HEALTH-IT TALK

Cybersicherheit und Ransomware
Prävention, erste Hilfe im Notfall und regulatorischer Rahmen

Dr. Jan Scharfenberg

Director Information Security

ISiCO

Raphael Jünemann

Rechtsanwalt, Senior Associate

SCHÜRMANN ROSENTHAL DREYER RECHTSANWÄLTE

Agenda

1. Erfahrungswerte
2. Best Practices
3. Regulatorischer Rahmen

Einleitung

Bedrohungslage

Politische Cyberangriffe

- Deutlicher Anstieg in den letzten Jahren (Ukraine-Russland) – auch Konflikt zw. Israel und Hamas
- Falschinformation, Sabotage, Datendiebstahl und -verschlüsselung bis hin zur langfristigen Spionage

Ransomware

- starker Anstieg in 2023; Attacken gezielter und ausgeklügelter; Vorbereitung (Auskundschaften; Eindringen, Kompromittieren) immer schneller (wenige Tage)
- Datenverschlüsselung/ Drohung der Veröffentlichung

KI

- neuer Bedrohungsgrad durch KI-Nutzung bei Social Engineering, insbesondere iRd Phishing (Qualität von Emails immer besser) + Deepfakes
- Abwehr profitiert auch: KI-basierte Anomalie-erkennung (Echtzeit), intelligente Authentifizierung und automatisierte Incident Response

IoT-Infrastruktur-Angriffe

- Enormer Anstieg der Anzahl von IoT-Geräten (2023: ca. 15 Mrd.; Prognose für 2030: ca. 30 Mrd.)
- vernetzt = angreifbar

IT-Sicherheitsschwachstellen

- Tendenz stark steigender Zahl der sog. Common Vulnerabilities and Exposures (CVEs) → BSI-Lagebericht 2022 : 2021 insg. 20.174 Schwachstellen (+10% im Vgl. zum Vorjahr)
- Suche nach solchen Schwachstellen eine der Hauptaktivitäten für Cyberkriminelle

Angriffe auf Lieferketten

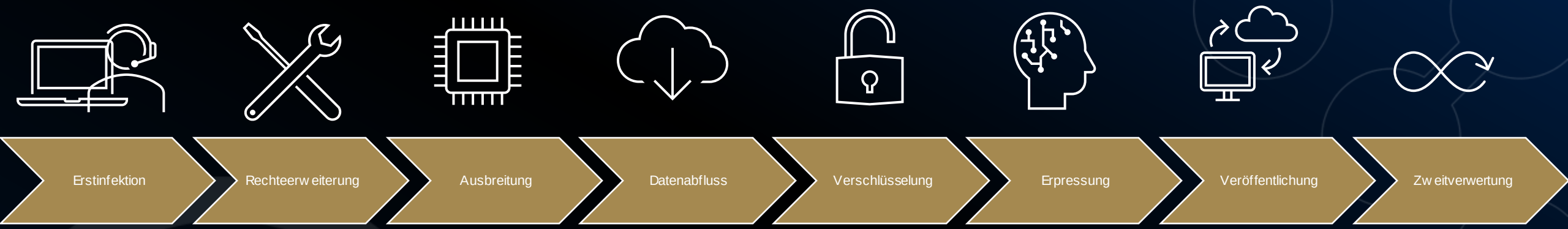
- Kompromittierung von Software- oder Hardware-Produkt eines Drittanbieters oder Zulieferers, um über diesen Weg das eigentliche Ziel anzugreifen

Risiken im Überblick

- Datenverlust
- Diebstahl von geistigem Eigentum
- Reputationsschäden/
  Verlust von Kundenvertrauen
- Betriebsunterbrechungen
- Finanzielle Verluste:
  - Entgangene Gewinne;
  - Bußgelder;
  - Schadenersatz

1. Erfahrungswerte

Angriffsablauf Ransomware:



