



Spionage . Sabotage . Cyberangriffe

„Ihre Daten im Visier“

24. Juni 2024

GELSEN-NET - Gelsenkirchen

Henning Voß

Abteilung Verfassungsschutz

Referat Wirtschaftsschutz



Inland

Ausland

Bundesamt für
Verfassungsschutz
– BfV –

Landesbehörden für
Verfassungsschutz
– LfV –

Militärischer
Abschirmdienst
– MAD –

Bundesnachrichtendienst
– BND –





Rechtsextremismus

Linksextremismus

Auslandsbezogener Extremismus

Islamismus

Spionageabwehr / Wirtschaftsschutz



Wirtschaftsspionage

Cyber-Kriminalität

Konkurrenzausspähung

Hybride Bedrohung

Sabotage (insb. KRITIS)

Analogie: Schäden durch Spionage, Sabotage und Datendiebstahl in der Wirtschaft

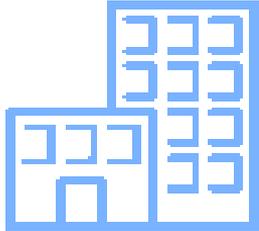


Deutschland ca. 208,6 Mrd.
NRW ca. 48 - 55 Mrd.

Quelle: Digitalverband Bitkom vom 01.09.2023



neun von zehn
Unternehmen



KMU

nicht DAX 30 Konzerne

VS NRW - VS NRW - VS NRW

nahezu alle Branchen

Schwerpunkte u.a. in den Bereichen
Maschinenbau, Automobil, Energie



Der Fall Bezos zeigt: Im Digitalzeitalter
sich die Spionage verändert
Das Beispiel von Amazon-Chef Jeff Bezos zeigt: Manager
und Unternehmer leben gefährlich. Die neue Bedrohung
kommt über ihr Mobiltelefon.

Vassungsschutz warnt: China wirbt
Spione über LinkedIn an
Soziale Netzwerke sind längst in den Fokus ausländischer
heimdienste gerückt. Aktuell sieht der Verfassungsschutz
LinkedIn im Visier chinesischer Spione.



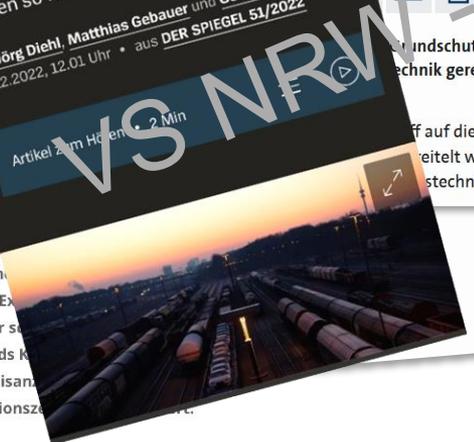
**Neuer Sabotageangriff auf
Steuersysteme der Bahn –
Staatsschutz ermittelt**
Durchtrennte Kabel
Die Bahn ist erneut Opfer eines
Sabotageangriffs geworden. Nach SPIEGEL-
Informationen durchtrennten Unbekannte in
Essen mehrere Kabelverbindungen und
sorgten so für Ausfälle im Steuerungssystem.
Von Jörg Diehl, Matthias Gebauer und Gerald Trauffetter
16.12.2022, 12.01 Uhr • aus DER SPIEGEL 51/2022

Angriff auf Uniklinik Düsseldorf hätte
verhört werden können



Wundschutz hätte laut Bundesamt für Sicherheit in der
Technik gereicht, um die Folgen des Angriffs zu verhindern.

Angriff auf die Düsseldorfer Uniklinik hätte mit einfachen
Maßnahmen verhindert werden können. Das teilt das Bundesamt für Sicherheit
in der Informationstechnik (BSI) mit.



MEISTGELESENE
Michael Bloomberg

ZfK
Zeitung
für kommunale
Wirtschaft

**"Cyberangriffe aus Russland
eine ernstzunehmende
Gefahr"**

Der Bundesverband zum Schutz Kritischer
Infrastrukturen (BSKI), aber auch Politiker warnen
angesichts der politischen Lage in der Ukraine vor
Cyber-Attacken. Kanzler Scholz will die Resilienz von
kritischen Infrastrukturen stärken.

