FINANCE ROUNDTABLE

Herzlich willkommen zum FINANCE-Roundtable Security ist Chefsache

VERANSTALTER

FINANCE
Das Magazin für Finanzchefs

MITVERANSTALTER

GREEN FIELD BECHTLE

FINANCE ROUNDTABLE

Begrüßung

Thomas Holzamer
Redakteur
FINANCE

FINANCE ROUNDTABLE

Begrüßung

Michael Beilfuss
Head of Customer Success
Bechtle

FINANCE ROUNDTABLE

Begrüßung

Alfred Neidhard
Bereichsvorstand
Bechtle

FINANCE ROUNDTABLE

Agenda

17.00 Uhr	Begrüßung
17.15 Uhr	Impulse
	- David Thornewill, Grey Beard Advisory
	- Frank Lorenz-Dietz, SAF Holland
	- Sandra Karger, BSI
18.15 Uhr	Arbeitsgruppen
ca. 19.15 Uhr	Wrap up & Abschluss
Anschließend	Get-together

FINANCE ROUNDTABLE

Erfahrungsbericht: Der CFO mit dem CISO

David Thornewill
Grey Beard Advisory

Erfahrungsbericht: Der CFO mit dem CISO

David Thornewill
Grey Beard Advisory

30-Nov-2023

Who is David Thornewill?

David Thornewill von Essen
Grey Beard[1] Advisory
Bonn, Germany

Career

• Group CISO – DP DHL Group (retired)	(2019 – 2022)
• Global CIO Group Functions – DP DHL Group - Chairman Group Information Security Council	(2008 – 2019) (2011 – 2022)
• VP Professional Services Europe, DHL (Prague)	(2004 – 2008)
• Program Director IT, DHL (Scottsdale, AZ)	(2002 – 2004)
• CEO, DirXon, Inc. (Tempe, AZ)	(2001 – 2002)
• Financial Controller, On Semiconductor (Phoenix, AZ)	(1999 – 2001)
• Supply Chain Mgmt, Motorola (Munich & Phoenix, AZ)	(1986 – 1999)

Education

• MBA International Management (Thunderbird, AZ)	1998
• Wirtschaftsinformatik (Munich)	1986

[1] In the US Military, retired officers, who advise and coach younger active officers, are known as "Grey Beards"

Volle Asset Transparenz

Man kann nur das schützen, worüber man Bescheid weiß

Volle Asset Transparenz

Fachbereichsaufgaben

- Welche Hardware- und Software-Assets existieren?
- Wer ist beschäftigt (auch Leiharbeiter)?
- Wo befinden sich Assets und Menschen, sowohl geografisch und organisatorisch?
- Hat jedes Asset und Mensch einen aktuellen Verantwortlichen?
- In welchen Zustand sind die Assets (Technical Debt)?

CFO-Fragen/Hilfestellung

- Prüfen ob Daten vollständig und aktuell sind?
- Werden Lücken stetig und programmatisch abgearbeitet?
- Werden diese Daten auch mit Führungskräften besprochen?
- Fühlen sich Abteilungs- und Bereichsleiter dafür verantwortlich?

Human Firewall

Eine vermeintliche Schwäche wird zur unüberwindlichen Stärke!

Human Firewall

Fachbereichsaufgaben

- Zielgruppengerechtes Training und Weiterbildung
- Gezieltes Training für Führungskräfte (Gamification)
- Durchgängige, Kommunikation über diverse Kanäle
- Kenntnis der gesetzlichen u. regulatorischen Anforderungen
- Verhalten in Krisen und Kommunikationsalternativen
- Simulationen regelmäßig abhalten

CFO-Fragen/Hilfestellung:

- Sind Trainingspläne turnusmäßig eingehalten?
- Sind Führungskräfte Musterbeispiele und Förderer?
- Sind gesetzlichen und regulatorischen Anforderungen bekannt und eingehalten?
- Nehmen Führungskräfte auch an Simulationen teil?
- Werden Erkenntnisse aus Simulationen in die Praxis umgesetzt?

Das Regelwerk

You can only follow the rules that you know about!

Das Regelwerk

Fachbereichsaufgaben

- Festlegung einer Dokumentenstruktur (z. B. Richtlinie, Ziele, Leitlinien, Kontinuitätspläne)
- Aktualität, besonders die Integration von rechtlichen u. regulatorischen Anforderungen
- Gewährleistung der internen Konsistenz von Inhalt, Format etc.
- Flexibilität für technischen Fortschritt und lokale gesetzliche Anforderungen
- Allgemeinen Zugang gewähren und Änderungen veröffentlichen

CFO-Fragen/Hilfestellung

- Ist die Dokumentation zugänglich und verständlich präsentiert?
- Entspricht die Dokumentation rechtlichen u. regulatorischen Anforderungen? [m. General Counsel]
- Wird die (nicht-) Einhaltung im Konzern Compliance Reporting aufgenommen?
- Werden Prüfungsergebnisse der Revision stetig abgearbeitet?

Lieferkette Überwachung

Lieferanten und Dienstleister sind unverzichtbar!

Lieferkette Überwachung

Fachbereichsaufgaben

- Festlegung der vertraglichen Mindestanforderungen (z.B. ISCOP)
- Aus- u. Weiterbildung der Einkaufsspezialisten
- Einführung eines Programms zur Lieferantenbewertung (Priorisierung, Zeitschiene, Risikobewertung usw.)
- Ermittlung der geeigneten Kontakte bei Lieferanten
- Anwendung von Security Rating Services (z. B. Bitsight, SecurityScorecard, o.ä.)

CFO-Fragen/Hilfestellung

- Stetige Fortschritt der Lieferantendeckung
- Überprüfung der Priorisierung und resultierende Risikobewertung
- Wie ist die Robustheit von Notfallpläne bzw. Alternativlieferanten?
- Werden Lieferanten-sanierungspläne eingefordert u. eingehalten?

Technologische Maßnahmen

Angemessene, ausgewogene Technologie-Roadmap

Technologische Maßnahmen

Fachbereichsaufgaben

- Identitätszugangsmanagement, MFA, AIP
- Zero-Trust, Verschlüsselung, Zertifikat-Mgmt
- Erkennungs- und Reaktionssysteme, SIEM-Systeme (mögl. KI-basiert)
- Strategie für Datensicherung, Datenwiederherstellung, und Reihenfolge der Wiederinbetriebnahme.
- Priorisierung und Automatisierung von Patching und Upgrades
- Cloud-Sicherheitsstrategie und Netzwerksegmentierung

CFO-Fragen/Hilfestellung

- Sind Investments priorisiert nach Geschäftsbedarf, z.B. eindeutige Reduzierung des Gesamt-risikowertes?
- Laufen Projekte wie erwartet?
- Gibt es einen klaren Prozess zur Bewertung von Risiken auf Euro-basis und zur Zuordnung eines Risikoprofils?

