

BCM und BIA auf
dem Weg zur NIS2
(BvD)



Alexander Karls #gerneperDu
Senior IT Security-Consultant
Teamlead NGD
Mail: a.karls@itventive.com
Tel.: +49 9402 503-214

Kurzprofil:

- ✘ Über 20 Jahre in professioneller IT tätig
- ✘ Mehr als 15 Jahre Erfahrung in leitender Funktion
- ✘ Langjährige Erfahrung aus selbständiger Tätigkeit
- ✘ Vorfall-Experte im CSN des BSI
- ✘ Angehender NIS2-Koordinator
- ✘ Erfahrener Trainer und Coach
- ✘ Podcast-Host von BlueScreen – Der Tech-Podcast
- ✘ Tech-YouTuber
- ✘ Mit-Gründer DFIR*-Connection
*Data Forensics & Incident Response





Alexander Karls #gerneperDu
Senior IT Security-Consultant
Teamlead NGD
Mail: a.karls@itventive.com
Tel.: +49 9402 503-214

Kurzprofil:

- ✘ Über 20 Jahre in professioneller IT tätig
- ✘ Mehr als 15 Jahre Erfahrung in leitender Funktion
- ✘ Langjährige Erfahrung aus selbständiger Tätigkeit
- ✘ Vorfall-Experte im CSN des BSI
- ✘ Angehender NIS2-Koordinator
- ✘ Erfahrener Trainer und Coach
- ✘ Podcast-Host von BlueScreen – Der Tech-Podcast
- ✘ Tech-YouTuber
- ✘ Mit-Gründer DFIR*-Connection
*Data Forensics & Incident Response

Die ITventive AG



4 Standorte

110 Mitarbeiter

Standorte:



Ludwigsburg (D)



Regenstau (D)



Bern (CH)



Brøndby (DK)




Zu Risiken und Nebenwirkungen
lesen Sie die Packungsbeilage und fragen
~~Sie Ihren Arzt oder Apotheker.~~
Ihren Rechtsanwalt.

Achtung:
Dieser Vortrag er-
setzt keine Rechts-
beratung!

Anwendbarkeit des NIS2UmsG ist:



1. Prüfung von Unternehmen/ Einrichtung zu verantworten
2. einzelfallabhängig
3. komplex, z. B. konzerninternen Leistungen, Auslandsbezug oder Mehrfachregulierung
4. eine Rechtsfrage, externe Prüfung nur durch Rechtsanwältin/ Rechtsanwalt (Rechtsdienstleistungsgesetz!)



NIS2UmsuCG*: Stand der nationalen Umsetzung

*NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Fakten zu NIS2

Bundesrat stimmt NIS-2-Gesetz zu

🕒 21.11.2025 - 14:48 📄 Veröffentlicht in: NEWS

Mit der Zustimmung des Bundesrats zum NIS2UmsuCG bekommt Deutschland noch vor Jahresende ein überarbeitetes IT-Sicherheitsgesetz – das neue BSI-Gesetz. Rund 29.000 Unternehmen müssen die neuen Vorgaben direkt anwenden. Die Geschäftsleitungen stehen stärker in der Verantwortung, sich aktiv um Cybersicherheit zu kümmern.



Quellen: zeit.de / Canva AI Image Gen.

Fakten zu NIS2 – Was hat sich zum Erstentwurf geändert? (1)



Was das BSIG ändert:

- Die Anzeigepflicht des Einsatzes kritischer Komponenten (kK) fällt weg.
- Wegfall des Moratoriums (2 Monate) vor Einsatz einer kK und des Prüfungszwangs von EU-Herstellern.
- Wegfall der Garantieerklärung.
- Die Festlegung kritischer Komponenten in den einschlägigen Fachgesetzen ist nicht mehr erforderlich. Die Bestimmung erfolgt in einer auf Grundlage von § 56 Abs. 7 und 7a BSIG zu erlassenen Rechtsverordnung (§ 2 Ziff. 23 BSIG).
- An die Stelle der bisherigen Anzeigepflicht (nach Regierungsentwurf) werden die zum Einsatz kommenden kK dem BSI nunmehr im Rahmen der Registrierung anzuzeigen sein, § 33 Abs. 2/ Abs. 5 BSIG.
- § 41 Abs. 1 BSIG: Befugnis des BMI im Benehmen mit dem zuständigen Fachressort in allen kritischen Anlagen, sofern betreffende Komponenten Teile der Rechtsverordnung (bzw. des Sicherheitskatalogs). Es gebe keine Änderung des Prüfungsmaßstabs und keine Ausweitung des Prüfrechts im Vergleich zu bisherigen Rechtslage.
- Widersprüche und Klagen haben künftig keine aufschiebende Wirkung mehr, § 41 Abs. 3 BSIG.
- An die Stelle der Mitwirkungspflicht nach dem allgemeinen Verwaltungsverfahrenrecht tritt eine ausdrückliche nach § 41 Abs. 5 BSIG.

Für Unternehmen ergeben sich daraus weiterhin herausfordernde Pflichten hinsichtlich der Lieferkette und dem Umgang mit der Aufsichtsbehörde.

Übersetzung / Handlungsempfehlungen für Unternehmen

1. Strategische Maßnahmen (Governance / IT-Grundschutz ORP / DER)

1.1 Aufbau eines verbindlichen „Critical Component Management“-Prozesses

Warum: Die Definition kritischer Komponenten wird künftig per Rechtsverordnung dynamisch geändert. Konsequenz: Unternehmen müssen **ständig** prüfen, ob eingesetzte Komponenten betroffen sind.

Konkrete Schritte:

Inventarisierung aller eingesetzten Komponenten (inkl. Hersteller, Firmware, Herkunft, Supportstatus). Verantwortlichkeiten definieren: Wer bewertet? Wer dokumentiert? Wer meldet an das BSI? Prozess in ISMS integrieren: Neue Komponenten erst nach Risikoanalyse zulassen.

IT-Grundschutz: ORP.3, DER.1

OWASP-SC: SC-01 (Inventory / Assets Mgmt.), SC-04 (Maintain Accurate SBOM)

1.2 Lieferantenbewertung verschärfen

Da Garantieerklärungen wegfallen, müssen Unternehmen selbst beurteilen, ob Hersteller vertrauenswürdig sind.

Konkrete Schritte:

Einführung eines **Supplier Security Assessment Frameworks** (Fragebogen + Score). Pflicht zur Bereitstellung von SBOM und Patch-Prozessen in Verträgen verankern. Mindestanforderungen definieren (z. B. ISO 27001, sichere Entwicklungsprozesse, CVE-Reaktionszeit).

OWASP-SC: SC-03 (Assess Supplier Risk)

1.3 Rechtliche Vorbereitung auf Sofortvollzug

Da Widersprüche keine aufschiebende Wirkung mehr haben, brauchst du:

Krisenprozess, der regelt, was passiert, wenn das BSI eine Komponente untersagt.

Technisches und organisatorisches **Fallback-Konzept**, um eine kritische Komponente schnell auszubauen/zu ersetzen.

Budget- und Ressourcenplanung für Notfälle.

IT-Grundschutz: ORP.4 Notfallvorsorge

Fakten zu NIS2 – Was hat sich zum Erstentwurf geändert? (2)



Was das BSIG ändert:

- Die Anzeigepflicht des Einsatzes kritischer Komponenten (kK) fällt weg.
- Wegfall des Moratoriums (2 Monate) vor Einsatz einer kK und des Prüfungszwangs von EU-Herstellern.
- Wegfall der Garantieerklärung.
- Die Festlegung kritischer Komponenten in den einschlägigen Fachgesetzen ist nicht mehr erforderlich. Die Bestimmung erfolgt in einer auf Grundlage von § 56 Abs. 7 und 7a BSIG zu erlassenen Rechtsverordnung (§ 2 Ziff. 23 BSIG).
- An die Stelle der bisherigen Anzeigepflicht (nach Regierungsentwurf) werden die zum Einsatz kommenden kK dem BSI nunmehr im Rahmen der Registrierung anzuzeigen sein, § 33 Abs. 2/ Abs. 5 BSIG.
- § 41 Abs. 1 BSIG: Befugnis des BMI im Benehmen mit dem zuständigen Fachressort in allen kritischen Anlagen, sofern betreffende Komponenten Teile der Rechtsverordnung (bzw. des Sicherheitskatalogs). Es gebe keine Änderung des Prüfungsmaßstabs und keine Ausweitung des Prüfrechts im Vergleich zu bisherigen Rechtslage.
- Widersprüche und Klagen haben künftig keine aufschiebende Wirkung mehr, § 41 Abs. 3 BSIG.
- An die Stelle der Mitwirkungspflicht nach dem allgemeinen Verwaltungsverfahrenrecht tritt eine ausdrückliche nach § 41 Abs. 5 BSIG.

Für Unternehmen ergeben sich daraus weiterhin herausfordernde Pflichten hinsichtlich der Lieferkette und dem Umgang mit der Aufsichtsbehörde.

Übersetzung / Handlungsempfehlungen für Unternehmen

2. Operative Maßnahmen (TECH / OPS)

2.1 Aufbau eines sauberen Komponenten-Inventars (SBOM / Asset Management)

Notwendig, weil die Anzeige der kK künftig über die Registrierung läuft und Fehler hier gefährlich sind.

Konkrete Schritte:

Einführung einer automatisierten SBOM-Erfassung (CycloneDX / SPDX).

Zuordnung zu Systemen, Netzen, Verantwortlichen.

Regelmäßige Aktualisierung (monatlich oder eventbasiert).

IT-Grundschutz: INF.10, SYS.1

OWASP-SC: SC-01, SC-02

2.2 Stärkere technische Lieferkettenkontrollen

Konkrete Maßnahmen:

Integritätsprüfung (Signaturen, Hashes, Secure Boot).

Prüfung der Build-Pipelines von Lieferanten.

Regelmäßiges Monitoring auf kompromittierte Lieferketten (z. B. SolarWinds-ähnliche Vorfälle).

OWASP-SC: SC-06, SC-07

2.3 Vorbereitete Dokumentation für BSI-Prüfungen

Weil das BMI/BMI-Prüfrecht bleibt und dynamischer genutzt werden kann.

Benötigt:

Technische Beschreibungen der Komponenten (Architektur, Schnittstellen, Risiken).

Nachweise zur Kontrolle der Lieferkette.

Change- und Patch-Historie.

IT-Grundschutz: OPS.1, CON.1

2.4 Interner Registrierungsprozess

Da kritische Komponenten nun im Rahmen der Registrierung gemeldet werden müssen, braucht es:

Checkliste: „Komponente kritisch? Ja/Nein?“

Technisch-juristische Plausibilitätsprüfung.

Interne Freigabe durch ISB/IT-Leitung/Compliance.

Fehler bei der Registrierung könnten künftig **aufsichtsrechtliche Konsequenzen** haben.

Quellen: LinkedIn / Bartels LL.M.

Fakten zu NIS2 – Was hat sich zum Erstentwurf geändert? (3)



Was das BSIG ändert:

- Die Anzeigepflicht des Einsatzes kritischer Komponenten (kK) fällt weg.
- Wegfall des Moratoriums (2 Monate) vor Einsatz einer kK und des Prüfungszwangs von EU-Herstellern.
- Wegfall der Garantieerklärung.
- Die Festlegung kritischer Komponenten in den einschlägigen Fachgesetzen ist nicht mehr erforderlich. Die Bestimmung erfolgt in einer auf Grundlage von § 56 Abs. 7 und 7a BSIG zu erlassenen Rechtsverordnung (§ 2 Ziff. 23 BSIG).
- An die Stelle der bisherigen Anzeigepflicht (nach Regierungsentwurf) werden die zum Einsatz kommenden kK dem BSI nunmehr im Rahmen der Registrierung anzuzeigen sein, § 33 Abs. 2/ Abs. 5 BSIG.
- § 41 Abs. 1 BSIG: Befugnis des BMI im Benehmen mit dem zuständigen Fachressort in allen kritischen Anlagen, sofern betreffende Komponenten Teile der Rechtsverordnung (bzw. des Sicherheitskatalogs). Es gebe keine Änderung des Prüfungsmaßstabs und keine Ausweitung des Prüfrechts im Vergleich zu bisherigen Rechtslage.
- Widersprüche und Klagen haben künftig keine aufschiebende Wirkung mehr, § 41 Abs. 3 BSIG.
- An die Stelle der Mitwirkungspflicht nach dem allgemeinen Verwaltungsverfahrenrecht tritt eine ausdrückliche nach § 41 Abs. 5 BSIG.

Für Unternehmen ergeben sich daraus weiterhin herausfordernde Pflichten hinsichtlich der Lieferkette und dem Umgang mit der Aufsichtsbehörde.

Übersetzung / Handlungsempfehlungen für Unternehmen

3. Kommunikation & Aufsichtsvorbereitung

3.1 Aufbau eines „BSI-Interface“-Teams

Es braucht definierte Rollen für:

Ansprechpartner für Registrierungen

Ansprechpartner für Prüfungen

Kommunikationsabsicherung bei Sofortvollzug

Ziel: Kein Chaos, wenn das BSI anknüpft und Unterlagen verlangt.

3.2 Schulungen für Einkauf, Technik und Management

Damit alle verstehen:

Was eine kritische Komponente ist

Welche Pflichten aus dem BSIG entstehen

Warum kurzfristige Umsetzungen angeordnet werden können

Welche Risiken Strafen oder Betriebsunterbrechungen bedeuten

Tipp aus der Praxis:

Einkauf ist oft der blinde Fleck. Ohne Schulung kaufen sie Dinge ein, die Compliance sprengen.

3.3 Kommunikationsplan für den Fall einer BSI-Anordnung

Da Anordnungen sofort wirksam werden, brauchst du:

Interne Kommunikationsmatrix

Entscheidungsschablone: „Weiterbetrieb trotz Risiko?“

Externe Kommunikationsstrategie (Kunden, Lieferanten, ggf. Öffentlichkeit)

Kurz gesagt:

Das neue BSIG nimmt uns kurzfristig Formalitäten ab – aber es zwingt Unternehmen dazu, ihre Lieferkette technisch, organisatorisch und rechtlich **viel professioneller** zu managen.

Wer keine Transparenz, kein Inventar, keine SBOMs und keine Lieferantenbewertung hat, steht im Ernstfall ohne Verteidigung da.

Fakten zu NIS2 – Das sagt die DKG



Grundhaltung: Unterstützung, aber mit großen Vorbehalten

- Die DKG begrüßt grundsätzlich die Umsetzung der NIS-2-Richtlinie im Gesundheitswesen — gerade wegen der zunehmenden Cyberangriffe und der damit verbundenen Risiken im Klinikbetrieb
- Die Verknüpfung mit dem parallel geplanten KRITIS-Dachgesetz (KRITIS-DachG) wird ausdrücklich als sinnvoll erkannt. So könnten bestehende Strukturen (z. B. Meldewesen, Registrierung) gemeinsam genutzt und Synergien gehoben werden. **Erwartet ca 05./06.2026**



Quelle: DKG EV

Fakten zu NIS2 – Das sagt die DKG



Kritikpunkt

Details

Die Pflicht zu Erst-, Zwischen-, Folge- und Abschlussmeldung bei „erheblichen Sicherheitsvorfällen“ wird als zu bürokratisch und in der Praxis kaum handhabbar bewertet, da bereits potentielle Gesundheitsgefährdungen meldepflichtig sein können.

Melde- und Verwaltungsaufwand

Begriffe wie „Cloud-Computing-Dienst“, „erheblicher Sicherheitsvorfall“ oder „Rechenzentrumsdienst“ sind aus Sicht der DKG zu unpräzise definiert. Das erschwere praktische Abgrenzungen und kann zu Überregulierung oder Rechtsunsicherheit führen.

Unklare bzw. schwammige Definitionen

>> RA und DSB hinzuziehen, schützt vor Überreaktionen



Quelle: DKG EV

Fakten zu NIS2 – Das sagt die DKG

Kritikpunkt

Details

Zeitdruck / fehlende Übergangsfristen

Viele der neuen Anforderungen (z. B. Risikomanagement gemäß § 30, Nachweispflichten) stellen eine qualitativ neue Belastung dar und brauchen Zeit für Planung und Umsetzung — eine realistische Übergangsfrist sei jedoch nicht vorgesehen. Unverzüglich = max 72 Stunden!

Haftung & Sanktionen ohne Berücksichtigung der Realbedingungen

Sanktionen und Auflagen bei Mängeln könnten insbesondere Rehakliniken und kleinere Einrichtungen treffen, obwohl deren personelle und finanzielle Ressourcen deutlich limitiert sind.

Probleme bei technischen Anforderungen im Krankenhausbetrieb

Manche technischen Maßnahmen (z. B. Multi-Faktor-Authentifizierung, Lieferkettenkontrollen, Auditpflichten) sind aus Sicht der DKG schwer mit dem laufenden Krankenhausbetrieb vereinbar — z. B. wegen Abhängigkeiten von Medizintechnik oder weil eine Abschaltung von Systemen lebensbedrohliche Folgen haben kann.



Quelle: DKG EV

Fakten zu NIS2 – Das sagt die DKG



Kritikpunkt

Details

Lieferkette / Abhängigkeit von großen Anbietern

Die geforderte Kontrolle der Lieferkette sei für einzelne Krankenhäuser kaum durchsetzbar. Große Anbieter hätten zu viel Marktmacht — individuelle Kliniken können kaum Einfluss auf deren Sicherheitsstandards nehmen.

> **Souveränität schaffen!**

Fehlende Finanzierung und politische Zuständigkeit

Die Umsetzung der geforderten Maßnahmen (Technik, Personal, Prozesse) erfordere erhebliche finanzielle Mittel — derzeit gibt es laut DKG aber keine Möglichkeit, diese Kosten refinanzieren zu lassen. Die bestehende Krankenhausfinanzierung decke solche Investitionen nicht ab.

> **Die Kosten eines Ausfalls und die damit verbundenen Folgekosten müssen immer gegen den Invest gehalten werden!**



Quelle: DKG EV

„Stand der Technik“ ...

Definition



"Stand der Technik (in der IT-Sicherheit)
bezeichnet die am Markt verfügbare Bestleistung
einer IT-Sicherheitsmaßnahme
zur Erreichung der gesetzlichen IT-Sicherheitsziele."



Quelle: <https://www.teletrust.de/>, Handreichung "Stand der Technik in der IT-Sicherheit"



Quelle: chatGPT

„Stand der Technik“...

Definition

"Stand der Technik (in der IT-Sicherheit)
bezeichnet die am Markt verfügbare Bestleistung
einer IT-Sicherheitsmaßnahme
zur Erreichung der gesetzlichen IT-Sicherheitsziele."

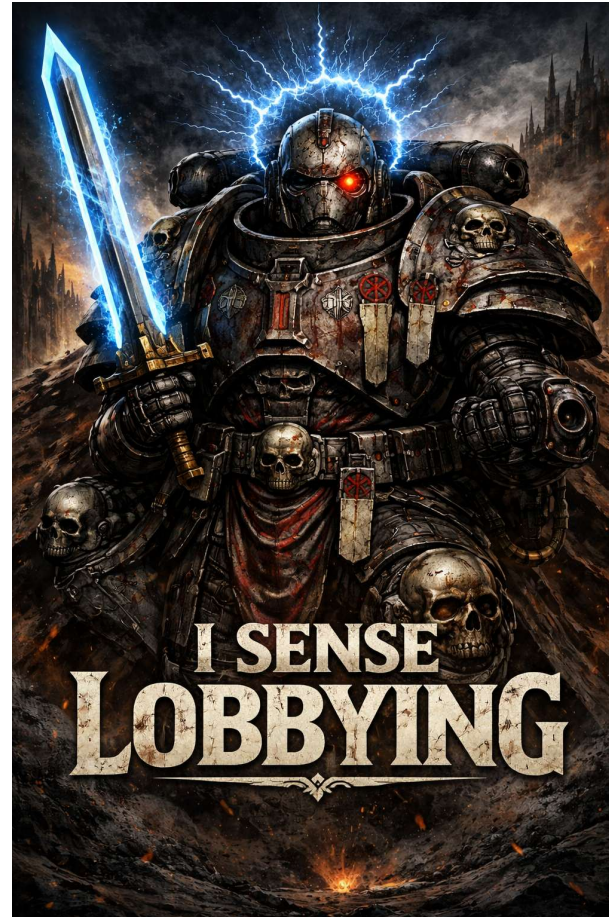
Quelle: <https://www.teletrust.de/>, Handreichung "Stand der Technik in der IT-Sicherheit"



Quellen: chatGPT



„Stand der Technik“ ...



Quellen: chatGPT

„Stand der Technik“ ...



- Für „Stand der Technik“ gibt es im Gesundheitswesen verschiedene Vorgaben:
- Arztpraxen, die Richtlinie der Kassenärztlichen Bundesvereinigung (analog Zahnärzte), siehe § 390 SGB V (https://www.gesetze-im-internet.de/sgb_5/390.html)
- Krankenhäuser, die Richtlinie der Krankenhausgesellschaft, siehe § 391 SGB V (https://www.gesetze-im-internet.de/sgb_5/391.html)
- Krankenkassen, die Richtlinie der GKV, siehe § 392 SGB V (https://www.gesetze-im-internet.de/sgb_5/392.html)
- Speziell Cloud-Einsatz siehe § 393 SGB V (https://www.gesetze-im-internet.de/sgb_5/393.html)
- Es ist fragwürdig, ob die Richtlinie der KBV (<https://www.kbv.de/praxis/digitalisierung/it-sicherheit>) dem „Stand der Technik“ genügt, ergänzende Vorgaben aus der NIS-2-Richtlinie wie beispielsweise Umgang mit Lieferketten wurden aber bei keiner der Richtlinie berücksichtigt, kommen also ggfs. on top hinzu, sofern (!) die eigene Einrichtung unter die NIS-2-Richtlinie fällt. Siehe Folie 48!

Wesentliche Inhalte des NIS2UmsuCG* - Was ist das?



NIS-1-Richtlinie legte Unternehmen fest, die besonders schützenswert waren.

