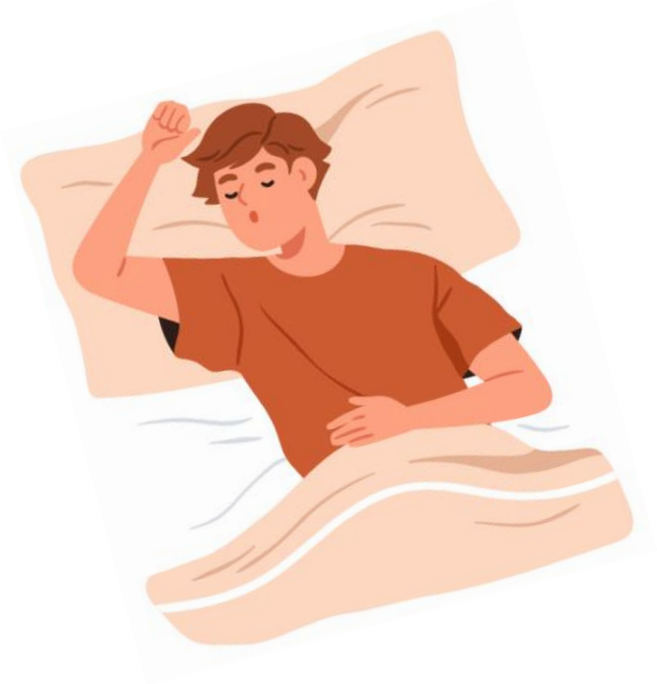
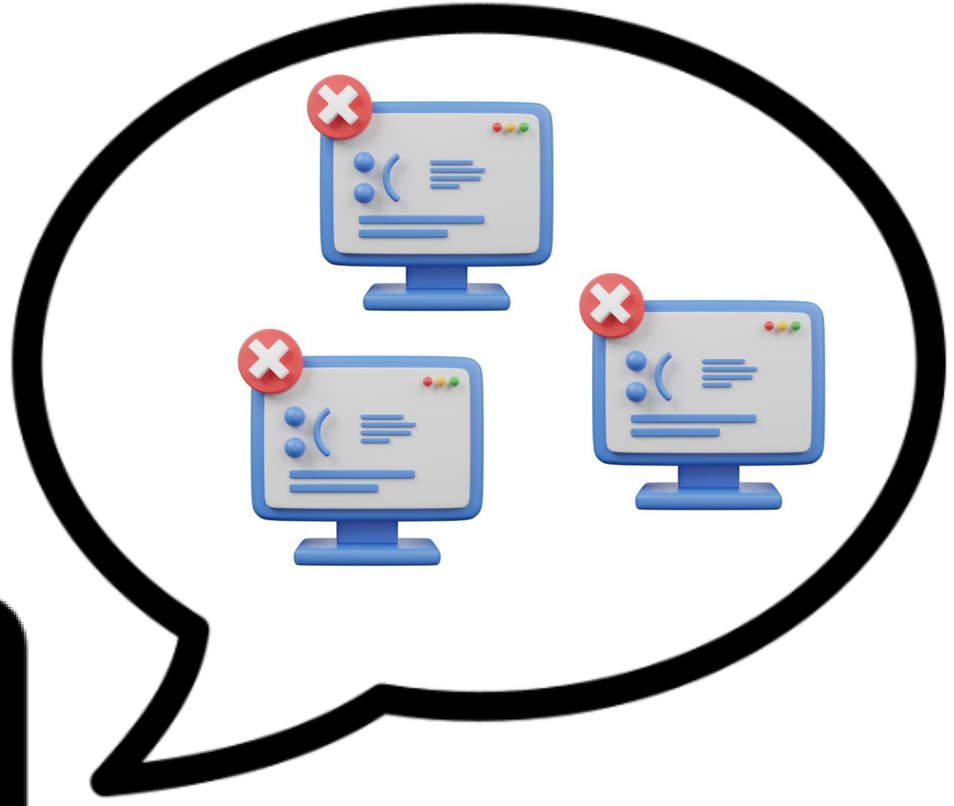
Kulmitzer Lukas

