Kompetenzzentrum
Energieeffizienz
durch Digitalisierung

18. Juni 2026

Herzlich willkommen zum KEDi-Webinar

Fit für NIS-2:

Cybersicherheitsstrategien für Industrie-KMU

Ein Projekt der

dena

Begrüßung & Einführung

Allgemeine Informationen

Webinar wird aufgezeichnet

Fragen gerne im Chat stellen

Mikrofone sind stumm geschalten

Vortragsfolien erhalten Sie im Nachgang

Allgemeine Informationen

- **Fortbildungsanerkennung**: Als Energieeffizienzexpertin oder -experte können Sie sich die Teilnahme am Webinar als Fortbildung anerkennen lassen.
- Anfrage an info@kedi-dena.de: Wir senden Ihnen die Teilnahmebescheinigung nach dem Webinar zu.

Kompetenzzentrum für Energieeffizienz durch Digitalisierung (KEDi)

KEDi: ein Projekt der Deutschen Energie-Agentur (dena)

Seit 2023 agiert das KEDi als **bundesweite Anlaufstelle** mit Sitz in Halle (Saale). Das KEDi unterstützt **Industrie-KMU** und die **Gebäudewirtschaft**, **Energieeffizienzpotenziale mit digitalen Anwendungen** besser zu erschließen.

Angebote – Produkte – Tools (Auswahl)

- **EMS-Finder**: Auswahl einer Energiemanagementsoftware
- **Förderwegweiser**: Suche nach passenden Fördermöglichkeiten
- **Showcases**: praxisrelevante Beispiele realer Unternehmen
- **Demonstrator:** interaktives, haptisches Modell für industrielle Energie- und Datenflüsse

Agenda

Einführung: NIS-2
Jörg Erdsack | KEDi

Cybersicherheit in KMU: Betroffenheitsprüfung, CyberRisikoCheck
Marius Dechand | dena

Diagnose: Cyberangriff
Romy Fieblinger | Digifors

Zeit für Fragen und Diskussion

Future Energy Lab

Cybersicherheit in KMU

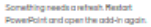
Ein Projekt der dena

Einführung

- Wir sprechen praxisnah über alle Schritte bis zur Umsetzung von Maßnahmen
  - 1. Betroffenheitsprüfung
  - 2. Registrierung BSI
  - 3. Pflichten verstehen & Maßnahmen identifizieren
  - 4. Umsetzung & Dokumentation
- Ich bin kein IT-Berater. Meine Inhalte beziehen sich auf frei verfügbare Ressourcen. Alle Quellen werden verlinkt.

Bin ich von NIS-2 betroffen?

- BSI NIS-2 Betroffenheitsprüfung
  - https://www.bsi.bund.de/dok/nis-2-betroffenheitspruefung



- Falls nein: CyberRisikoCheck
  - https://transferstelle-cybersicherheit.de/cyberrisiko-check/
  - https://www.bsi.bund.de/dok/crc

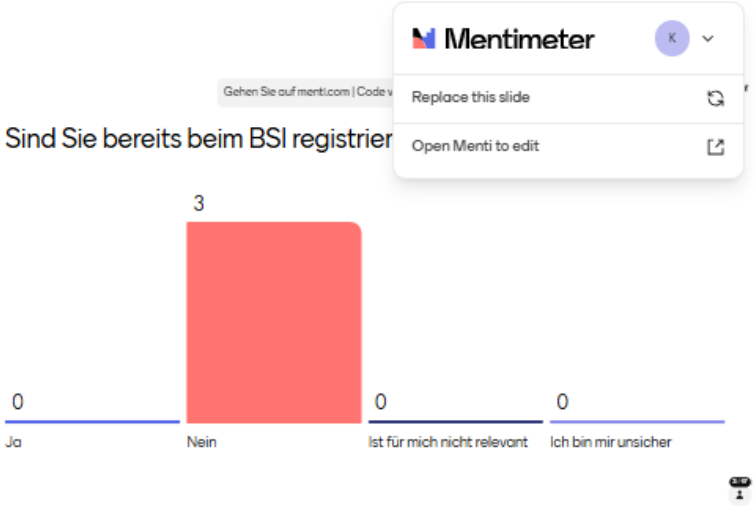
Future Energy Lab

CyberRisikoCheck

- Von BSI und BVMW mit einem Konsortium ca. 20 Organisationen als Standard (Beratungsstandard DIN SPEC 27076) entwickelt
- Hilft bei der Feststellung des Sicherheitsniveaus und Identifikation von „low hanging fruits“
- Wird normalerweise im Rahmen eines Beratungsgesprächs von einem IT-Dienstleister durchgeführt (förderfähig)
- Tipp: DIN Standard runterladen und intern durchsprechen

Registrierung beim BSI

- Registrierung Mein Unternehmenskonto (MUK)
  - https://info.mein-unternehmenskonto.de/
  - Aktivierungsdaten per E-Mail; **Aktivierungsbrief per Pos**t -> man kann nicht sofort loslegen
- Registrierung BSI-Portal
  - https://portal.bsi.bund.de/
  - ELSTER Zertifikat notwendig für Authentifizierung
  - Ähnliche Angaben wie in der Betroffenheitsprüfung zur autom. Einstufung
  - Angaben zum Unternehmen (Name, Rechtsform, Handelsregisternummer, Anschrift, Kontaktdaten, **öffentliche IP-Adressbereiche**, Sektor, Auflistung EU-Mitgliedstaaten in denen man tätig ist, zuständige Aufsichtsbehörde)
  - Kontaktdaten einer Kontaktperson



Pflichten verstehen & Maßnahmen identifizieren

- BSI-Gesetz §30 - §42 durchlesen
  - https://www.gesetze-im-internet.de/bsig_2025/
  - Tipp: Bei LLM hochladen, anweisen sich nur darauf zu beziehen und Fragen zum Gesetz stellen. Best Practices im Umgang mit LLMs berücksichtigen!
- Maßnahmen identifizieren & priorisieren
  - Einstieg: CyberRisikoCheck
  - Fortgeschritten: GAP-Analyse zu Vorgaben der NIS-2 anhand von Umsetzungsempfehlungen
    - Annex zur NIS2-Umsetzungsverordnung der Europäischen Kommission: https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj?locale=de
    - ENISA Technical Guideline auf Basis des Annex: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance
  - Einbezug von IT-Dienstleister sinnvoll!