- Auf europäischer Ebene wurde NIS-1 jedoch nicht einheitlich umgesetzt.
- NIS-1 wurde in Deutschland durch die Novelle des BSiG (Stichwort: „ITSiG“) umgesetzt.
- Eines der Ziele der NIS-2-Richtlinie war, eine einheitliche(re) Regelung zu verfassen.

Die NIS-2-Richtlinie trat am 16. Januar 2023 in Kraft.

- Die Mitgliedsstaaten mussten die NIS-2-Richtlinie bis spätestens zum 17. Oktober 2024 in nationales Recht umsetzen, dieses war dann ab dem 18. Oktober 2024 anzuwenden.

Zum Nachlesen: t.ly/Dc9Eq

(<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32022L2555>)



Wer ist betroffen vom NIS2UmsuCG*?

Stark vereinfachter Grundsatz: *Unternehmen ab 50 Mitarbeitende oder mehr als 10 Mio. Euro Jahresumsatz und mehr als 10 Mio. Euro Bilanzsumme, die in den definierten Sektoren aktiv sind, müssen die geforderten Maßnahmen umsetzen.*

- Achtung: Dabei gibt es zahlreiche Sonderregelungen. 😊

Falls ein Unternehmen in eine andere Kategorie „wechselt“, gilt diese erst, *„wenn es in zwei aufeinander folgenden Geschäftsjahren zu einer Über- oder Unterschreitung kommt.“* (Art. 4 Abs. 2 der Empfehlung 2003/361/EG)

In NIS-2 gibt es grundsätzlich *„essential entities“* und *„important entities“*.

- Diese Unterscheidung hat aber keine große Auswirkung.



Sonst. Vorschriften

Weitere Vorschriften



BSI-KRITIS-VO

- KRITIS-Einrichtungen (werden im BSIG zu Betreibern kritischer Anlagen), Verordnung von Änderungen durch das NIS2UmsuCG nicht erfasst
- Können als Unternehmen zugleich NIS und in Bezug auf die Anlage der KRITIS-Verordnung und KRITIS-DachG unterfallen

DORA

- Digital Operational Resilience Act
- Dienstleister für Finanzsektor, insbesondere Cloud Provider, Anbieter von TK-Lösungen oder Managed Services Provider; evtl. auch gruppeninterne IT-Dienstleister
- für Finanzunternehmen selbst gilt NIS2

EnWG

- Energiewirtschaftsgesetz, Bsp: Anbieter örtliches Stromverteilernetz
- Neben NIS2 für das Unternehmen im Energiesektor Sicherheitsanforderungen nach **EnWGIT-SiKat BNetzA (IT-Sicherheitskatalog der BNetzA)**
- Resilienz-Anforderungen nach **KRITIS-DachG**

TKG

- Für Bereich des TK-Betriebs gilt TKG und BNetzA-Sicherheitskatalog
- Geltung der NIS2-Pflichten ausgenommen.

DSGVO!



DSGVO – die Frage nach den TOM

- **Verantwortliche schulden** nach Art. 32 DSGVO unabhängig von NIS2 die **Sicherheit der Datenverarbeitung**
- Technisch-organisatorische Maßnahmen sind **Pflicht!**
- Wer TOM zur Datensicherheit nicht so genau nimmt, riskiert im Falle einer Datenschutzverletzung nicht nur ein **Bußgeld**, sondern auch erhebliche **Schadenersatzansprüche** (EuGH, Urteil vom 14.12.2023 – Az. C-340/21)
- Siehe aktuelles BGH-Urteil zum Facebook-Scraping: **Unterlassungsansprüche** und Schadenersatz für jeden Betroffenen möglich! (Urteil vom 18.11. 2024 – Az. VI ZR 10/24)
- Darlegungs- und Nachweispflicht im Falle der Cyberattacke, dass ausreichende Maßnahmen zur Datensicherheit getroffen

Gutes IT-Sicherheitsmanagement für alle Unternehmen zu empfehlen!

Betroffenheitsprüfung zu NIS2UmsuCG*? Neue Seite des BSI:



KONTAKT ENGLISH GEBÄRDENSPRACHE LEICHTE SPRACHE NUTZUNGSBEDINGUNGEN LOGIN

Deutschland
Digital•Sicher•BSI

Das BSI Themen IT-Sicherheitsvorfall Karriere Service

Themen > Regulierte Wirtschaft > NIS-2-regulierte Unternehmen



#nis2know für Unternehmen

Viele Unternehmen und Einrichtungen, die mit NIS-2 erstmals durch das BSI reguliert werden, stehen vor der Frage, was sie jetzt tun müssen.

Lesen Sie hier, auf welche neuen Pflichten Sie sich einstellen müssen.

[MEHR ERFAHREN](#)

#nis2know: Schneller Einstieg in NIS-2

Sie wollen gleich loslegen? Hier finden Sie die wichtigsten Informationen auf einen Blick.

 NIS-2-Betroffenheitsprüfung	 NIS-2 - Was tun?	 NIS-2-Richtlinie	 Sektorspezifische Informationen
--	---	---	--

➔ t.ly/d2Qz3

Sind Sie unsicher, ob Ihr Unternehmen von der NIS-2-Richtlinie der EU betroffen ist?

Die NIS-2-Betroffenheitsprüfung des BSI bietet Ihnen in wenigen Schritten dafür eine erste Orientierung.

Die NIS-2-Betroffenheitsprüfung stellt Ihnen konkrete, an der Richtlinie orientierte Fragen, um Ihr Unternehmen einzuordnen. Die Fragen sind kurz und präzise gehalten und werden bei Bedarf im Kleingeschriebenen tiefergehend erläutert.

Nachdem Sie den Fragenkatalog durchlaufen haben, erhalten Sie ein auf Ihren Angaben basierendes Ergebnis. Dieses gibt eine automatisierte Ersteinschätzung, ob Ihr Unternehmen von der NIS-2-Richtlinie betroffen ist.

Die Nutzung der NIS-2-Betroffenheitsprüfung erfolgt anonym. Das BSI stellt diese im Rahmen seiner Kooperationsaufgabe zur Verfügung. Sie erfasst keine Daten, die personenbezogen sind oder Rückschlüsse zur Identifizierung Ihres Unternehmens geben. Bitte beachten Sie, dass die Hilfe zur Betroffenheitsprüfung von NIS-2 lediglich als Orientierungshilfe dient und Ihr Ergebnis rechtlich nicht bindend ist, da Ihre Antworten automatisiert erstellt und nicht vom BSI oder anderen unabhängigen Stellen geprüft werden. Es besteht kein Anspruch auf Vollständigkeit und Richtigkeit der Inhalte.

Zurzeit basieren die Abfragen der NIS-2-Betroffenheitsprüfung auf dem Gesetzentwurf des NIS-2 Umsetzungsgesetzes des BMI (Stand 25.07.2025). Sobald das finale Umsetzungsgesetz beschlossen und verabschiedet wurde, wird das BSI die NIS-2-Betroffenheitsprüfung anhand dieses Gesetzes anpassen und aktualisieren.

Haben Sie zu oder nach der Nutzung noch Fragen? Das BSI steht gerne zur Verfügung.

Die NIS-2-Betroffenheitsprüfung dient als automatische Orientierungshilfe auf Grundlage von Eigenangaben, deren Ergebnis nicht rechtlich bindend ist. Die NIS-2-Betroffenheitsprüfung ersetzt die Prüfung zur Selbst-Identifizierung nicht und hat für eventuelle Verfahren keine Indizwirkung.

Einrichtungen der Bundes-, Landes- und Kommunalverwaltung werden in der NIS-2-Betroffenheitsprüfung nicht betrachtet.



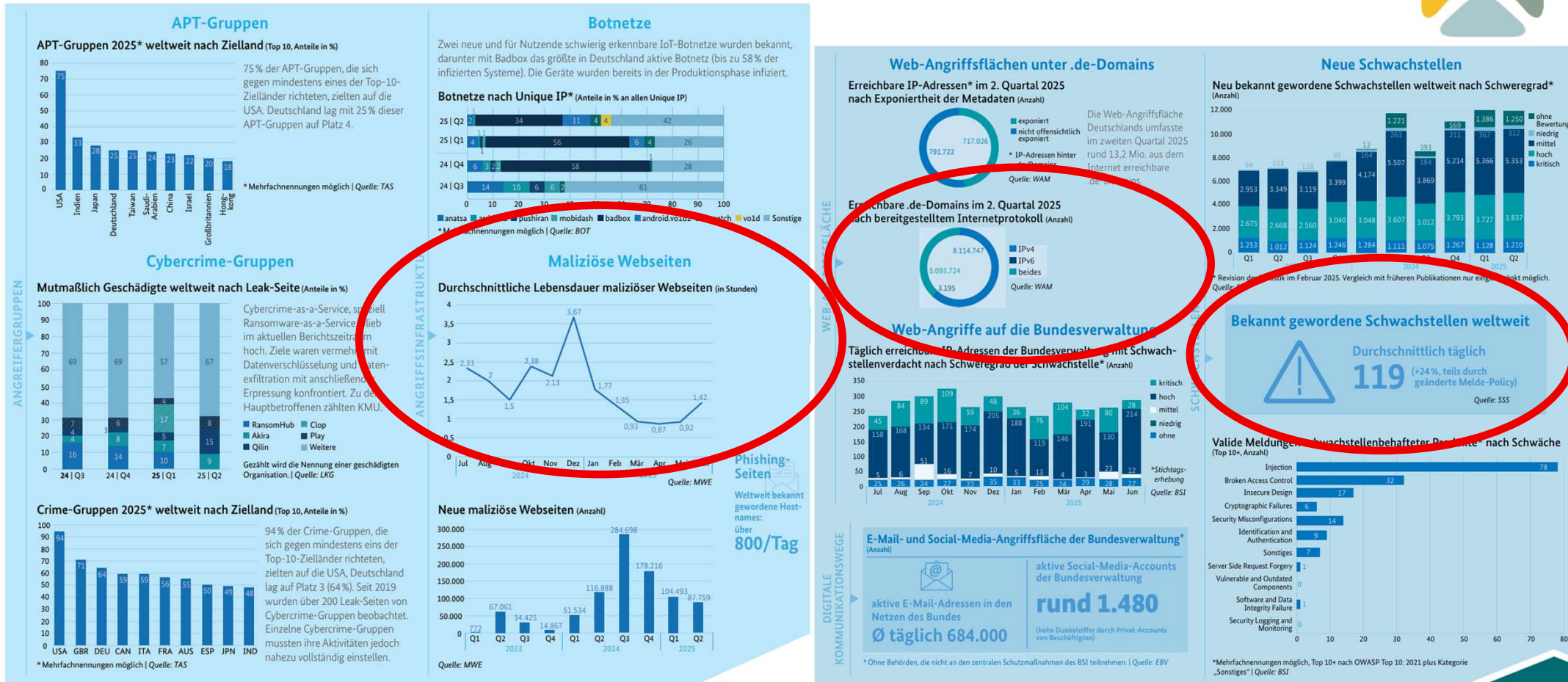
BSIG - Einrichtungen der Bundesverwaltung

- Erstmalige Aufnahme in den Anwendungsbereich des BSIG, § 29 BSIG
- Dadurch Harmonisierung diverser nationaler und europäischer Vorgaben
- Umfasst:
 - Bundesbehörden
 - ÖR'lich organisierte IT-Dienstleister der Bundesverwaltung
 - Weitere Körperschaften, Anstalten und Stiftungen des Ö'Rechts und ihre Vereinigungen auf Bundesebene, soweit durch BSI im Einvernehmen mit zust. Ressort angeordnet

Keine Verpflichtung der Länder und Kommunen!

Grund: Kompetenzordnung des Grundgesetzes

Warum NIS2UmsuCG*?



Quellen: BSI > t.ly/QcRn-

*NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Warum NIS2UmsuCG*?



This page displays the **100 most recent victim** disclosures attributed to ransomware groups, as detected by **Ransomware.live**. Our platform continuously monitors and scrapes ransomware group leak sites to identify and list newly published victims.

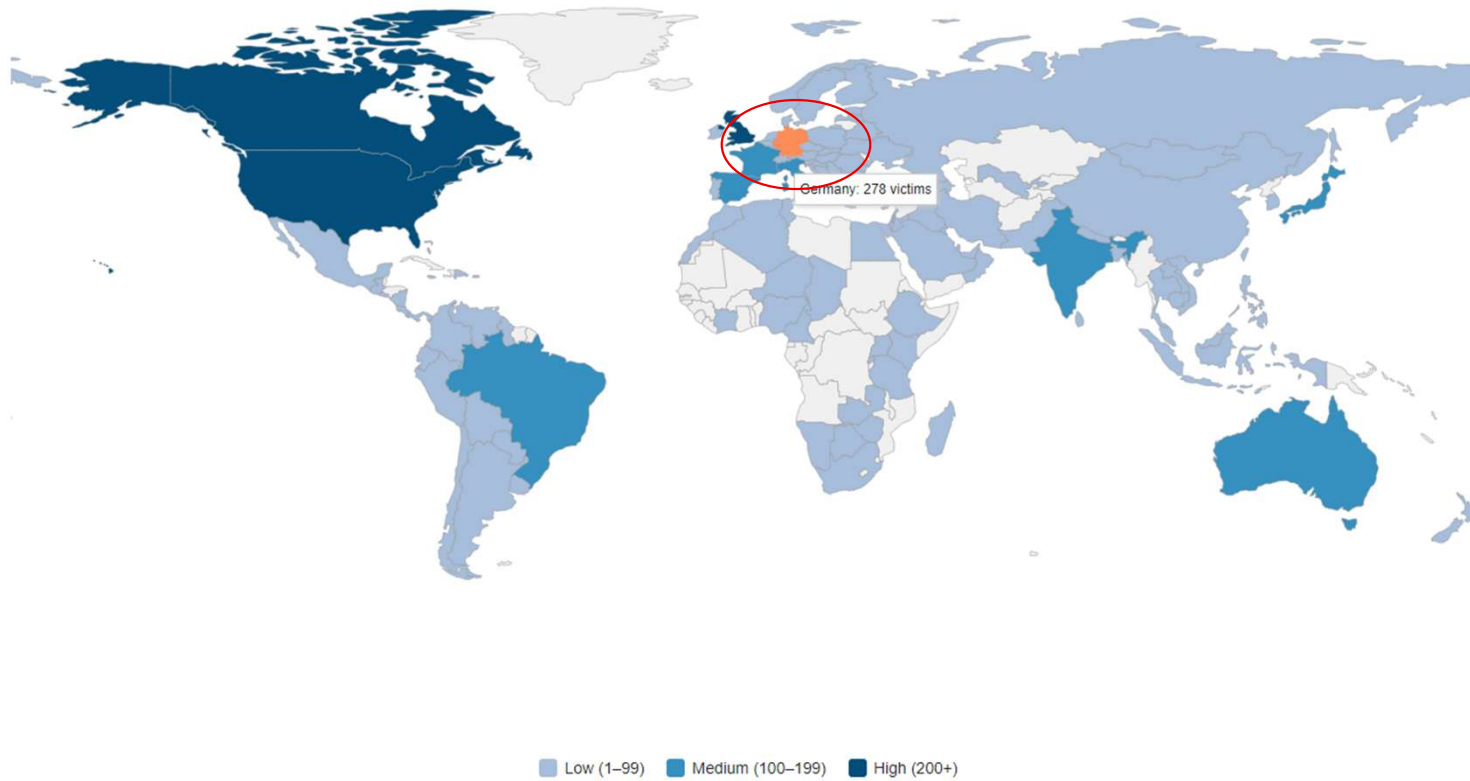
Search victims...

Santa Paula Qilin Discovery Date: 2025-11-27 N/A...	PFMI Incransom Discovery Date: 2025-11-27 Audit documents, clients, client data, financial transactions, contracts...	Enerre Pharma Lda Dragonforce Discovery Date: 2025-11-27 A Enerre Pharma nasce da necessidade de adaptação aos novos tempos. Tendo como base fundadora, a e...
WLR Precision Engineering Qilin Discovery Date: 2025-11-27 N/A...	Rama Judicial Killsec Discovery Date: 2025-11-27 Price ??? Disclosures 0/1...	St Stephens International Thegentlemen Discovery Date: 2025-11-27 Estimated Attack Date: 2025-02-19 https://www.zoominfo.com/c/st-stephens-international-school/1293733677 www.sis.edu St Stephens Inter...

Quelle: ransomware.live

Warum NIS2UmsuCG*?

 Ransomware Victims by Country (2025)



Quelle: ransomware.live

Warum NIS2UmsuCG*?



Companies
News
Sign Up

World Clocks
Los Angeles
C 12:33 AM
New York
C 03:33 AM
London
08:33 AM
Paris
09:33 AM
Moscow
10:33 AM
Beijing
03:33 PM
Tokyo
04:33 PM

Visitors
Last 24 hours
7,140
Last 7 days
49,866
Last month
217,891
Online
38

Companies

All ⁸² Awaiting ¹ Disclosed ¹ Published ⁸¹

Filter

CHRIST Juweliere 1d 23h 26m
Germany
Revenue: \$550M Employees: 2,100 Views: 12

Washington Prime Group Inc Published
United States of America
Revenue: \$512.3M Employees: 500 Views: 3,306

Mavis Tire Supply Published
United States of America
Revenue: \$1.3B Employees: 7,000 Views: 3,217

CHRIST Juweliere 1d 23h 26m
Germany
Revenue: \$550M Employees: 2,100 Views: 12

Saint Mary's Home Published
United States of America
Revenue: \$66.1M Employees: 129 Views: 852

KIPP DC Published
United States of America
Revenue: \$97M Employees: 1,000 Views: 2,880

Sika Footwear Published
Denmark
Revenue: \$9.4M Employees: - Views: 2,305

Sapp Bros Published
United States of America

Description
The leak contains data of CHRIST Juweliere, VALMANO and BRINCKMANN & LANGE. CHRIST is a well-established jewelry company based in Germany, founded in 1863. It specializes in high-quality jewelry and watches, focusing on the mid-to-upper price segment. With over 200 stores across Germany and Austria, CHRIST combines a strong retail presence with a big e-commerce platform, offering a wide range of exquisite pieces online. The company emphasizes customer satisfaction through personalized services, bespoke creations, and expert repairs.

Revenue: \$550M Employees: 2,100 Stocks: - Country: Germany

Website: christ.de

Status: **Disclosed** Updated: 33m

RANSOMWARE.LIVE

Share on:

Infostealer activity detected by [HudsonRock](#)

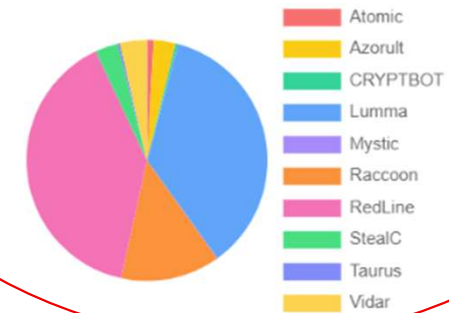
Compromised Employees: 0

Compromised Users: 1133

Third Party Employee Credentials: 0


External Attack Surface: 69

Infostealer Distribution



Quelle: ransomware.live

*NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz



Warum NIS2? (kurzer Grusel- Ausflug)

Cyber Security News und Trends



Ransomware ist und bleibt die größte Bedrohung

Bei Cyberangriffen mit Ransomware beobachtet das BSI eine Verlagerung der Attacken: Nicht mehr nur große, zahlungskräftige Unternehmen stehen im Mittelpunkt, sondern zunehmend auch kleine und mittlere Organisationen sowie staatliche Institutionen und Kommunen. Insbesondere von erfolgreichen Cyberangriffen auf Kommunalverwaltungen und kommunale Betriebe sind die Bürgerinnen und Bürger unseres Landes oft auch unmittelbar betroffen: So kann es dazu kommen, dass bürgernahe Dienstleistungen eine Zeit lang nicht zur Verfügung stehen oder persönliche Daten in die Hände Krimineller gelangen.



Cyberkriminalität wird professioneller

Wie die Realwirtschaft setzen auch Cyberkriminelle zunehmend auf Arbeitsteilung, einen wachsenden Dienstleistungscharakter und eine enge Vernetzung über Länder- und Branchengrenzen hinweg. Mit dem Konzept des „Cybercrime-as-a-Service“ agieren Cyberkriminelle immer professioneller, denn die Spezialisierung auf bestimmte Dienstleistungen ermöglicht es ihnen, ihre „Services“ gezielt zu entwickeln und einzusetzen.

Top 3-Bedrohungen je Zielgruppe:



Cyber Security News und Trends (2023)



TOP 10 Ransomware-Varianten^a

1. LockBit
2. Phobos
3. BlackBasta
4. Akira
5. BlackCat
6. MedusaLocker
7. Play
8. LokiLocker
9. Qilin
10. Royal;
C3RB3R

Durchschnittlich gezahlte Lösegeldsumme^c:

621.858 US-Dollar

Die Gesamtsumme der Lösegeldzahlungen ist 2023 stark angestiegen.