Auswertung und Berichterstattung

Wissen, wo Sie sind und wohin die Reise geht

Auswertung und Bericht-erstattung

Fachbereichsaufgaben

- Erstellung eines integrierten, Online-Dashboards mit einheitlichen Daten mit Zugriff auf allen Ebenen
- Risikoerkennung, -bewertung und Integration in Konzernrisikomatrix
- Unterstützung von Bewertungen Dritter, z. B. Versicherungen
- Einbindung im ESG Reporting

CFO-Fragen/Hilfestellung

- Gibt es Transparenz über den Fortschritt und ernsthafte Diskussionen auf Vorstands- und Geschäftsführungsebene?
- Liefern externe Bewertungen (zB Wirtschaftsprüfer, Versicherungen) überraschende Ergebnisse?
- Welche Kennzahl(en) kann man dauerhaft veröffentlichen?

The **THRUSTER Approach**

Summary

- **T**ransparency
  - You can only protect what you know of
- **H**uman Firewall
  - Convert a weakness into a strength
- **Ru**les and Governance
  - You can only follow rules that you know about
- **S**upply Chain Monitoring
  - Hold suppliers accountable and follow up
- **T**echnological Defenses
  - Monitoring and response, reduction of technical debt
- **E**valuation and **R**eporting
  - Know where you are and where you're going

Vielen Dank

FINANCE ROUNDTABLE

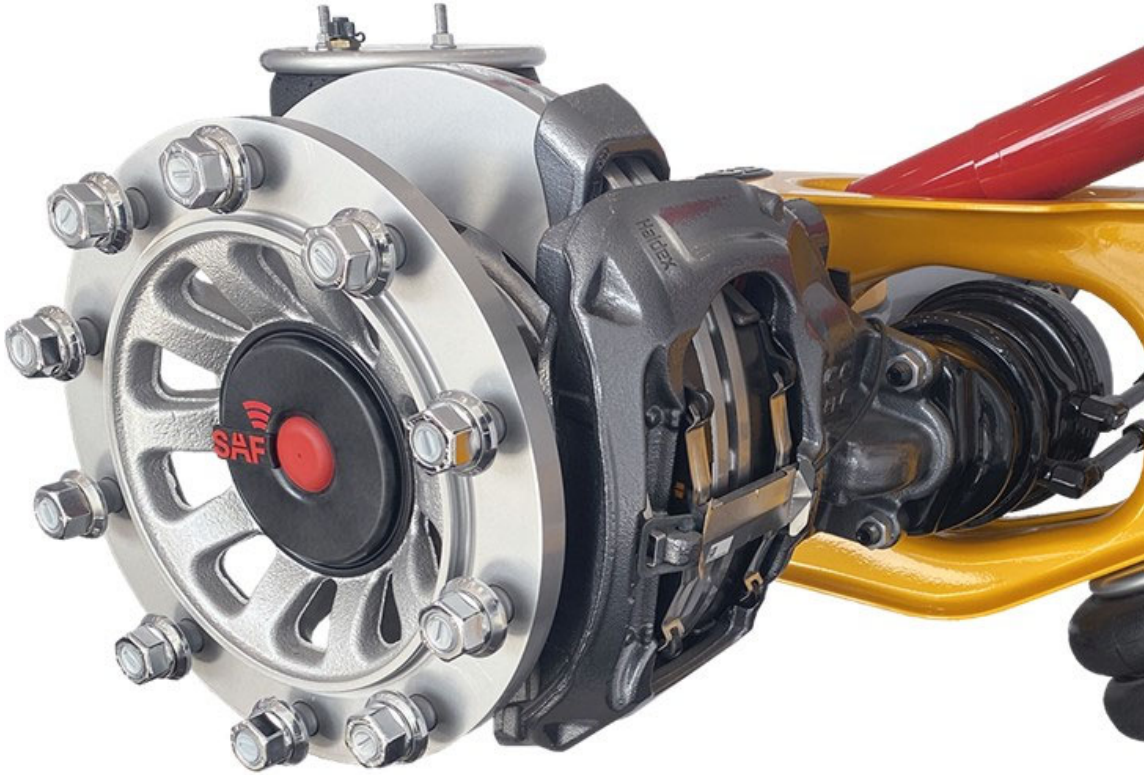
Praxisbericht – Management einer Cyberattacke

Frank Lorenz-Dietz
CFO
SAF-Holland

SAF-HOLLAND SE

Finance Magazin
IT Security Roundtable

Management einer
Cyberattacke



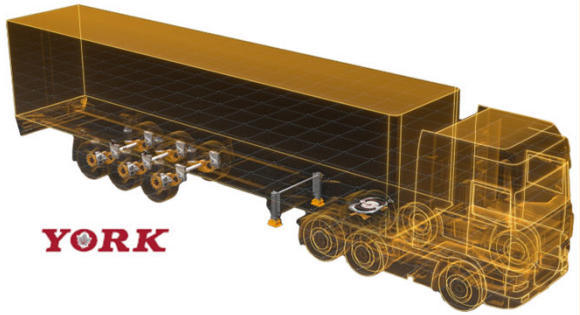
FRANK LORENZ-DIETZ, NOVEMBER 2023

Ein kurzer Überblick zu SAF-HOLLAND und wer heute präsentiert

Unternehmensprofil

- SAF-HOLLAND SE mit Sitz im bayrischen Bessenbach zählt zu den **international führenden Herstellern von fahrwerksbezogenen Baugruppen und Komponenten**, vor allem für Trailer und Lkw**,** sowie auch für Busse
- Die **Produktpalette** umfasst neben Achs-, Federungs- und Bremssystemen auch Kupplungssysteme, Königszapfen und Stützwinden
- SAF-HOLLAND erwirtschaftete in 2022 Umsätze von ~ 1,6 Mrd. €. **Inklusive Haldex liegt der Konzernumsatz bei ~ 2 Mrd. €.**