Future Energy Lab

Vielen Dank

Marius Dechand
marius.dechand@dena.de

Ein Projekt der dena

KEDi
Kompetenzzentrum
Energieeffizienz
durch Digitalisierung

Jörg Erdsack | KEDi | 18. Juni 2026

NIS-2-Umsetzungsgesetz und KMU

Einführung und Grundlagen

Ein Projekt der
dena

Rechtliche Rahmen

EU

D

EU-Richtlinie

NIS 2
EU 2022/2555

EU-Richtlinie

CER
EU 2022/2557

EU-Verordnung

CRA
EU 2024/2847

Umsetzung in nationales Recht

(keine Umsetzung in nationales Recht)

NIS2UmsuCG
Dezember 2025

KMU in bestimmten Sektoren

Prozesse

KRITISDachG
Februar 2026

für Versorger > 500.000 Personen

Prozesse

Technische Richtlinie
TR-03183 (BSI)

KMU potenziell betroffen

Produkte

Ist Ihr Unternehmen von NIS 2 betroffen?

Unternehmen

betreibt eine kritische Anlage nach KRITISDachG

- Energie
- Transport und Verkehr
- Finanzen, Versicherungen
- Gesundheit
- Wasser
- IT und Telekommunikation
- Ernährung
- Entsorgung
- Weltraum

Betreiber kritischer Einrichtung

und ist tätig in

NIS2UmsuCG Anlagen 1, 2

NIS-2-Sektoren aus Anlage 1

- Energie
- Transport und Verkehr ohne Post-/Kurierdienste
- Finanzwesen
- Gesundheit
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Weltraum

≥ 250 MA

oder

> 50 € Umsatz und > 43 Mio. € Bilanz

wird zu

besonders wichtige Einrichtung

NIS-2-Sektoren aus Anlage 2

- Transport und Verkehr (Post-/Kurierdienste)
- Abfallbewirtschaftung
- Chemikalien (Produktion und Handel)
- Lebensmittel (Produktion, Verarbeitung, Vertrieb)
- Verarbeitendes Gewerbe/Herstellung von Waren
- Anbieter digitaler Dienste
- Forschung

≥ 50 MA

oder

> 10 € Umsatz und > 10 Mio. € Bilanz

wird zu

wichtige Einrichtung

Quelle: KRITISDachG §4; NIS2UmsuCG § 28

NIS-2-Umsetzungsgesetz und KMU

Welche Pflichten haben betroffene Unternehmen?

NIS2UmsuCG Kapitel 2, §30-42 (Auswahl):

§ 30 Risikomanagement

- Sicherung der Diensterbringung: Sicherheitskonzept, Notfallplan, Dokumentation
- Maßnahmenpaket mit 10 Basismaßnahmen (Grundschutz) einschl. Schulung und Sensibilisierung Ihrer Mitarbeiter

§ 32 Meldepflichten

- Unverzügliche Meldung von Sicherheitsvorfällen (≤ 24 h)
- Zwischenmeldungen, Aktualisierungen, Abschlussbericht

§ 33 Registrierung

- Selbständige Registrierung (3-Monats-Frist)
- (Registrierung durch das BSI möglich)
- Dokumentation und Nachweise: Organisationsangaben, krit. Anlagen, Komponenten etc.

§ 35 Unterrichtung

- bei erheblichen Sicherheitsvorfällen Unterrichtungspflicht für Dienstempfänger (=Kunden und andere Stakeholder!) (nach Anordnung durch das BSI, ggf. via Webseite)

§ 38 Geschäftsleitung

- Haftung der Geschäftsführung
- Cybersicherheit als „Chefsache“: Pflicht der Geschäftsführungen zur Umsetzung, Kontrolle und Teilnahme an Schulungen

Welche Rechte haben betroffene Unternehmen?

NIS2UmsuCG, Kapitel 2 (§32, 36)

- Pflicht des BSI zur Bestätigung des Eingangs von Vorfallmeldungen (≤ 24 h)
- Auf Ersuchen der meldenden Einrichtung: (1) Ersthilfe zur Orientierung o d e r operative Beratung zu Abhilfemaßnahmen – (2) zusätzliche technische Hilfe
- In besonders gefährlichen Situationen *(= Sensibilisierung der Öffentlichkeit durch Veröffentlichung des Vorfalls erforderlich*): vorab Anhörung der betroffenen Organisation durch das BSI (*unter bestimmten Voraussetzungen auch ohne Anhörung*)

Nützliche Links

- 1. KEDi-Webinar zum Einstieg in NIS 2 mit FAQs (dena) KEDi Webinar | Augen auf: (Cyber)Sicher in die Zukunft
- Betroffenheitsprüfung mit dem FitNIS2-Navigator (DsiN) Start - FitNIS2-Navigator
- CYBERsicher Notfallhilfe (FZI) CYBERsicher Notfallhilfe - Unterstützung bei IT-Vorfällen, Ransomware & Cyberangriffen
- Informationen und Hilfestellungen für KMU (BSI) BSI - Kleine- und Mittlere Unternehmen
- KMU-Portal mit Grundschutzmaßnahmen (SECO) Cybersicherheit
- Allianz für Cybersicherheit (BSI) https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html
- Nationales Koordinierungszentrum für Cybersicherheit (BSI) Nationales Koordinierungszentrum für Cybersicherheit | NKCS

Kompetenzzentrum
Energieeffizienz
durch Digitalisierung

Vielen Dank für Ihre Zeit!

KEDi Newsletter

Dr. Jörg Erdsack
Tel. +49 345 - 570 28 509
E-Mail joerg.erdsack@dena.de

Mehr Info:
www.kedi-dena.de

Ein Projekt der
dena

www.kedi-dena.de/das-kedi/newsletter

DigiFors
erkennen. ermitteln. aufklären.

