T.I.S.P. Community Meeting 2023

Berlin, 07. - 08.11.2023

"Wirtschaftsschutz und Cyberbedrohungen"

Henning Voß, Ministerium des Innern NRW, Verfassungsschutz

Ministerium des Innern
des Landes Nordrhein-Westfalen

Spionage . Sabotage . Cyberangriffe

„Wirtschaftsschutz und Cyberbedrohungen“

07. November 2023
T.I.S.P. Community Meeting | Berlin

Henning Voß
Abteilung Verfassungsschutz
Referat Wirtschaftsschutz

Nachrichtendienste in Deutschland

Ministerium des Innern
des Landes Nordrhein-Westfalen

Inland **Ausland**

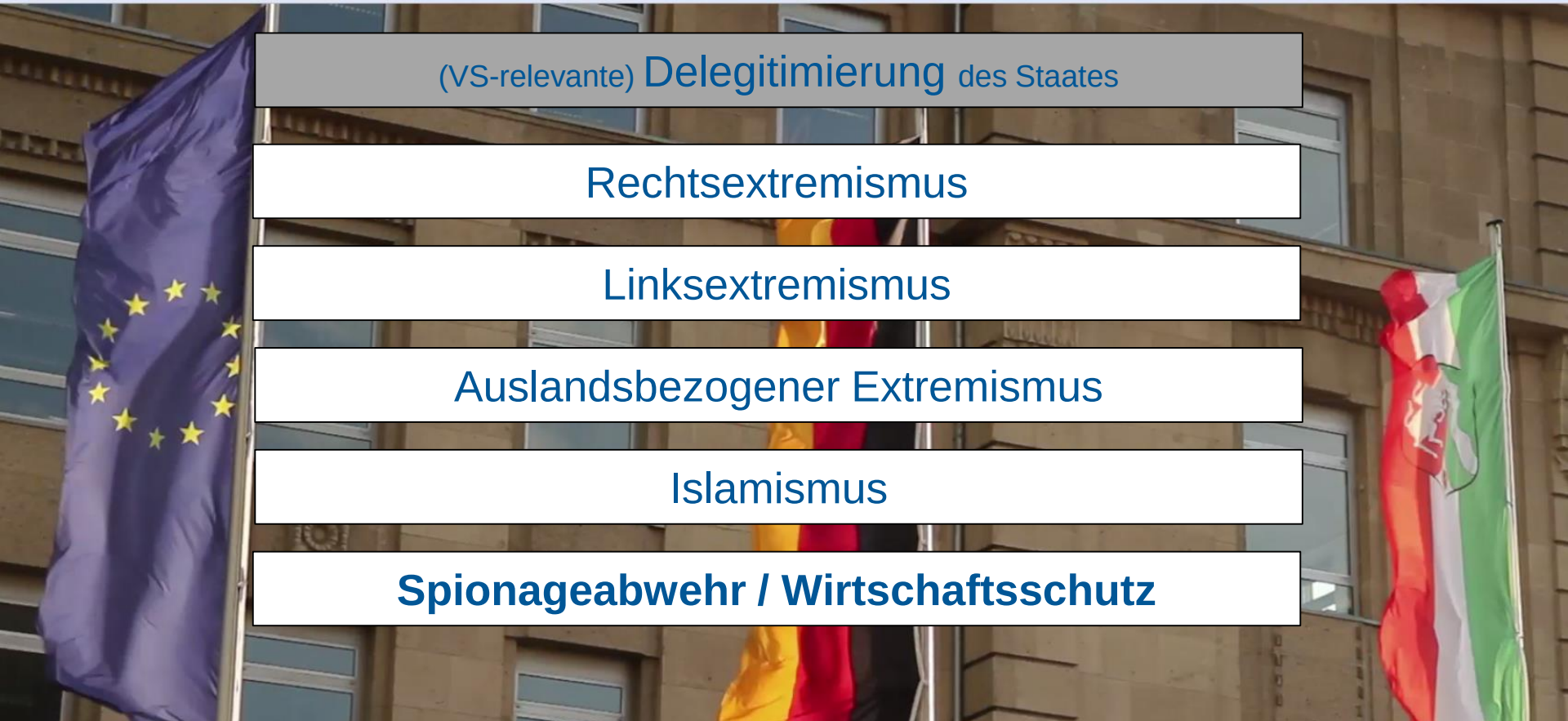
Bundesamt für Verfassungsschutz
– BfV –

Landesbehörden für Verfassungsschutz
– LfV –

Militärischer Abschirmdienst
– MAD –

Bundesnachrichtendienst
– BND –

Ministerium des Innern
des Landes Nordrhein-Westfalen



(VS-relevante) **Delegitimierung** des Staates

Rechtsextremismus

Linksextremismus

Auslandsbezogener Extremismus

Islamismus

Spionageabwehr / Wirtschaftsschutz

Wirtschaftsschutz: Prävention

Ministerium des Innern
des Landes Nordrhein-Westfalen

BUND

LAND

Bedrohungen

Wirtschaftsspionage

Cyber-Kriminalität

Konkurrenzausspähung

Hybride Bedrohung

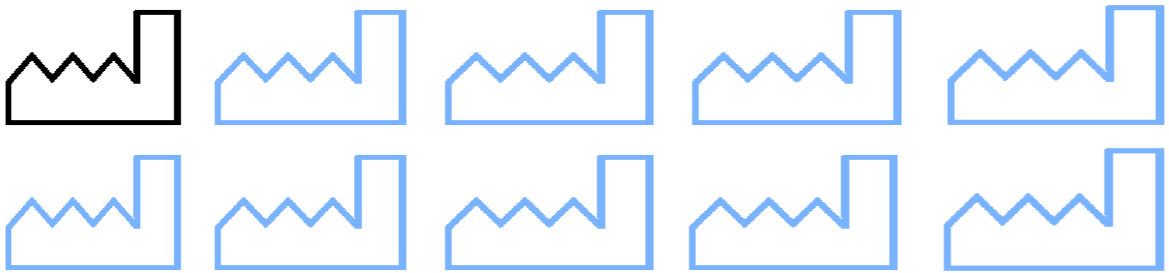