Marken



Frank Lorenz-Dietz

- **CFO** seit Januar 2023
- **Ressorts**: Finanzen, IT, Recht & Compliance, Corporate Audit, Investor Relations, Corporate Communications, ESG, Global Operations
- Zuvor **25 Jahre Automotive Industrie,** darunter 20 Jahre bei Bosch

Hintergrund und mögliche Folgen einer Cyberattacke

Hintergrund zum Thema Cyberattacke

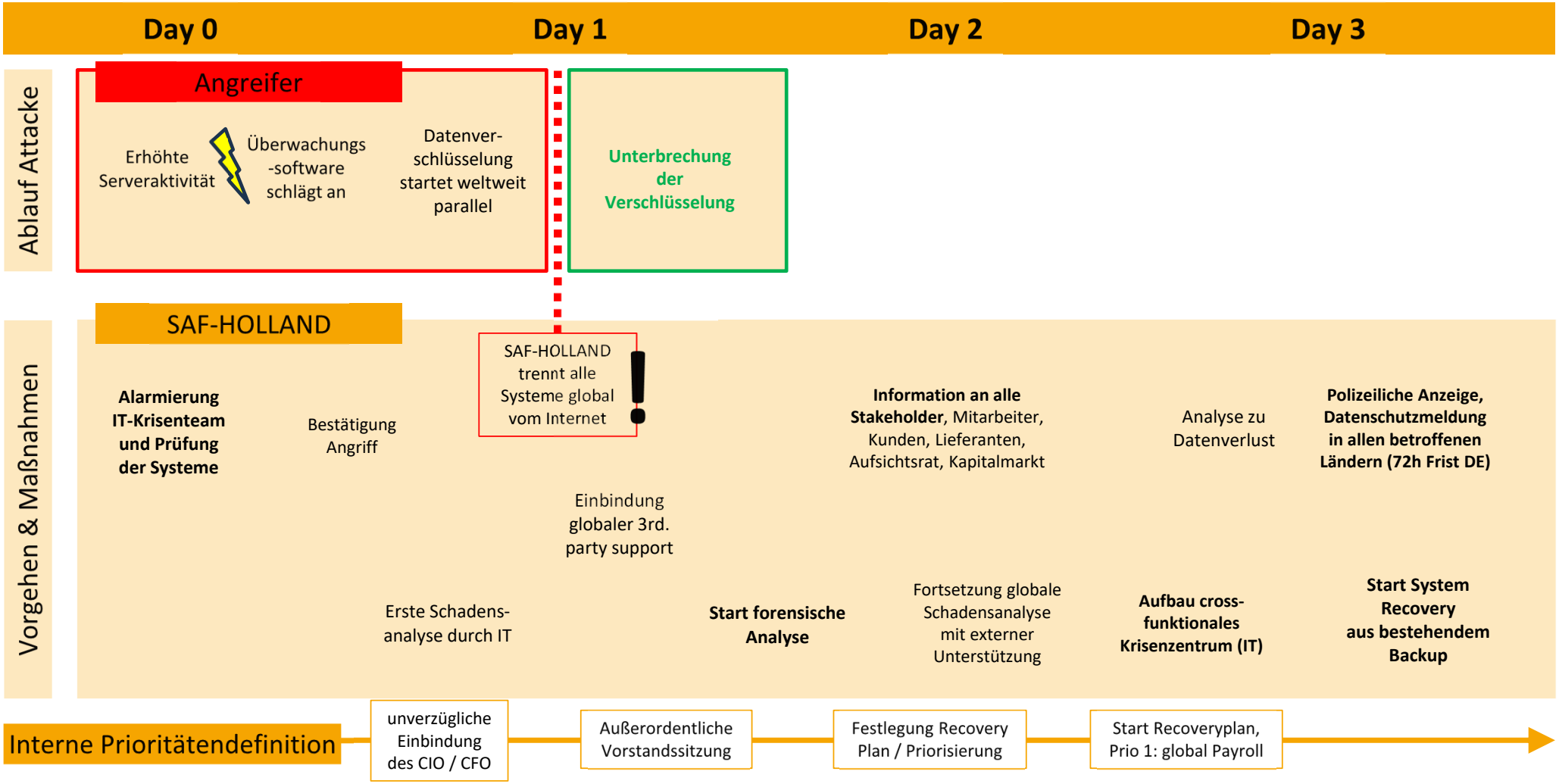
- **Zunahme der Angriffe**: Die Anzahl und Komplexität von Cyberattacken hat in den letzten Jahren exponentiell zugenommen
- **Diverse Ziele**: Angreifer könnten motiviert sein durch finanziellen Gewinn, Industriespionage, politische Motive oder schlicht Vandalismus
- **Beispiele**: Bekannte Fälle von Cyberattacken, (z.B. über WannaCry Ransomware, Equifax Datenverletzung) sind u.a. Evotec, Rheinmetall, Bauer

Mögliche Folgen einer Cyberattacke

- **Betriebsunterbrechung**: Cyberattacken können Betriebsabläufe stören oder komplett lahmlegen
- **Finanzielle Auswirkungen**: Neben direkten finanziellen Verlusten durch z.B. Lösegeldforderungen können auch rechtliche Konsequenzen und Strafen folgen
- **Datenschutzverletzung**: Ein Angriff kann die persönlichen Daten von Kunden oder Mitarbeitern gefährden
- **Reputationsschaden**: Ein unzureichendes Management einer Cyberattacke kann zu irreparablen Reputationsverlusten führen

Preperation is key: eine guter **Maßnahmen- und Reaktionsplan** für den Fall der Fälle kann 1) den Schaden minimieren 2) den Wiederherstellungsprozess beschleunigen sowie 3) rechtliche Risiken verringern

Ablauf des Cyberangriffs und Sofortmaßnahmen von SAF-HOLLAND



SAF-HOLLAND Krisenmanagement und wesentliche Erfolgsfaktoren

1 Vorbereitung als Erfolgsfaktor

- **IT-Sicherheit inkl. regelmäßige Sicherheitsschulungen zentrales Element** der Unternehmensführung
- **Netzwerksegmentierung** bereits vor dem Angriff **teilweise vorhanden**
- **Maßnahmen- und Reaktionspläne** waren vorhanden

2 Wesentliche Maßnahmen / Entscheidungen

- **Kurze Eskalations- / Kommunikationswege & schnelle Entscheidungsfindung**
- **Transparente & offene Kommunikation** mit allen wichtigen Stakeholdern
- Prozess der **Wiederherstellung einer segmentierten IT-Landschaft über bestehende back-up Lösungen** sowie alle IT-Geräte auf Schadsoftware untersuchen
- **Entscheidung: keine lange Ursachenforschung,** sondern **Ziel alle Systeme schnell wieder hochzufahren**