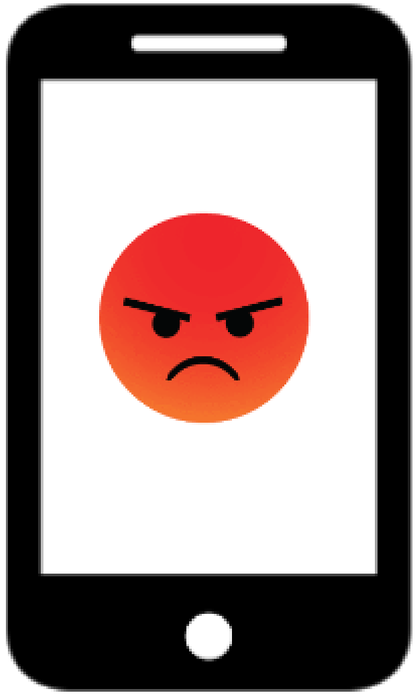
19.11.2024

Auswirkungen von NIS-2 auf die Supply Chain Security

Herausforderungen und Lösungsansätze







“Was ist passiert?”

SOLARWINDS-HACK

Ein Hackerangriff, der um die Welt geht

Der Angriff auf das Unternehmen SolarWinds gilt als größter Hack seit Jahren. Zehntausende Firmen könnten betroffen sein. Um was geht es, wie gefährlich ist es und wie kann man sich schützen? Antworten auf die wichtigsten Fragen.

von Eike Kühl

Supply-Chain-Attacken

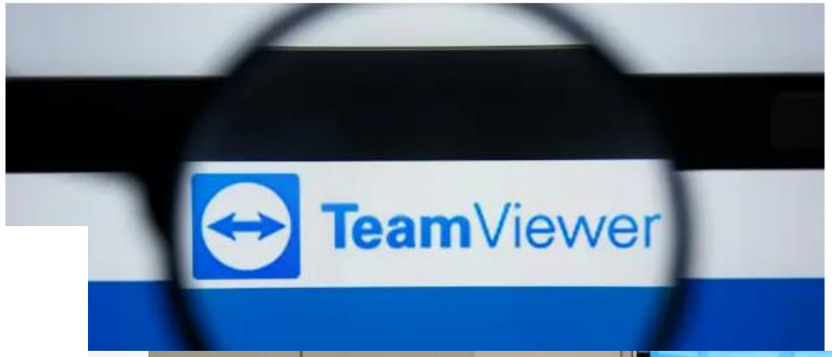
Cyber-Angriff auf GitHub-Verzeichnisse zeigt die Gefahr von Supply-Chain-Attacken

22.08.2022, München, Check Point | Autor: Christine Schönig

APT-Angriff auf Fernwartungssoftware? Sicherheitsvorfall bei TeamViewer

Noch ist über das Ausmaß des Angriffs gegen die Fernwartungssoftware nicht viel bekannt - erste Hinweise auf die Urheber deuten auf Profis hin.