Sabotage (insb. KRITIS)

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

Ministerium des Innern
des Landes Nordrhein-Westfalen

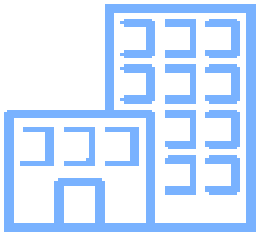
Deutschland ca. 208,6 Mrd.
NRW ca. 48 - 55 Mrd.

Quelle: Digitalverband Bitkom vom 01.02.2023



neun von zehn Unternehmen

Hauptangriffsziele



KMU

nicht DAX 30 Konzerne

nahezu alle Branchen

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

Ministerium des Innern
des Landes Nordrhein-Westfalen

Handelsblatt Handelsblatt Premium FÜR 1 € TESTEN »

KOMMENTAR

Der Fall Bezos zeigt: Im Digitalzeitalter h… sich die Spionage verändert

Das Beispiel von Amazon-Chef Jeff Bezos zeigt: Manager und Unternehmer leben gefährlich. Die neue Bedrohung kommt über ihr Mobiltelefon.

WDR

Wetter Verkehr im WDR such…

Nachrichten Sport Wissen Verbraucher Kultur Unterhaltung

…rangriff auf Uniklinik Düsseldorf hätte …ehrt werden können

…Grundschutz hätte laut Bundesamt für Sicherheit in der …chnik gereicht, um die Folgen des Angriffs zu verhindern.

…f auf die Düsseldorfer Uniklinik hätte mit einfachen …eitelt werden können. Das teilt das Bundesamt für Sicherhe… …stechnik (BSI) mit.