Vertraulichkeitsverlust

Verfügbarkeitsverlust

Datenverlust

Diebstahl von geistigem Eigentum

Betriebsunterbrechungen

Bußgelder, Strafen & Schadenersatz

Reputationsschäden

Finanzielle Verluste

Verlust von Kunden-vertrauen

Prävention und Readiness durch TOM

Technisch

- Update- und Patch-Management
- Sperren von Anhängen, Makros, Dateiformaten; Sandboxing
- Kompartmentalisierung von Systemen
- Rechte- und Rollenkonzept
- Verschlüsselung
- Datenminimierung/Löschkonzepte
- Backups
- Engmaschige Logs
- Pentests

Prävention und Readiness durch TOM

Organisatorisch

- Awareness
  - Regelmäßige Schulungen
  - Test-Phishing
  - Regelmäßige Sensibilisierungen
- Doku: Systemübersichten + Verfahrensverzeichnisse
- Auftraggeber-/Dienstleistermanagement
- Meldeverfahren
- DSMS + ISMS : PDCA

Interne Kommunikation

- Kommunikation ist essentiell!
- Kommunikationsfähigkeit muss bestehen, Notfallkommunikation sicherstellen
- Stakeholderidentifikation
- Krisenkommunikation **intern**
  - Task Forces
  - DSB
  - Kanzlei
  - APT-Response-Dienstleister
  - Beschäftigte → Kommunikationsvorlagen intern
  - Sprachregelungen für Beschäftigte | Vorsicht bei Presseanfragen!

Externe Kommunikation

- *Wer?* (Aufsichtsbehörden, Staatsanwaltschaft und Polizei; B2B-Kunden & Partner; Patienten; Endkunden; Beschäftigte; Ehemalige; Öffentlichkeit; Versicherung)
- *Was?*
  - Inhalte klären, Mustertexte mit austauschbaren Bausteinen schaffen
  - mit Stakeholdern und ggf. Versicherung abklären, was und in welchem Umfang kommuniziert werden soll (Granularität von Ablauf und Umfang, Ursache)
  - Rechtlich klären, was herausgegeben werden muss (IT-Berichte, Umfang des Hergangs etc., Verursacher (ggf. andere Kunden?))
- *Wann?* (Fristen- und Ablaufmanagement)
- *Wie?* (Website, E-Mail etc.)
  - Kommunikationswege schaffen, planen, abwägen
  - Website: Erreicht nicht alle zielgenau, schlechte PR, etc.
- Zusatzinhalte & Maßnahmen vorbereiten, z.B. Identitätsschutzdienst

Aufsichtsbehörden

- Meldepflicht an Datenschutzbehörden aus Art. 33 DSGVO
  - Verantwortliche binnen 72h ab Kenntnisnahme
  - Ggf. vorläufig und abgestuft
  - Auftragsverarbeiter unverzüglich
- Vorsicht bei Angaben, die zu einer Selbstbelastung führen könnten
- Vorsicht bei Meldungen als kombinierter Verantwortlicher/Auftragsverarbeiter
- NIS2 o.ä.?
  - Weitere Behörden
  - Andere Meldegrundsätze
  - Andere Fristen

Verantwortlichkeiten und Verträge

- Eigenes Pflichtenprogramm klären
- Übersicht über Vertragspartner
- Regelungen in Verträgen prüfen
  - Datenschutz: Eigene / gemeinsame Verantwortlichkeit / Auftragsverarbeitung
  - Welche Vertragsversionen gibt es (Vertragshistorie, Vertragshygiene, Vertragsmanagement)
  - Regelungen zu Vorfällen (höhere Gewalt? Ausfallzeiten? Informationspflichten?)