Diagnose: Cyberangriff

DigiFors GmbH

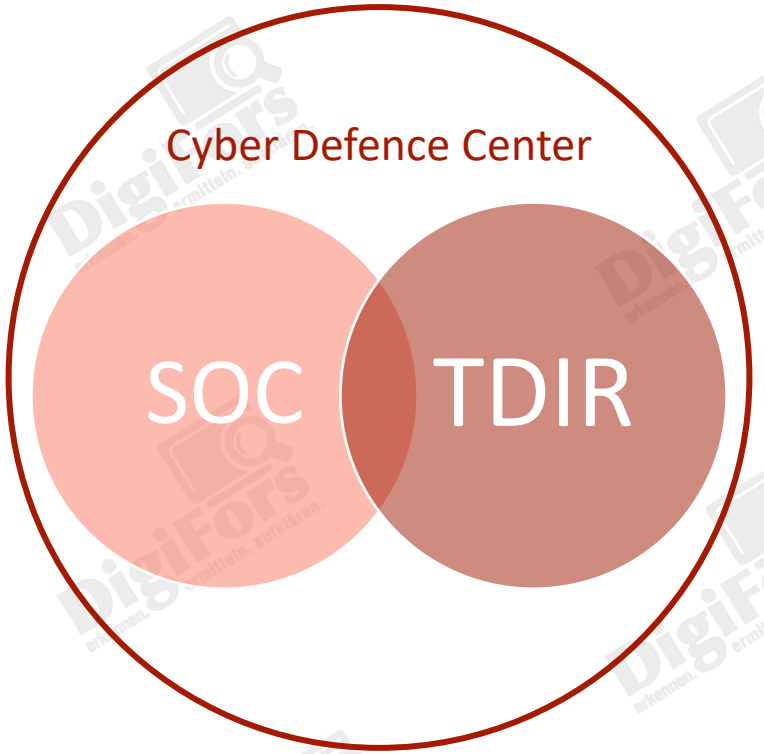
Erkennen.
Ermitteln.
Aufklären.

WIR bei DigiFors GmbH

Gegründet 2011

Hauptgeschäftsfeld:
IT-forensische Analysen

BSI APT-Response
Dienstleister



Threat Detection und Incident Response

Alle Maßnahmen zur **Erkennung, Analyse und Reaktion** auf Cyber-Bedrohungen in IT-Systemen.

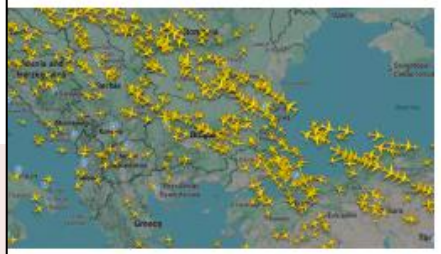
Threat Detection	Forensik & Analyse	Incident Response
Identifizierung von Anomalien & Angriffen	Untersuchung der Ursachen & Angriffswege	Maßnahmen zur Eindämmung & Behebung

Aktuelle Bedrohungslage

„Nächste Woche läuft alles wieder…“

„Betrifft uns doch nicht…“

Aktuelle Bedrohungslage



UPDATE

Massive Störung legt Flugverkehr in Griechenland lahm

Griechenlands Flughäfen waren vorübergehend lahmgelegt. Es war ungewiss, wann es weitergeht. Jetzt ist die Ursache bekannt.

04.01.2026 17 | heise online

Jaguar Land Rover nimmt Produktion wieder auf

Der britische Autobauer wurde Ende August Ziel einer Cyberattacke. Danach stand die Produktion still. Jetzt geht es langsam wieder voran.

08.10.2025 7 | heise Security

NHS England: Erster offiziell anerkannter Todesfall infolge eines Cyberangriffs

Ein Cyberangriff auf einen Pathologiedienstleister 2024 legte zahlreiche Londoner Kliniken und Praxen lahm. In der Folge kam es auch zum Tod eines Patienten.

30.06.2025 54 | heise Security

Kommentar: Russlands Cyber-Angriffe erfordern eine Reaktion

Jürgen Schmidt sprach sich lange Zeit gegen offensive Cyber-Aktionen aus. Russlands Sabotage-Angriff auf Polens Energieversorgung hat seine Meinung geändert.

20.02.2026 296 | heise Security

Trellix: Angreifer erlangten Zugriff auf Quellcode

Trellix, das aus FireEye und McAfee hervorging, hat einen IT-Vorfall gemeldet. Angreifer haben Zugriff auf Quellcode erlangt.

04.05.2026 8 | heise Security

UPDATE

Mobilfunk und Internet: Netzbetreiber nach Stromausfall im Alarm-Modus

Nach dem Anschlag auf die Stromversorgung in Berlin sind auch Mobilfunkstationen und andere Netzinfrastruktur ohne Strom. Was die Anbieter jetzt unternehmen.

07.01.2026 144 | heise online

Restore-My-Files.txt

```
LockBit 2.0 Ransomware

Your data are stolen and encrypted
The data will be published on TOR website
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4yky
https://bigblog.at if you do not pay the ransom
You can contact us and decrypt one file for free on these TOR
http://lockbitsup4yezcd5enk5unncx3zcy7kw6wllyqmiyhvanjj352jayi
http://lockbitsap2oaqhcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2di
OR
https://decoding.at

Decryption ID: [redacted]
```

Your HACKED by BlackByte team.

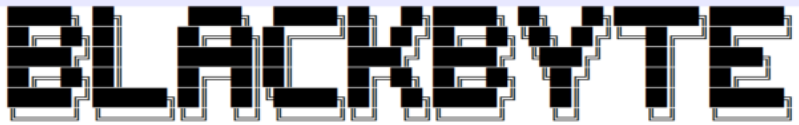
Connect us to restore your system.

Your HACKED by BlackByte team.

Connect us to restore your system.

Your HACKED by BlackByte team.

Connect us to restore your system.




```
+----------------------------------------------------------------------------+
| All your files have been encrypted, your confidential data has been stolen, |
| in order to decrypt files and avoid leakage, you must follow our steps.    |
+----------------------------------------------------------------------------+

+-----------------------------------------------------------------------------------------------------------------------------+
| 1) Download and install TOR Browser from this site: https://torproject.org/                                                 |
|                                                                                                                             |
| 2) Paste the URL in TOR Browser and you will be redirected to our chat with all information that you need.                  |
|                                                                                                                             |
| 3) If you do not contact us within 4 days, your chat access key won't be valid.                                            |
|    Also, your company will be posted on our blog, which will attract unnecessary attention from journalists and not only them. |
|    You are given 4 days to think over the situation, and take reasonable actions on your part.                             |
+-----------------------------------------------------------------------------------------------------------------------------+

+-------------------------------------------------------------------------------------------+
| Warning! Communication with us occurs only through this link, or through our mail on our blog. |
| We also strongly DO NOT recommend using third-party tools to decrypt files,               |
| as this will simply kill them completely without the possibility of recovery.             |
| I repeat, in this case, no one can help you!                                              |
+-------------------------------------------------------------------------------------------+


Your URL:
http://36

Your Key

Your Encr
[redacted]

Find our
```

```
Hello! All your files are encrypted and only I can decrypt them.
Contact me:

cryptolifeguard@tutanota.com or cryptolifeguard@cock.li

Write me if you want to return your files - I can do it very quickly!
The header of letter must contain extension of encrypted files.
I'm always reply within 24 hours. If not - check spam folder, resend your letter or try send letter from another email service (like tutanota.com).

Attention!
Do not rename or edit encrypted files: you may have permanent data loss.

To prove that I can recover your files, I am ready to decrypt any three files (less than 1Mb) for free (except databases, Excel and backups)

HURRY UP!
```