Kriminelle Einnahmen:

> 1,1 Mrd. US-Dollar

Festgestellte Lösegeldzahlungen auf Kryptowallets von Ransomware-Akteuren^d

Angriffe mit über

70

unterschiedlichen Ransomware Varianten^b

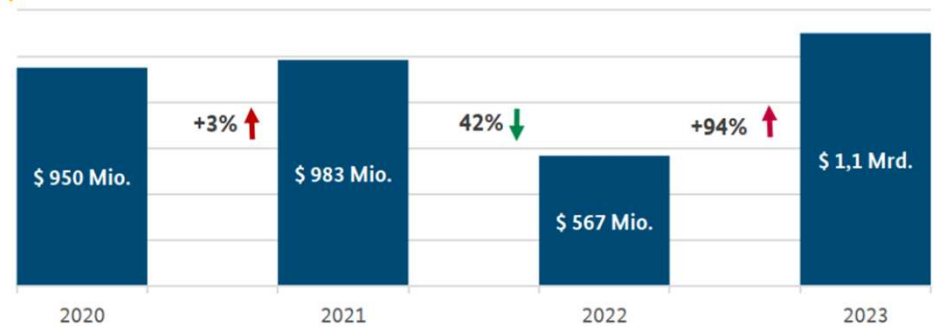
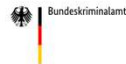
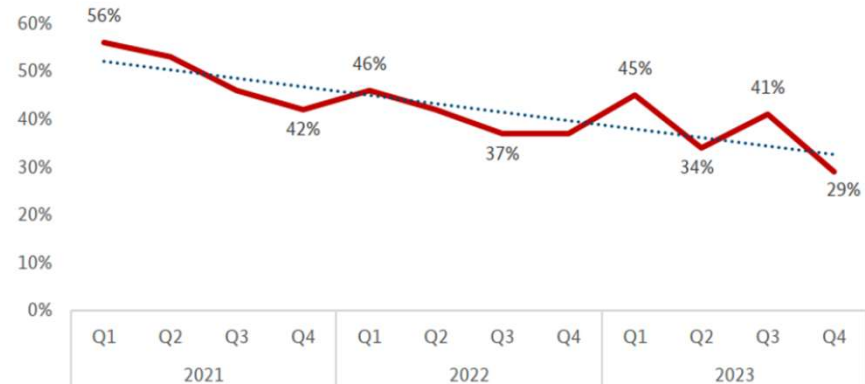


Abbildung 8: Weltweit festgestellte Lösegeldzahlungen auf Kryptowallets von Ransomware-Akteuren 2020 bis 2023. Quelle: Chainalysis (2024). The 2024 Crypto Crime Report




Cyber Security News und Trends - Ursachen



Die IT-Sicherheitslage in Deutschland bleibt auch im Jahr 2024 / 2025 angespannt und herausfordernd. Laut dem Lagebericht 2024 des BSI sind die Bedrohungen durch Ransomware, Advanced Persistent Threats (APT) und andere Cyberattacken weiter gestiegen. Ransomware-Gruppen haben ihre Angriffsmethoden professionalisiert und nutzen häufig Zero-Day-Schwachstellen, um Zugang zu Netzwerken zu erlangen und hohe Lösegelder zu erpressen. Besondere Gefahr geht auch von sogenannten Access Brokern aus, die kompromittierte Zugangsdaten verkaufen und damit die Angriffsfläche vergrößern.

Schwachstellen in Software, Hardware und vernetzten Geräten

Ein weiteres bedeutendes Thema ist die Angriffsfläche, die sich durch die fortschreitende Digitalisierung vergrößert. Schwachstellen in Software, Hardware und vernetzten Geräten bieten Cyberkriminellen zahlreiche Angriffspunkte. Die Angreifer setzen vermehrt auf Malware-as-a-Service (MaaS) und Ransomware-as-a-Service (RaaS), was die Angriffe breiter zugänglich und schwieriger kontrollierbar macht. Auch die Anzahl der DDoS-Angriffe hat im ersten Halbjahr 2024 zugenommen, was auf eine gezielte Stärkung der Angreiferkapazitäten hinweist.



Wer sind die
Täter?

Top Cybergang und Ransomware-Akteure



REWARD
OF UP TO

\$1,000,000 USD

FOR INFORMATION LEADING TO THE ARREST AND/OR CONVICTION OF



Tim Vakhaevich Stigal
a/k/a "Key"

FOR VIOLATIONS INCLUDING AGGRAVATED IDENTITY THEFT; ACCESS DEVICE FRAUD; COMPUTER FRAUD AND ABUSE; WIRE FRAUD; ATTEMPT AND CONSPIRACY.

Submit tips to U.S. Secret Service via:

Email: MostWanted@uss.s.dhs.gov

SECRETSSERVICE.GOV STATE.GOV

U.S. Secret Service UPDATED: 05/2023
WANTED FUGITIVE

UP TO **\$10,000,000 REWARD**

The U.S. Secret Service in concert with the State Department is offering a reward of up to \$10,000,000 for information leading to the arrest and/or conviction of this fugitive. Individuals with information are directed to contact their local U.S. Embassy, consulate or local U.S. Secret Service field office.



Kulkov, Denis Gennadievich

Alias(es): "Денис Геннадьевич Кульков", "Try2Check", "Kreenjo", "Nordex", "Nordexin"
Date of Birth: April 8, 1980
Place of Birth: Russia
Citizenship: Russia
Height (ft./in.): 5'7"
Weight (lbs.): 170
Eye Color: Brown
Hair Color: Black / Balding
Wanted for: ACCESS DEVICE FRAUD, COMPUTER INTRUSION, AND MONEY LAUNDERING
Field Office: New York



ALTERNATE IMAGE 1



ALTERNATE IMAGE 2



ALTERNATE IMAGE 3

CONTACT

Individuals with information are directed to email the U.S. Secret Service at: **MostWanted@uss.s.dhs.gov** **

** Information can be submitted via email in any language

WANTED BY THE FBI

RIM JONG HYOK

Conspiracy to Commit Computer Hacking; Conspiracy to Commit Promotion Money Laundering



DESCRIPTION

Alias: Rim Chong-Hyo'k
Sex: Male
Race: Asian
Languages: English, Korean

REWARD

The Rewards For Justice Program, United States Department of State, is offering a reward of up to \$10 million for information leading to the identification or location of any person who, while acting at the direction or under the control of a foreign government, engages in certain malicious cyber activities against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act, to include Rim Jong Hyok.

REMARKS

Rim Jong Hyok is a North Korean citizen last known to be in North Korea.

CAUTION

Rim Jong Hyok, a member of the Andaril Unit of the North Korean Government's Reconnaissance General Bureau (RGB), a North Korean military intelligence agency, is wanted for allegedly conspiring to violate the Computer Fraud and Abuse Act. Acting on behalf of North Korea's RGB, Rim Jong Hyok allegedly conspired to use the Mau ransomware software to conduct computer intrusions against U.S. hospitals and healthcare companies, extort ransoms, launder the proceeds, and purchase additional internet servers to conduct cyber espionage hacks against government and technology victims in the United States, South Korea, and China.

On July 24, 2024, a federal arrest warrant was issued for Rim Jong Hyok in the United States District Court, District of Kansas, after he was charged with conspiracy to commit computer hacking and conspiracy to commit promotion money laundering.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Kansas City

Cyber Security News und Trends – Der Fall „Darcula“

Strukturen hinter Phishing-Netzwerk rund um "Darcula" aufgedeckt

Eine internationale Recherche hat Strukturen eines Betrugs-Netzwerks aufgedeckt. Rund 900.000 Menschen fielen darauf herein.



(Bild: Bild erstellt mit KI in Bing Designer durch heise online / dmk)

04.05.2025, 13:46 Uhr Lesezeit: 4 Min.



Phishing-Masche per SMS:

Nutzer erhalten vermeintliche Paketbenachrichtigungen (z. B. DHL) mit dem Ziel, Kreditkartendaten über gefälschte Webseiten abzugreifen.

Internationales Cyberkriminellen-Netzwerk:

Ein arbeitsteilig organisiertes Netzwerk mit rund 600 Beteiligten in ca. 130 Ländern steckt hinter den Angriffen.

Entlarvt durch Sicherheitsforscher:

Das norwegische Unternehmen Mnemonic analysierte die Infrastruktur nach Erhalt einer Fake-SMS und infiltrierte interne Chats und eine Telegram-Gruppe.

Phishing-Tool „Magic Cat“:

Mit Hilfe dieses Tools – angeblich KI-gestützt – werden täuschend echte Webseiten erzeugt; es wird als SaaS für mehrere hundert Dollar pro Woche vermietet.

Hauptverdächtiger Entwickler:

Der mutmaßliche Entwickler „Darcula“ (Yucheng C., 24 Jahre, vermutlich aus China) vermietet das Tool, soll aber selbst keine Daten gestohlen haben.

Massive Verbreitung:

In sieben Monaten wurden 13 Mio. Links angeklickt und 884.000 Mal Kartendaten eingegeben – etwa jeder 14. Versuch war erfolgreich.

Umfangreiche Zielauswahl:

Magic Cat bietet Fälschungen von ca. 300 Webseiten, darunter deutsche Anbieter wie DHL, Telekom, Hermes und der Rundfunkbeitrag.

Top Cybergangs und Ransomware-Akteure



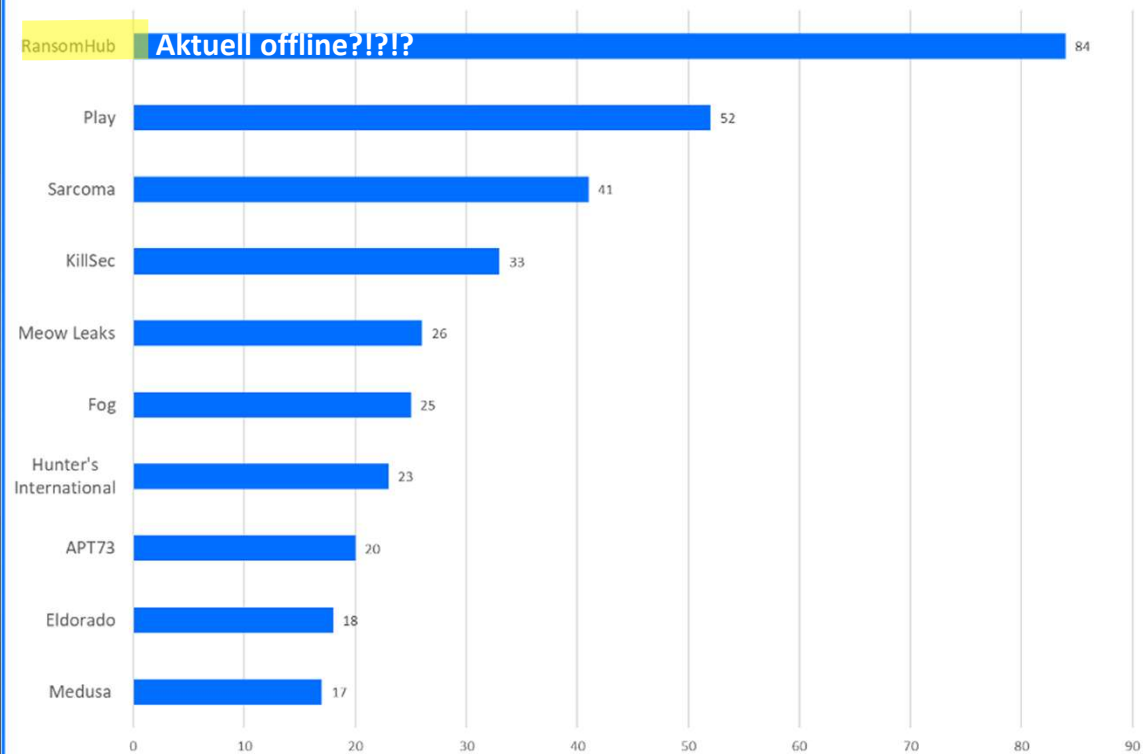
CYBERCRIME INDEX

Ranking countries by cybercrime threat level

Ranking	Country	WCI score	Ranking	Country	WCI score
1	Russia	58.39	11	Iran	4.78
2	Ukraine	36.44	12	Belarus	3.87
3	China	27.86	13	Ghana	3.58
4	United States	25.01	14	South Africa	2.58
5	Nigeria	21.28	15	Moldova	2.57
6	Romania	14.83	16	Israel	2.51
7	North Korea	10.61	17	Poland	2.22
8	United Kingdom	9.01	18	Germany	2.17
9	Brazil	8.93	19	Netherlands	1.92
10	India	6.13	20	Latvia	1.68

Top 10 Ransomware Groups by No. of Victims

October 2024



RansomHub

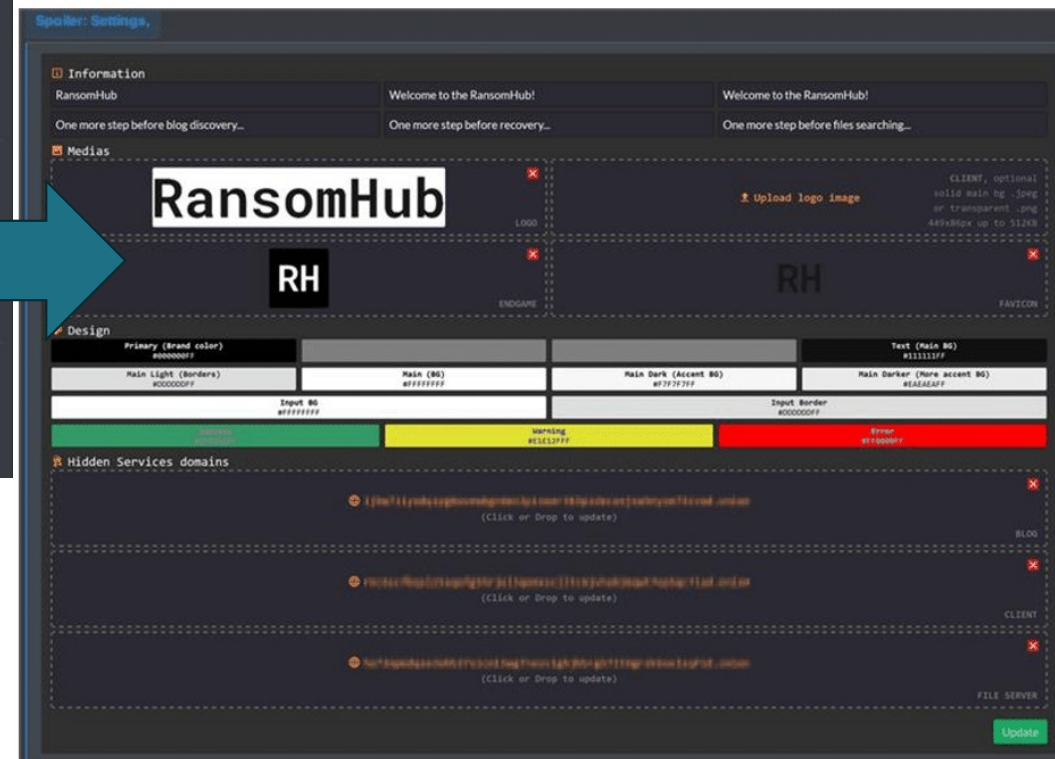
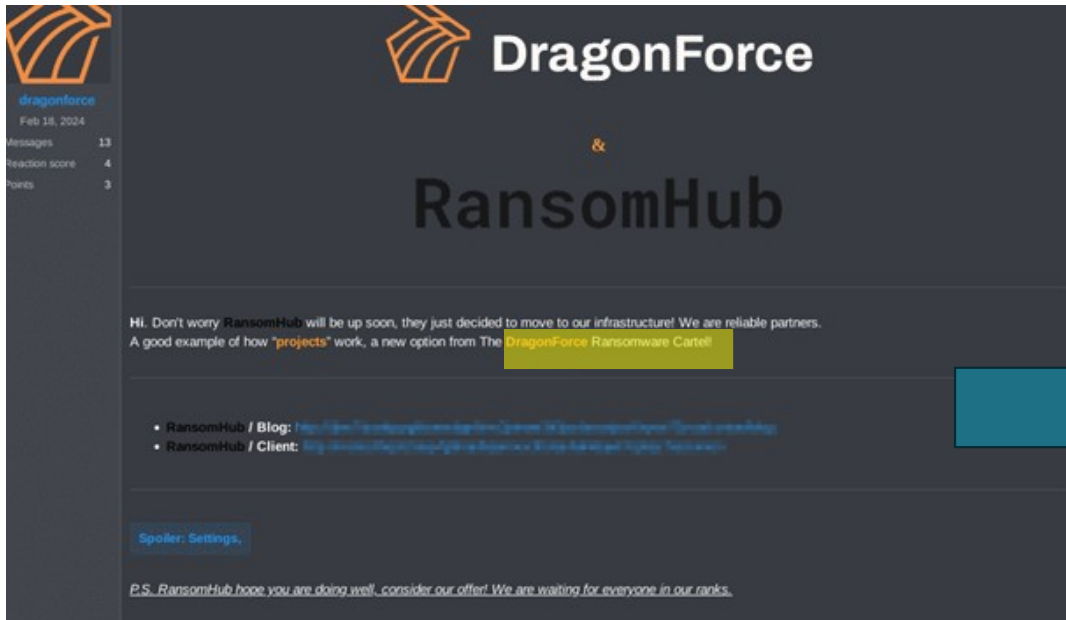



THIS DOMAIN HAS BEEN SEIZED

This domain for PM2BTC and related entities has been seized by the United States Secret Service pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Virginia as part of law enforcement operations by the United States Secret Service and the U.S. Attorney's Office for the Eastern District of Virginia.

In addition, PM2BTC has been identified by the United States Department of Treasury's Financial Crimes Enforcement Network (FinCEN) as a "primary money laundering concern in connection with Russian illicit finance, pursuant to section 9714(a) of the Combating Russian Money Laundering Act, as amended.

RansomHub is gone? Echt? Dragonforce = Ransomhub?





Was geschieht
mit den
gestohlenen
Daten?

Benutzer-Daten: Exfiltration und Handel



Applications ▾ Places ▾ Firefox ESR ▾ Fri 23:56

@tesla.com — DeHashed - Mozilla Firefox

@tesla.com — DeHas: x Pricing — DeHashed x +

https://dehashed.com/search?query=%40tesla.com 133%

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

DEHASHED @tesla.com

Home / Results

473 RESULT(S) FOUND 169MS SEARCH ELAPSED TIME 12,387,953,776 ASSETS SEARCHED 24,552 AGGREGATED DATA WELLS

Search Data Wells Blog Support FAQ Pricing API WHOIS My Account

Results:

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

george@tesla.com
Sourced from ShareThis data
Request entry removal ↗

Safety@Tesla.com
Sourced from ShareThis data
Request entry removal ↗

Tesla@tesla.com
Sourced from ShareThis data

What's DeHashed and those results?
DeHashed is a public data search-engine created for Security Analysts.

Result #240834786

Name	george@tesla.com
Email	george@tesla.com
Username	fc458d6f4759d2799286dda8

Simply click on request entry removal below results and complete the automated on-screen process.

Sonstige Daten: Exfiltration und Handel



Hilfe zur Selbsthilfe – ID-Diebstahl



';--have i been pwned?

Check if your email address is in a data breach

pwned?

Using Have I Been Pwned is subject to [the terms of use](#)

883

pwned websites

14,952,812,162

pwned accounts

115,799

pastes

229,165,825

paste accounts

Largest breaches

- 772,904,991 [Collection #1 accounts](#)
- 763,117,241 [Verifications.io accounts](#)
- 711,477,622 [Onliner Spambot accounts](#)
- 622,161,052 [Data Enrichment Exposure From PDL Customer accounts](#)
- 593,427,119 [Exploit.In accounts](#)
- 509,458,528 [Facebook accounts](#)
- 457,962,538 [Anti Public Combo List accounts](#)
- 393,430,309 [River City Media Spam List accounts](#)
- 361,468,099 [Combollists Posted to Telegram accounts](#)
- 359,420,698 [MySpace accounts](#)

Recently added breaches

- 54,357 [TehetségKapu accounts](#)
- 216,333 [Samsung Germany Customer Tickets accounts](#)
- 984,519 [Qraved accounts](#)
- 2,077,078 [Boulangier accounts](#)
- 162,373 [German Doner Kebab accounts](#)
- 16,627 [Troy Hunt's Mailchimp List accounts](#)
- 1,977,011 [SpyX accounts](#)
- 672,546 [Lexipol accounts](#)
- 220,503 [Color Dating accounts](#)
- 33,294 [Flat Earth Sun, Moon and Zodiac App accounts](#)

HPI Hasso Plattner Institut

Start
Statistiken
FAQ
Antwort-E-Mails

Nutzerkonten	Leaks	Geleakte Accounts pro Tag
14.235.910.752	1.940	1.509.887

Wurden Ihre Identitätsdaten ausspioniert?

Täglich werden persönliche Identitätsdaten durch kriminelle Cyberangriffe erbeutet. Ein Großteil der gestohlenen Angaben wird anschließend in Internet-Datenbanken veröffentlicht und dient als Grundlage für weitere illegale Handlungen.

Mit dem HPI Identity Leak Checker können Sie mithilfe Ihrer E-Mailadresse prüfen, ob Ihre persönlichen Identitätsdaten bereits im Internet veröffentlicht wurden. Per Datenabgleich wird kontrolliert, ob Ihre E-Mailadresse in Verbindung mit anderen persönlichen Daten (z.B. Telefonnummer, Geburtsdatum oder Adresse) im Internet offengelegt wurde und missbraucht werden könnte.

Die von Ihnen eingegebene E-Mail-Adresse wird lediglich zur Suche in unserer Datenbank und das anschließende Versenden einer Benachrichtigungs-E-Mail benutzt. Sie wird von uns in verschleierter Form gespeichert, um Sie vor E-Mail-Spam zu schützen. Die Weitergabe an Dritte ist dabei ausgeschlossen.