265



„GRÖSSTER AUSFALL DER GESCHICHTE“

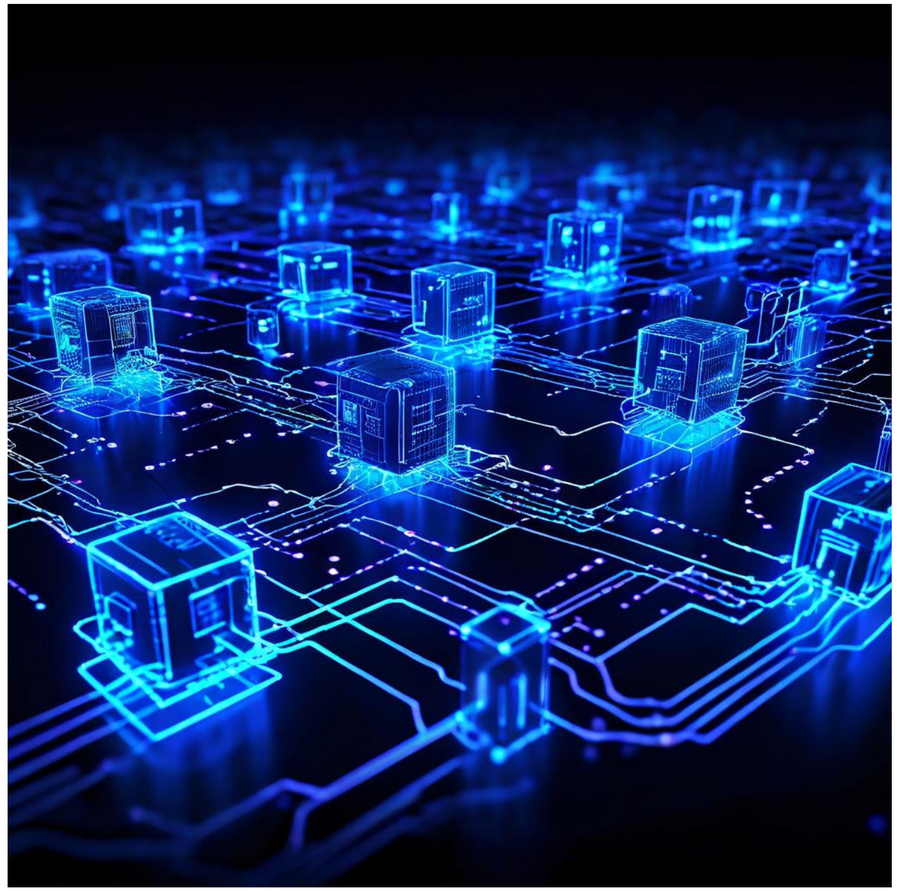
Fehleranalyse nach globaler IT-Panne läuft

Nachdem ein einziges Update der IT-Sicherheitssoftware der Firma CrowdStrike am Freitag zum laut Experten „größten IT-Ausfall der Geschichte“ geführt hat, ist weiter unklar, warum der fehlerhafte Code ohne Überprüfung so großflächig ausgerollt worden ist. Betroffen sind vor allem Flughäfen, aber auch Banken, Unternehmen, Telekomfirmen, Krankenhäuser und Rundfunksender haben teils noch immer mit Störungen zu kämpfen.

Komplexität der Lieferkette

Moderne Lieferketten sind aufgrund der globalen Vernetzung, der Vielzahl an beteiligten Akteuren, technologischen Abhängigkeiten und der Notwendigkeit, ständig auf wechselnde Marktbedingungen und regulatorische Anforderungen zu reagieren, äußerst komplex.

Globalisierung
Compliance Technologie
Komplexität IoT Security
Vernetzung Preismodelle
Regulatorien Wettbewerb Prozesse
Abhängigkeiten
Marktanforderungen



Was fordert NIS-2 ?

Aufgrund des raschen Aufkommen von neuen Technologien sowie dem Entstehen von neuen Abhängigkeiten wird die digitale Bedrohungs-landschaft immer komplexer. Aus diesem Grund ist es notwendig eine klare Baseline hinsichtlich Sicherheitsmaßnahmen zu definieren.