3 Negative Folgen für SAF-HOLLAND minimal

- Produktionsstillstand und dadurch **entgangene Umsätze von insg. 40 Mio. Euro** sowie der entsprechendem Ergebnisbeitrag konnten **nahezu komplett aufgeholt werden**
- **Sonderkosten** von ~ 4 Mio. Euro für IT-Beratung
- **Kein Reputationsverlust,** belastete Kunden- oder sonstige Stakeholder Beziehung

Vorbereitung inkl. Maßnahmen- und Reaktionsplan hat SAF-HOLLAND vor größerem Schaden bewahrt

Was der Maßnahmen- und Reaktionsplan vorgab
Zentral sind schnelle und gleichzeitig koordinierte Handlungen

Tag 1 - Sofortige Reaktion

- **Erkennung und Bestätigung** der Cyberattacke durch das IT-Team
- **Sofortige Berichterstattung** an die Geschäftsleitung (24/7)
- **Aktivierung des Krisenteams** inkl. IT, Kommunikation und Rechtsabteilung
- **Isolierung betroffener Systeme**, um Schaden zu minimieren

Tag 2 - Bewertung und Kommunikation

- **Einschätzung des Schadens** – Welche Daten und Systeme sind betroffen?
- **Kommunikation** – Intern und ggf. extern (relevante Behörden, Kunden, Partner, Öffentlichkeit)
- **Beauftragung externer Experten** – Forensiker, Sicherheitsberater

Tag 3 - Wiederherstellung und Verteidigung

- **Implementierung von Gegenmaßnahmen** – Systeme absichern, Schwachstellen schließen
- **Strategieentwicklung** für die kommenden Tage: Weiteres Vorgehen, Kommunikation, rechtliche Schritte

Rollenaufteilung von Management und Aufsichtsrat bei Cyberattacken

Management:

- **Aktive Rolle im Krisenmanagement**:
  - Trifft schnelle, informierte Entscheidungen
  - Arbeitet eng mit dem Krisenteam und externen Beratern zusammen
- **Entscheidungen über Gegenmaßnahmen und Kommunikation**:
  - Legt die Kommunikationsrichtlinien fest: Was wird kommuniziert, wann und an wen?
  - Entscheidet über den Einsatz von Ressourcen zur Schadensbehebung
- **Sicherstellung der Geschäftskontinuität**:
  - Plant und implementiert Maßnahmen, um den Geschäftsbetrieb aufrechtzuerhalten oder wiederherzustellen
  - Berücksichtigt hierbei sowohl kurzfristige als auch langfristige Auswirkungen

Aufsichtsrat:

- **Beratende Rolle**:
  - Stellt Ressourcen und Expertise zur Verfügung
  - Kann das Management bei der Einholung von Drittmeinungen unterstützen und Kontakte zu Branchenexperten herstellen
- **Überwachung des Managements**:
  - Sicherstellung, dass das Management angemessen auf den Vorfall reagiert
  - Beurteilt, ob das Management alle notwendigen Ressourcen zur Verfügung hat und gegebenenfalls bereit ist, weitere bereitzustellen
- **Langfristige Perspektiven und Strategien**:
  - Arbeitet mit dem Management zusammen, um langfristige Strategien zur Vermeidung zukünftiger Angriffe zu entwickeln
  - Betrachtung der Auswirkungen auf das Geschäftsumfeld und mögliche Veränderungen der Geschäftsstrategie

Typische Schwächen vs. einer idealen Aufstellung um einer Cyberattacke zu begegnen

Typische Schwächen:

- **Fehlende Notfallpläne**:
  - Ohne vorgefertigte Maßnahmenpläne können Reaktionen verzögert oder unangemessen sein
  - Mangelnde Vorbereitung bedeutet oft, dass Ressourcen nicht effizient eingesetzt werden
- **Unzureichende Schulung der Mitarbeiter**:
  - Mitarbeiter sind oft die erste Verteidigungslinie, können aber auch das potentielle Einfallstor für eine Cyberattacke sein
  - Ohne ausreichende Schulung & Sensibilisierung können sie leicht zu Opfern von Schadsoftware, Phishing oder anderen Betrugsversuchen werden
- **Veraltete Sicherheitssysteme**:
  - Alte Systeme sind oft anfälliger für bekannte Sicherheitslücken
  - Das Fehlen regelmäßiger Updates kann das Unternehmen anfällig für Zero-Day-Angriffe machen
- **Mangelnde Kommunikation und Zusammenarbeit**:
  - Wenn Abteilungen isoliert arbeiten, kann das Erkennen und Reagieren auf Bedrohungen behindert werden

Ideale Aufstellung:

- **Krisenteam**:
  - Ein interdisziplinäres Team, das regelmäßig geschult wird und für den Fall einer Cyberattacke bereit ist
  - Sollte aus IT-Spezialisten, Kommunikationsexperten, HR und Rechtsexperten bestehen
- **Regelmäßige Schulungen**:
  - Sicherheitsschulungen für alle Mitarbeiter, um das Bewusstsein für potenzielle Bedrohungen zu schärfen.
  - Szenariobasiertes Training für das Krisenteam, um auf tatsächliche Angriffe vorbereitet zu sein
- **Investition in aktuelle Sicherheitstechnologie**:
  - Implementierung moderner Sicherheitssysteme, Netzwerksegmentierung und regelmäßige Aktualisierungen
  - Einführung eines proaktiven Monitoring, um Angriffe frühzeitig zu erkennen
- **Externe Berater**:
  - Aufbau eines Netzwerks aus externen Sicherheitsexperten
  - Diese können im Krisenfall herangezogen werden oder bei der regelmäßigen Überprüfung der Sicherheitsmaßnahmen helfen

Eine Cyberattacke kann prinzipiell jeden treffen!