Wie groß ist d… auf die kritisch… beschäftigt IT-Ex… Behörden zwar s… durch Russlands K… nochmal an Brisan… IT-Krisenreaktionsze…

MEISTGELESE…

Michael Bloomb…

Zurück

Durchtrennte Kabel

Neuer Sabotageangriff auf Steuersysteme der Bahn – Staatsschutz ermittelt

Die Bahn ist erneut Opfer eines Sabotageangriffs geworden. Nach SPIEGEL-Informationen durchtrennten Unbekannte in Essen mehrere Kabelverbindungen und sorgten so für Ausfälle im Steuerungssystem.

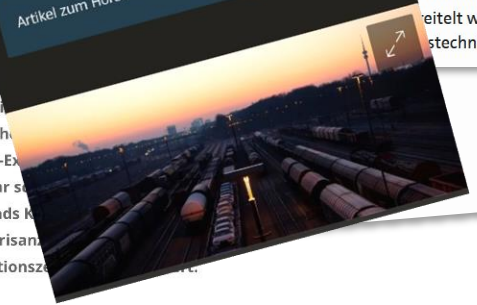
Von Jörg Diehl, Matthias Gebauer und Gerald Traufetter
16.12.2022, 12.01 Uhr • aus DER SPIEGEL 51/2022

Artikel zum Hören • 2 Min

Aktuelles

EIN CYE… „KOLLA…

Von Green Planet



Handelsblatt Handelsblatt Premium FÜR 1 € TESTEN »

KARRIERENETZWERK

…Vassungsschutz warnt: China wirbt Spione über LinkedIn an

…oziale Netzwerke sind längst in den Fokus ausländischer …heimdienste gerückt. Aktuell sieht der Verfassungsschutz … LinkedIn im Visier chinesischer Spione…

…e über …t

…eue Angriffstechnik …in Firmennetze ein.

190

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

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

Aktuell: Verschärfung der Bedrohungslage

Ministerium des Innern
des Landes Nordrhein-Westfalen

Ministerium des Innern
des Landes Nordrhein-Westfalen

Cyberangriff auf Entega

Hacker verö

Energievers

reb/dpa 20.07.2022 - 16:02 Uhr

Hacker haben d
abgegriffen. (Sy

Ein Tochter
wurde von
Kundendat
Bankverbi

SPI

Me

Cyberattacken auf westliche

rch prorussische

Attack

e Cyber-
gen einen
ss man ein Baustein in der
n Europa sei, so die norwegische

hörde.

tagesschau

Sendung verpasst?

"Russland ist in unseren Netzen"

Stand: 28.07.2022 05:02 Uhr

Seit Jahren warnen deutsche Behörden vor einer Hackergruppe, die gezielt das Stromnetz ausspioniert. Ermittlern ist es gelungen, einen mutmaßlichen Täter zu identifizieren. Die Spur führt zum russischen Geheimdienst FSB.

Von Hakan Tanriverdi, BR, und Florian Flade, WDR

Es war eine breit angelegte Spionageoperation, bei der allein in Deutschland mehr als 150 Unternehmen gehackt werden sollten - vor allem aus dem Bereich der sogenannten Kritischen Infrastrukturen. Konkret ging es den Hackern darum, die Strom- und Wasserversorgung auszukundschaften. Nach Informationen von *BR* und *WDR* ist es dem Landeskriminalamt Baden-Württemberg nach jahrelangen Ermittlungen gelungen, einen der mutmaßlichen Täter zu identifizieren.