Risikomanagement-Maßnahmen

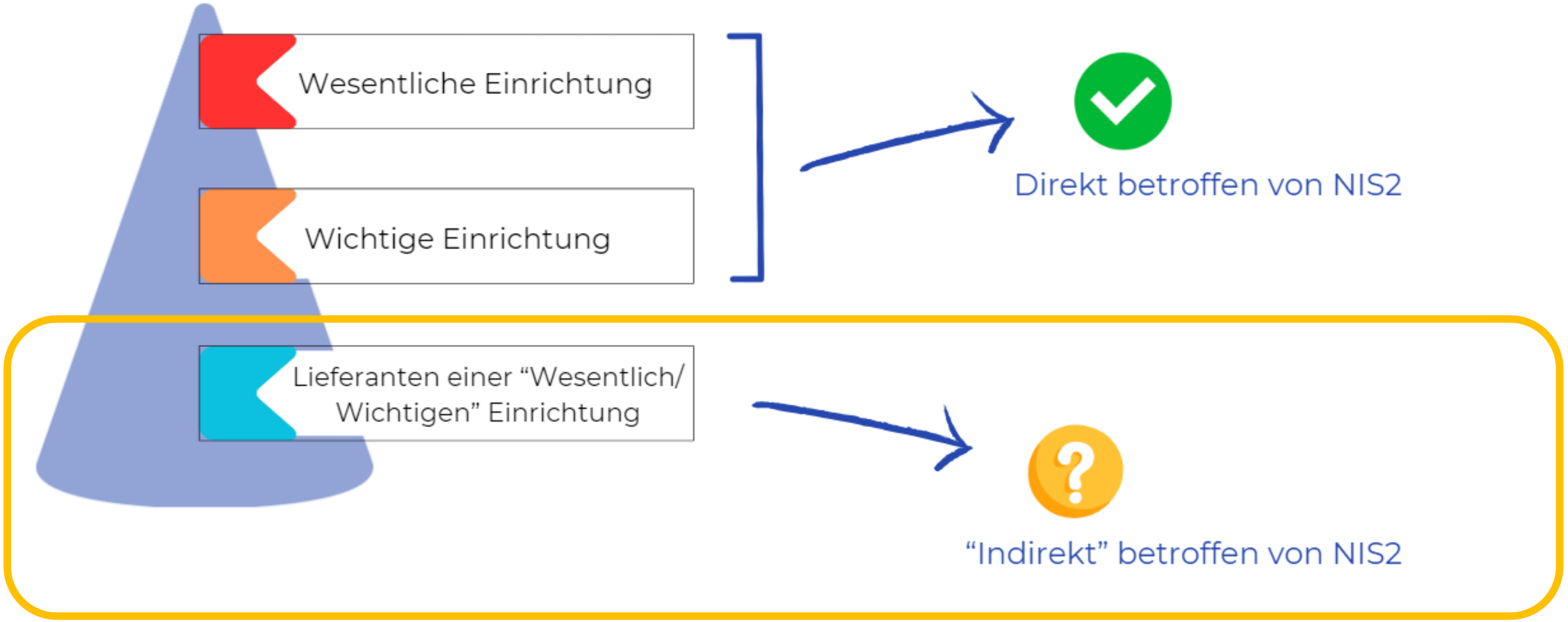
- Technische und organisatorische Sicherheitsmaßnahmen etablieren
- Cyberbedrohungen identifizieren
- **Lieferkettenrisiken berücksichtigen (=Supply Chain Risk)**

Berichtspflichten

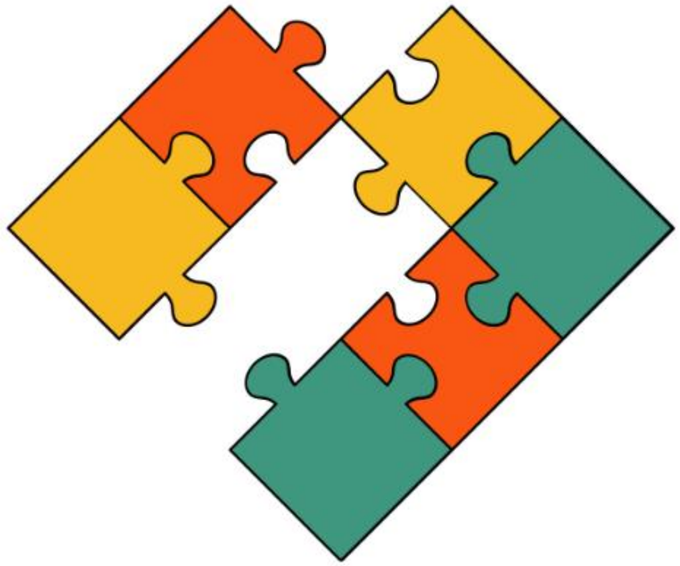
- Meldepflicht für erhebliche Sicherheitsvorfälle
- Einführung zeitlicher Meldefristen
- Laufender Informationsaustausch
- Übergreifende Zusammenarbeit mit Behörden

NIS2
Directive

Wer sind die Betroffenen nach NIS-2 ?



Herausforderungen in der Supply Chain Security



- Wer sind meine (geschäftskritischen) Lieferanten?
- Welche Sicherheitsanforderungen gelten für diese? (=Supply Chain Security)
- Wie kann ich sicherstellen, dass meine Lieferanten diese Anforderungen auch erfüllen?

Wer sind meine (geschäftskritischen) Lieferanten?

Lieferantenrisiken müssen bereits im Beschaffungsprozess evaluiert werden!