27.02.2022



...e über
...t
...neue Angriffstechnik
in Firmennetze ein.
190



Die Regierungskoalition ist laut Grünen-
Bundesparteichef Omid Nouripour dabei, sich
auf mögliche Hacker-Angriffe auch auf die
kritische Infrastruktur in Deutschland
vorzubereiten.



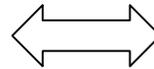
Zeitenwende

VS NRW - VS NRW - VS NRW

24.02.2022



**Nachrichtendienste
fremder Staaten**



**ausländische
Wirtschaft**

„Angreifer“ ?



„Geheimdienste müssen einheimische Unternehmen im Ausland unterstützen. (...) So sollten der SWR und andere russische Geheimdienste ihr technisches und intellektuelles Potential aktiver einsetzen.“
(PUTIN in Ria Novosti)

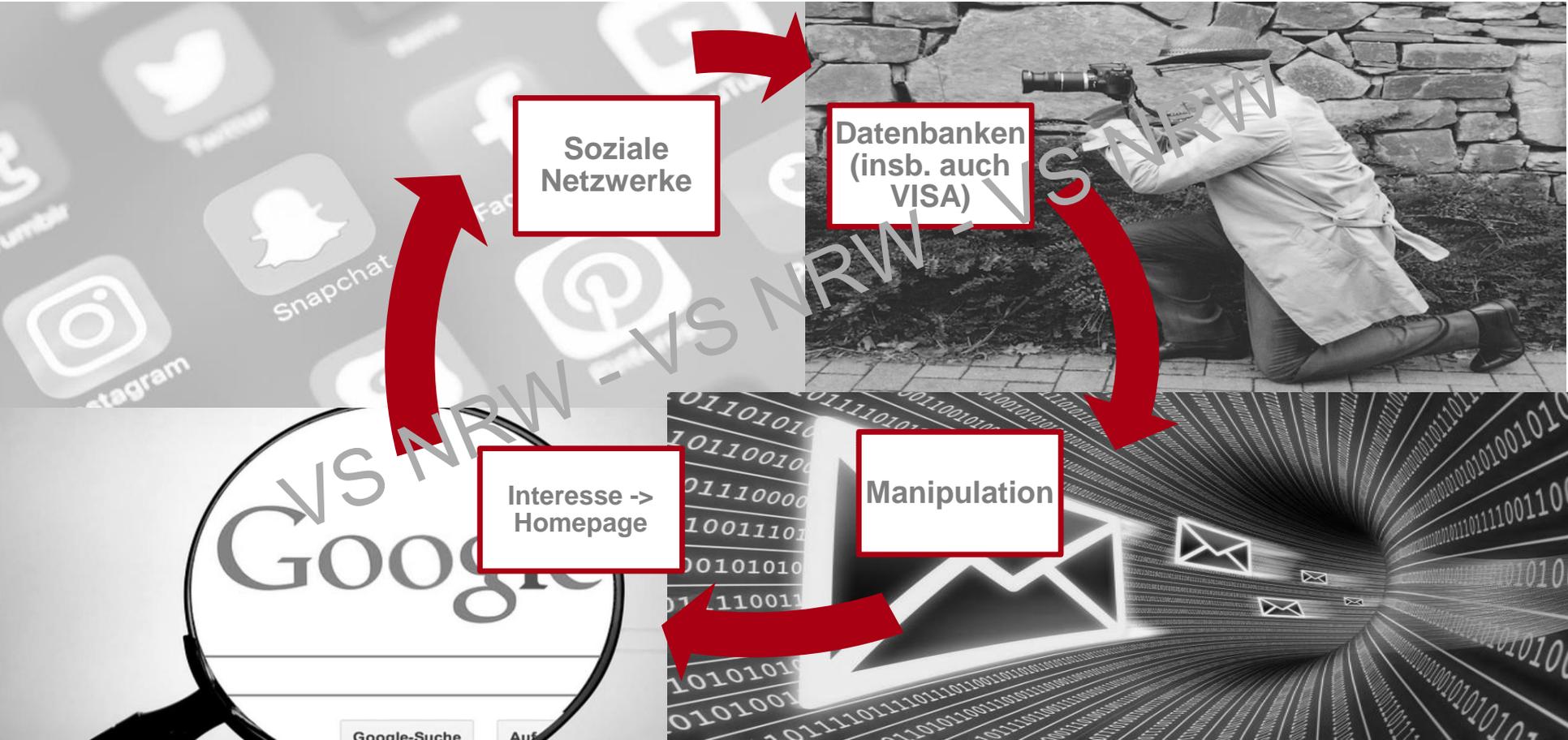
"Ich denke, dass der Staat bei der Beschaffung moderner Technologien aus dem Ausland unterstützend tätig sein muss."
(Auszug aus der Rede von Präsident PUTIN zur Lage der Nation)



Sorm 2
(Sistema Operativno-Rozysknykh Meropriyatii)



„Spionage“, die (noch) keine ist...