[E-Mail-Adresse prüfen!](#)

IT-Security für Unternehmen

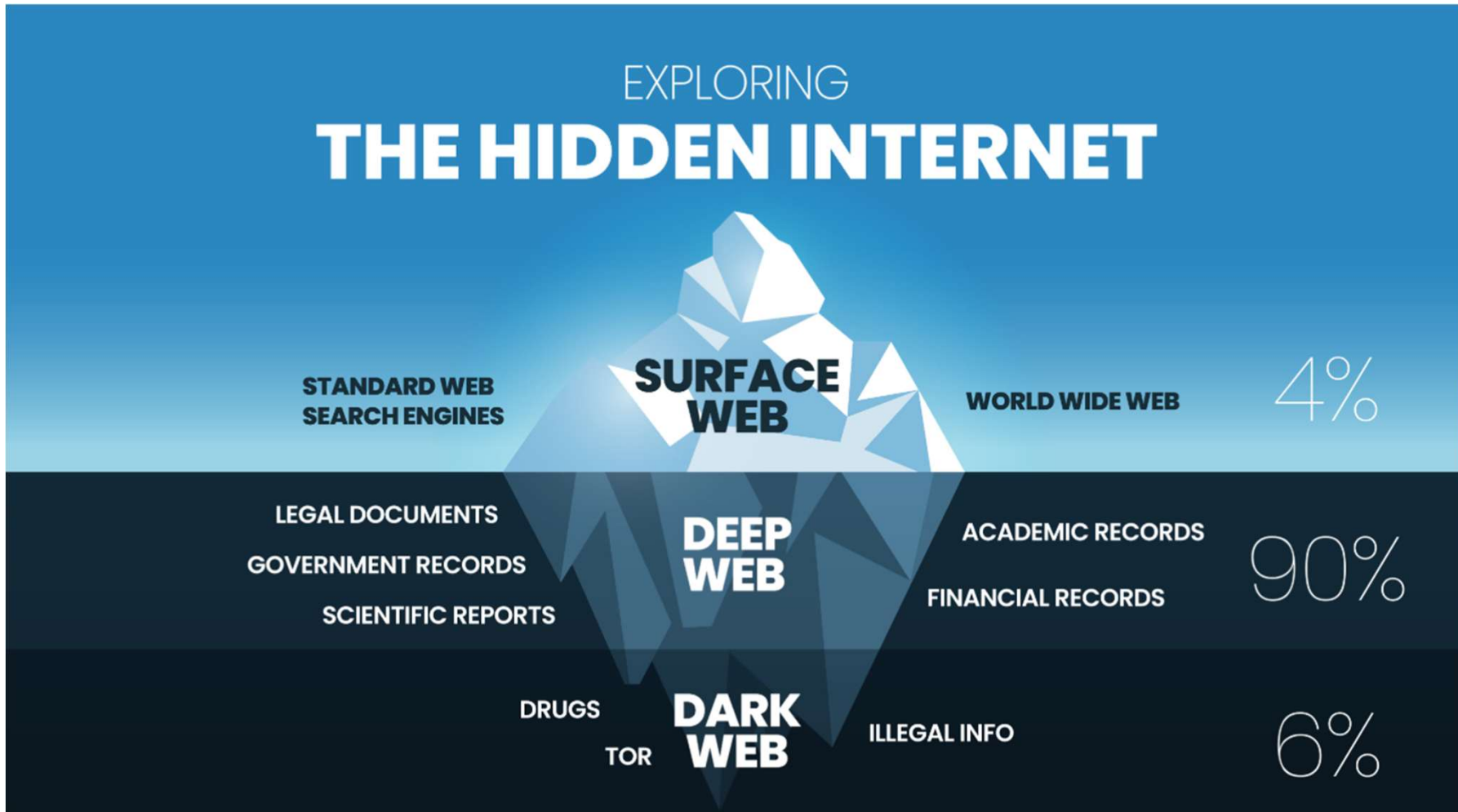
HPI Identity Leak Checker Desktop Client

Täglich werden Unternehmen Opfer von Datendiebstählen. Ein Großteil dieser Daten wird im Internet veröffentlicht. Der ILC Desktop Client hilft Unternehmen und Organisationen dabei, eigene Domänen fortlaufend zu überwachen und mit der ILC-Datenbank abzugleichen. Nach jedem Importvorgang von neuen Leaks wird überprüft, ob E-Mail-Adressen der überwachten Domänen betroffen sind. Der Desktop Client bietet in einem solchen Fall die Möglichkeit, die betroffene(n) E-Mail-Adresse(n) umgehend zu warnen,

Quelle: have i been pwned? / Hasso Plattner-Institut

46

Hilfe zur Selbsthilfe – Dark Web Monitoring



Hilfe zur Selbsthilfe – Dark Web Monitoring



DARK WEB MONITORING

DAS FRÜHWARNSYSTEM FÜR IHRE UNTERNEHMENS SICHERHEIT

ERKENNEN SIE BEDROHUNGEN, BEVOR SIE ESKALIEREN. MADE AND RUN IN GERMANY.

Unsere Darkweb-Analyse kombiniert führende Technologien und tiefgehendes Fachwissen, um ständig nach kompromittierten Daten, gestohlenen Passwörtern und sich anbahnenden Phishing-Angriffen zu scannen. Mit präzisen, maßgeschneiderten Berichten erhalten Sie frühzeitig wertvolle Informationen, um Bedrohungen zu erkennen, bevor sie Schaden anrichten. Schützen Sie sich proaktiv vor Datenverlust und Hackerangriffen und reagieren Sie schneller, um Ihr Unternehmen sicher zu halten.

Cyber Security News und Trends - Lösungsversuche



Mangelnde Cybersicherheit in der Cloud

Die Cybersicherheit in der Cloud bleibt ebenfalls ein kritisches Thema. Mehrere Angriffe auf Cloud-Infrastrukturen haben gezeigt, dass Identitätsdiebstahl und Zugriffe auf sensitive Daten durch Schwachstellen in den Cloud-Services erleichtert werden. Staatlich unterstützte Hackergruppen, etwa aus China, haben gezielt Cloud-Schwachstellen ausgenutzt, was die Dringlichkeit verstärkter Sicherheitsmaßnahmen unterstreicht.

NIS-2 und Cyber Resilience Act

Die Bundesregierung und das BSI reagieren mit neuen Regelungen, darunter die Umsetzung der EU-Richtlinie NIS-2 und des Cyber Resilience Act (CRA). Diese Maßnahmen zielen darauf ab, die Sicherheitsanforderungen für Unternehmen zu erhöhen und zu standardisieren. Insbesondere Betreiber kritischer Infrastrukturen (KRITIS) sind jetzt verpflichtet, Sicherheitsmanagementsysteme (ISMS) zu etablieren und regelmäßig zu überprüfen.

Fazit

Zur Stärkung der Cyberresilienz gibt es Fortschritte. Das BSI hat die IT-Infrastruktur der Bundesverwaltung auf Schwachstellen untersucht und eine hohe Zahl an Sicherheitswarnungen ausgegeben. Auch in der Bevölkerung wächst das Bewusstsein für Cybersicherheit, jedoch bleiben Bildungsmaßnahmen zur Erhöhung der digitalen Kompetenz von zentraler Bedeutung, um gegen Phishing und Social Engineering besser gewappnet zu sein. Abschließend zeigt der Lagebericht, dass Cybersicherheit eine Gemeinschaftsaufgabe ist: Staat, Wirtschaft und Gesellschaft müssen zusammenarbeiten, um die digitalen Räume sicher zu gestalten und die Resilienz Deutschlands gegenüber Cyberbedrohungen weiter zu erhöhen.



Was ist Resilienz?

Was ist Resilienz?

Resilienz

Fähigkeit, Veränderungen im Umfeld zu absorbieren und sich an diese anzupassen

Resilienz der Organisation

Fähigkeit einer Organisation, Veränderungen im Umfeld aufzunehmen und sich an diese anzupassen

Resilienz gewinnt zunehmend an Bedeutung

- Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie)
- Digital Operational Resilience Act (DORA)
- Gesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz) (NIS2)



Wozu / wogegen Resilienz?



Quellen: MidJourney

Wozu / wogegen Resilienz?

Ein **Brand**, ein Wasserschaden oder ein Stromausfall sind klassische Beispiele dafür, wie aus kleinen Unachtsamkeiten schnell ernste Situationen werden können. **Wer sich vorher Gedanken gemacht hat – etwa durch geeignete Versicherungen, Checklisten oder klare Abläufe – steht im Ernstfall deutlich besser da.**

Genügend Beispiele für schwerwiegende Katastrophen gab es in den letzten Jahren ja bereits:

- Das **Jahrhunderthochwasser** in Regensburg im Juni 2013 hat verheerende Schäden in der Weltkulturerbe-Altstadt verursacht. Und das Wasser kommt jedes Jahr wieder. Weiter die Donau abwärts trifft es Passau, Linz und Wien auch Jahr für Jahr aufs Neue!

- Die **Flutkatastrophe** im Ahrtal im Juli 2021 war eine der verheerendsten Naturkatastrophen in Deutschland der letzten Jahrzehnte, bei der über 180 Menschen starben und massive Zerstörungen entstanden.

- Der **Stromausfall** in Berlin 2026 war ein bedeutendes Ereignis, das zehntausende Haushalte betraf und durch einen Brandanschlag auf eine Kabelbrücke verursacht wurde.



Berliner Morgenpost · 1 T.

Stromausfall in Berlin: So steht es um die Rückzahlung der Hotelkosten

Nach dem großen Stromausfall reichten Berliner einen Antrag auf Erstattung der Hotelkosten ein. Wie die Bearbeitung vorangeht ...

Haufe · 4 T.

Lehren aus dem Berliner Stromausfall

Mehrere Tage hatten Tausende Berliner Haushalte keinen Strom und damit meist Heizung. Deutschlands größter Blackout ...

Berliner Kurier · 15 T.

Was wirklich hinter den vielen Stromausfällen in Berlin steckt

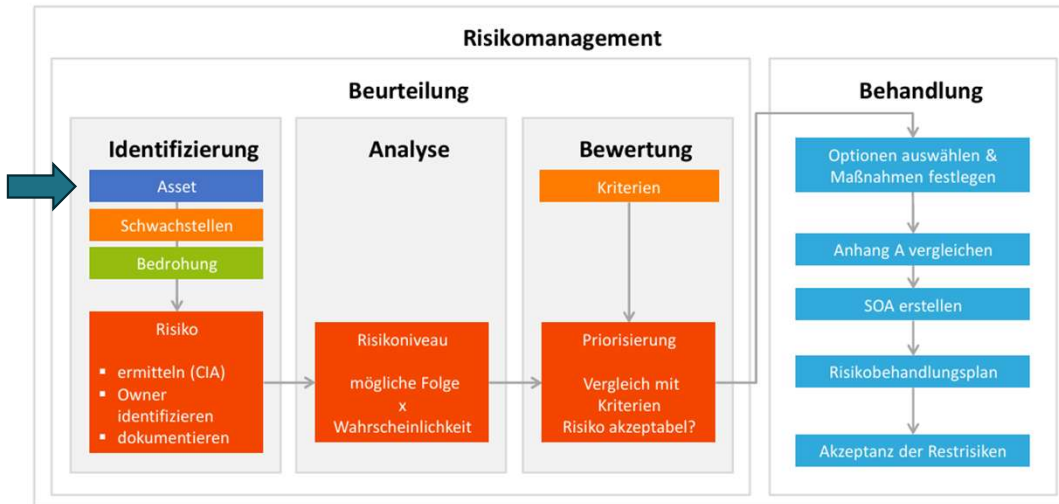
Wieso fällt in Berlin eigentlich ständig der Strom aus? Wir haben bei der Stromnetznachgefragt und eine erstaunliche ...

Wozu / wogegen Resilienz? Gegen Katastrophen! ↓



Brand in Büro-Anlage / Brand im RZ,
Quellen:
Oben rechts: Schaffhauser Polizei /
t.ly/Me93p
Oben links: Alexander Karls /
t.ly/FwEd2 (2026)
Unten R: Alexander Karls /
Hochwasser in Regensburg (2026)
Unten L: Berlin bei Nacht (01.2026)

Wie erreicht man Resilienz? Durch Risikomanagement!

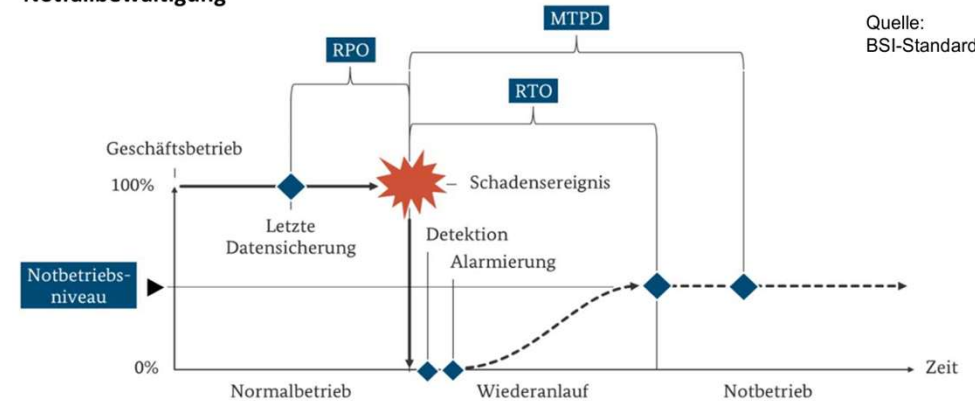


Business Impact Analyse (BIA)

- Welche Prozesse sind kritisch?
- Welche Schäden entstehen bei Ausfall?
- Festlegung von:
 - **RTO** (Recovery Time Objective)
 - **RPO** (Recovery Point Objective)
 - **MTPD** (Maximum Tolerable Period of Disruption)



Notfallbewältigung



Quelle:
BSI-Standard 200-4

Quellen: BSI 200-4

Risikomanagement? So bitte nicht!



Die das-wird-schon-gutgehen-GmbH

- „Das wird schon gutgehen.“ – Die teuerste Form der Risikobewertung und mindestens so wirksam wie ein Schild mit „**Bitte nicht hacken**“ drauf. Oder Weihwasser in der Wasserkühlung und Knoblauch auf dem Server.
- „Das macht unser IT-Dienstleister schon.“ – Verantwortung lässt sich nicht outsourcen.
- „Wir haben doch eine Firewall.“ – Technik ohne Konzept ist Kosmetik.
- „Sicherheitsvorfälle passieren nur den Großen.“ – Angreifer interessieren sich nicht für deine Mitarbeiterzahl. Aber für dein Geld. Und die Angreifer wissen, wie dein Business läuft, dank Bundeswirtschafts-Anzeiger kennen die deine Bilanz! Ach so, Du bilanzierst nicht und bist safe? Guter Take xD Naja, wenn die Angreifer lange genug „drin“ sind, lesen sie auch deine Dokumente, Verträge, Rechnungen etc. Also wissen sie auch mehr als genug. Aus diesem Grund: **Die Police der Cyber-Risiko Versicherung bitte NICHT im Netzwerk speichern, da steht alles drin, was einen Angreifer interessiert und daran wird oft auch die Forderung festgemacht.**
- „Wir haben keine sensiblen Daten.“ – Jeder hat Daten, die jemandem etwas wert sind. Und der Datenschutz / die DSGVO regelt eigentlich sehr genau, was schützenswert ist und was nicht!

Risikomanagement? So bitte nicht!



„Das macht unser IT-Dienstleister.“

Der Dienstleister wartet Systeme, aber niemand im Unternehmen weiß:

Wer entscheidet im Ernstfall?

Wer informiert Kunden?

Wer meldet an Behörden?

Verantwortung wurde delegiert. Risiko nicht.

„Wir haben doch eine Firewall.“

Ja, prima! AAAABER:

Keine Netzwerksegmentierung

Keine MFA für Admin-Zugänge

Kein Monitoring

Technik ohne Konzept ist wie ein Airbag ohne Sicherheitsgurt.

Risikomanagement? So bitte nicht!



„Sicherheitsvorfälle passieren nur den Großen.“

Die Realität:

- Bilanzdaten sind öffentlich einsehbar.
- Umsätze und Liquidität sind grob abschätzbar.
- Die Cyber-Versicherungspolice liegt als PDF im Fileshare.

Der Angreifer weiß:

- Was das Unternehmen verdient
- Welche Versicherungssumme existiert
- Wie lange ein Produktionsstillstand weh tut
- **Und danach richtet sich die Forderung.**

Sicherheit & Resilienz sind kein Produkt!



- Keine Checkbox im Audit.
- Kein „haben wir doch“.

Sicherheit ist Verhalten – und ein Gefühl!

- Wie konsequent patchen / updaten wir?
- Wie klar sind Rollen definiert? Was sind Rollen?
- Wie oft üben wir den Ernstfall?
- Wie ernst nehmen wir Meldewege? Gibt's sowas bei uns?
- Wie bewusst gehen wir mit Informationen um?

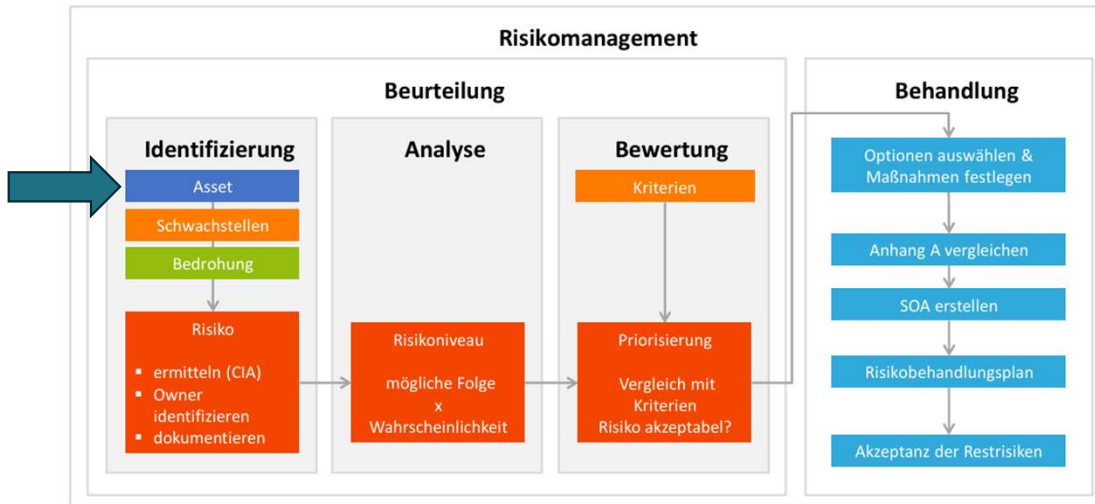
Resilienz entsteht durch Haltung! Nicht durch Hoffnung!

Sicherheit & Resilienz sind kein Produkt!



Sicherheit und Resilienz sind kein Hexenwerk, sondern Handwerk!

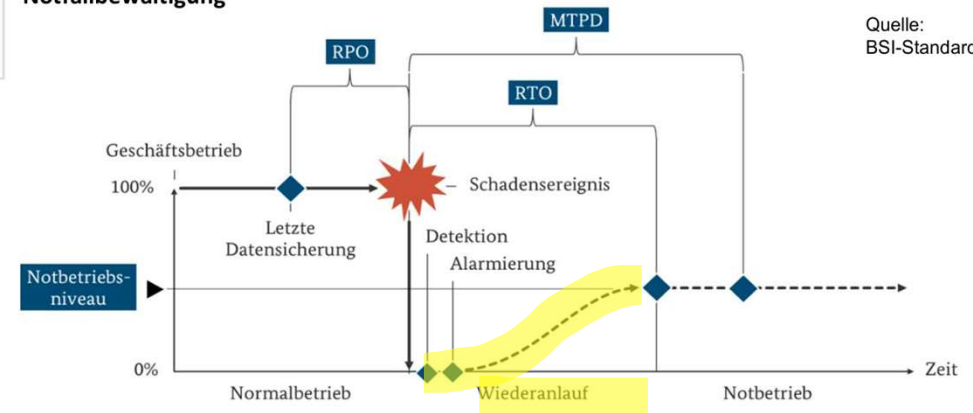
Zurück zum Risikomanagement:



Business Impact Analyse (BIA)

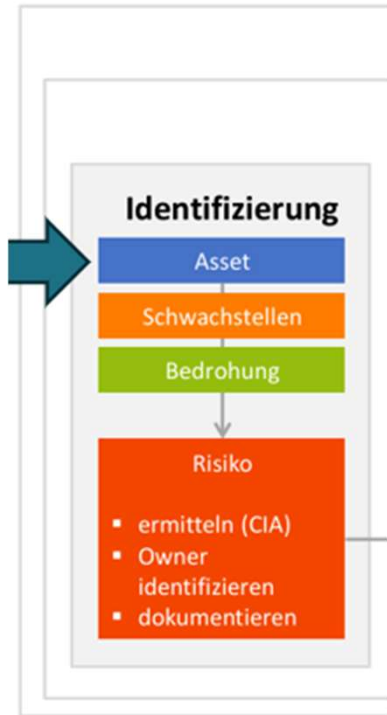
- o Welche Prozesse sind kritisch?
- o Welche Schäden entstehen bei Ausfall?
- o Festlegung von:
 - **RTO** (Recovery Time Objective)
 - **RPO** (Recovery Point Objective)
 - **MTPD** (Maximum Tolerable Period of Disruption)

Notfallbewältigung



Quellen: BSI 200-4

Risikomanagement - Assets



Anlage 7 - Kritische IT-Systeme

GAP-Analyse, Version 1.0
ITVentive AG

Datum:
Ersteller:

Legende: (H)ardware, (S)erver, (N)etzwerk, (V)irtualisierung, (C)loud, (St)orage

systeme							Abhängigkeiten	
index	Reihenfolge	Verfügbarkeit bei Wiederanlauf	IT-System	(P)hysikalisch / (V)irtuell / (C)loud	Max. tolerierbare Ausfallzeit in Stunden (h)	Priorität	Erforderliche Ressourcen	Single-Point-of-Failures (SPOF)
h1	1		USV	P	4	A	Strom Stadtwerke	Stadtwerke, keine redundante Stromzuführung, kein Diesel
st1	2		Primäres Storage System (Pure Storage X20 R2)	P	4	A	H1, Frontend-Netzwerk, Storage-Netzwerk, Stromversorgung, Routing, DNS, Klimatisierung	Stadtwerke, keine redundante Stromzuführung, kein Diesel
vi1	3		Virtualisierungs-System für Server (VMWare ESXi auf Lenovo ThinkSystem SR665), bestehend aus drei Servern (physikalische Nodes)	P	4h für Cluster, 24h für einzelne Nodes	A	3 Server / Hypervisor (Redundanz 2+1), Frontend-Netzwerk, Storage-Netzwerk, DMZ-Netzwerk, St1, H1, Routing, DNS, Klimatisierung	Stadtwerke, keine redundante Stromzuführung, kein Diesel
v1	2		Core-Netzwerk	P	2	A	Strom Stadtwerke	Stadtwerke, keine redundante Stromzuführung, kein Diesel
v2	2		Core-Router	P	1	A	Strom Stadtwerke	Stadtwerke, keine redundante Stromzuführung, kein Diesel
v3	2		Firewall	P	1	A	Strom Stadtwerke	Stadtwerke, keine redundante Stromzuführung, kein Diesel, Single Instance
c1	99		MS365	C	6	A	Internet, Netzwerk, DNS	Internet nicht redundant
c2	99		Azure	C	6	A	Internet, Netzwerk, DNS	Internet nicht redundant

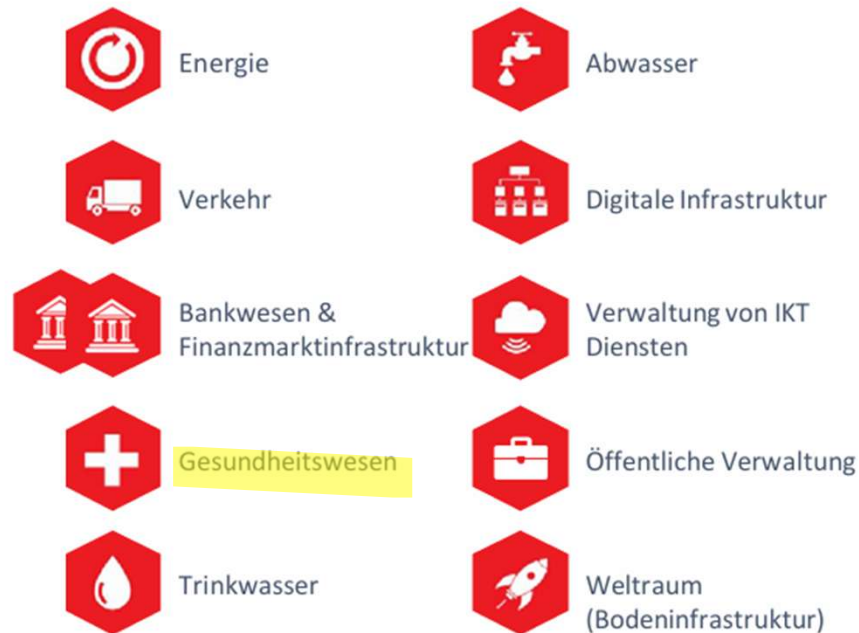


Zurück zu NIS2



Wen betrifft NIS2?