1. **IT-Security** (Investitionen, Netzwerksegmentierung, Mitarbeiterschulung, Prozesse) darf man **nicht auf die auf die lange Bank schieben**
2. **Regelmäßige IT-Sicherheitsschulungen der Mitarbeiter** können eine Cyberattacke nicht ausschließen, aber die Wahrscheinlichkeit deutlich reduzieren
3. **Kurze Eskalations- / Kommunikationswege & schnelle Entscheidungsfindung sind zentral** für die Schadensvermeidung sowie Systemwiederherstellung
4. Im Falle eines Angriffs sollten Sie eine **transparente & offene Kommunikation mit allen wichtigen Stakeholdern** führen

Vielen Dank für Ihre Aufmerksamkeit

FINANCE ROUNDTABLE

Regulatorische Anforderungen im Übergang

Sandra Karger
Referatsleiterin
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Regulatorische Anforderungen im Übergang

Assessing Today, Preparing for Tomorrow

BSI, Sandra Karger, 30. November 2023

Kurzprofil des BSI

Gründung
01. Januar 1991

254 Mio. Euro
Budget Haushalt 2023

Stellen 2022
1.733 ↗

183
Neue Stellen zum Vorjahr

BSI vor Ort

- Standorte
- Stützpunkte
- Verbindungsstellen

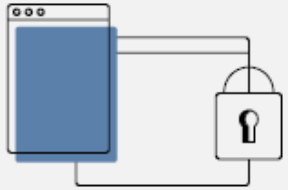
Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.

Die Lage der IT-Sicherheit in Deutschland 2023 im Überblick

Ransomware

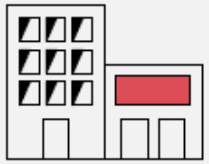
ist weiterhin die größte Bedrohung.

2 **Ransomware-Angriffe** auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.



68 erfolgreiche **Ransomware-Angriffe auf Unternehmen** wurden bekannt.

15 davon richteten sich gegen **IT-Dienstleister**.



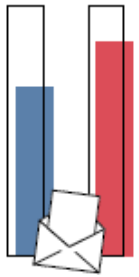
Mehr als **2.000** **Schwachstellen** in Softwareprodukten **(15 % davon kritisch)** wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %.**

Eine Viertelmillion

neue **Schadprogramm-Varianten** wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.

66%

aller **Spam-Mails** im Berichtszeitraum waren Cyberangriffe:
34 % Erpressungsmails,
32 % Betrugsmails



84%

aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.

Top-3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl Sextortion Phishing	***Ransomware*** Abhängigkeit innerhalb der IT-Supply-Chain Schwachstellen, offene oder falsch konfigurierte Onlineserver	***Ransomware*** APT Schwachstellen, offene oder falsch konfigurierte Onlineserver

Rund **21.000** **infizierte Systeme** wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.

Durchschnittlich rund **775** **E-Mails mit Schadprogrammen** wurden an jedem Tag im Berichtszeitraum in deutschen Regierungsnetzen abgefangen.

370 **Webseiten** wurden im Durchschnitt an jedem Tag des Berichtszeitraums für den Zugriff aus den Regierungsnetzen gesperrt. **Der Grund:** Die Seiten enthielten Schadprogramme.

6.220 2022
5.100 2021

7.120 Teilnehmer hatte die **Allianz für Cyber-Sicherheit** im Jahr 2023.

Deutschland Digital•Sicher•BSI•

Bundesamt für Sicherheit in der Informationstechnik

Schaden pendelt sich über 200 Milliarden Euro ein

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch...	Schadenssummen in Mrd. Euro (2023)	Schadenssummen in Mrd. Euro (2022)	Schadenssummen in Mrd. Euro (2021)
Imageschaden bei Kunden oder Lieferanten, Negative Medienberichterstattung	35,3	23,6	12,3
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	35,0	41,5	61,9
Kosten für Rechtsstreitigkeiten	29,8	16,2	12,4
Kosten für Ermittlungen und Ersatzmaßnahmen	25,2	10,1	13,3
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	21,5	41,5	29,0
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	16,1	10,7	24,3
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	15,3	21,1	22,7
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	12,4	18,3	17,1
Patentrechtsverletzungen (auch schon vor der Anmeldung)	10,4	18,8	30,5
Geldabfluss durch Betrugsversuche	3,9	-	-
Sonstige Schäden	1,1	0,9	0
Gesamtschaden pro Jahr	**205,9**	**202,7**	**223,5**

4 Basis: Alle Unternehmen (n=1.002) | Mehrfachnennungen möglich | rundungsbedingt kann die Summe der Einzelschäden vom Gesamtschaden abweichen. |

bitkom

Cybersicherheit in neuen und kommenden EU-Gesetzen

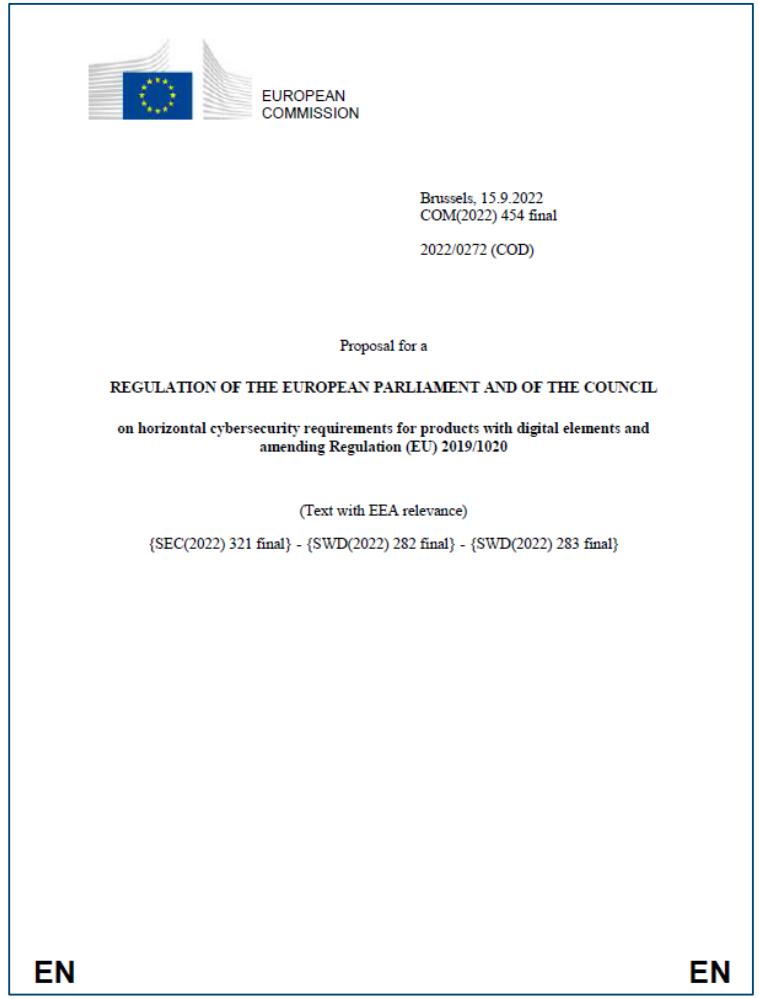
- **Framework**: übergreifende Regeln/Grundsätze
  - NLF - New Legislative Framework Overarching Policy
- **Direktive**: müssen in nationales Recht überführt werden
  - NIS2 - Network and Information Security
  - CER - Directive on the Resilience of Critical Entities
- **Act**: sofort gültig
  - CRA - Cyber resilience act
  - DSA - Digital Services Act
  - CSA - Cyber Security Act – not to mix up with
  - ECSA - EU Cyber Solidarity Act