Schadsoftware
(als Anhang einer E-Mail – „Trojaner“)



USB-Sticks



(kompromittierte)
**Notebooks / Tablets /
Smartphones**

Schäden begrenzen

Ministerium des Innern
des Landes Nordrhein-Westfalen



Ganzheitliches Sicherheitskonzept





1. Organisatorische Schutzmaßnahmen

- 1.1 Richtlinien und Anweisungen
- 1.2 Notfall- und Krisenkonzepte
- 1.3 Sicherheitsanalyse und -konzepte
- 1.4 Externe Absicherungsmaßnahmen

2. Personalbezogene Schutzmaßnahmen

- 2.1 Zuständigkeiten
- 2.2 Integritätsprüfung
- 2.3 Sensibilisierung und Schulung

3. Cyberangriffsschutz

- 3.1 Verschlüsselung
- 3.2 Zugriffsschutz
- 3.3 Schutz vor Cyberattacken und Datenverlust

4. Physischer Gebäudeschutz

- 4.1 Äußerer Schutz des Gebäudes und Betriebsgelände
- 4.2 Schutz innerhalb des Gebäudes



ENTEGA.ag Karriere

Über ENTEGA

DATENSCHUTZ UND INFORMATIONSSICHERHEIT

- + Gab es ein Datenleak?
- + Ist die Datenschutzbehörde informiert?
- + Welche personenbezogenen Daten sind veröffentlicht worden?
- + Was sollte ich als Betroffener(r) des Datenleaks jetzt tun?
- + Welche Konsequenzen drohen mir, wenn meine Daten unbefugt verwendet werden?
- + Ich habe einen Anruf von der ENTEGA Abwasserreinigung GmbH & Co. KG erhalten. Darin wurde mir mitgeteilt, dass ich vom Datenleak betroffen sei und nun beraten werden soll.
- + Welche Maßnahmen hat die ENTEGA Abwasserreinigung GmbH & Co. KG für die Zukunft ergriffen?
- + Wurden die zuständigen Behörden rechtzeitig informiert?
- + Warum wurde der Sicherheitsvorfall nicht sofort öffentlich gemacht?

PRESEMITTEILUNG

Daten von Cyberkriminalität

CYBERANGRIFF

- + Was ist über...
- + Was weiß...
- + Gab es eine...
- + Womit hat...
- + Konnten di...

INFORMATIONSSICHERHEIT

Der IT-Dienstleister ENTEGA Abwasserreinigung GmbH & Co. KG hat die Pressemitteilung über den Folgen der Informationssicherheitsvorfälle der ENTEGA...



Aufklärung und
Sensibilisierung

VS NRW - VS NRW - VS NRW



Initialberatung
für Sicherheits-
konzepte



Ministerium des Innern
des Landes Nordrhein-Westfalen

Wir unterstützen kompetent vertraulich kostenlos

Schützen Sie Ihr Unternehmen!

Extremismus-Prävention und Wirtschaftsschutz

Vortrags- und Workshop-Angebote des Verfassungsschutzes

Kostenlose Informations- und Sensibilisierungsveranstaltungen für Unternehmen

Die nordrhein-westfälische Verfassungsschutz klärt mit Vorträgen und Fortbildungen zu extremistischen Bestrebungen Ideologien auf und unterstützt bei der Vermittlung von Hilfsangeboten.

Zudem sensibilisiert er vor den Gefahren durch Spionage und Sabotage, um die Eigenschutzmechanismen von Unternehmen zu aktivieren.

Die nächsten Schritte

1. Relevante Bereiche in der eigenen Organisation bzw. im Unternehmen identifizieren
2. Passende Präventionsangebote auswählen
3. Kontakt zum Wirtschaftsschutz aufnehmen
4. Gemeinsam einen Zeitplan erstellen

Kontakt zum Wirtschaftsschutz

Der Wirtschaftsschutz ist der zentrale Ansprechpartner für Unternehmen im nordrhein-westfälischen Verfassungsschutz. Er ist zu erreichen unter:

- Telefon 0211 071-2021
- wirtschaftsschutz@iml.nrw.de
- www.iml.nrw/wirtschaftsschutz

Wir freuen uns auf Ihre Zusammenarbeit!