Durchführung einer Business Impact Analyse (BIA) - Beispielfragen:

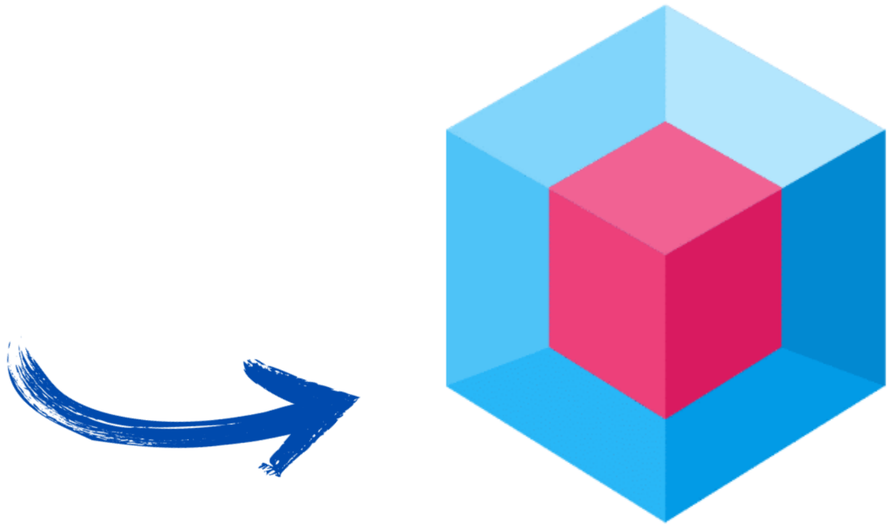
- Zugriff auf (sensible) Informationen?
- Zugriff auf System- bzw. Netzwerkinfrastruktur vorhanden?
- Physischer Zutritt zu (kritischen) Geschäftsbereichen möglich?
- Prozessuale Abhängigkeiten vom jeweiligen Lieferanten?
- Kundenauswirkungen bei Ausfall?
- Ersetzbarkeit des Lieferanten möglich? („Lock-in“ Risiko)

Beispiel für Business Impact Analyse (BIA)

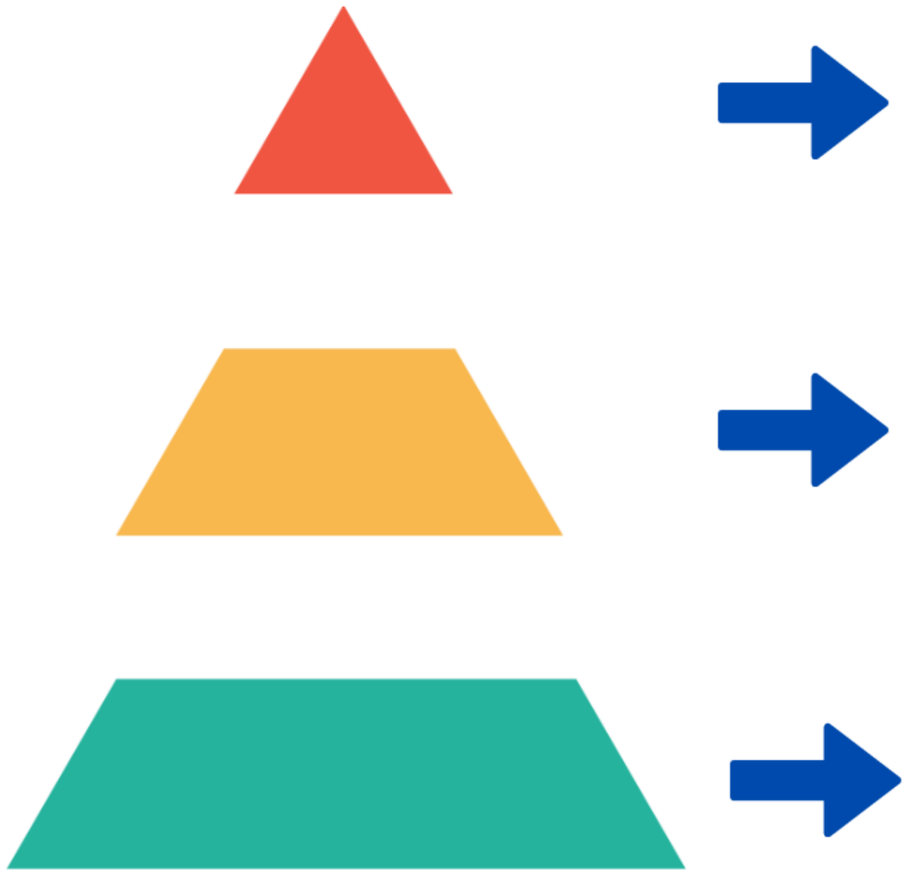
Es müssen angemessene Bewertungsebenen geschaffen werden, um eine **risiko-orientierte** Einstufung zu gewährleisten