Angreifer / Auftraggeber





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)

Hacking im Staatsauftrag

staatlich unterhaltene und gesteuerte Hackergruppierungen

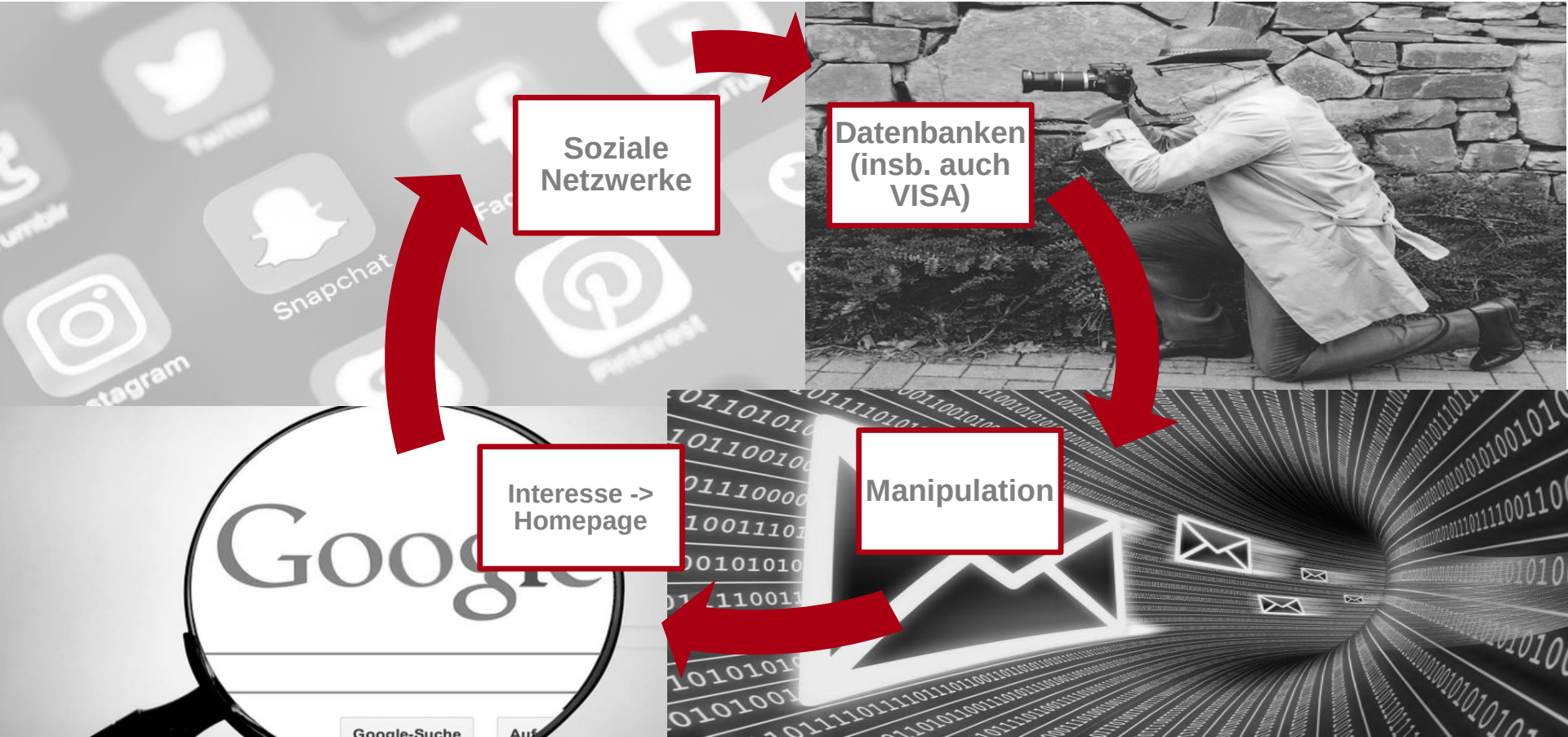
- großes technisches Know-how
- hohe personelle und finanzielle Ressourcen
- Advanced Persistent Threads (APT)

Ziele

- Ausspionierung von Know-how und Technologien
- Kompromittierung von IT-Infrastruktur
  für spätere Angriffe