All your files have been encrypted!

ave been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail h3lp2022@proton.me
n the title of your message [redacted]
nswer in 24 hours write us to this e-mail:h3lp2022@tuta.io
y for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the tool that will decrypt all your files.

ption as guarantee

paying you can send us up to 5 files for free decryption. The total size of files must be less than 4Mb (non archived), and files should not contain valuable information.
ses,backups, large excel sheets, etc.)

tain Bitcoins

siest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
coins.com/buy_bitcoins
nd other places to buy Bitcoins and beginners guide here:
ndesk.com/information/how-can-i-buy-bitcoins/

t rename encrypted files.
t try to decrypt your data using third party software, it may cause permanent data loss.
ption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

RECOVER -FILES.txt

```
>> What happened?

Important files on your network was ENCRYPTED and now they have "zyh8sim" extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your system was DOWNLOADED.
If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Private financial information including: clients data, bills, budgets, annual reports, bank statements.
- Manufacturing documents including: datagrams, schemas, drawings in solidworks format
- And more...
```

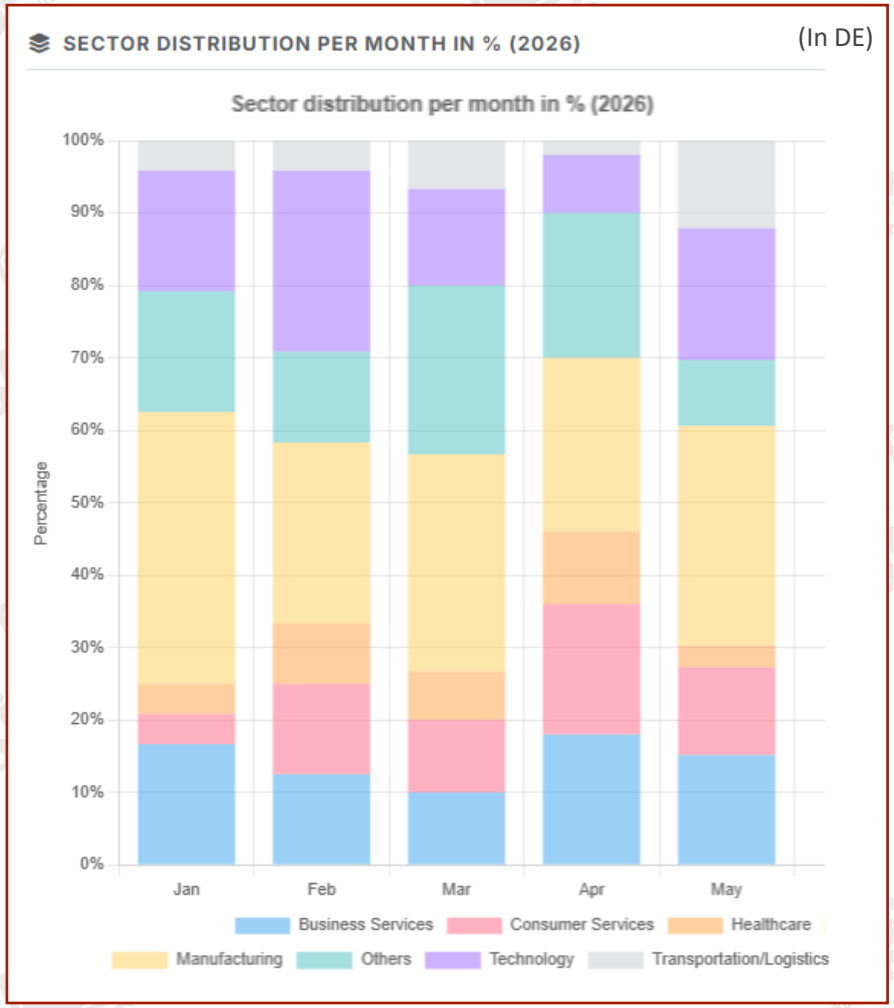
FILES YOURSELF.
OFTWARE TO RESTORE YOUR DATA.
ES, IT WILL RESULT IN PERMANENT DATA LOSS.

t?