Sektoren mit hoher Kritikalität (nach Anlage I der Richtlinie)



Sonstige kritische Sektoren (nach Anlage II der Richtlinie)



Die Sektoren nach den Anlagen gem. NIS2UmsuCG*



Gesundheitswesen



Es gibt 1841 Krankenhäuser in Deutschland, davon besitzen einige wenige große Krankenhäuser eine 27001-Zertifizierung, meist mit Fokus auf Rechenzentrum.

Fragen:

- Bin ich selbst betroffen? > Siehe Betroffenheitsprüfung


- Was ist mit der Lieferkette? Art. 21 Abs. 2 lit. d und Abs. 3 NIS-2-RL verlangt Sicherheit bei Lieferketten!

- Anhang 1 Ziff. 8, sicherlich für IT-Hersteller von Interesse.

Beispielsweise „Anbieter von Cloud-Computing-Diensten“: Anbieter von Arztpraxissystem as a Service, Krankenhausinformationssystemen as a Service. Oder allgemeiner SaaS-Anbieter im Gesundheitswesen: fallen die darunter? Muss SBOM** eingeführt werden? Wenn ja, wie geht man vor? < Lieferketten-Audits, nächste 2 Folien!

SBOM*-Lösungen



 **LocateRisk** +49 6151 6290246

Auditieren Sie Ihre Zulieferer

Geschäftspartner Risikomanagement

Sind die IT-Systeme Ihrer Geschäftspartner nicht angemessen geschützt, kann das Ihre eigene IT-Sicherheit bedrohen. Mit LocateRisk erhalten Sie jederzeit schnellen Einblick in das Cyberrisiko von Lieferanten und Dienstleistern.

[Demo anfragen](#)

Effizienz erhöhen, Risiken reduzieren mit Lieferanten-Monitoring

- ✓ Cyberrisiken in der Lieferkette kontinuierlich überwachen – auf Basis objektiver Daten
- ✓ Lieferanten-Risikomanagement-Prozesse automatisieren und beschleunigen
- ✓ Optimierungsabläufe verbessern – durch proaktive Zusammenarbeit mit Geschäftspartnern
- ✓ Regelmäßige Sicherheitskontrollen nachweisen

OPSWAT.

GUIDE

SBOM Guide for 2025: Turn Compliance into a Security Asset

Everything you need to know about SBOM concepts, how they work, and how your organization can stay compliant while securing your software supply chain.

SBOM (Software Bill of Materials) has evolved far beyond a simple list of components. As organizations implement software supply chain security protocols, SBOM functions as a strategic asset that guides risk management, drives compliance, and serves as a security compass to keep up with changes in the SDLC (software development lifecycle).

Share this Guide

[f](#) [X](#) [in](#) [✉](#)

Kostenlose SBOM*-Lösungen



microsoft / sbom-tool

Code Issues 43 Pull requests 39 Actions Projects Models Security Insights

sbom-tool Public Watch 30 Fork 183 Star 1.9k

main 65 Branches 88 Tags

Go to file Add file Code

ZhengHong-Tan and zhongtan Upgrade .NET SDK version in global.json (#1334) 3621337 · 3 days ago 580 Commits

File	Commit Message	Time Ago
.github	Bump actions/setup-dotnet from 4.3.1 to 5.0.0 (#1202)	2 months ago
docs	Major version bump for Component Detection (#1323)	2 weeks ago
pipelines	Remove GH packages release step from pipeline (#1333)	4 days ago
samples	Add plumbing to collect packages from SPDX 2.2 files (#1117)	5 months ago
src	Bump NuGet.Frameworks from 6.13.2 to 6.14.0 (#1179)	2 months ago
test	Add COSE paths to SbomConfig (#1152)	3 months ago
.editorconfig	disable this prefix convention (#1088)	6 months ago
.gitattributes	Initial commit	3 years ago
.gitignore	ignore Rider + ReSharper temp (#1046)	6 months ago
CODE_OF_CONDUCT.md	Initial commit	3 years ago
Directory.Build.props	move strong naming config into dir props (#1061)	6 months ago
Directory.Build.targets	Use tool-driven indents for *.props (#750)	last year
Directory.Packages.props	Major version bump for Component Detection (#1323)	2 weeks ago
Dockerfile	Clean apt cache in Dockerfile to reduce image size	9 months ago
LICENSE	Initial commit	3 years ago
Microsoft.Sbom.sln	Move spdx extensions to common utils and refactor SPDX 2...	8 months ago
README.md	We are changing policy and will no longer accept external c...	2 months ago

About

The SBOM tool is a highly scalable and enterprise ready tool to create SPDX 2.2 compatible SBOMs for any variety of artifacts.

sbom sbom-generator

Readme MIT license Code of conduct Security policy Activity Custom properties 1.9k stars 30 watching 183 forks Report repository

Releases 69

v4.1.4 Latest last week + 68 releases

Packages 9

- Microsoft.SBOM.Adapters
- Microsoft.Sbom.Extensions
- Microsoft.Sbom.Parsers.Spdx22SbomParser



Mehr unter
t.ly/oeXFH

Betroffenheitsprüfung zu NIS2UmsuCG*. Neue Seite des BSI:



KONTAKT ENGLISH GEBÄRDENSPRACHE LEICHTE SPRACHE NUTZUNGSBEDINGUNGEN LOGIN

Deutschland
Digital•Sicher•BSI

Das BSI Themen IT-Sicherheitsvorfall Karriere Service

Themen > Regulierte Wirtschaft > NIS-2-regulierte Unternehmen



#nis2know für Unternehmen

Viele Unternehmen und Einrichtungen, die mit NIS-2 erstmals durch das BSI reguliert werden, stehen vor der Frage, was sie jetzt tun müssen.

Lesen Sie hier, auf welche neuen Pflichten Sie sich einstellen müssen.

[MEHR ERFAHREN](#)

#nis2know: Schneller Einstieg in NIS-2

Sie wollen gleich loslegen? Hier finden Sie die wichtigsten Informationen auf einen Blick.

 NIS-2-Betroffenheitsprüfung	 NIS-2 - Was tun?	 NIS-2-Richtlinie	 Sektorspezifische Informationen
--	---	---	--

➔ t.ly/d2Qz3

Sind Sie unsicher, ob Ihr Unternehmen von der NIS-2-Richtlinie der EU betroffen ist?

Die > NIS-2-Betroffenheitsprüfung des BSI bietet Ihnen in wenigen Schritten dafür eine erste Orientierung.

Die NIS-2-Betroffenheitsprüfung stellt Ihnen konkrete, an der Richtlinie orientierte Fragen, um Ihr Unternehmen einzuordnen. Die Fragen sind kurz und präzise gehalten und werden bei Bedarf im Kleingeschriebenen tiefergehend erläutert.

Nachdem Sie den Fragenkatalog durchlaufen haben, erhalten Sie ein auf Ihren Angaben basierendes Ergebnis. Dieses gibt eine automatisierte Ersteinschätzung, ob Ihr Unternehmen von der NIS-2-Richtlinie betroffen ist.

Die Nutzung der NIS-2-Betroffenheitsprüfung erfolgt anonym. Das BSI stellt diese im Rahmen seiner Kooperationsaufgabe zur Verfügung. Sie erfasst keine Daten, die personenbezogen sind oder Rückschlüsse zur Identifizierung Ihres Unternehmens geben. Bitte beachten Sie, dass die Hilfe zur Betroffenheitsprüfung von NIS-2 lediglich als Orientierungshilfe dient und Ihr Ergebnis rechtlich nicht bindend ist, da Ihre Antworten automatisiert erstellt und nicht vom BSI oder anderen unabhängigen Stellen geprüft werden. Es besteht kein Anspruch auf Vollständigkeit und Richtigkeit der Inhalte.

Zurzeit basieren die Abfragen der NIS-2-Betroffenheitsprüfung auf dem Gesetzentwurf des NIS-2 Umsetzungsgesetzes des BMI (Stand 25.07.2025). Sobald das finale Umsetzungsgesetz beschlossen und verabschiedet wurde, wird das BSI die NIS-2-Betroffenheitsprüfung anhand dieses Gesetzes anpassen und aktualisieren.

Haben Sie zu oder nach der Nutzung noch Fragen? Das BSI steht gerne zur Verfügung.

Die NIS-2-Betroffenheitsprüfung dient als automatische Orientierungshilfe auf Grundlage von Eigenangaben, deren Ergebnis nicht rechtlich bindend ist. Die NIS-2-Betroffenheitsprüfung ersetzt die Prüfung zur Selbst-Identifizierung nicht und hat für eventuelle Verfahren keine Indizwirkung.

Einrichtungen der Bundes-, Landes- und Kommunalverwaltung werden in der NIS-2-Betroffenheitsprüfung nicht betrachtet.

Quelle: BSI



Die Anforderungen gem. NIS2UmsuCG*

Registrierungspflicht

Umsetzung von Risikomanagementmaßnahmen

- Geltungsbereich ist die gesamte IT
- Dokumentation bzw. (regelmäßiger) Nachweis der Umsetzung

Meldepflichten für (erhebliche) Sicherheitsvorfälle

Pflichten und Haftung der Geschäftsleitung

- Steuerung und Überwachung des gesamten Risikomanagement-Prozesses
- Regelmäßige Schulung zum „Cybersicherheits-Risikomanagement“
- Haftung nach den üblichen Grundsätzen, jetzt aber explizit „kodifiziert“

(Pflicht zum Einsatz von Produkten mit Cybersicherheitszertifizierung)

Risikomanagement nach Art. 21 Abs. 2 NIS2UmsuCG*



- **Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;**
- Bewältigung von **Sicherheitsvorfällen**;
- Aufrechterhaltung des Betriebs, wie **Backup-Management und Wiederherstellung** nach einem **Notfall**, und **Krisenmanagement**;
- **Sicherheit der Lieferkette** einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;
- **Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung** von Netz- und Informationssystemen, einschließlich **Management und Offenlegung von Schwachstellen**;
- **Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen** im Bereich der Cybersicherheit;
- grundlegende Verfahren im Bereich der **Cyberhygiene** und **Schulungen im Bereich der Cybersicherheit**;
- Konzepte und Verfahren für den Einsatz von **Kryptografie** und gegebenenfalls Verschlüsselung;
- **Sicherheit des Personals**, Konzepte für die Zugriffskontrolle und Management von Anlagen;
- Verwendung von Lösungen zur **Multi-Faktor-Authentifizierung** oder kontinuierlichen Authentifizierung, **gesicherte Sprach-, Video- und Textkommunikation** sowie gegebenenfalls gesicherte **Notfallkommunikationssysteme** innerhalb der Einrichtung.

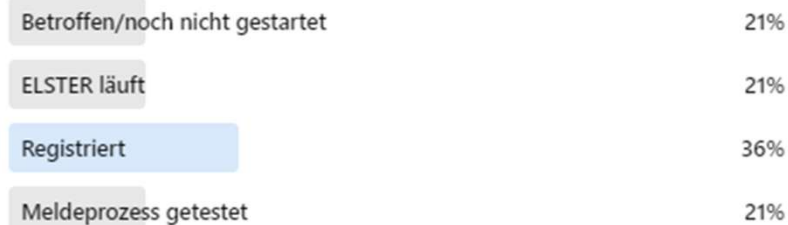


NIS2: Meldung und Registrierung

1. Betroffenheitsprüfung durchführen. Sofern „betroffen“:
2. Rücksprache mit Rechtsanwalt
3. Aktuelles (!) Elster Zertifikat besorgen
4. Registrierung starten und Zertifikate zur Hand haben (oder noch wissen, wo man das Zertifikat gespeichert hat. Kennwort zum Zertifikat kennen!
5. Meldung und Registrierung durchführen 😊

Wo stehst Du aktuell bei NIS-2? (ehrlich 😊)

Die Person, die die Umfrage erstellt hat, kann sehen, wie Sie abgestimmt haben. [Mehr erfahren](#)



14 Stimmen • Umfrage geschlossen

Quelle: Lina Hampe auf LinkedIn



NIS2: Meldung und Registrierung – Noch Fragen?

Für rund 29.500 Unternehmen in Deutschland gelten seit Inkrafttreten des [NIS-2-Umsetzungsgesetzes](#) am 06.12.2025 neue gesetzliche Pflichten in der [IT-Sicherheit](#). Sie müssen sich registrieren, dem Bundesamt für Sicherheit in der Informationstechnik ([BSI](#)) erhebliche Sicherheitsvorfälle melden, Risikomanagementmaßnahmen implementieren und dokumentieren.

Das [NIS-2-Starterpaket](#) des [BSI](#) gibt betroffenen Unternehmen Hilfestellungen, wie sie die ersten Schritte der neuen Regulierung konkret angehen.

Anleitungen [BSI-Portal](#)

Das [BSI-Portal](#) ermöglicht Unternehmen, ihren gesetzlichen Registrierungs- und Meldepflichten nachzukommen.

Wichtig: Bevor Sie sich im [BSI-Portal](#) registrieren können, benötigen Sie ein [ELSTER-Organisationszertifikat](#). Dieses können Sie auf der Webseite ["Mein Unternehmenskonto"](#) (MUK) generieren lassen.

› [Eine Anleitung zu "Mein Unternehmenskonto" finden Sie hier.](#)

Für die wichtigsten Funktionen des [BSI-Portals](#) haben wir Klickanleitungen erstellt, um den Einstieg in die Nutzung zu erleichtern:

- › [Nutzeroberfläche und Administration](#)
- › [Registrierung im \[BSI-Portal\]\(#\)](#)
- › [Meldung von Sicherheitsvorfällen über das \[BSI-Portal\]\(#\)](#)

Quelle: [BSI: t.ly/QRf5r](#)

Zum Thema Resilienz, Souveränität und Geopolitik:



ITventive
digital future today

FOLGE #110

BLUESCREEN

ZWISCHEN RECHT UND RISIKO WIE CYBERSECURITY ZUR GEOPOLITISCHEN WAFFE WURDE

ALEXANDER KARLS **PROF. DR. KIPKER**

Willkommensbildschirm mit ITventive-Logo, Titel 'BLUESCREEN FOLGE #110', Haupttitel 'BLUESCREEN ZWISCHEN RECHT UND RISIKO WIE CYBERSECURITY ZUR GEOPOLITISCHEN WAFFE WURDE', Porträts der beiden Gäste, ein Mikrofon-Symbol und ein Audiogramm am unteren Rand.

BLUESCREEN - DER TECH-PODCAST!

Startseite Alle Episoden Abonnieren

BlueScreen - Der Tech-Podcast!

Willkommen bei BlueScreen, deinem neuen Lieblings-Podcast der ITventive AG, ehemals pegasus IT (pegasus GmbH)!

Unseren Podcast stellen wir zusätzlich zu unseren anderen Kanälen wie Facebook, LinkedIn und YouTube für unsere Kunden und Interessenten zur Verfügung. Die Themen sind in erster Linie technischer Natur, wir haben auch immer wieder Gäste aus der Wirtschaft und Technologie-Anbieter im Interview.

Über unseren Host und Gastgeber, Alex: Keyboard-Jockey seit 1985 (SX64 <3) und schon seit mehr als 20 Jahren im professionellen IT-Bereich unterwegs. Spricht fließend l3375p34k, "EDV-Chinesisch" und CEO-taugliches Hochdeutsch. Als Unternehmer-Sohn geboren und aufgewachsen, mit VHS und Tapedeck groß geworden und mit den Clouds dieser Welt laufen gelernt. Technik-Verliebter Consultant, Berater, Trainer, Coach und Vater. Automatisierer, Scripter, Coder und Logs-Lesender Mensch.


Ihr findet uns im Web unter folgender Adresse: <https://www.itventive.com>

Du willst uns mal so richtig was sagen? Dann bitte hier entlang > <https://www.speakpipe.com/bluescreen>

Aktuelle Episode abspielen **Podcast abonnieren**

Webseite des Podcasts mit Überschrift, Begrüßungstext, Beschreibung des Hosts, Kontaktinformationen und zwei Handlungsknöpfe. Ein Thumbnail zeigt den Host mit dem Text 'STAFFEL 5'.

<https://bluescreen.podigee.io/>



NIS2 einführen und umsetzen (Theorie)



Maßnahmen zum Risikomanagement

§ 30 Abs. 1 BSIG-E:

Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, ... , zu ergreifen,

um Störungen der **Verfügbarkeit, Integrität und Vertraulichkeit** der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten.


Bei der Bewertung der Verhältnismäßigkeit der Maßnahmen nach Satz 1 sind das **Ausmaß der Risikoexposition**, die Größe der Einrichtung, die Umsetzungskosten und die **Eintrittswahrscheinlichkeit** und **Schwere von Sicherheitsvorfällen** sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen.

Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu **dokumentieren**.

Mindestmaßnahmen nach § 30 Abs. 2 BSIG-E



1. Risikoanalyse und Sicherheit
2. Bewältigung von Sicherheitsvorfällen
3. Betriebsaufrechterhaltung: Backup, Wiederherstellung & Krisenmanagement
4. Sicherheit der Lieferkette (...) und ihren unmittelbaren Anbietern oder Diensteanbietern
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von IT-Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen.
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der IT-Sicherheit
7. Cyberhygiene und Schulungen im Bereich der Sicherheit in der IT
8. Einsatz von Kryptografie und Verschlüsselung.
9. Konzepte für die Zugriffskontrolle und für das Management von Anlagen.
10. (...) Multi-Faktor-Authentifizierung und gesicherte Notfallkommunikation.