„Spionage“, die (noch) keine ist…

Ministerium des Innern
des Landes Nordrhein-Westfalen



Wirtschaftsspionage – Die Methoden

Ministerium des Innern
des Landes Nordrhein-Westfalen

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

USB-Sticks

(kompromittierte)
Notebooks / Tablets / Smartphones

Wirtschaftsspionage – Die Methoden

„Neue Methoden – Neue Gefahren“

China: Apple bekommt eigene Wächter fürs iCloud-Rechenzentrum

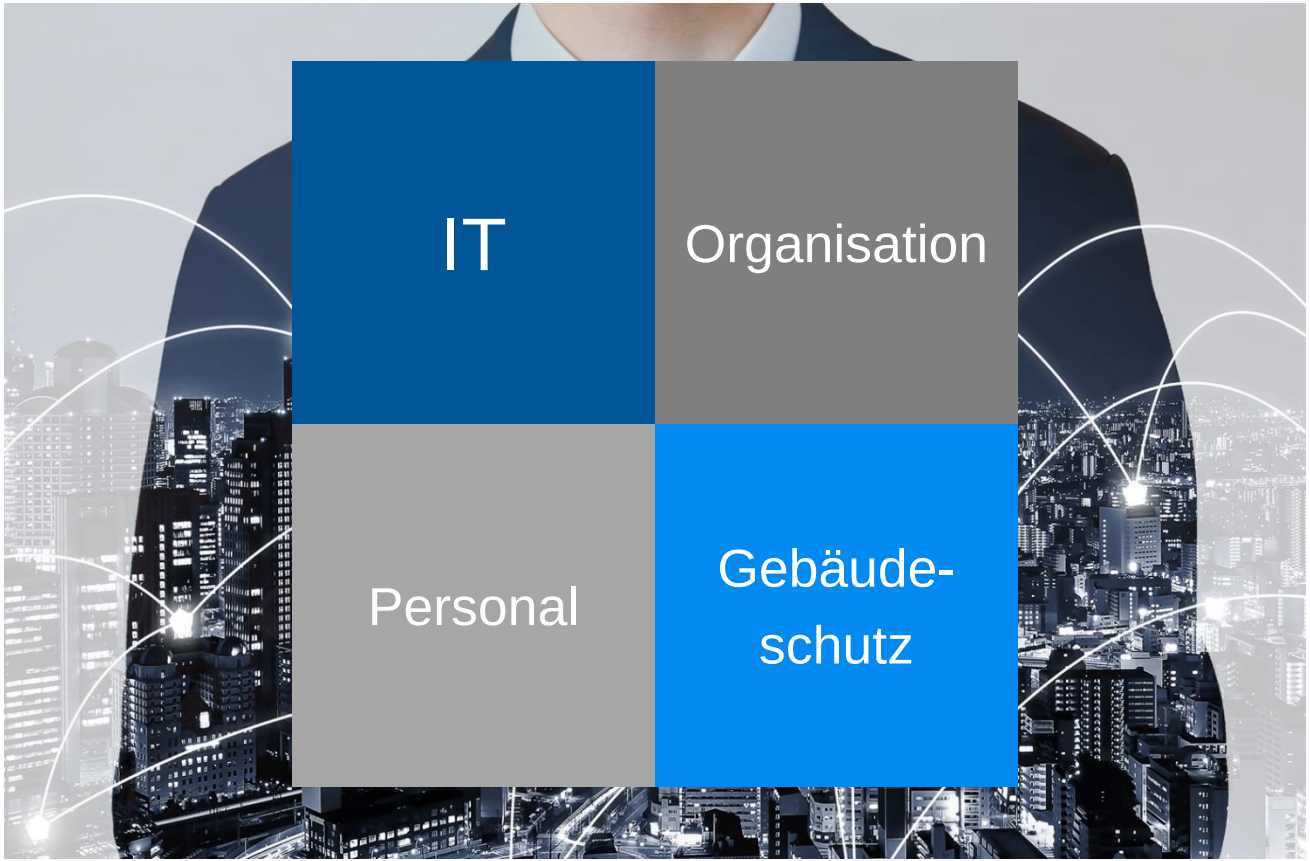
15.08.2017 10:25 Uhr – Ben Schwan vorlesen

Eine von der chinesischen Regierung eingesetzte Kommission soll dafür sorgen, dass der iPhone-Konzern sein Projekt "beschleunigen" kann. Das Land hatte kürzlich seine Cybersecurity-Gesetze verschärft.