Unsere Vortrags- und Workshop-Angebote in den Extremismus-Bereichen richten sich an die folgenden Zielgruppen:

- AZ - Auszubildende allgemein oder besonderer Fachrichtung
- MP - Multiplikatoren wie Ausbilder, Ausbildungsbeauftragte, Beschäftigte im Bereich Fortbildung
- FK - Führungskräfte (Leiter von Abteilungen oder anderen Organisationseinheiten)
- VL - Vorstand/Leitungsebene
- EX - Experten z.B. in den Bereichen Personalwesen, IT, Organisation, Forschung und Entwicklung
- SO - Sonderfunktionen wie z.B. Diversitäts-/Gleichstellungsbeauftragte, Soziale Ansprechpartner, Geheimenschutzbeauftragte

Angebote zum Rechtsextremismus und zu Delegitimierung des Staates

REX Basis
Aufklärung und Sensibilisierung zu Erscheinungsformen des Rechtsextremismus
Empfohlene Zielgruppen: AZ, MP, FK, EX, SO
Vortragsgespräch (90 - 100 Minuten)

REX Experte
Aufklärung und Sensibilisierung zu Erscheinungsformen des Rechtsextremismus, Informationen zu Vorfällen, Fragen der Teilnehmenden
Empfohlene Zielgruppe: AZ
Vortragsgespräch (ca. 2 Unterrichts- oder Zertifikatsgespräch/Fragerunde (90-100 Minuten))

Angebote zum **Wirtschaftsschutz** - jeweils Vortragsgespräch (45-90 Minuten) -

WiSchutz Basis

Gefahren von Spionage, Sabotage und Cyberkriminalität, Tipps für einen grundlegenden Schutz am eigenen Arbeitsplatz
Empfohlene Zielgruppen: alle Beschäftigten, heterogene Teilnehmergruppen möglich

WiSchutz Ausbildung

Gefahren von Spionage, Sabotage und Cyberkriminalität
Empfohlene Zielgruppen: Auszubildende, Trainees, Werkstudenten

WiSchutz Entscheider

Sensibilisierung von Entscheidungsträgern (insb. in KMU), den Prozess zur Verbesserung der Unternehmenssicherheit ganzheitlich und individuell zu gestalten
Empfohlene Zielgruppen: Leitungsebene (Vorstand, Geschäftsführung, Aufsichtsräte, Abteilungsleitungen), Sonderfunktionen (CIO, CSO)

WiSchutz Cyber

Sensibilisierung von Beschäftigten, die in Bereichen der Informationstechnik eingesetzt sind bzw. für einen solchen Bereich Verantwortung tragen
Empfohlene Zielgruppen: CIO oder vergleichbare Funktion, IT-Personal

WiSchutz Auslandskontakte

Gefahren bei Geschäftsreisen und allgemein bei Auslandskontakten
Empfohlene Zielgruppen: Geschäftsführungen und (leitende) Angestellte in sensiblen Arbeitsbereichen, im Ausland Beschäftigte, Personen mit Kontakten zu ausländischen Delegationen

WiSchutz KRITIS

Risiken und Herausforderungen für Unternehmen der sogenannten kritischen Infrastrukturen im Bereich Unternehmenssicherheit
Empfohlene Zielgruppen: Verantwortliche in KRITIS-Unternehmen bzw. in vergleichbaren Unternehmen mit ähnlich hohem Schutzbedarf

WiSchutz Besuchermanagement

Geeignete Regelungen und deren Umsetzung im Bereich des Besuchermanagements
Empfohlene Zielgruppen: Beschäftigte im Bereich Besuchermanagement

WiSchutz Mensch (HR-Abteilung)

Sensibilisierung von Beschäftigten im Personalbereich
Empfohlene Zielgruppen: HR-Manager, Personalreferenten, -sachbearbeiter und -entwickler, Ausbildungsleitungen



**Vielen Dank für Ihre Aufmerksamkeit.
Fragen? Jetzt! Oder auch später vertraulich....**

Henning Voß

Abteilung Verfassungsschutz

Referat Wirtschaftsschutz

Mail: henning.voss@im1.nrw.de

Mail: wirtschaftsschutz@im1.nrw.de

Telefon: 0211 871 2835