Versicherungen

Klärung der Abdeckung:

- Ausschluss Ransomware-Fälle? Lösegelder? Bußgelder? Schadensersatzforderungen? Dienstleister- und Rechtsberatungskosten?
- Deckungshöhe
- Klärung von Obliegenheiten, insb. Anzeige- und Abstimmungspflichten
- Dokumentation, dass keine Obliegenheitsverletzungen vorliegen
- Klärung zu den über Versicherung eingesetzten Dienstleistern

2. Best practices

Best practices:
be prepared but assume breach

Präventionsmaßnahmen und Risikomanagement

- Eintrittswahrscheinlichkeit senken
- Schwere eines Angriffs und Auswirkungen abmildern

Vorbereitung auf den Ernstfall

- zeitdruck-/stress-/übermüdungsbedingte Fehler vermeiden
- Sicherheit in der Kommunikation
- klare Prozesse unter Einbindung aller relevanten Stakeholder etablieren
- Verträge sachgerecht? (Dienstleister, Partner, Versicherer)

Im Ernstfall:

- Stringentes und planvolles Handeln
- nach klaren Ablaufplänen
- Rückgriff auf spezialisierte Dienstleister (APT-Response-Dienstleister, Kanzlei)

NIS2 oder andere Rechtsakte?:

- Anwendbarkeitsanalyse
- Compliance-Setup ergänzen & Risikomanagement ausbauen

3. Regulatorischer Rahmen

Regulatorischer Rahmen

Europäischer Rechtsrahmen

- (z.B. DSGVO, NIS-RL, Cyber Security Act, CER-Richtlinie, *Cyber Resilience Act*, *KI-VO*)

Nationale Gesetzgebung

- (z.B. BSI-G, TKG, BDSG)

Standards und Zertifizierungen

- (z.B. ISO/IEC 27XXX-Reihe, B3S)

NEU: *Network Information Security Directive* (NIS2) - Überblick

Hintergrund

- **Ziel**: Vereinheitlichung des Cybersecurity Niveaus auf EU-Ebene und Sicherstellung eines hohen Sicherheitsniveaus in für die Gesellschaft wichtigen (nicht nur kritischen) Organisationen
- **Schwerpunkt:** Sicherheit der Lieferkette
- **Nachweis ordnungsgemäßer Umsetzung:** u.a. regelmäßige Sicherheitsaudits

Wesentliche Pflichten

- Risikomanagement - Geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen zur IT-Sicherheit
- Meldung und Bericht bei Sicherheitsvorfällen
- Business Continuity Management
- Lieferanten-/Dienstleistermanagement

Anwendungsbereich NIS2

1. Kriterium: Sektor

Sektoren mit hoher Kritikalität
(Anhang I NIS2)

Sonstige kritische Sektoren
(Anhang II NIS2)

Anwendungsbereich NIS2

2. Kriterium: Unternehmensgröße

Größenklasse	Einstufung nach NIS2	Mitarbeiter		Jahresumsatz
~~Kleines Unternehmen~~	~~Wichtige Einrichtung~~	~~<50~~	~~UND~~	~~<10 Mio. EUR~~
Mittleres Unternehmen	**Wichtige Einrichtung**	50-249	UND	<50 Mio. EUR
	Wichtige Einrichtung	<50	UND	>10 Mio. EUR
Großes Unternehmen	**Wesentliche Einrichtung** (wenn Anhang I) **Wichtige Einrichtung** (Anhang II)	>250	ODER	>50 Mio. EUR

Anwendbarkeit Gesundheitsbranche

Ziff. 5 Anhang 1 NIS2-RL	
Gesundheitswesen	Gesundheitsdienstleister (Artikels 3 Buchstabe g der Richtlinie 2011/24/EU)
	EU-Referenzlaboratorien (Artikels 15 der Verordnung (EU) 2022/2371)
	Einrichtungen mit Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel
	Hersteller pharmazeutischer Erzeugnisse
	Hersteller von Medizinprodukten

Anwendbarkeit Gesundheitsbranche

Bisher KRITIS unterliegende Unternehmen: **keine großen Auswirkungen**

- → KH: > vollstationäre Fälle/ Jahr
- → Apotheken: > 4,65 Mio. Packungen/ Jahr

Besonders wichtige Einrichtungen (Umsatz>50 Mio .€ od. >250 MAs)