Schäden begrenzen

Ganzheitliches Sicherheitskonzept

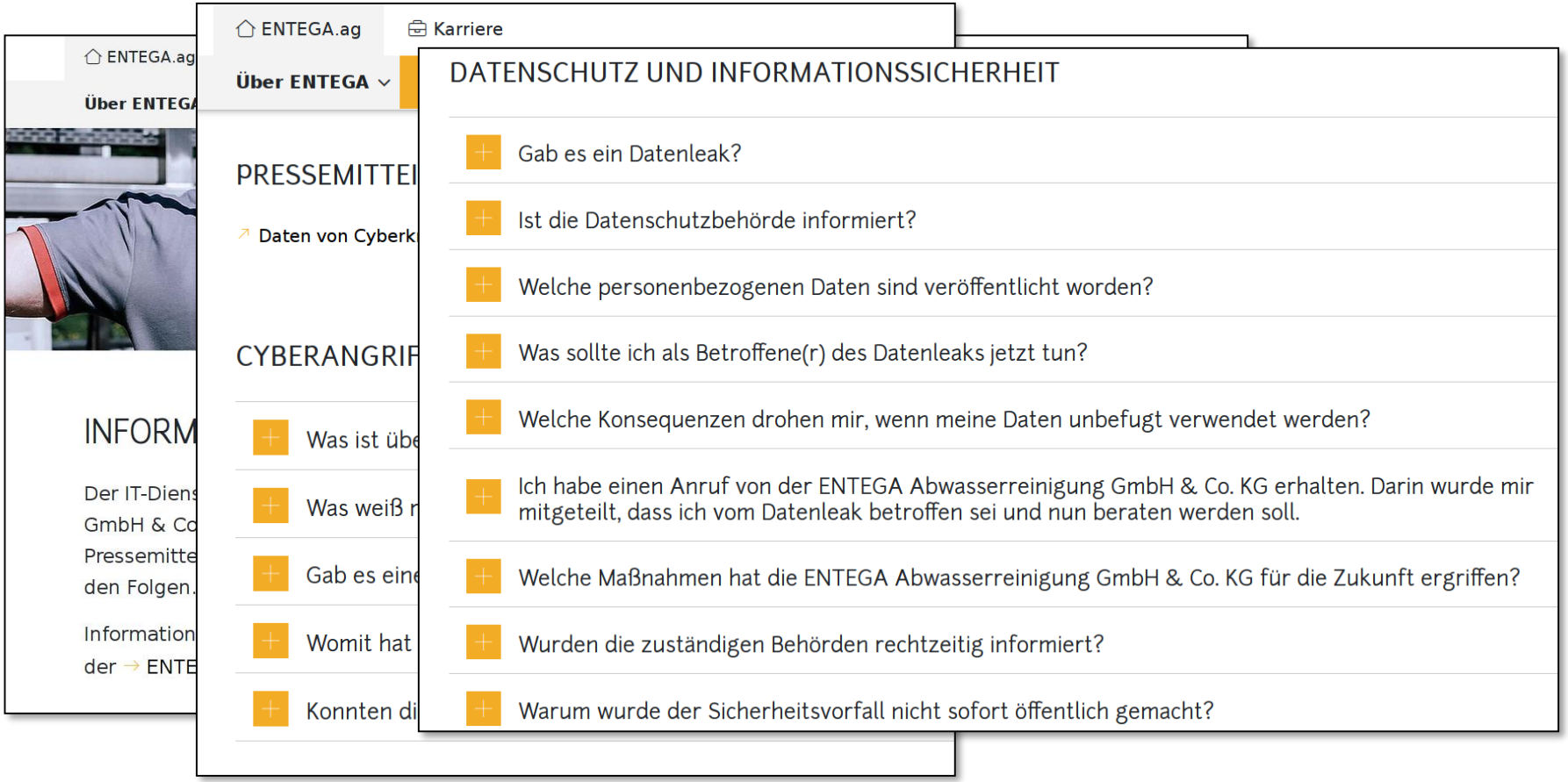
Ministerium des Innern
des Landes Nordrhein-Westfalen