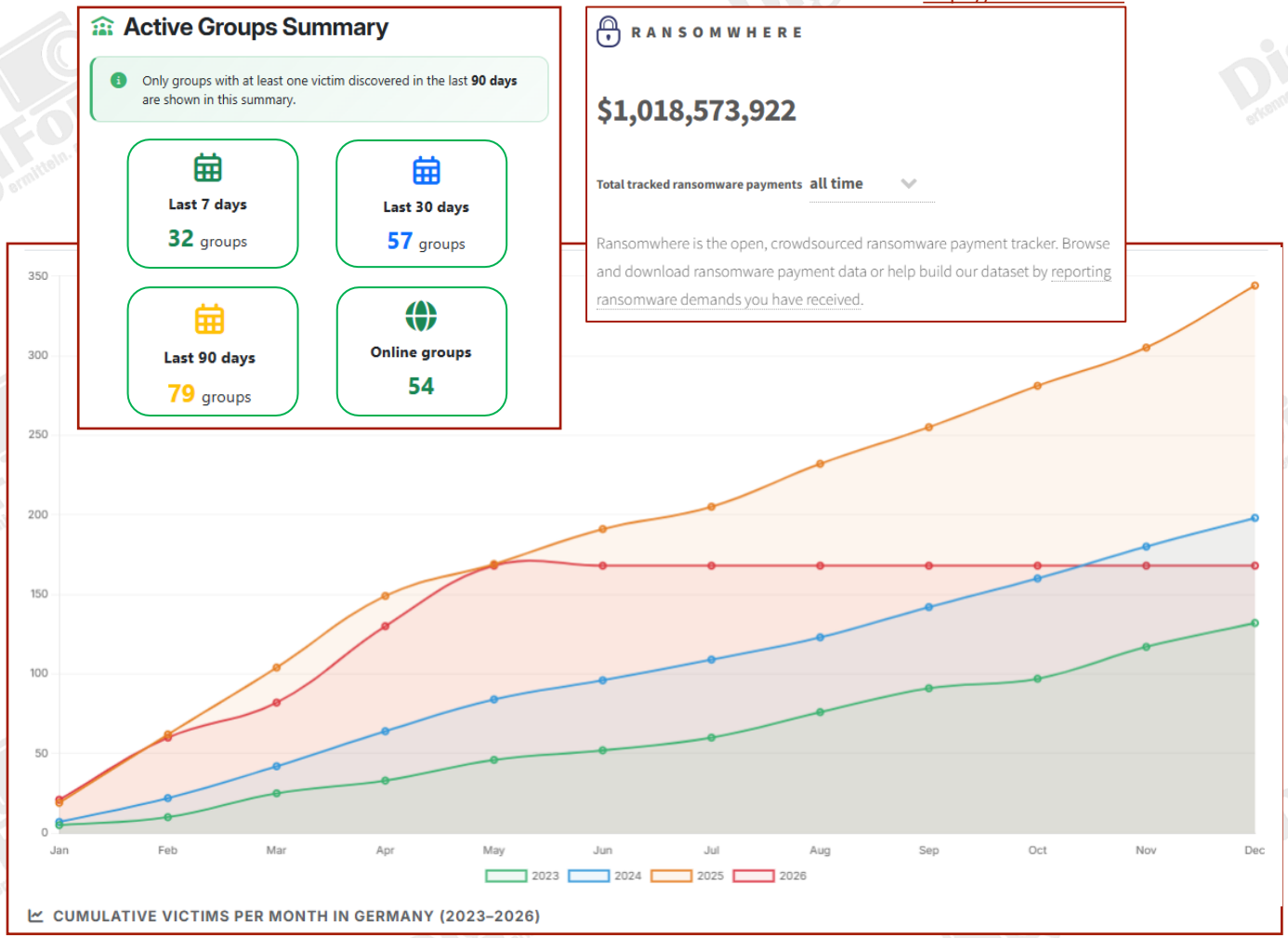
ps to get everything back to normal:
Tor Browser from: https://torproject.org/

[redacted]

Zahlen, Daten, Fakten



https://ransomwhe.re



https://ransomware.live/stats

Aktuelle Bedrohungslage

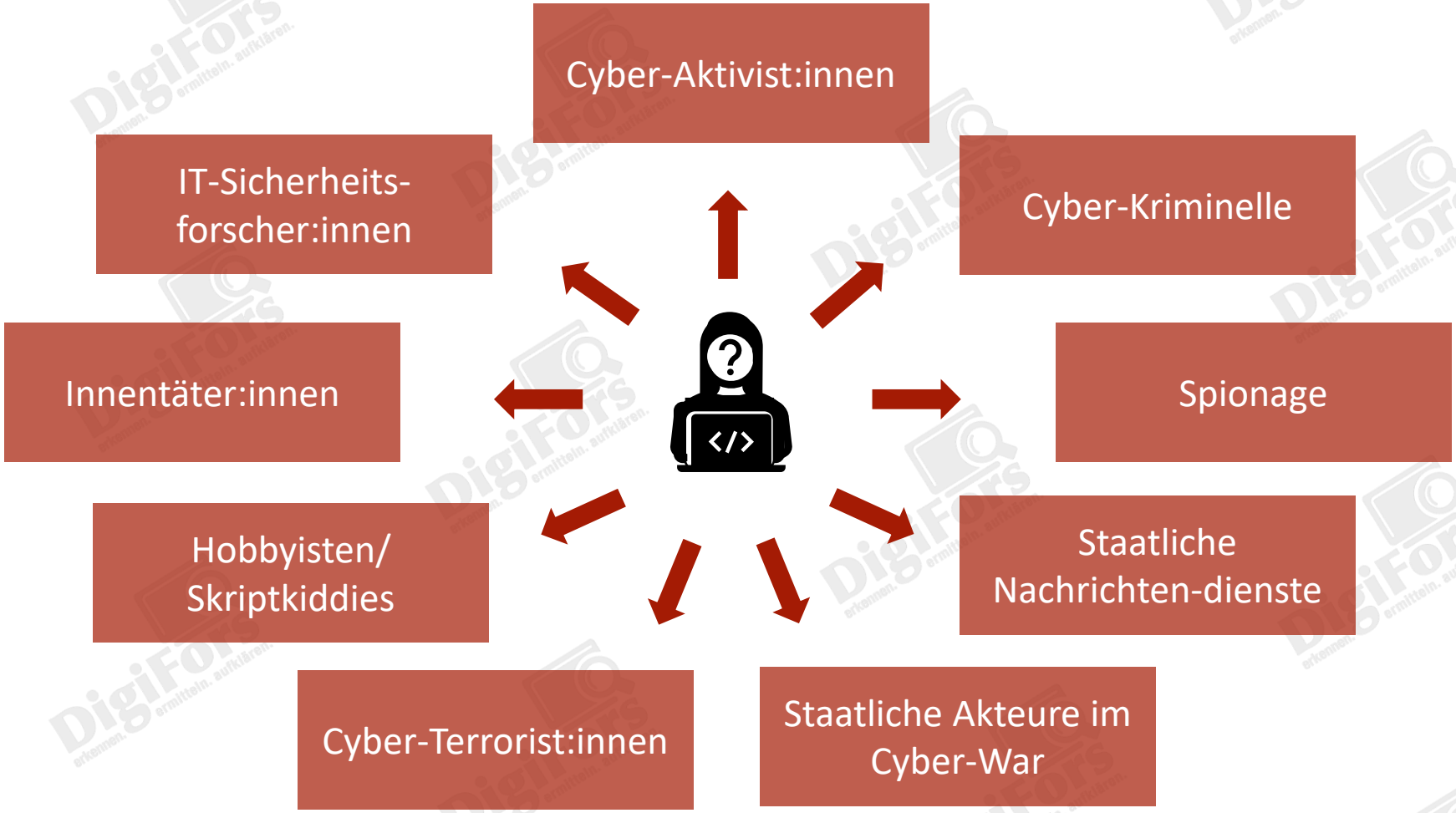
Die Frage ist nicht, *ob* man eines Tages betroffen ist,
sondern *wann*.

