkeitsbereich

**ES IST KEINE FRAGE, OB
ICH ANGEGRIFFEN
WERDE, SONDERN WANN!**

KEIN UNTERNEHMEN IST

**ZU JUNG,
ZU KLEIN,
ZU UNBEDEUTEND,
ZU UNATTRAKTIV,**

UM ANGEGRIFFEN ZU WERDEN.





UND JETZT?

TIPPS, GEGEN DIE EINFALLSVEKTOREN

**ÜBERPRÜFEN SIE IHRE
MAILS MIT DER
3-SEKUNDEN-REGEL!**



**PFLEGEN SIE IHRE
GERÄTE UND
PROGRAMME!**



**NUTZEN SIE EINEN
PASSWORTMANA
GER & 2FA!**



**MACHEN SIE
BACKUPS!**



NOTFALLPLANUNG!



DIE FÜHRUNGSEBENE IST ENTSCHEIDEND!



Verantwortung übernehmen:

- digitale Sicherheit = strategische Notwendigkeit

Regelmäßige Bestandsaufnahme:

- der Bedrohungslage
- der Einfallstore in Ihrem Betrieb
- der getroffenen Schutzmaßnahmen

Handlungsfähigkeit gewährleisten:

- Ressourcen und Budget bereitstellen
- Problembewusstsein schaffen
- Mitarbeitende schulen



Kontinuität: Digitale Sicherheit ist kein einmaliges Projekt, sondern ein fortlaufender Prozess!

CYBERSICHERHEIT IST SACHE DER GESCHÄFTSFÜHRUNG



WAS BEDEUTET DAS?

Sich der **Bedeutung** bewusst werden und **Verantwortung** für die Cybersicherheit der eigenen Organisation übernehmen.

ZIELE

Schäden vermeiden und **Risiken senken** für:

- Die eigene Organisation, Mitglieder, Partnerinnen und Partner sowie Mitarbeitende.

DAS WICHTIGSTE FÜR DEN EINSTIEG

- **Cybersicherheitsstrategie festlegen**
Sollte die wichtigsten Risiken für das Unternehmen identifizieren und Maßnahmen festlegen.
- **Regelmäßige Sicherheitsaudits und –tests durchführen**
Helfen dabei, Schwachstellen in den IT-Systemen sowie der Infrastruktur zu identifizieren und zu beheben.
- **Mitarbeitende & Führungskräfte schulen**
Bewusstsein für die wichtigsten Bedrohungen und deren Konsequenzen schaffen.
- **Notfallplanung für den Ernstfall erstellen**
Reaktion & Vorgehen im Fall eines Vorfalls planen, externe Hilfe klären, Verantwortlichkeiten festlegen und gewappnet sein.

DIE NOTFALLNUMMER DES LKA NRW



0211/939-4040

LKA Cybercrime-Kompetenzzentrum Single Point of Contact (SPoC)

Diese Hotline steht allen Unternehmen und Organisationen **rund um die Uhr** in Nordrhein-Westfalen kostenfrei zur Verfügung.
Sie dient als erste Ansprechstelle im Falle eines Cyberangriffs.

DIGITALE ERSTBERATUNG



individuelle Analyse

Wir schauen, was in Ihrem Betrieb bereits gut läuft und wo noch Luft nach oben ist – auf Augenhöhe und transparent.



passende Maßnahmen

Gemeinsam finden wir Lösungen, die wirklich zu Ihrem Unternehmen passen – individuell und praxisnah.



einfache Umsetzung

Wir erklären Ihnen, wie Sie die besprochenen Schritte in Ihrem Betrieb umsetzen können – verständlich und effektiv.



**Vereinbaren Sie einen kostenfreien
Termin zur digitalen Erstberatung!**

IT-SICHERHEITSKOMPASS

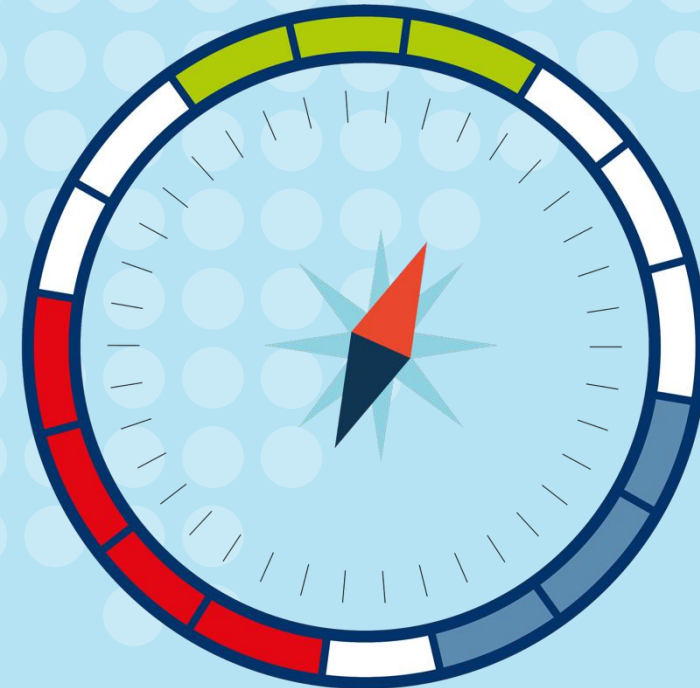
Schauen Sie unbedingt auf
unserer Webseite vorbei oder
sprechen Sie uns an!

www.digital-sicher.nrw

Grundregeln der IT-Sicherheit

Fast alle mittelständischen Unternehmen in Nordrhein-Westfalen haben sich in den letzten Jahren zunehmend digitalisiert. Das hat einerseits viele Arbeiten enorm erleichtert. Andererseits wurden so neue Angriffsflächen innerhalb von Unternehmen geschaffen. Diese zu schließen und sich vor einem Großteil digitaler Kriminalität zu schützen, ist für kleine und mittlere Unternehmen ein zentrales Zukunftsthema.

Passwörter	▼
Passwortmanager	▼
Smartphones und Tablets	▼
Internet und Browser	▼
Spam und Anti-Virus	▼
Backups (Sicherheitskopien)	▼
Löschen und Zerstören	▼
Home-Office und mobiles Arbeiten	▼
Online-Shops	▼
Verschlüsselung	▼



Newsletter,

stelle mir bitte regelmäßig Informationen und Veranstaltungen rund um das Thema digitale Sicherheit zusammen. Danke!

Melden Sie sich an,
um nichts mehr zu
verpassen.



**DIGITAL
SICHER
NRW**



Ratgeber mit hilfreichen Tipps



aktuelle Veranstaltungen



Neues vom Kompetenzzentrum

1 x monatlich

Kompetenzzentrum für Cybersicherheit in der Wirtschaft in NRW

Die Grundlagen der digitalen Sicherheit sind nicht aufwändig in der Umsetzung, aber wirkungsvoll für den Schutz Ihrer digitalen Daten und Wertgegenstände.

Besuchen Sie unsere Website: www.digital-sicher.nrw

Adresse

Standort Bochum
Lise-Meitner-Allee 4
44801 Bochum

Standort Bonn
Rheinwerkallee 6
53227 Bonn

Kontakt

 +49 234 - 5200 7334
 info@digital-sicher.nrw

Social Media



**DIGITAL
SICHER
NRW**