NIS 2 einführen und umsetzen (Praxis)

NIS2 einführen und umsetzen




Bestandsaufnahme & Risikobewertung	Kritische Systeme identifizieren, Risikoanalyse durchführen
Zuständigkeiten festlegen	Verantwortliche Person benennen, Notfallteam festlegen
Sicherheitsstrategie entwickeln	IT-Sicherheitsstrategie mit Geschäftsleitung entwickeln
IT-Sicherheitsrichtlinien erstellen	Passwortrichtlinien, Netzwerkzugriff, Verschlüsselung
Technische Schutzmaßnahmen implementieren	Firewall, Anti-Malware, Backup-Systeme implementieren
Notfallmanagement und Meldesystem einrichten	Meldesystem und Notfallplan etablieren, Meldewege klären
Regelmäßige Mitarbeiterschulung	Mitarbeiterschulung, Sensibilisierung für Cyber-Risiken
Vorfall-Dokumentation und Berichterstattung	Vorfälle dokumentieren, regelmäßig Bericht erstellen
Kontinuierliche Überprüfung und Verbesserung	Kontinuierliche Überprüfung, Penetrationstests



Die sechs häufigsten Fehler bei der Umsetzung

1. **Geltungsbereich nicht eindeutig identifiziert** – Viele Unternehmen prüfen nicht sorgfältig, ob sie als „wesentliche“ oder „wichtige Einrichtung“ unter NIS-2 fallen. Damit läuft man Gefahr, die Anforderungen zu unterschätzen.
2. **Auf finale nationale Gesetzesfassung warten statt früh anfangen** – Einige Organisationen verschieben Maßnahmen, bis das deutsche Umsetzungsgesetz vollständig verabschiedet ist. Das führt oft zu Zeitdruck und unzureichender Vorbereitung.
3. **Compliance nur auf dem Papier („PowerPoint-Security“)** betreiben – Dokumentation und Prozesse können existieren, ohne dass sie im Alltag gelebt werden. Das gibt ein falsches Sicherheitsgefühl.
4. **Incident-Response und Wiederherstellung nicht geübt**. Backup- und Recovery-Pläne existieren zwar, werden aber selten oder nie auf Funktionalität getestet — im Ernstfall droht Chaos statt Kontrolle.
5. **Mangelnde Verankerung im Management und fehlende Verantwortlichkeit** – IT-Sicherheit wird weiterhin als technische Aufgabe gesehen, statt als Management- und Führungsaufgabe mit klaren Verantwortungen.
6. **Lieferketten- und Drittanbieter-Risiken werden ignoriert** – Viele sehen nur die eigene Infrastruktur und lassen Drittparteien-Risiken außen vor — ein gefährlicher Fehler unter NIS-2. Security-Insider

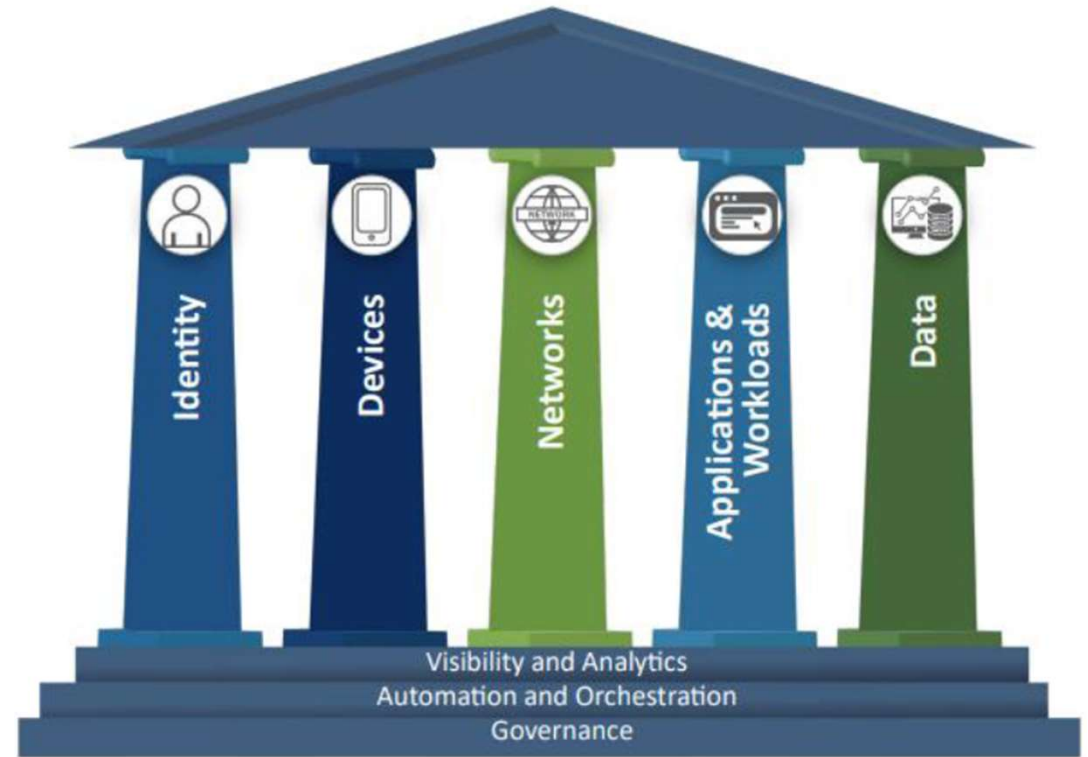


Regel Nr. 1:
Kenne deine
Assets / Werte!

Know your Assets / Werte!



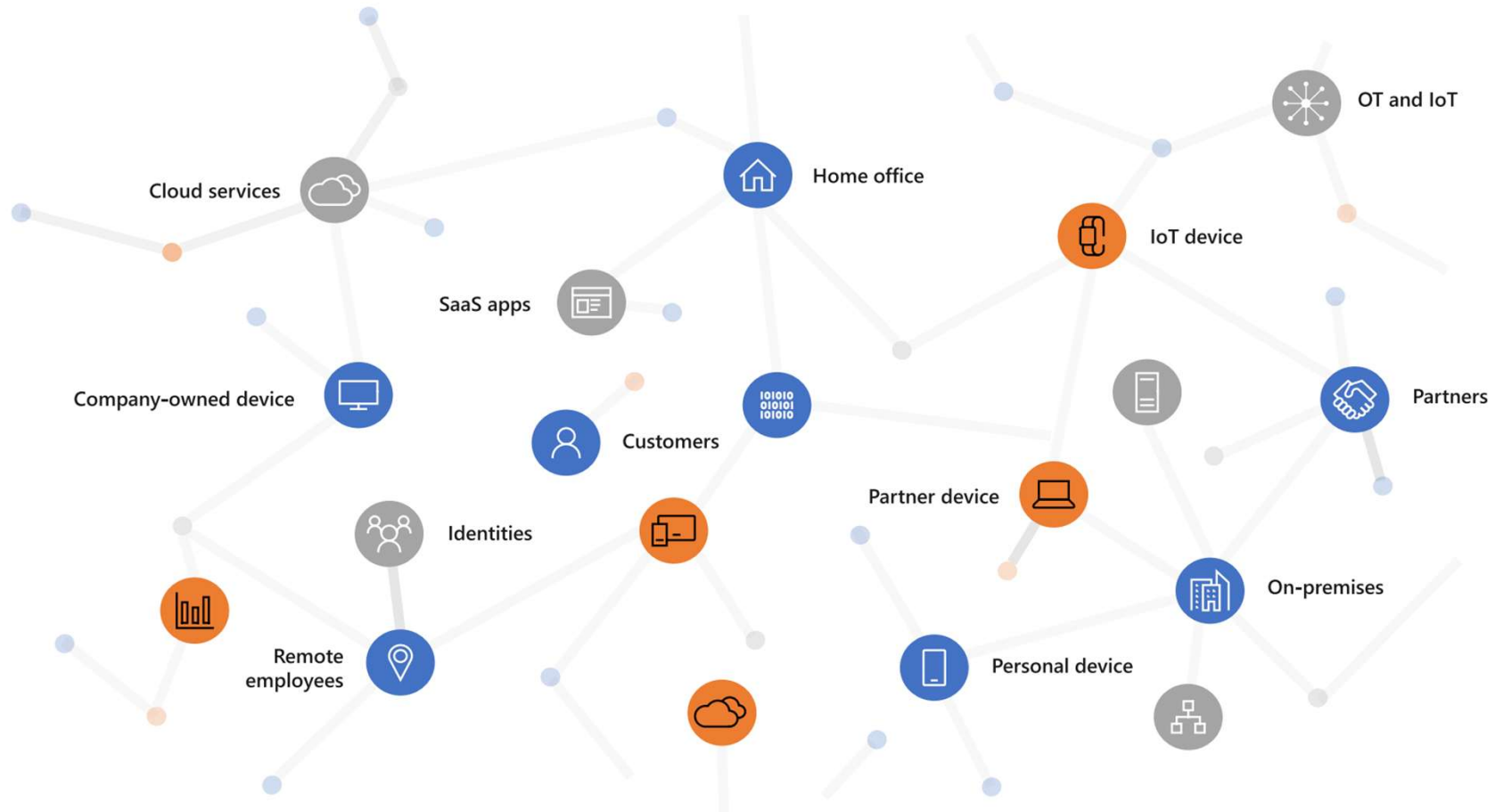
Erstellt mit MidJourney:
cybercrime in a house



Callback zu „Stand der Technik!“

Quelle: CISO Guidelines Handbook

Kenne deine Assets / Werte!



Quelle: Microsoft

Know your Assets / Werte!



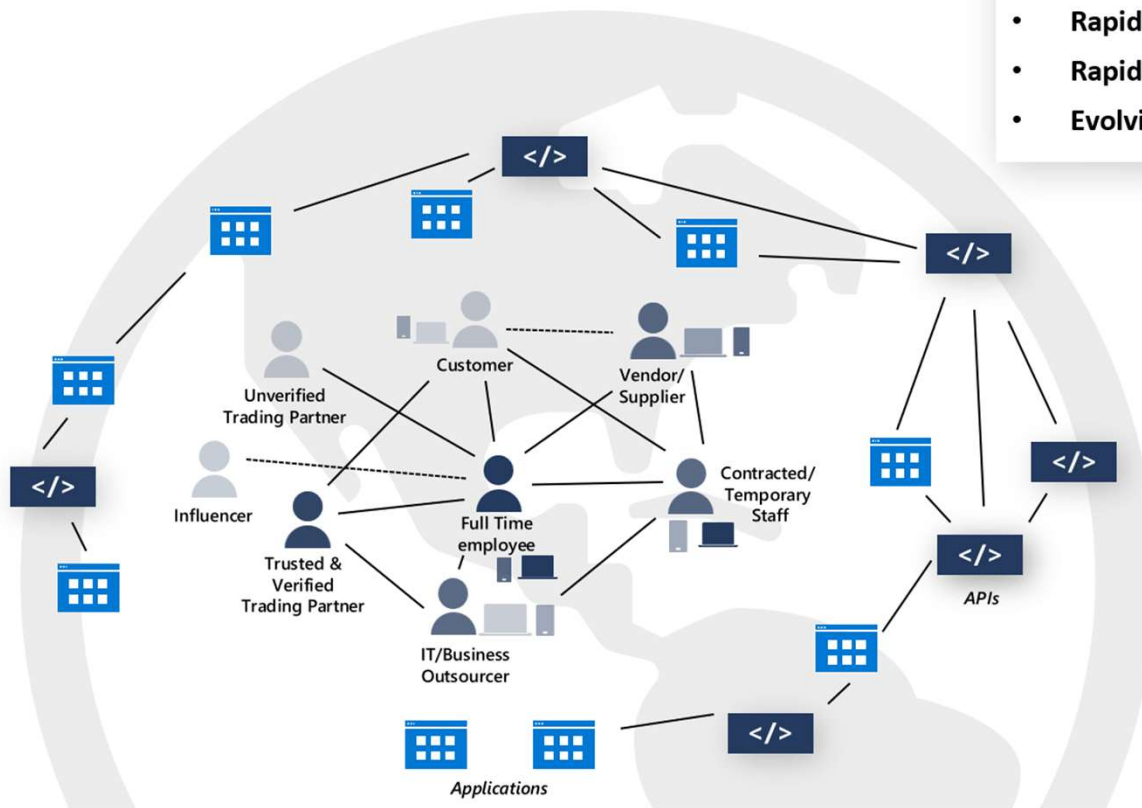
Quelle: Microsoft


Modern Work Use Cases

- Normalization of remote work
- Rapidly evolving partnerships and competitors
- Rapidly changing communication patterns
- Evolving national interests and regulations

Security Modernization Imperatives

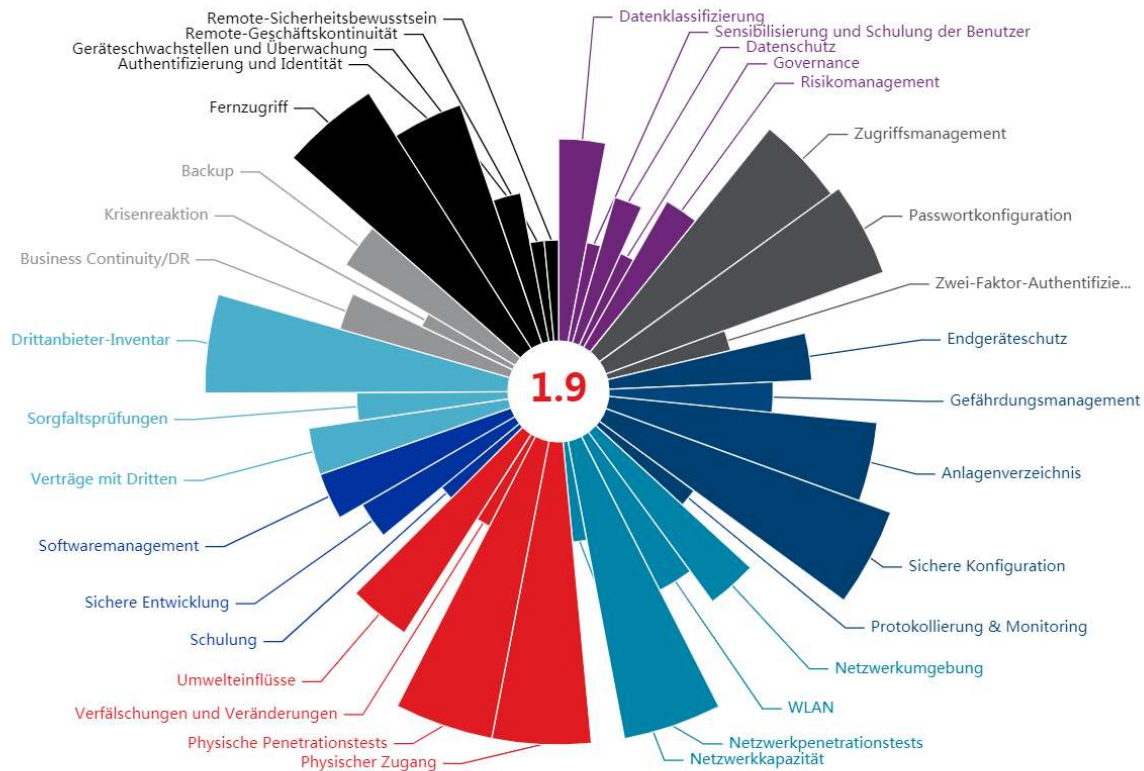
- **Automated Policy Enforcement** - to address changing processes and models in an agile manner at minimum cost
- **Adaptive identity management** - to respond to rapidly changing roles, responsibilities and relationships
- **Data-centric and asset-centric approaches** – to
 - **Better focus security resources** by limiting the scope of what to protect (via trusted zones, tokenization, or similar approaches)
 - **Better monitor assets and respond to threats** regardless of network location.





Regel Nr. 2:
Risiken ganzheitlich
betrachten!

Risiken ganzheitlich betrachten („Raus aus dem Silo!“)



Quelle: Cyber Quotient Evaluation“ (CyQu)



Erstellt mit MidJourney:
risks cost money



Risiken ganzheitlich betrachten („Raus aus dem Silo!“)

ITQ - Sicherer Mittelstand in einer unsicheren Welt

Um die Qualität und das Sicherheitsniveau der IT im deutschsprachigen Mittelstand zu erhöhen, hat das **Institut für Technologiequalität** ein maßgeschneidertes Prüfsystem mit vielen Vorteilen geschaffen:

- ✓ Maßgeschneidert für den Mittelstand
- ✓ Unabhängiges Prüfsystem nach BSI-Standards
- ✓ Gesetzliche Anforderungen erfüllen
- ✓ Unternehmerische Sorgfaltspflicht nachweisen
- ✓ Private Haftung vermeiden
- ✓ IT-Sicherheit messbar machen

Was die Basisprüfung ITQ mit der DSGVO zu tun hat

Um die Anforderungen der DSGVO umsetzen zu können, müssen Sie sich zuerst zwei Fragen stellen: **Wo stehe ich?** und **Was ist der Ist-Stand?**

Mit der **Basisprüfung ITQ** gehen Sie einen wichtigen Schritt zur Erfüllung der DSGVO.

Das Resultat kann sich sehen lassen!

- ✓ Idealer Einstieg in das Thema IT-Sicherheit
- ✓ Detaillierter Ergebnisbericht
- ✓ Konkrete Handlungsanweisungen
- ✓ Prüfsiegel **Basisprüfung ITQ**
- ✓ Grundstein für die Implementierung von Folgemaßnahmen

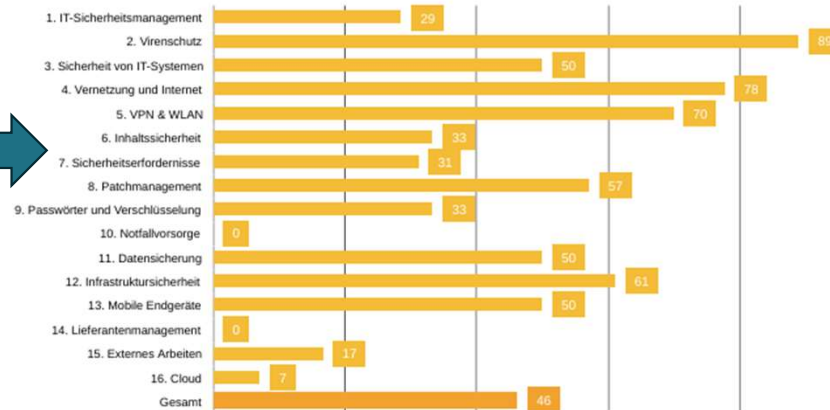


ITQ - Analyse und Bewertung



Erfüllungsgrad Basisprüfung ITQ

Nachfolgend erhalten Sie eine grafische Übersicht der geprüften Unternehmensbereiche, unterteilt in Prüfgruppen. Der Erfüllungsgrad wird in Prozent angegeben, **100% entsprechen einer vollständigen Erfüllung** der jeweiligen Prüfgruppe.



Risikobewertung gesamt

Bitte beachten Sie - bei der Risikobewertung handelt es sich um eine von ITQ-Standards abgeleitete Einschätzung. Anhand des, diesem Bericht im Bereich ‚Anhänge‘ beigelegten Dokumentes **Risiko-Matrix** können Sie einzelne Probleme selbstständig bewerten und entsprechend einstufen.



Risikoeinstufung 6088



ITQ – auch für KBV (nach § 75b SGB V)!

Name	Anzahl
ITQ-KBV-Richtlinie § 75b SGB V	1
ITQ-Infrastrukturanalyse	1
ITQ-Cybersicherheitsanalyse	1
ITQ-Infrastrukturanalyse (as-a-Servi...	1
ITQ-Basisprüfung 13v7	1
ITQ-Ransomware Checkup v3	1

Die Kassenärztliche Bundesvereinigung hat nach § 75b SGB V den Auftrag, Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen Versorgung zu regeln. Sie hat damit den Auftrag, den Stand der Technik der technisch-organisatorische Maßnahmen im Sinne von Artikel 32 Datenschutz-Grundverordnung zu standardisieren. Die hier getroffenen Richtlinien erfüllen diesen Auftrag und dienen damit dem Zweck, die Handhabung der Vorgaben der DatenschutzGrundverordnung im Zusammenhang mit der elektronischen Datenverarbeitung für die vertragsärztliche Praxis zu vereinheitlichen und zu erleichtern.

Die Richtlinie adressiert die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme in der vertragsärztlichen –psychotherapeutischen Praxis. Die Richtlinie legt technischen Anforderungen fest und beschreibt das Mindestmaß der zu ergreifenden Maßnahmen, um die Anforderungen der IT-Sicherheit zu gewährleisten. Mit der Umsetzung der Anforderungen werden die Risiken der IT-Sicherheit minimiert. Bei der Umsetzung können Risiken auch an Dritte, wie ITDienstleister oder Versicherungen, übertragen oder durch den Verantwortlichen akzeptiert werden.



ITQ – auch für KBV (nach § 75b SGB V)!

ITQ-KBV-Richtlinie § 75b SGB V

Audit Facts

Fazit

Prüfungsumgebung

1. A1: Mobile Anwendungen (Apps)
2. A1: Office-Produkte
3. A1: Internet-Anwendungen
4. A1: Endgeräte
5. A1: Endgeräte mit dem Betriebssystem Windows
6. A1: Smartphone und Tablet
7. A1: Mobiltelefon
8. A1: Wechseldatenträger / Speichermedien
9. A1: Netzwerksicherheit
10. A2: Mobile Anwendungen (Apps)
11. A2: Internet-Anwendungen
12. A2: Endgeräte
13. A2: Endgeräte mit dem Betriebssystem Windows
14. A2: Smartphone und Tablet
15. A2: Mobiltelefon
16. A2: Wechseldatenträger / Speichermedien
17. A2: Netzwerksicherheit
18. A3: Smartphone und Tablet
19. A3: Mobile Device Management (MDM)
20. A3: Wechseldatenträger / Speichermedien
21. A3: Netzwerksicherheit



Audit Facts

Fazit

Prüfungsumgebung

1. A1: Mobile Anwendungen (Apps)
2. A1: Office-Produkte
3. A1: Internet-Anwendungen
4. A1: Endgeräte
- A1: Endgeräte mit dem Betriebssystem Windows
- 5.1 Konfiguration von Synchronisationsmechanismen
- 5.2 Datei- und Freigabeberechtigungen
- 5.3 Datensparsamkeit

Die Synchronisierung von Nutzerdaten mit Microsoft-Cloud-Diensten sollte vollständig deaktiviert werden.