Deshalb:
Sichtbarkeit schaffen
Angriffskette unterbrechen
Schaden abwenden

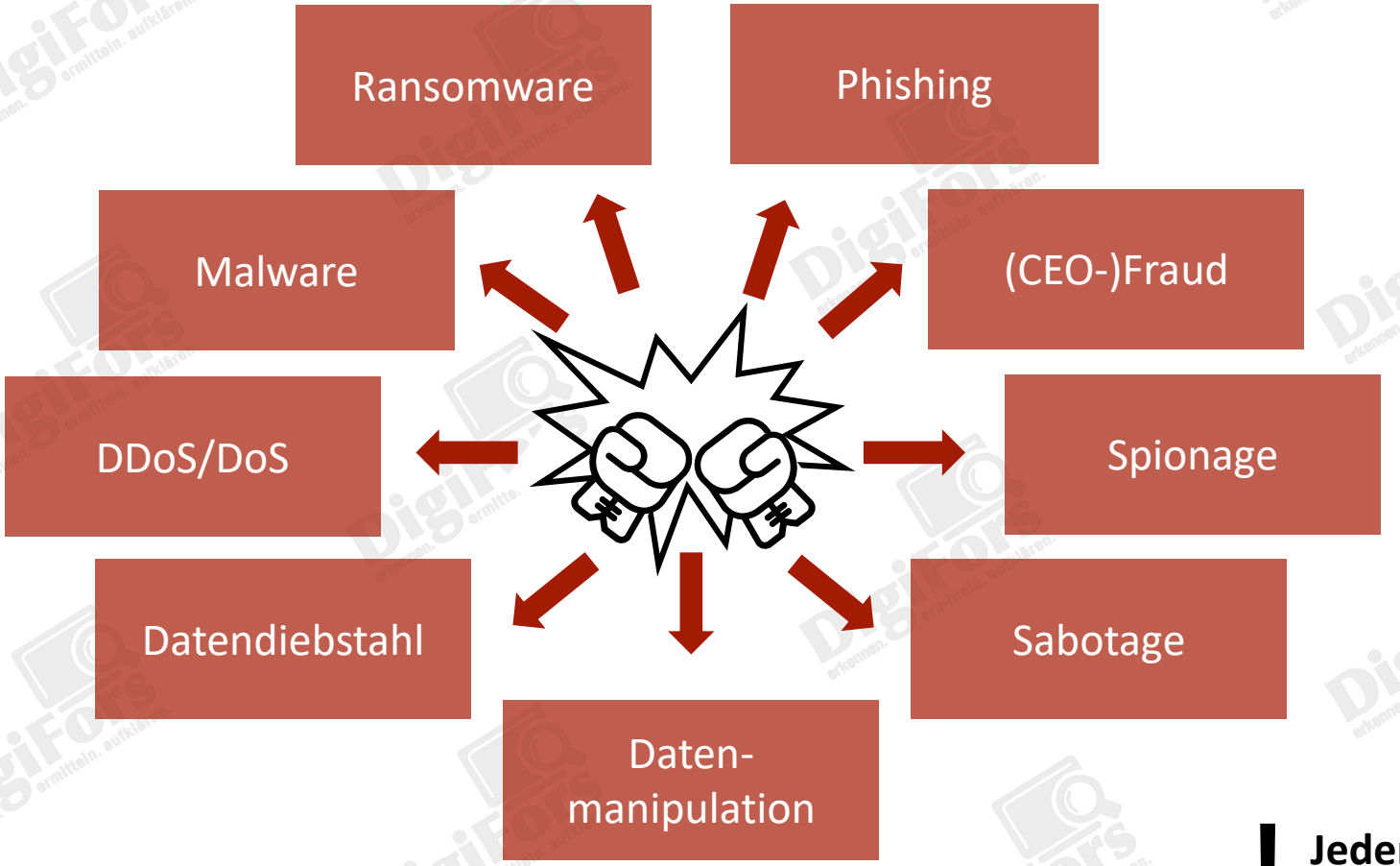
Die Anatomie eines Angriffs

	Störung	Notfall	Krise	Katastrophe
Dauer	Kurz	Länger	Kurz	Anhaltend
Schaden	Gering	Zunehmend	Groß	Enorm
Umfang	Lokal	Lokal	Lokal	Global
Behandlung	Im Tagesgeschäft möglich; Beobachten; Dokumentieren	Im Tagesgeschäft erschwert möglich, zügig handeln	Sofortige Schadensbegrenzung	Unterstützung durch externe Kräfte nötig

Die Anatomie eines Angriffs



I. Bedrohungslage - Angriffe



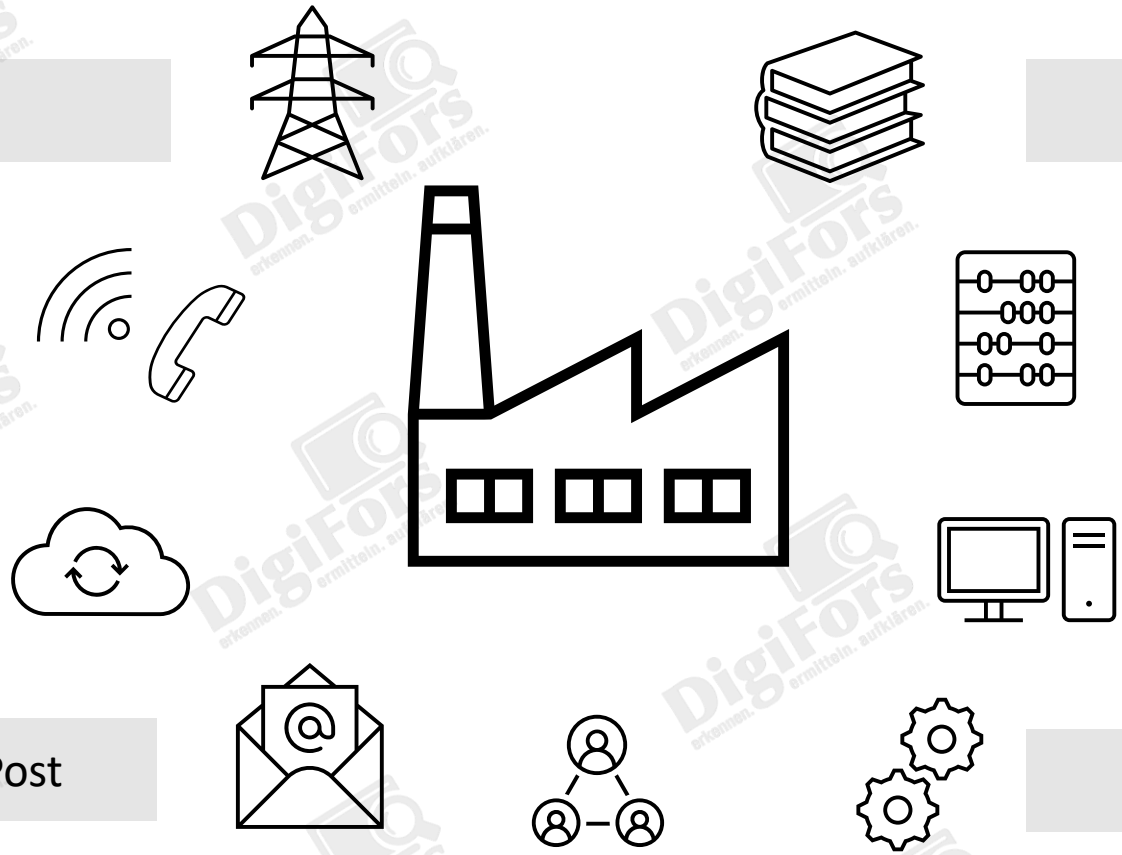
! Jeder Vorfall erfordert eine spezifische Reaktion.