Dimensionen und Indikatoren

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

Vorbereitung auf den Notfall



Organisation – Lösungen statt Verbote

Personal – besondere Gefahr „Innentäter“

UMFRAGE: RISKANTES ONLINE-VERHALTEN AM ARBEITSPLATZ

Trend Micro belegte mit einer Umfrage, dass viele IT-Anwender in Großunternehmen am Arbeitsplatz ein wesentlich riskanteres Online-Verhalten an den Tag legen als zu Hause [TrM].

- *39 % aller Befragten glauben, dass ihre IT-Abteilung sie davor bewahrt, Opfer von Spyware- oder Phishing-Bedrohungen zu werden.*
- *In Deutschland gaben 76 % zu, dass sie verdächtige E-Mails oder Internetlinks eher am Arbeitsplatz als zu Hause öffnen, da Sicherheitssoftware auf ihrem Rechner installiert sei.*
- *29 % der deutschen Mitarbeiter gaben an, dass sie deswegen verdächtige Inhalte am Arbeitsplatz öffnen, da es sich bei der Computer-Ausstattung nicht um ihr Eigentum handelt.*

Kostenfreie Angebote

Wirtschaftsschutz

als staatliches Präventionsprogramm

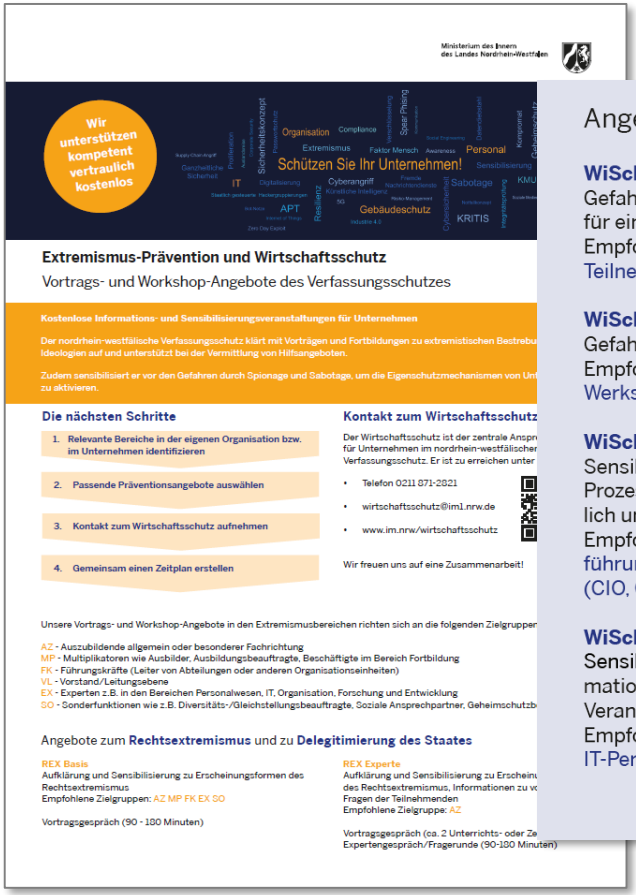
Aufklärung und
Sensibilisierung

Transparenz für
Eigenverantwortung
und rechtliche
Pflichten

Initialberatung
für Sicherheits-
konzepte

Kostenfreie Angebote des Wirtschaftsschutzes

Ministerium des Innern
des Landes Nordrhein-Westfalen



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