BIA für einen Software-Supplier (SaaS):

Fragestellungen	**Mittel (Risiko)**	**Hoch (Risiko)**
Zugriff auf (sensible) Daten?		**x**
Zugriff auf interne (kritische) Systeme oder Unternehmens-Netzwerke?		
Physischer Zutritt zu (kritischen) Bereichen möglich?		
(Kritische) prozessuale Abhängigkeiten vorhanden?		**x**
(Kritische) Kundenauswirkungen bei Ausfall?	**x**	
Besteht ein (kritisches) „Lock-In“ Risiko?	**x**	



Welche Sicherheitsanforderungen gelten für Lieferanten?



Hohe Kritikalität:

- Relevante Reports & Zertifizierungen (SOC-2, ISO27001, TISAX, BSI IT-Grundschutz)
- „Delta“ zu NIS-2 Anforderungen individuell über „**TOMs+**“ definieren!
- Laufendes Monitoring & Lieferantenaudits

Mittlere Kritikalität:

- Relevante Reports & Zertifizierungen (SOC-2, ISO27001, TISAX, BSI IT Grundschutz)
- TOMs (Tech./Org. Maßnahmen) einfordern und auf DSGVO Konformität überprüfen
- Lieferantenaudits / Questionnaires

Keine bzw. geringe Kritikalität:

- Allgemeine Richtlinien müssen eingehalten werden
- Re-Evaluierung im Sinne des zyklischen Supplier Rating (beides gilt für alle Kategorien)

Beispiel für „Delta“ zu NIS-2 Anforderungen

NIS-2 Anforderungen gehen über technische/organisatorische Maßnahmen nach DSGVO hinaus – Stichwort: Stand der Technik!

Beispiele ergänzende Maßnahmen (TOMs+) für Supplier:

Kategorie: ***Software Supplier (SaaS)***

- ✓ Strukturiertes (IT)-Risikomanagement
- ✓ Schulungen Cybersicherheit
- ✓ Incident Response Prozess und Vulnerabity Disclosure Policy
- ✓ Zyklische Schwachstellenscans / Pentests
- ✓ Redundante Systeme / Notfallmanagement
- ✓ Durchführung von Application Security Testing / SBOM definieren

Wie kann ich sicherstellen, dass mein Lieferant dies auch erfüllt

Risikomanagement → Transparenz schaffen!!

Unterschiedliche Möglichkeiten nutzen!

Beispiele aus der Praxis:

- ✓ SLA-Penalties vorab schriftlich vereinbaren
- ✓ Auditrecht einräumen
- ✓ Zeitnahes Reporting etablieren (z.B.: Vulnerabilities, Risiken, Security Incidents, Notfallübungen/Recovery Tests)
- ✓ Sicherheitsbewertung von Sub-Lieferanten einfordern
- ✓ Zyklische Besprechung der Sicherheitsmaßnahmen samt Status

WAS tun wenn der Lieferant Anforderungen nicht erfüllen kann/will ???

„Paul´s Cheat Sheet“

Schritt 1:
Lieferanten identifizieren

Schritt 2:
Faktoren für Ermittlung der Kritikalität definieren und Bewertungsskala bauen

Schritt 3:
Business Impact Analyse durchführen und Lieferanten auf Skala einstufen

Schritt 4:
Individuelle Sicherheits-anforderungen basierend auf der Einstufung definieren/ableiten

Schritt 5:
Laufendes Monitoring etablieren (risiko-orientiert)

Danke für die Aufmerksamkeit!

Lukas Kulmitzer, MSc.

CISO // eurofunk Kappacher GmbH

CISSP, CCSP, CCSK

eurofunk
creating safety by technology

ALPEN-ADRIA UNIVERSITÄT
KLAGENFURT | WIEN GRAZ