Die Anatomie eines Angriffs

Cyberkill-Chain

Reconnaissance	Informationen über Netzwerk und Schwachstellen sammeln
Weaponization	Entwicklung von Strategien und Tools
Delivery	Einschleusen der Schadsoftware
Exploitation	Ausführen der Schadsoftware
Installation	Persistenz und dauerhaften Zugriff ermöglichen
Command & Control	Etablieren eines Kanals zur Fernsteuerung
Acions on Objectives	Aktionen zur Erreichung des Ziels ausführen

Die Anatomie eines Unternehmens



Strom

Buchhaltung

Internet und Telefonie

Abrechnung

Online-Dienste

Hardware

Mail und Post

Software

Mitarbeitende

Externe Abhängigkeit?

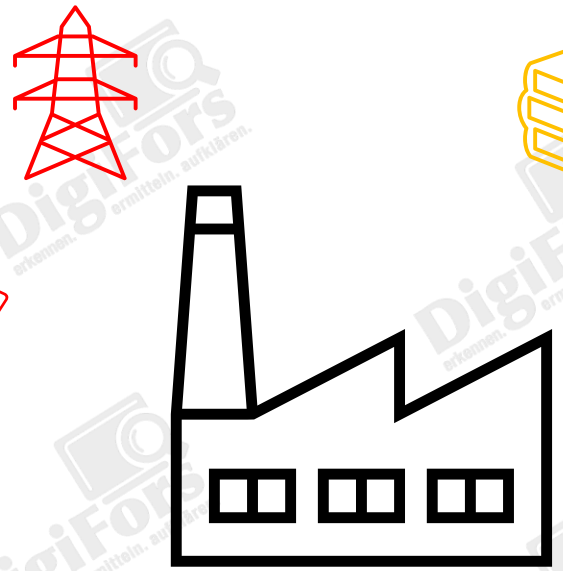
Die Anatomie eines Unternehmens

Strom

Internet und Telefonie

Online-Dienste

Mail und Post



Buchhaltung

Abrechnung

Hardware

Software

Mitarbeitende

Externe Abhängigkeit?

Eingeschränkt, falls selbst verantwortlich

i.d.R. vollständig

Die Anatomie eines Unternehmens

Stromausfall

Social Engineering

Internetausfall

CEO-Fraud,
Lieferanten-Betrug

Dienst-Ausfall,
Data Breach

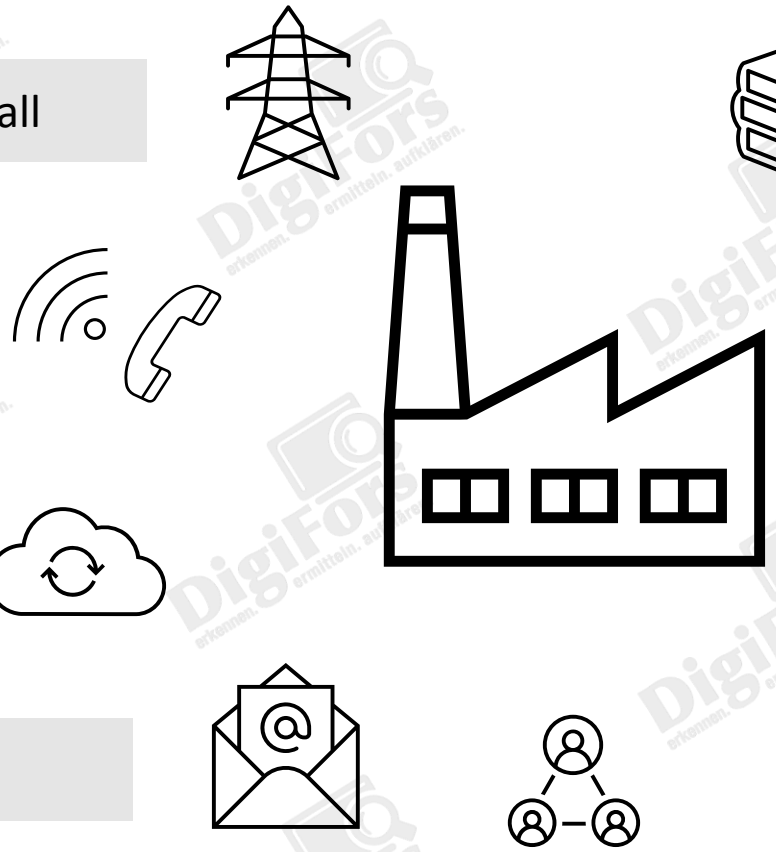
Schadsoftware

Phishing

Codier-Fehler

Innentäter

Schadenspotenzial?