Cybersicherheit in neuen und kommenden EU-Gesetzen

- **Framework**: übergreifende Regeln/Grundsätze
  - NLF - New Legislative Framework Overarching Policy
- **Direktive**: müssen in nationales Recht überführt werden
  - **NIS2 - Network and Information Security**
  - CER - Directive on the Resilience of Critical Entities
- **Act**: sofort gültig
  - CRA - Cyber resilience act
  - DSA - Digital Services Act
  - CSA - Cyber Security Act – not to mix up with
  - ECSA - EU Cyber Solidarity Act

Cyber Resilience Act (CRA)

- regelt den Marktzugang in Form von **horizontalen europäischen Cybersicherheitsanforderungen** für eine breite Palette von digitalen Produkten und Dienstleistungen
- beinhaltet **Anforderungen für Produkte** über den gesamten Lebenszyklus
- Teil des New Legislative Framework
  → erweitert die Gesetzgebung erstmals von
  safety only to security



EUROPEAN
COMMISSION

Brussels, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

(Text with EEA relevance)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

EN EN

„Network and Information Security (NIS) Directive“

NIS 2-Direktive

1) **Sektoren wurden deutlich erweitert und neu definiert**
„Wesentlich“ („Essential“) und „Wichtig“ („Important“)

2) **hohen Geldstrafen** insbesondere bei schweren Verstößen
→ Strafen von bis zu 20 Millionen Euro oder vier Prozent des globalen Umsatzes des Unternehmens

3) Die **Anforderungen wurden in großen Teilen detaillierter konkretisiert**.

Betroffene Unternehmen

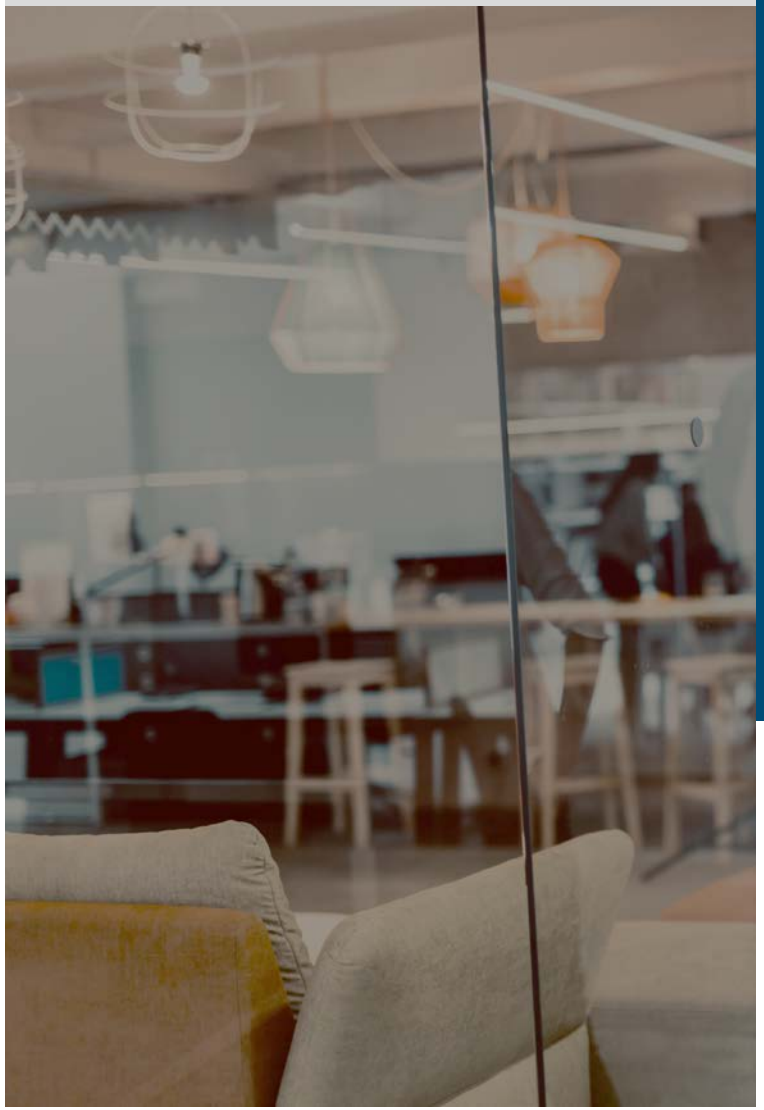
Netz- und Informationssystemdienste
Operatoren von Kritischen Infrastrukturen (KRITIS)

besonders wichtige Einrichtungen

- mindestens 250 Mitarbeiter
- einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro
- qualifizierte Vertrauensdiensteanbieter, DNS-Diensteanbieter
- Anbieter von Telekommunikationsdiensten/-netzen

wichtige Einrichtungen

- mindestens 50 Mitarbeiter
- einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro
- Betreiber kritischer Anlagen