- Erfüllt
- Teilweise erfüllt
- Nicht erfüllt
- Entbehrlich


Ausgabertext

Bemerkung *Im Bericht ausgeben*

ITQ - Priorisierung und Fahrplan gem. DSGVO

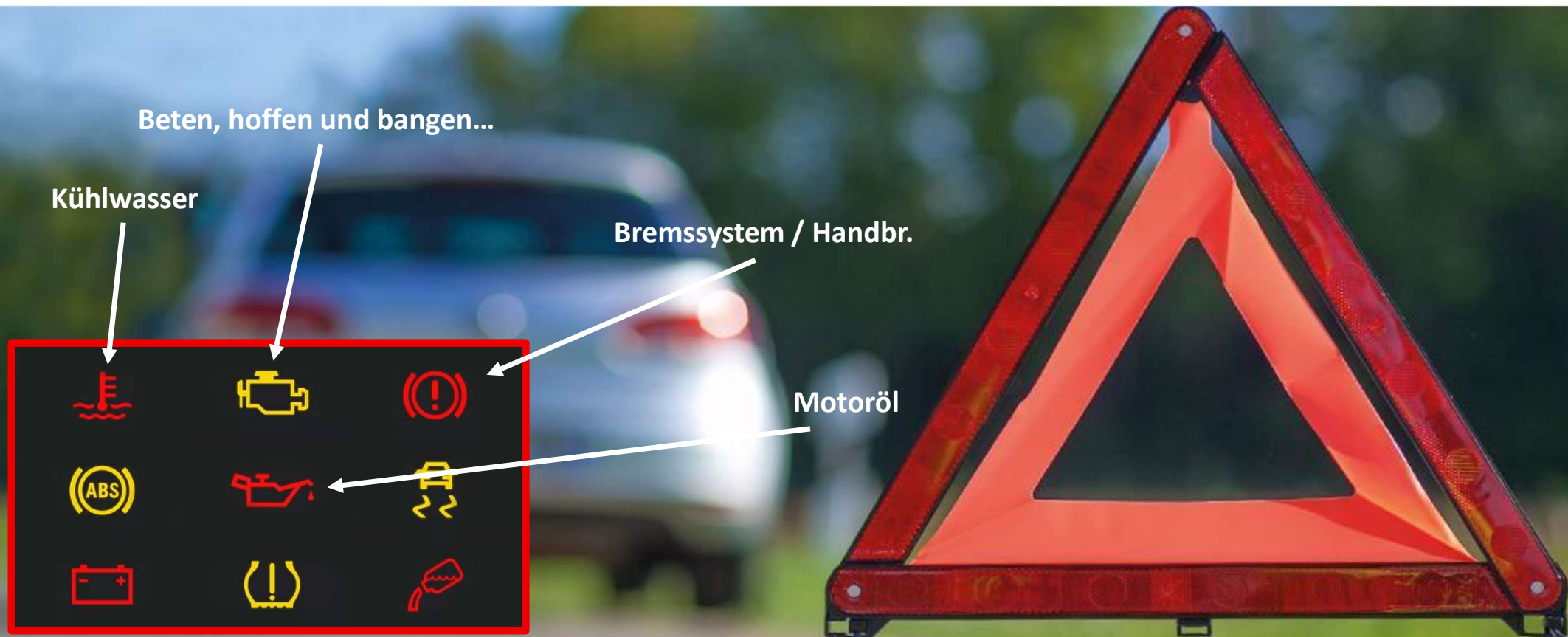


Maßnahmen-Fahrplan (Prioritäten von 1 = Sofort, 5 = Mittelfristig, 10 = langfristig und entsprechende Zwischenstufen)						
Zuständigkeiten: N = Name, P = Pegasus						
Kennung	Maßnahmenempfehlung	Prüfpunkt	Risiko	Prio	Zuständigkeit	Umsetzung bis
A06	Erstellen einer Informationssicherheitsleitlinie	1.1	Hoch	5	N	
A08	Erstellen eines Sicherheitskonzeptes	1.2	Hoch	5	N / P	
A17	Ungenutzte aktive Benutzerkonten deaktivieren	1.9	Hoch	1	P	
A16	Erstellen von Mitarbeiter-Eintritts- und Austritts-Prozessbeschreibungen	1.12	Hoch	5	N	
A15	Verfassen einer Richtlinie zur IT-Nutzung	1.15	Hoch	1	N	
E09	Die Ausgabe bzw. den Entzug von Zugangsmitteln dokumentieren	3.3	Hoch	10	N	
E05	Dokumentation der Rechtsstruktur	3.4	Hoch	5	N / P	
E02	Systemdokumentationen erstellen oder aktualisieren	3.10	Hoch	1	N / P plus Elektriker	
E10	Einführung eines Monitoring-Systems	3.11	Hoch	2	N / P	
K10	Penetrationstest	4.4	Hoch	2	N	
K09	Netzwerk-Topologieplan erstellen	4.7	Hoch	1	N / P plus Elektriker	
L02	Trennung von LAN und WLAN	5.8	Hoch	1	P	
L10	Patch Management für WLAN-Komponenten	5.11	Hoch	5	P	
H02	Einführung eines Content-Filters, Regulierung des Internet-Verkehrs	6.1	Hoch	3	P	
H01	Regulierung der privaten Nutzung von Internet und e-Mail	6.4	Hoch	1	N	
G05	Erstellen einer Richtlinie ‚Löschung und Vernichtung von Daten‘	7.3	Hoch	5	N	
M05	Einführen einer Patch- und Änderungs-Management-Strategie	8.1	Hoch	1	P	
M07	Informationsfluss bei Update Roll Outs	8.5	Hoch	2	P	
J03	Notfall-Management-Strategie erstellen	10.1	Hoch	1	N	
A10	Durchführen einer Schutzbedarfsanalyse	10.2	Hoch	1	N / P	
J04	Notfallpläne erstellen	10.3	Hoch	1	N	
J01	Speicher- und Ablageorte der Notfallpläne prüfen	10.5	Hoch	3	N	
J02	Einführung von Notfalltests	10.6	Hoch	1	N	
D04	Abgleich mit den Verfügbarkeitsanforderungen	11.2	Hoch	1	N	
N04	Wasserleitungen regelmäßig prüfen	12.4	Hoch	3	N	
N06	Rauchmelder installieren	12.6	Hoch	1	N	
N10	Lizenz-Management	12.10	Hoch	5	N / P	



BCM und BIA
sind („eigentlich“...)
ganz einfach!

Ursachenforschung: Das „Source of Trouble“-Prinzip



Ursachenforschung: Das „Source of Trouble“-Prinzip



Instrumententafel

1 – 27

Instrumententafel

	Seite	
1 – Luftaustrittsdüsen	22	21 – Lenkanlaßschloß
2 – Lichtschalter und Regler für Instrumentenbeleuchtung	19	22 – Parkmünzenhalter
3 – Tachometer mit Kurzstreckenzähler	17	23 – Scheibenwischer- und Scheibenwascherhebel
4 – Kühlmitteltemperatur-Anzeige	18	24 – Überblendregler ¹⁾
5 – Kontrollleuchten	15	25 – Zigarettanzünder/Steckdose
6 – Digitaluhr	17	26 – Radio ¹⁾ oder Ablagefach
7 – Kraftstoffvorrats-Anzeige und Drehzahlmesser	18	27 – Ablagefach
8 – Frei für Zusatzschalter oder Rändelrad für Sitzheizung	19	
9 – Schalter für Nebelscheinwerfer/ Nebelschlußleuchte		
10 – Schalter für Warnlichtanlage		
11 – Schalter für Heckscheibenbeheizung		
12 – Lautsprecheröffnung		
13 – Gebläseschalter und Hebel für Heizung und Belüftung		
14 – Ascher		
15 – Zugriff für Motorraumklappen-Entriegelung		
16 – Frei für Zusatzschalter		
17 – Blinker- und Abblendhebel		
18 – Ablagefach		
19 – Bordbuch-Ablage		
20 – Signalhornbetätigung		

Das Richtlinien-Paket der ITventive AG:



Inhalt (Auszug):

- Krisenpläne
- Notfallvorsorge
- Kritische Geschäftsprozesse
- Passwortrichtlinie
- Administratorenrichtlinie
- Verhalten bei Virenbefall
- Netzwerkarchitektur
- Externes Arbeiten
- Cloud-Nutzung
- WLAN

Wofür sind die Dokumente sinnvoll?

- Keine Zertifizierung ohne Dokumente möglich
- „Enthaftungsmittel“ bei Fehlverhalten der Mitarbeiter
- Teil der TOMs die durch Art.32 DSGVO gefordert werden
- Risiko der Fehlerquelle „Mensch“ reduzieren

Name	Geändert	Dokumententyp	Umsetzungsaufwand	Basisprüfung ITQ	Cybersicherheitsana...	Inhalt
Module	19. April					
01_Administratortrichtlinie.docx	2. Juni	Richtlinie	Gering	Nein	Ja	Grundsätze und Aufgabendefinition der Administration
02_Allgemeiner Server.docx	2. Juni	Richtlinie	Gering	Ja	Ja	Vorgaben zur Konfiguration und der Administration von Servern im Allgemeinen
03_Änderungsmanagement.docx	2. Juni	Prozessbeschreibung	Mittel	Nein	Ja	Prozessbeschreibung für anfallende Aufgaben bei Änderung am Informationsverbund
04_Anforderungen zur Nutzung externer Di...	2. Juni	Richtlinie	Gering	Ja	Ja	Vorgaben zum Anforderungsprofil und der Beauftragung von externen Dienstleistern für das Unternehmen
05_Anlage von Benutzern und Gruppen.docx	2. Juni	Richtlinie	Gering	Nein	Ja	Namensgebung für Benutzer und Gruppen
06_Arbeiten mit mobilen Endgeräten.docx	2. Juni	Richtlinie	Gering	Ja	Ja	Regelung des Umganges und der Mitnahme von mobilen Endgeräten
07_Außerbetriebnahme von IT-Systemen.d...	2. Juni	Richtlinie	Gering	Ja	Ja	Regelung zur Außerbetriebnahme von IT-Systemen, Umgang mit Datenträgern und Datenlöschung

Das Richtlinien-Pakete der Itventive AG



Module:

<ul style="list-style-type: none"> 📁 BSI 100-4 📁 BSI 200-4 📁 Module 📁 Notfallmanagement 📁 Prozessbeschreibungen 📁 Richtlinien und Vorlagen 		<ul style="list-style-type: none"> 📁 Incident Response - Begleitmaterial 📁 Notfallpläne einzeln 📄 Anlage 1 - Muster-Netzwerkplan.png 📄 Anlage 2 - Muster-Gebäudeplan.png 📄 Anlage 3 - Muster-Verkabelung.jpg 📄 Anlage 4 - Muster-Serverraum.png 📄 Anlage 5 - Geschäftsprozesse.docx 📄 Anlage 6 - wichtige Anwendungen.docx 📄 Anlage 7 - Kritische IT-Systeme.docx 📄 Anlage 8 - Alarmierungsrufplan.xlsx 📄 Anlage 9 - GAP Analyse.xlsx 📄 Anlage 10 - Playbooks und Runbooks.docx 📄 Muster Notfallplan - Unbefugtes Eindringen in IT-Systeme.docx 📄 Notfallhandbuch.docx
--	--	--



A. Allgemeines	4
I. Definition eines Notfalls	4
II. Schadensdefinition	5
IV. Zielsetzung	7
V. Geltungsbereich	8
VI. Verantwortlichkeiten und Organisation	8
VII. Verhalten in Notfällen	9
1. Allgemeine Regeln für alle Mitarbeiter	9
2. Sofortmaßnahmen	9
a) Alarmierung	9
b) Vorfallbewertung und Untersuchung	10
3. Maßnahmen zur Problemlösung	11
a) Voraussetzungen für kurze Wiederherstellung	11
b) Notbetrieb	11
4. Nachbereitung von Vorfällen	11
5. Revision	11
6. Präventive Maßnahmen und Vorbereitung	12
a) Datensicherung	12
b) Vertragliche Absicherung	12
c) Versicherungsschutz	12
d) Technische Maßnahmen	12
(1) Frühwarnsysteme	12
(2) Infrastruktursicherheit	13
e) Schulung und Sensibilisierung	13
B. Verantwortliche Personen	13
I. Notfallbeauftragte	13
II. IT-Sicherheitsbeauftragter	13
III. IT-Benutzer	14
IV. Unternehmensleitung	14
V. Sonstige Rollen	14
C. Struktur der Notfallpläne	15
D. Dokumentationsvorlage Notfall	16
E. Allgemeine Handlungsanweisungen / Best Practice	16
F. Spezifische Notfallpläne	18
I. Brand (in einer Kollokationsfläche)	18

Kostenfreie Richtlinien



The screenshot shows the GitHub profile of Mrskos-SMP. The profile includes a circular avatar with a purple wolf head and the text 'SMP SECURITY MIT PASSION'. Below the avatar, it says 'Mrskos-SMP' and 'Follow'. The profile statistics show '15 followers · 1 following'. Under 'Achievements', there is a 'Block or Report' button. The 'Pinned' section lists six repositories: 'policies' (34 Policy Templates, 87 stars, 24 forks), 'prozessbeschreibungen' (Kostenlose Prozessbeschreibungen, 12 stars, 5 forks), 'pta_report_pr-sentation_beispiele', 'SecureCodingCheckliste', 'soc_fuer_kmu_bootcamp' (3 stars), and 'CSPM_VM_FUER_KMUS_BOOTCAMP' (Vulnerability Management & Posture Management Bootcamp, 2 stars). The '10 contributions in the last year' section shows a calendar grid for 2025 with contributions on March 1st and 3rd, and January 1st. The calendar grid has columns for Dec, Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov and rows for Mon, Wed, Fri. A legend indicates 'Less' and 'More' contributions with green squares.

➔ Quelle: <https://github.com/Mrskos-SMP>

Kostenfreie Richtlinien

polices Public

Watch 16

prozessbeschreibungen Public



Watch 1

main 1 Branch 0 Tags

Go to file

Add file

Code

Mrskos-SMP Initial	Initial	last year	2 Commits
Sources	Initial	last year	
00_Anleitung.pdf	Initial	last year	
01_Richtlinie zur akzeptablen Nutzung von Unt...	Initial	last year	
02_Richtlinie zur akzeptablen Nutzung von KI-...	Initial	last year	
03_Richtlinie fuer Change Management.pdf	Initial	last year	
04_Richtlinie fuer Clear Desk Policy.pdf	Initial	last year	
05_Richtlinie zur Nutzung von Cloud-Diensten...	Initial	last year	
06_Richtlinie zur Datensicherung.pdf	Initial	last year	
07_Richtlinie zur Informationsklassifizierung un...	Initial	last year	
08_Richtlinie zur Informationssicherheit.pdf	Initial	last year	
09_Richtlinie zur Protokollierung und Überwac...	Initial	last year	
10_Richtlinie zur Netzwerksicherheit.pdf	Initial	last year	
11_Richtlinie zur Personalsicherheit.pdf	Initial	last year	
12_Richtlinie zur Handhabung von Wechseldat...	Initial	last year	
13_Richtlinie zum Management von Drittanbie...	Initial	last year	
14_Richtlinie zum Benutzerzugangsmanageme...	Initial	last year	

main 1 Branch 0 Tags

Go to file

Add file

Code

Mrskos-SMP Create README.md	Initial Commit	last year	2 Commits
Source	Initial Commit	last year	
00_Anleitung.pdf	Initial Commit	last year	
01_Prozessbeschreibung- Erstellung und Pfleg...	Initial Commit	last year	
02_Prozessbeschreibung- Regelmäßige Schulu...	Initial Commit	last year	
03_Prozessbeschreibung- Meldung und Nachs...	Initial Commit	last year	
04_Prozessbeschreibung- Regelmäßiges Repor...	Initial Commit	last year	
05_Prozessbeschreibung- Pflege und Überprüf...	Initial Commit	last year	
06_Prozessbeschreibung- Identifikation und Ve...	Initial Commit	last year	
07_Prozessbeschreibung- Überprüfung der Sic...	Initial Commit	last year	
08_Prozessbeschreibung- Serverhärtung.pdf	Initial Commit	last year	
09_Prozessbeschreibung- Verwaltung von Ben...	Initial Commit	last year	
10_Prozessbeschreibung- Handhabung von IT-...	Initial Commit	last year	
11_Prozessbeschreibung- Steuerung und Über...	Initial Commit	last year	



Quelle: <https://github.com/Mrskos-SMP>

Kostenfreie Richtlinien



Leichter Einstieg

Die Rubrik **Leichter Einstieg** bietet die Möglichkeit, sich Stück für Stück der Thematik zu nähern. Basiselemente der Cyber-Sicherheit werden erläutert. Im Anschluss verdeutlichen kurze Erklärvideos die wichtigen Grundlagen der Informations- und Cyber-Sicherheit. Es folgen Informationen bei Vorliegen eines IT-Sicherheitsvorfalls und zur IT-Notfallkarte.

Fortgeschrittene Absicherung

Die Rubrik **Fortgeschrittene Absicherung** bietet einen Überblick für Unternehmen, die bereits über interne oder externe IT-Fachkräfte mit Kenntnissen gängiger IT-Gepflogenheiten und -Sprachgebräuchen verfügen.

Hilfestellungen bei einem IT-Sicherheitsvorfall



[> Ich habe einen IT-Sicherheitsvorfall, was kann ich tun?](#)

[> Top 10 Ransomware-Maßnahmen \(Detektion\)](#)

[> Top 10 Ransomware-Maßnahmen](#)

Das Dokument [Ransomware: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall Version 1.2](#) enthält Erste-Hilfe-Maßnahmen bei einem schweren IT-Sicherheitsvorfall.

Der [Maßnahmenkatalog Ransomware](#) dient zur Vorbereitung auf einen Ransomware-Angriff und stellt die notwendigen präventiven Grundlagen vor.

Das Managementabstract [Ransomware: Managementabstract Fortschrittliche Angriffe](#) berichtet über die neue Qualität aktueller Angriffe.

[> Ransomware – Fakten und Abwehrstrategien](#)

Broschüre "Cybersicherheit für KMU"



Mit der Broschüre **„Cybersicherheit für KMU“** bietet das BSI einen leicht verständlichen Einstieg, um das Cyber-Sicherheitsniveau von kleinen und mittleren Unternehmen (KMU) zu verbessern. Sie informiert unter anderem darüber, wer für die Informationssicherheit im Unternehmen verantwortlich ist, warum Patches und Updates regelmäßig installiert werden sollten, warum ein Virenschutzprogramm notwendig ist und warum eine Datensicherung so wichtig ist.



Quelle: t.ly/WRHuH (BSI)

Kostenfreie Richtlinien



Leichter Einstieg

Hilfestellungen und Videos zur Sensibilisierung für die Cyber-Sicherheit

In Zeiten der Digitalisierung kommen auch kleine und mittlere Unternehmen nicht umher, sich in Sachen Cyber-Sicherheit weiterzuentwickeln. Der leichte Einstieg bietet die Möglichkeit, sich Stück für Stück der Thematik zu nähern. Grundregeln der Cyber-Sicherheit werden erläutert. Im Anschluss verdeutlichen kurze Erklärvideos die wichtigen Grundlagen der Informations- und Cyber-Sicherheit. Das letzte Video zeigt am Beispiel eines realen weltweiten Hackerangriffs in 2021 wie das BSI im Ernstfall KMU helfen kann. Es folgen Informationen bei Vorliegen eines IT-Sicherheitsvorfalls und zur IT-Notfallkarte.

Sofern sich im Unternehmen keine Personen mit hinreichenden Kenntnissen im Bereich Informationstechnik und Cyber-Sicherheit befinden, empfehlen wir die dauerhafte Beauftragung eines IT-Dienstleisters.

Basiselemente der Cyber-Sicherheit

Man muss kein Experte für Cyber-Sicherheit sein, um ein paar Grundregeln im verantwortungsbewussten Umgang mit Informationstechnik zu beachten.



Quelle: Bundesamt für Sicherheit in der Informationstechnik

➔ Quelle: t.ly/TxgeM (BSI)

Kostenfreie Richtlinien



Das BSI Themen IT-Sicherheitsvorfall Karriere

CyberRisikoCheck

Wirkungsvoller Schutz für kleine und Kleinunternehmen nach [DIN SPEC 27076](#)



Viele kleine und mittlere Unternehmen (KMU) würden gerne mehr für ihre IT-Sicherheit unternehmen, wissen aber oftmals nicht wie. Bereits existierende Standardwerke zum Aufbau eines Informationssicherheitsmanagementsystems, wie das IT-Grundschutz-Kompodium des BSI oder die Norm ISO/IEC 27001, sind insbesondere für Unternehmen mit weniger als 50 Beschäftigten nicht optimal geeignet.

Konsortium zur Erarbeitung einer DIN SPEC

Um auch kleine und mittlere Unternehmen zu unterstützen, wurde in Kooperation mit dem Bundesverband mittelständische Wirtschaft (BVMW) ein Konsortium zur Erarbeitung einer [DIN SPEC](#) gegründet. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) leitete das Konsortium, der BVMW übernahm die stellvertretende Leitung. Insgesamt waren fast 20 weitere Partner beteiligt, u. a. das Deutsche Institut für Normung (DIN), Wirtschaftsförderungen, eine Tochter des Gesamtverbandes der deutschen Versicherungswirtschaft, IT-Grundschutz-Expertinnen und -Experten, -Auditorinnen und -Auditoren sowie Fachkundige zum Thema Datenschutz und IT-Dienstleister. Finanziert wurde das Projekt durch das Bundesministerium für Wirtschaft und Klimaschutz im Rahmen des Programmes "Mittelstand Digital".

Ergebnis der achtmonatigen Arbeit des Konsortiums ist die [DIN SPEC 27076](#) "IT-Sicherheitsberatung für kleine und Kleinunternehmen" und der darauf basierende CyberRisikoCheck. Durch diesen können KMU bei IT-Dienstleistern eine standardisierte Beratung erhalten, die speziell auf ihre Bedürfnisse angepasst ist. In der [DIN SPEC](#) wurden auch die Handlungsempfehlungen für KMU standardisiert. Dadurch wissen sowohl Auftraggeber als auch Auftragnehmer, welche Leistung zu erwarten bzw. zu erbringen ist.