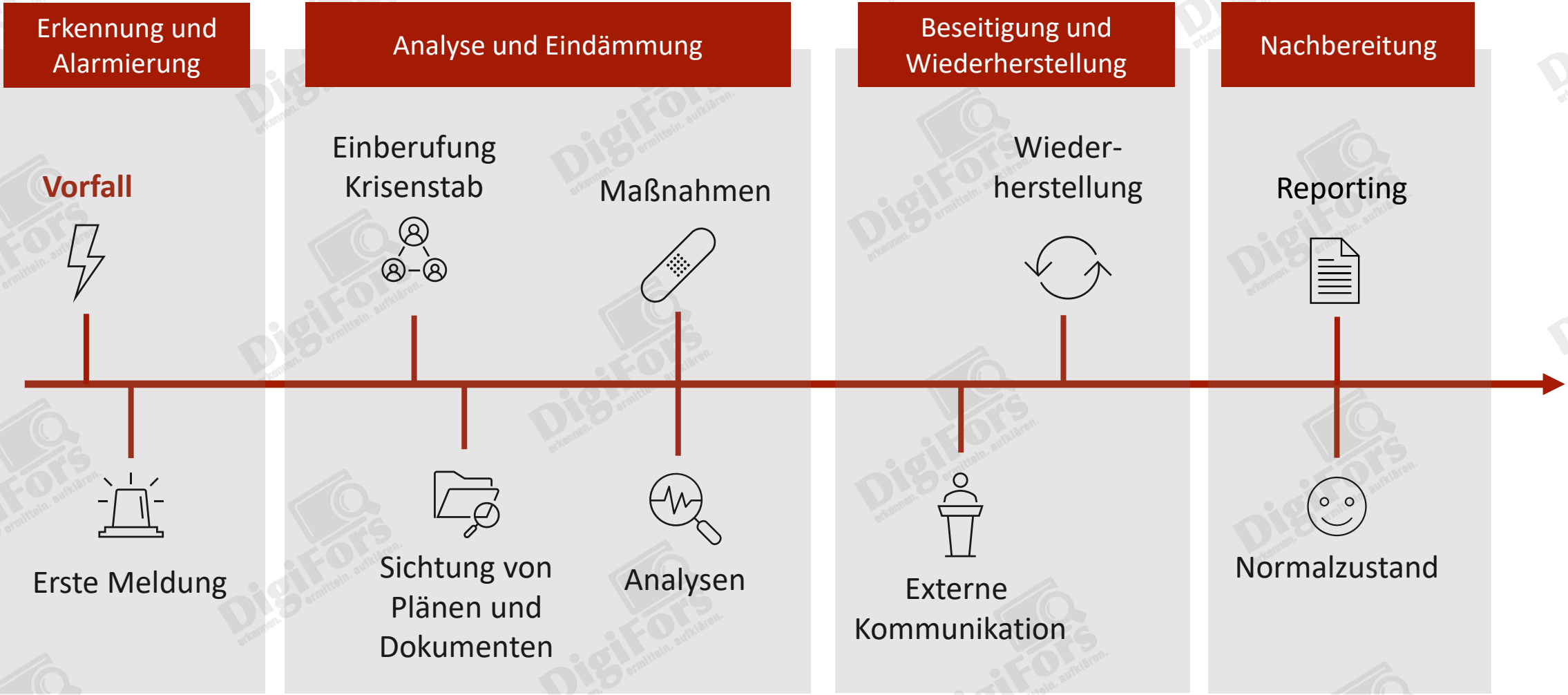
Die Anatomie eines Unternehmens

Du kannst nicht kontrollieren, was Dir passiert.
Aber Du kannst kontrollieren, wie Du darauf reagierst.

Schadenspotenzial?

Innentäter

Incident Response und Digitale Forensik

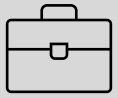


Incident Response und Digitale Forensik

Mitteilungen an Kunden und Behörden sind Pflicht und müssen qualifiziert erfolgen.

Die Auswertung eines Vorfalls schützt vor Wiederholung durch ähnliche Angriffe.

Ein gerichtsfestes Gutachten ermöglicht die Durchsetzung von Schadenersatz- und Unterlassungsansprüchen.



Cyberversicherungen verlangen eine nachvollziehbare Aufklärung und einen belastbaren Schadensnachweis.

Die Anatomie einer richtigen Reaktion

Wie reagiere ich im Ernstfall richtig?

Die Anatomie einer richtigen Reaktion

Sicherheitsbewusstsein fördern

- Regelmäßige Schulungen: Phishing, sicherer Passwörter, Verhalten im Ernstfall

Notfallpläne

- Incident-Response Plan/Notfall-Plan griffbereit haben
- Notfallübungen (Krisensimulation/Papertest) regelmäßig durchführen

Zuständigkeiten und Rollen

- Verantwortlichkeiten vorher abklären (Krisenstab, Sicherheitsbeauftragter)
- Kommunikationswege festlegen (intern, extern, Behörden)

Datenschutz

- Meldepflichten nach DSGVO und anderen Vorschriften
- Bei Cybervorfällen: Dokumentation und rechtsichere, gerichtsfeste Beweissicherung

Checkliste

- ✓ Krisenteam steht
- ✓ Meldewege bekannt
- ✓ Notfallhandbücher/Anleitungen offline verfügbar
- ✓ Technisches Inventar und ggf. Zugänge bekannt
- ✓ Evtl. dediziertes Notfall-System außerhalb der Domäne

Checkliste

Noch keine Übung gehabt?

Noch keinen Notfall-Plan erstellt?

Noch keinen Incident Response-Partner an der Hand?

Wir unterstützen Sie – Egal ob vor oder im Incident!

DigiFors
erkennen. ermitteln. aufklären.

Fragen oder Anregungen?

Vielen Dank für Ihre Aufmerksamkeit!

https://digifors.de/

https://www.linkedin.com/company/digifors/

info@digifors.de
notfall@digifors.de

DigiFors GmbH, Torgauer Str. 231a, 04347 Leipzig

#KEDiOnTour

Die nächsten Termine

23. Juni 2026
KEDi Webinar in Kooperation mit IFB Hamburg
Energieeffizienz und Digitalisierung in Hamburg

18. & 19. August 2026
KEDi Roadshow
Mainz

24. November 2026
KEDi Convention
Halle (Saale)

Jetzt kostenlos anmelden
www.kedi-dena.de/veranstaltungen

Kompetenzzentrum
Energieeffizienz
durch Digitalisierung

Vielen Dank und bleiben Sie mit uns in Kontakt!

KEDi Newsletter

Katharina Staffa
katharina.staffa@dena.de

Dr. Jörg Erdsack
joerg.erdsack@dena.de

Weitere Informationen finden Sie unter **www.kedi-dena.de**

Ein Projekt der dena

www.kedi-dena.de/das-kedi/newsletter