Konkrete Auswirkungen von NIS 2 auf Unternehmen

- bestehende Sicherheitsmaßnahmen überprüfen

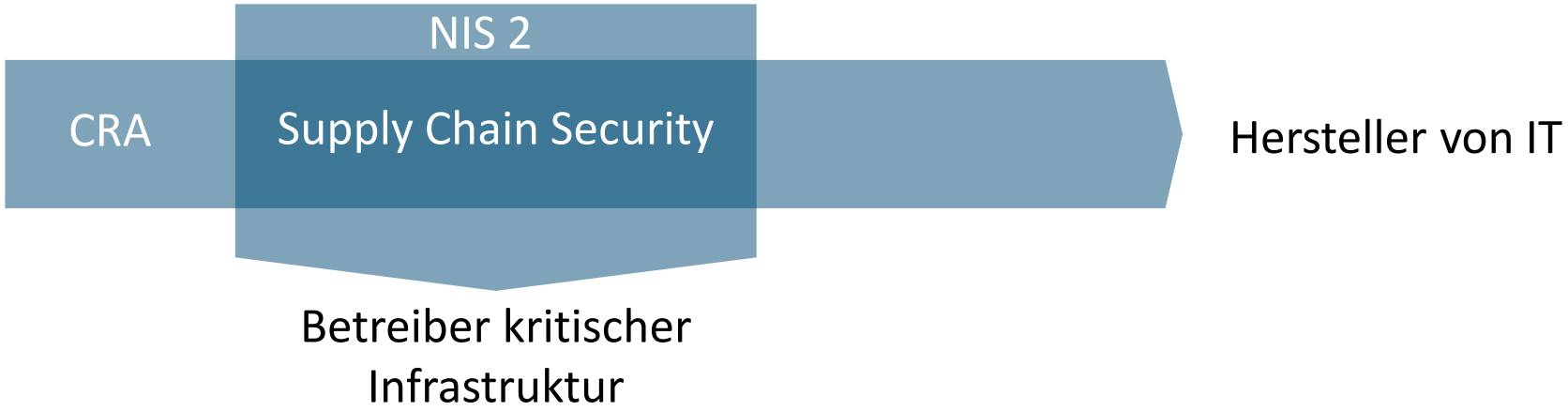
  → verbessern
- Risikobewertung
- Implementierung eines Sicherheitsmanagementsystems

  + Meldung an Behörden

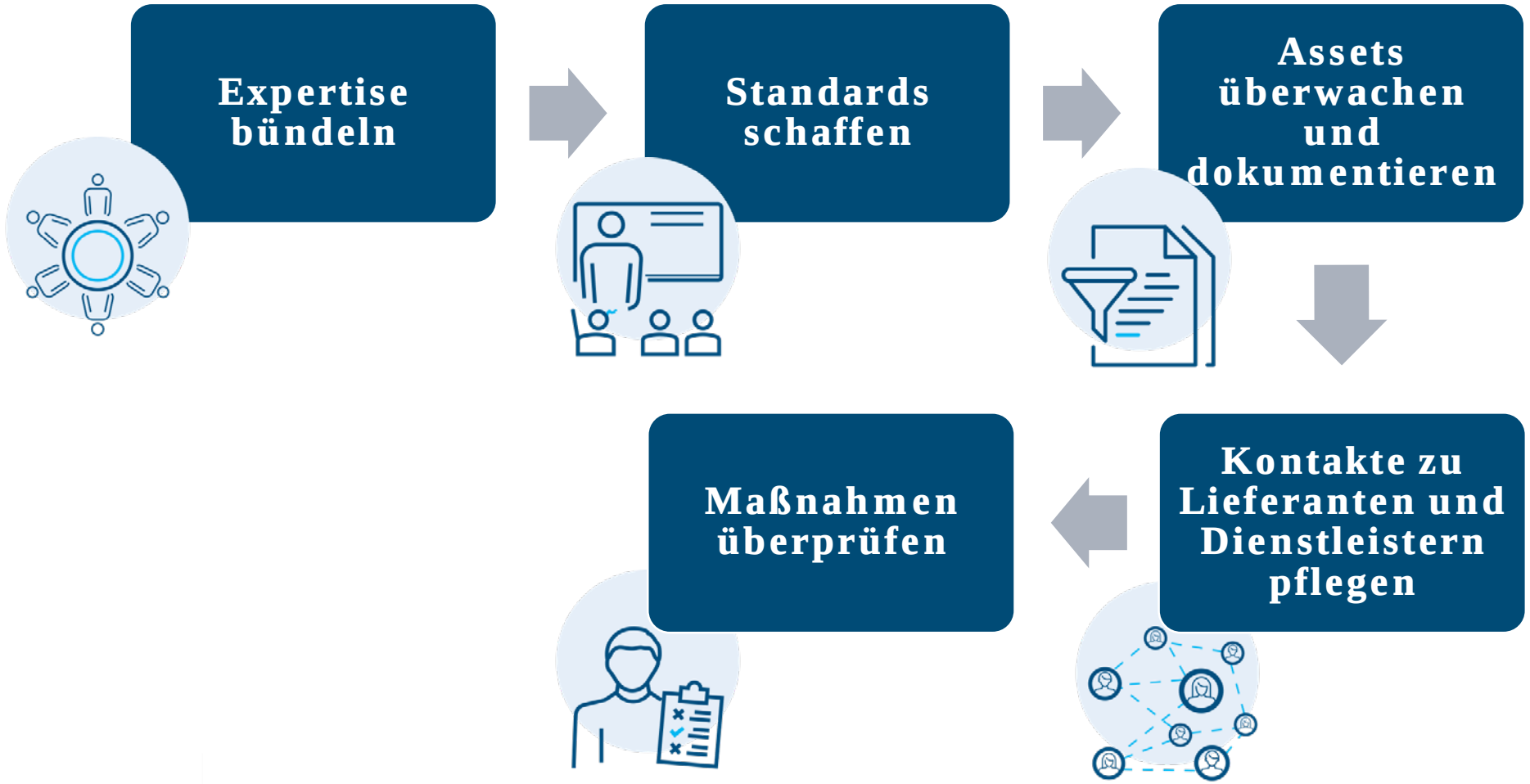
  + Information an Mitarbeitende

Supply Chain Security hält Einzug in die NIS 2-Direktive

- Erweiterung des Risikomanagements in der **Lieferkette** und im Lieferbeziehungsrisikomanagement für wesentliche und wichtige Einrichtungen (Art. 21)
- SCS als verpflichtender Teil der nationalen Cybersicherheitsstrategie (Art. 7)
- Koordinierte Risikobewertung in Bezug auf die Sicherheit kritischer Lieferketten (Artikel 22) durch Kooperationsgruppe (nach Vorbild 5G-Toolbox)



Risikomanagement



„Management Blitzlicht“ – C-SCRM

- Grundlagen des Cyber-Supply Chain Risk Management
- 5 Maßnahmenempfehlungen

Effektives Cyber-Supply Chain Risk Management in 5 Schritten

Der Schutz Ihres Unternehmens vor Cyberrisiken in einer digital vernetzten Welt erfordert ein Verständnis für die (Cyber-)Sicherheitsrisiken, die in Verbindung mit der Lieferkette stehen. Um diese Risiken bewältigen zu können und die Resilienz Ihres Unternehmens zu stärken, bedarf es eines ganzheitlichen Cyber-Supply Chain Risk Management, kurz C-SCRM.