DIN SPEC 27076:2023-05



■ TECHNISCHE REGEL [AKTUELL]

DIN SPEC 27076:2023-05

IT-Sicherheitsberatung für Klein- und Kleinunternehmen

Englischer Titel:

IT security consulting for small and micro enterprises

Ausgabedatum:

2023-05

Originalsprachen:

Deutsch

Seiten:

34

Verfahren:

PAS



Quelle: t.ly/Dv8-e (BSI) / t.ly/_ZY5i (DIN Media)



Kostenfreie Vorlage – Notfallhandbuch „Light“

- A. Allgemeines 4**
 - I. Definition eines Notfalls 4
 - II. Schadensdefinition 5
 - IV. Zielsetzung 7
 - V. Geltungsbereich 8
 - VI. Verantwortlichkeiten und Organisation 8
 - VII. Verhalten in Notfällen 9
 - 1. Allgemeine Regeln für alle Mitarbeiter 9
 - 2. Sofortmaßnahmen 9
 - a) Alarmierung 9
 - b) Vorfallbewertung und Untersuchung 10
 - 3. Maßnahmen zur Problemlösung 11
 - a) Voraussetzungen für kurze Wiederherstellung 11
 - b) Notbetrieb 11
 - 4. Nachbereitung von Vorfällen 11
 - 5. Revision 11
 - 6. Präventive Maßnahmen und Vorbereitung 12
 - a) Datensicherung 12
 - b) Vertragliche Absicherung 12
 - c) Versicherungsschutz 12
 - d) Technische Maßnahmen 12
 - (1) Frühwarnsysteme 12
 - (2) Infrastruktursicherheit 13
 - e) Schulung und Sensibilisierung 13
- B. Verantwortliche Personen 13**
 - I. Notfallbeauftragte 13
 - II. IT-Sicherheitsbeauftragter 13
 - III. IT-Benutzer 14
 - IV. Unternehmensleitung 14
 - V. Sonstige Rollen 14
- C. Struktur der Notfallpläne 15**
- D. Dokumentationsvorlage Notfall 16**
- E. Allgemeine Handlungsanweisungen / Best Practice 16**
- F. Spezifische Notfallpläne 18**
 - I. Brand (in einer Kollokationsfläche) 18

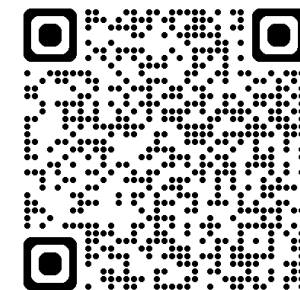
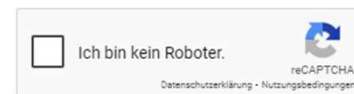
Seite 2 von 93



Name *

Vorname **Nachname**
E-Mail *

* Ja, ich habe die **Datenschutzbestimmungen** zur Kenntnis genommen und bin damit einverstanden, dass die von mir angegebenen Daten elektronisch erhoben und gespeichert werden. Die pegasus verarbeitet Ihre Daten im Zusammenhang mit ihrer Security-Kampagne. Natürlich können Sie der Speicherung Ihrer Daten nach Kampagnenende jederzeit widersprechen. Ihre personenbezogenen Daten werden dar

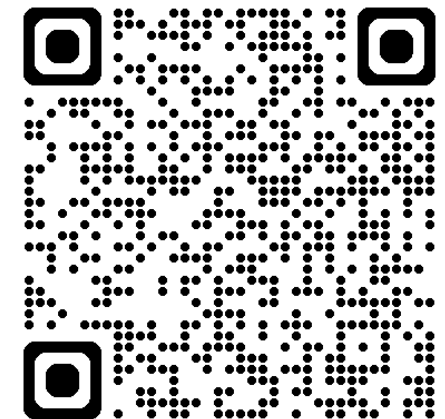


Download: itventive.com/bvd




Kostenfreie Vorlage – Incident Response Playbook „Light“

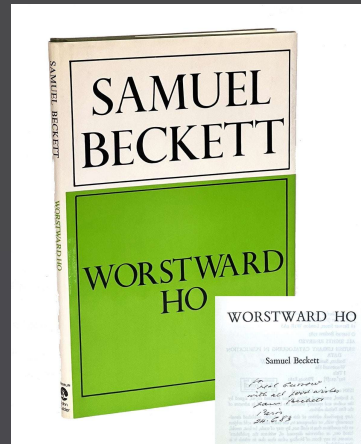
1. Einleitung	4
2. Playbooks für spezifische Cyber-Bedrohungen	5
2.1. Phishing-Angriff	5
2.2. Ransomware-Angriff	6
2.3. DDoS-Angriff	7
2.4. Insider-Bedrohung	8
2.5. Zero-Day-Exploit	9
2.6. Advanced Persistent Threat (APT)	10
2.7. Supply-Chain-Angriff	11
2.8. Identitätsdiebstahl und Credential Stuffing	12
2.9. IoT- und SCADA-Systemangriff	13
2.10. Rogue-Administrator-Angriff	14
2.11. Datenleak oder unautorisierte Datenexfiltration	15
2.12. DNS-Tunneling und Angriffe auf DNS-Infrastruktur	16
2.13. Malware-Infektion und Trojaner	17
2.14. Cloud-Sicherheitsvorfall	18
2.15. KI-gestützte Cyberangriffe	19
2.16. Man-in-the-Middle (MitM)-Angriff	20
2.17. Exploit-Angriffe auf Webanwendungen	21
2.18. Business Email Compromise (BEC)	22
2.19. Bluetooth- und NFC-Angriffe	23
2.20. Fake-Update- und Malvertising-Angriffe	24
2.21. Watering-Hole-Angriff	25
2.22. Session Hijacking	26
2.23. Hypervisor-Angriffe	27
2.24. Deepfake- und Social Engineering-Angriffe	28
2.25. Angriffe auf künstliche Intelligenz (AI Poisoning)	29
2.26. SIM-Swapping (Mobilfunknummer-Übernahme)	30
2.27. GPS-Spoofing	31
2.28. Data Poisoning (Datenmanipulation)	32
2.29. Spear-Phishing per Voice (Vishing)	33
2.30. Quanten-Computing-Angriffe	34
2.31. Zero-Click-Exploits (Angriffe ohne Benutzerinteraktion)	35
2.32. AI-Powered Malware	36
2.33. Shadow IT (Ungesicherte IT-Systeme)	37



➔ Download: itventive.com/bvd



Regel Nr. 3:
Übung macht den
Meister!



Ever tried. Ever failed. No matter. Try again.
Fail again. Fail better.

- Samuel Beckett, 1983

Worstward Ho / Aufs schlimmste zu (1983)

ISBN: 9780714539799



Don't panic and carry a towel

Douglas Adams

Per Anhalter durch die Galaxis (1979)

ISBN: 9783453146714



Incident Response Training / Table-Top Übungen

Kontext in dem wir Table-Top Übungen durchführen

Qualitativ hochwertige Security auch für kleinere Organisation zugänglich machen

- Fachkräftemangel und Kostendruck auf Seiten der Verteidiger treffen auf gut skalierende Angreifer (Organisation, Technik, Methoden, Arbeitsteilung).
- Kleinere Organisationen besonders betroffen.
- Gruppen-Projekte statt Einzelberatung als Evolution des Community-Gedanken: „Kohorte“.
- Kohorte „Incident Response Readiness“ (wie bereite ich mich auf einen Vorfall vor) enthält Table Top Exercise mit Teilnehmenden aus verschiedenen, nicht-verbundenen Organisationen.
- (Im Konzern, über verschiedene Abteilungen hinweg, kennen sich die Menschen auch nicht wirklich)



Incident Response Training / Table-Top Übungen

Ziel von Table-Top Übungen

Konzentration ermöglichen und Reibungsverluste minimieren

- Konzentration und Zeit sind rar.
- Technik (und ggf. Prozesse) dagegen meist in ausreichendem Maße vorhanden.
- Primär: Ausnahmezustand erleben und Agieren unter psychologischer Belastung testen.
- Sekundär: Antrainieren des Prozesses und Defizite darin identifizieren.
- "Kostenlos" dazu: Unter Unsicherheiten agieren lernen.

Incident Response Training – Ein Beispiel



Digitaler Alptraum im Herzen des Unternehmens

Es ist ein gewöhnlicher Dienstagmorgen in der Zentrale der Regensburger Softwarefirma "ByteBavaria". Michael Huber, ein erfahrener Buchhalter in der Finanzabteilung, nimmt pünktlich um 8 Uhr an seinem Schreibtisch Platz. Doch als er seinen Computer hochfährt, stockt ihm der Atem. Statt der vertrauten Exceltabellen und Finanzberichte starrt er auf ein Gewirr aus unlesbaren Zeichen und Symbolen. Mit zitternden Händen greift Huber zum Telefon und wählt die Durchwahl der IT-Abteilung. "Alle meine Dateien... sie sind verschlüsselt! Ich kann auf nichts mehr zugreifen!", stammelt er aufgeregt in den Hörer. Kaum hat er aufgelegt, bricht in den Büroräumen das Chaos aus. Die Nachricht von Hubers Entdeckung verbreitet sich wie ein Lauffeuer. Mitarbeiter eilen von Schreibtisch zu Schreibtisch, diskutieren aufgeregt – bis plötzlich ein kollektiver Aufschrei durch das Gebäude hallt.

Der Moment des Schreckens

Auf jedem einzelnen Bildschirm im Unternehmen, vom Empfang bis zum Chefbüro, erscheint wie aus dem Nichts dieselbe Nachricht: "Ihre Daten sind nun unser Schatz. Zahlen Sie 500.000 Euro in Bitcoin, oder sagen Sie Ihren Geschäftsgeheimnissen für immer Lebewohl. Sie haben 48 Stunden. Die Uhr tickt." In der Chefetage bricht Hektik aus. Geschäftsführerin Dr. Sabine Meier ruft sofort einen Krisenstab zusammen. Während die IT-Experten fieberhaft an einer Lösung arbeiten, muss eine folgenschwere Entscheidung getroffen werden: Zahlen oder kämpfen? Die nächsten Stunden entscheiden über die Zukunft von ByteBavaria. Und während die Geschäftsführung um eine Lösung ringt, fragt sich jeder im Unternehmen bange: Wer steckt hinter diesem perfiden Angriff? Und was passiert, wenn der Countdown abläuft?

Incident Response Training – Das richtige Maß



Chaos in der richtigen Dosis

- Zu wenig Chaos: Nicht spürbar und nicht hilfreich für den Ernstfall.
- Zu viel Chaos: Überfordernd oder frustrierend und nicht hilfreich für den Ernstfall.
- Daher: Schon in der Vorbereitung Flexibilität mitdenken!

▼ Phase 1: Detection & Analysis Pt 1

10:45 - Email to helpdesk: ✓

"I clicked a DocuSign link about an invoice, but it asked for my password twice. Now my Outlook keeps crashing." - Cliff, Finance

10:48 - Helpdesk ticket surge: ✓

"5 tickets: PC running slow, strange pop-ups, can't access shared drives"

10:50 - Security alert: ✓

"Firewall: Unusual outbound connections to 185.174.x.x from multiple internal IPs"

INJECT #1 (10:55): ✓

"IT Manager calls: 'Should we block internet access for Finance department? They're panicking about month-end closing tomorrow!'"

Vorgehensweise Incident Response Training



▪ Vorbereitung

- Szenario und Rollen
- Organisation (Termin/Raum/...)
- Einspieler

▼ **Tabletop Exercise**

- ▶ **Company Profile**
- ▶ **Process Diagram**
- ▶ **Role Assignment**
- ▶ **Rules**
- ▶ **Phase 1: Detection & Analysis Pt 1**
- ▶ **Phase 2: Analysis Pt 2**
- ▶ **Phase 3: Containment**
- ▶ **Debrief Guide**



Vorgehensweise Incident Response Training

Ein Beispiel für einen Übungsablauf

- Vorbereitung
 - Szenario und Rollen
 - Organisation (Termin/Raum/...)
 - Einspieler

- Währenddessen
 - Gegenstab darstellen
 - Einspieler justieren
 - Beobachten und Abgleich

▼ Phase 1: Detection & Analysis Pt 1

10:45 - Email to helpdesk: ✓

"I clicked a DocuSign link about an invoice, but it asked for my password twice. Now my Outlook keeps crashing." - Cliff, Finance

10:48 - Helpdesk ticket surge: ✓

"5 tickets: PC running slow, strange pop-ups, can't access shared drives"

10:50 - Security alert: ✓

"Firewall: Unusual outbound connections to 185.174.x.x from multiple internal IPs"

INJECT #1 (10:55): ✓

"IT Manager calls: 'Should we block internet access for Finance department? They're panicking about month-end closing tomorrow!'"

▼ Expected Actions:

- Isolate affected machines
- Get the team together
- Correlate more information
- Declare Security Incident
- Start communication to relevant parties
- Use Notion for documentation

SecurityCards (Training für Entscheider)

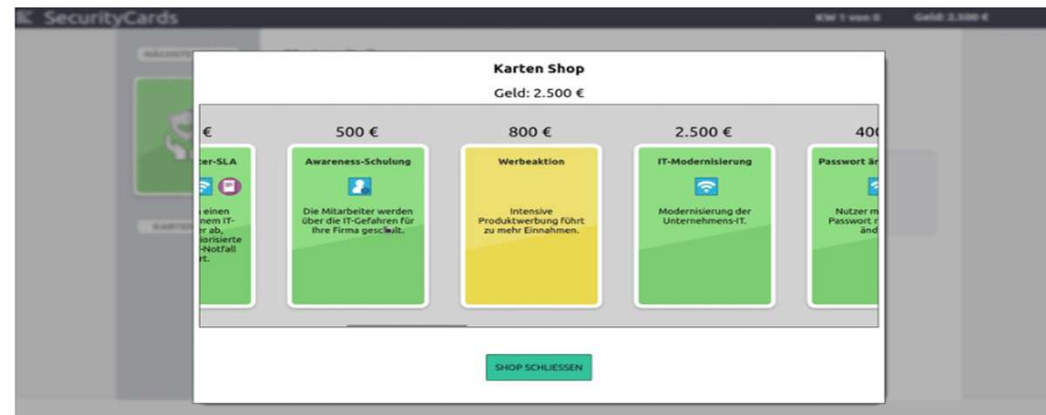


SecurityCards

KW 0 von 0

Geld: 0 €

SecurityCards Anleitung



In SecurityCards spielen Sie einen Entscheidungsträger für ein Unternehmen. Abhängig davon für welches Unternehmen Sie sich entscheiden, werden Sie mit unterschiedlichen Ereignissen konfrontiert.

Informationen über den Kontostand Ihres Unternehmens erhalten Sie durch die Geldanzeige in der Mitte des Spielfeldes.

Ziel des Spiels ist es, den Kontostand im Plus zu halten. Dazu muss der Spielende auftretende Bedrohungen für das Unternehmen erkennen und passende Gegenmaßnahmen ergreifen.

Hierfür stehen dem Spielenden unterschiedliche Karten zur Verfügung. Eine Karte kann eine Entscheidung oder eine präventive Investition in Schutzmaßnahmen darstellen.

Quelle: <https://play.bakgame.de/SecurityCards/>



Backdoor and Breaches (Training für Admins)

Setting the Board

TRUSTED RELATIONSHIP


A trusted third party who has access to your network is compromised. The attackers use this to pivot to your internal resources.

DETECTION

SIEM Log Analysis
User and Entity Behavior Analytics

TOOLS

An unfortunate and unfounded trust in humanity and business partners who are complete strangers.



INTERNAL PASSWORD SPRAY


The attackers start a password spray against the rest of the organization from a compromised system.

DETECTION

User and Entity Behavior Analytics
SIEM Log Analysis

TOOLS

Domain Password Spray



<https://github.com/BlackbookCyber/PaswordSpray>
<https://www.blackbookcyber.com/technical-attack-tactics-5-how-to-hack-attack/>

MALICIOUS DRIVER


The attacker's load a malicious driver into the operating system.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis

TOOLS

Poam
Wingard
Sedulake



<https://en.wikipedia.org/wiki/Poam>

DNS AS C2


The attackers use DNS as a C2 channel.

DETECTION

NetFlow, Zeek/Tre, RITA Analysis

TOOLS

dnscat2



https://www.dnscat2.net/index.php?option=com_content&view=article&id=23:using-dnscat2

Setup Attack Cards

Setup Procedure Cards

Start Game

Save Setup

TRUSTED RELATIONSHIP

A trusted third party who has access to your network is compromised. The attackers use this to pivot to your internal resources.

DETECTION

SIEM Log Analysis
User and Entity Behavior Analytics

TOOLS

An unfortunate and unfounded trust in humanity and business partners who are complete strangers.



Quelle: <https://bnb.silverday.de/>

Try Hack Me (Training für Admins)



Alexander.Karls [0x9][MAGE] 🇩🇪

Rank ^{top 5%} 87969

Badges 17

Streak 0

Completed rooms 97

Log In Join for FREE

Anyone can learn cyber security with TryHackMe

Hands-on cyber security training through real-world scenarios

Email Join for FREE

✓ Beginner Friendly ✓ Guides and Challenges

Real-world offensive & defensive cyber security training

Access over 900 training labs and learning pathways suited to all levels, from the complete beginner to the seasoned hacker. TryHackMe makes learning engaging, entertaining, accessible, and affordable.



Learn by doing



Guided learning for all skills



Real-world training



Engaging and fun lessons



Online on-demand learning



Cost-effective

Quelle: <https://tryhackme.com/>

Last but not least – SCHULUNGEN für jeden anbieten!



Schulung

Beratung

Wissen

News

Über uns



Anmelden

Deutschland

ONLINE-SCHULUNGEN
ANGEBOT ANFRAGEN
INHOUSE-SCHULUNGEN
VIELBUCHER-RABATTE
FÖRDERMÖGLICHKEITEN

KÜNSTLICHE INTELLIGENZ

KI-Schulungen im Überblick
KI-Führerschein gem. AI Act
AI Foundation/Professional
KI-Manager
ISO 42001 KI-Beauftragter
ISO 42001 AIMS Auditor
AI Compliance Experte
MS 365 Copilot Schulung
KI Innovationsworkshop
KI Prompt Engineering

INFORMATIONSSICHERHEIT

ISO/IEC 27001
NIS-2 Schulungen
Business Continuity
BSI IT-Grundschutz
Datenschutz
Cybersecurity & Pentesting
VDA ISA und TISAX®
IT Risk Management
Weitere Security-Themen

SERVICE MANAGEMENT

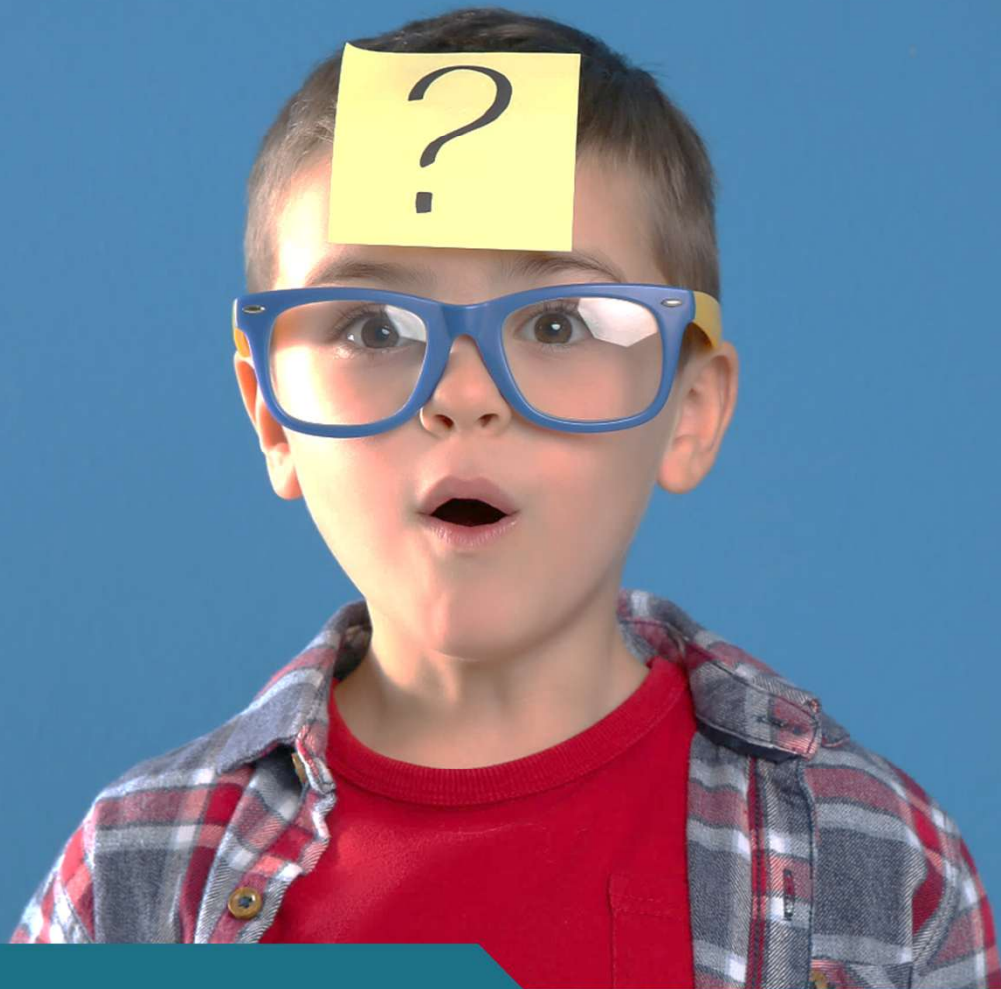
ITIL® Zertifizierung
ISO/IEC 20000
DevOps
FitSM Lightweight ITSM
Prozess-Simulation

PROJEKTMANAGEMENT

PRINCE2® Zertifizierung
Scrum
Hybrides PM
IREB® Zertifizierung
Kanban
Change Management
Design Thinking
OKR
Soft Skills im Projekt
Scrum-Simulationen

MEHR THEMEN

Quelle: <https://www.mitsm.de/>



Haben Sie Fragen
oder Anregungen?

ITventive AG

Monreposstrasse 57, D-71634 Ludwigsburg
Bayernstrasse 10, D-93128 Regensburg
Digital Solutions AG, Uferweg 17, CH-3013 Bern
Scandinavia ApS, Park Alle 295, 2. floor, DK-2605 Brøndby

[Itventive.com](https://www.itventive.com)



ITventive® ist eine eingetragene Marke der eviatec Systems AG und der pegasus GmbH in Deutschland und/oder anderen Ländern. eviatec® ist eine eingetragene Marke der eviatec Systems AG in Deutschland und/oder anderen Ländern. Weitere Unternehmens-, Produkt- oder Servicennamen können Marken anderer Hersteller sein.

Diese Veröffentlichung dient nur der unverbindlichen allgemeinen Information und ersetzt nicht die eingehende individuelle Beratung. Die in dieser Veröffentlichung enthaltenen Informationen können jederzeit, auch ohne vorherige Ankündigung, geändert werden. Insbesondere können technische Merkmale und Funktionen auch landesspezifisch variieren. Die Produktinformationen geben den derzeitigen Stand wieder. Gegenstand und Umfang der Leistungen bestimmen sich ausschließlich nach den jeweiligen Verträgen. Die Einhaltung bestimmter Rechtsvorschriften von Produkten und sonstigen Leistungen wird seitens ITventive weder gewährleistet, noch garantiert oder als Eigenschaft zugesichert. Der Kunde ist für die Einhaltung anwendbarer Sicherheitsvorschriften und sonstiger Vorschriften des nationalen und internationalen Rechts verantwortlich.

Änderungen, Irrtümer und Druckfehler bleiben vorbehalten. Nachdruck und Vervielfältigung, auch auszugsweise, nur mit schriftlicher Genehmigung der eviatec Systems AG & pegasus GmbH.

© Copyright ITventive AG 2025. Alle Rechte vorbehalten.