- → mittelgroße KHs
- → Therapiezentren

Wichtige Einrichtungen (>49 MAs od. >10 Mio. € Umsatz)

- → größere MVZs
- → Radiologische Einrichtungen
- → Fachkliniken

NIS2 und Sanktionen

Bußgelder

Wesentliche Einrichtungen	Wichtige Einrichtungen
Geldstrafen bis zu 10 Mio. €	Geldstrafen bis zu 7 Mio. €
oder 2 % des weltweiten Vorjahresumsatzes	oder 1,4 % des weltweiten Vorjahresumsatze

Weitere Sanktionen

- Warnungen
- Verbindliche Anweisungen
- Umsetzung der Empfehlungen der Sicherheitsüberprüfung
- Benennung eines Überwachungsbeauftragten
- Veröffentlichung von Verstößen gegen die Richtlinie

Genügen im Falle Wesentlicher Einrichtungen Maßnahmen nicht:

→ Entzug von Zertifizierung oder Genehmigung für den Geschäftsbereich möglich

→ Außerdem kann einzelnen Mitgliedern von Vorstand oder Geschäftsführung Ausübung leitender Tätigkeit in der Organisation vorübergehend untersagt werden.

Besondere Verantwortung Management

Geschäftsleitung ist verpflichtet:

- **Risikomanagementmaßnahmen** zur Cybersicherheit zu **billigen**, und
- deren **Umsetzung** zu **überwachen**.

  → *Beachte: Verpflichtung nicht durch Beauftragung eines Dritten erfüllbar*

- Im Falle von Pflichtverletzungen **haftet** die **Geschäftsleitung persönlich** gegenüber dem jeweiligen Unternehmen für den entstandenen Schaden.

Was kann Schürmann Rosenthal Dreyer für Sie tun?

Ransomware Readiness Audit:

- Rechtliche Prüfung der bestehenden technischen und organisatorischen Maßnahmen und Dokumentation
- Empfehlungen zur Verbesserung der Ransomware Readiness und umzusetzenden Maßnahmen
- Review und Anpassung von Verträgen, insb. im Rahmen des Dienstleister- und Auftraggebermanagements
- Prüfung und Empfehlungen hinsichtlich des Schutzes durch Cyberversicherungen
- Planung und Durchführung von Awareness-Maßnahmen und Schulungen

Akute Hilfe im Notfall

- Schnelle Unterstützung im Falle von Cyberangriffen zur Koordination und rechtlichen Begleitung der Behebung, Aufarbeitung und Kommunikation, z.B. gegenüber Aufsichtsbehörden, Betroffenen und der Öffentlichkeit
- Unterstützung und Vertretung bei der Abwehr bzw. Durchsetzung von Ansprüchen

Nachbereitung von Cyberangriffen:

- Identifikation der Lessons Learned, Empfehlungen und Dokumentation im Rahmen des PDCA-Zyklus
- Beratung und Vertretung in Behördenverfahren
- Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter.

Was kann ISiCO für Sie tun?

Anwendbarkeitsanalyse:

- Gap-Analyse zu den Compliance Vorschriften.
- Identifikation und Priorisierung von bestehenden Sicherheitslücken.
- Empfehlungen für Verbesserungsmaßnahmen für volle Compliance

Bestimmung notwendiger Maßnahmen:

- Erstellung einer Roadmap zur Umsetzung der Empfehlungen.
- Definition klarer Ziele und Sicherheitsstrategien für die Compliance.

Unterstützung bei der Umsetzung:

- Implementierung von Sicherheitsmaßnahmen und -kontrollen.
- Laufende Überwachung und Anpassung der Sicherheitsinfrastruktur.
- Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter.

Kontakt

Raphael Jünemann
Rechtsanwalt | Senior Associate
Schürmann Rosenthal Dreyer Rechtsanwälte PartmbB

juenemann@srd-rechtsanwaelte.de

Dr. Jan Scharfenberg
Rechtsanwalt | Director Information Security
ISiCO Datenschutz GmbH

scharfenberg@isico-datenschutz.de