Lieferketten Risiken bedrohen...

... Ihre Handlungsfähigkeit.
... Ihre Firmengeheimnisse.
... Ihre Vertrauenswürdigkeit.
... Ihre Reputation.

Effektives Cyber-Supply Chain Risk Management in 5 Schritten

Folgende 5 Schritte helfen Ihnen, ein effektives Cyber-Supply Chain Risk Management zu etablieren, um angemessen auf Gefahren in der Lieferkette reagieren zu können:

1. **Identifizieren** Sie alle Mitarbeitenden, die in Verbindung mit der Lieferkette stehen.
2. **Entwickeln** Sie die Richtlinien, Strategien und Prozesse zum Schutz Ihrer Lieferkette.
3. **Wissen** Sie, welche Hardware, Software und Dienstleistungen Sie beziehen und woher.
4. **Erlangen** Sie ein tieferes Verständnis Ihrer Lieferkette und Ihrer Zulieferer.
5. **Evaluieren** Sie die Effektivität Ihrer Lieferkettenpraktiken.

Expertise bündeln
Identifizieren Sie alle Mitarbeitenden, die in Verbindung mit der Lieferkette stehen. Lieferkettensicherheit ist ein vielschichtiges und abteilungsübergreifendes Thema. Bilden Sie ein Team mit Vertreterinnen und Vertretern aller relevanten Abteilungen, wie etwa IT-Sicherheit, Produktentwicklung, Recht, Logistik, Beschaffung oder Marketing, um die verschiedenen Perspektiven und Expertisen zusammenzubringen. Nur durch enge Zusammenarbeit der verschiedenen Abteilungen kann ein ganzheitliches Verständnis gewonnen und die richtige strategische Entscheidung getroffen werden.

Standards schaffen
Entwickeln Sie Richtlinien, Strategien und Prozesse, um Risiken in der Lieferkette begegnen zu können. Stellen Sie standardisierte Prozesse für das Supply-Chain Risk Management her und stellen Sie sicher, dass Best Practices, Industriestandards und insbesondere rechtliche Vorgaben berücksichtigt werden. Legen Sie ebenfalls Vorgaben für Ihre Lieferanten fest. Achten Sie stets auf die Angemessenheit Ihrer Maßnahmen.

Assets überwachen und dokumentieren
Sorgen Sie dafür, dass Sie wissen, welche Hardware, Software und Dienstleistungen Ihre Firma von wem bezieht und nutzt. Listen Sie alle Assets auf, die Sie für den Geschäftsbetrieb benötigen oder die in Zusammenhang mit kritischen Vermögenswerten stehen und kennen Sie ihre jeweiligen Zulieferer. Priorisieren Sie ihre Assets entsprechend ihrer Kritikalität für den Geschäftsbetrieb bzw. ihrer möglichen negativen Auswirkungen auf Ihr Unternehmen oder Ihre Kunden. Tragen Sie weiterhin Sorge dafür, dass der gesamte Lebenszyklus Ihrer Assets überwacht und dokumentiert wird.

Kontakte zu Lieferanten und Dienstleistern pflegen
Erlangen Sie ein tieferes Verständnis für Ihre Lieferkette und Ihre Zulieferer. Lieferketten erstrecken sich oftmals über viele Unternehmen weltweit. Um Risiken managen zu können, welche sich aus der Beziehung Ihrer Zulieferer zu deren Zulieferern oder aus anderen technischen und nicht-technischen Einflüssen ergeben, sollten Sie die bestmögliche Transparenz schaffen. Stellen Sie sicher, dass Sie einen engen Kontakt zu Ihren Lieferanten pflegen. Führen Sie entsprechende Kontrollstrukturen und Kommunikationspläne ein, um festzustellen, ob Ihre Zulieferer über eine angemessene Sicherheitskultur verfügen.

Maßnahmen überprüfen
Evaluieren Sie regelmäßig die Effektivität Ihres C-SCRM. Entwickeln Sie die benötigten Metriken, mit denen Sie die Effektivität Ihrer Maßnahmen überprüfen können. Bestimmen Sie, in welcher Frequenz eine Überprüfung stattfinden soll und ggf. Änderungen vorgenommen werden sollen. Nur so können Sie dauerhaft sicherstellen, dass Sie angemessen auf (Cyber-)Sicherheitsrisiken und Disruptionen in Ihrer Lieferkette reagieren können.

Bundesamt für Sicherheit in der Informationstechnik
Deutschland Digital•Sicher•BSI

MANAGEMENT BLITZLICHT | 2023

Grundlagen des Cyber-Supply Chain Risk Management (C-SCRM)

Vielen Dank für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI•

Sandra Karger
Referatsleiterin
Referat WG 21 - Kooperation mit Herstellern und Dienstleistern

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185 -189
53175 Bonn
Telefon: +49 228 99 9582-5027
Mobil: +49 160 91807974
E-Mail: sandra.karger@bsi.bund.de
Internet: www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

FINANCE ROUNDTABLE

Gruppenarbeit

Gruppenarbeit

FINANCE ROUNDTABLE

Frage 1:

Informationssicherheit braucht eine starke Stimme am Tisch des Vorstands:
Wie kann der CFO zum Executive Sponsor der IT- und Informations-sicherheit im Vorstand werden und diese Rolle wirksam gestalten?

FINANCE ROUNDTABLE

Frage 2:

Der Cybersicherheits-Notfallplan ist ein Kernelement einer wirksamen Sicherheitsstrategie:
Was sollte der Notfallplan in jedem Fall beinhalten und worauf kommt es an, damit der Notfallplan auch wirklich erfolgreich eingesetzt werden kann?

FINANCE ROUNDTABLE

Frage 3:

Compliance-Anforderungen im Bereich der IT-Sicherheit entwickeln sich dynamisch:
Wie sollte der IT-Compliance Prozess durch den CFO und weitere Stakeholder im Unternehmen gestaltet, etabliert und gelebt werden?

FINANCE ROUNDTABLE

Ergebnisse/ Rundgang

FINANCE
ROUNDTABLE

FINANCE ROUNDTABLE

Wrap up & Abschluss

FINANCE ROUNDTABLE

Herzlichen Dank für Ihre Aufmerksamkeit!

https://www.finance-magazin.de/events/future-finance-festival/