

Wie realisiere ich als Anwender die Informationssicherheit meiner Lieferketten

it.sec



Herausforderungen für Anwender

Bei der **Absicherung der Informationssicherheit in der Supply Chain** sind für Anwender insbesondere folgende **Herausforderungen** zu bewältigen:

- Teil der Supply Chain sind IT-Dienstleister, Hard- und Software-Lieferanten, Managed Service Provider, Entsorger etc., welche wiederum **unterschiedliche Marktmacht** haben
- Schon bei KMU ist mindestens eine **3-stellige Anzahl** relevanter (!) unterstützender Dritte zu betrachten, die realen Einfluss auf die eigene Informationssicherheit haben
- Teilweise sind diese einmalig, aber entscheidend, oder wiederkehrend für einen tätig
- Unterstützende Dritte haben **unterschiedlichen Anteil an Informationssicherheit**:
 - Verarbeitung geschützter Information (→ Zugriff auf Geschäftsgeheimnisse)
 - Lieferung von Kernkomponenten für eigene Verarbeitung bzw. Produktion (→ mittelbare Wirkung auf Output & Leistungsfähigkeit der Organisation)
 - Unterstützung bei Erbringung von Leistungen in der Wertschöpfungskette (→ unmittelbar beteiligt am Output für Kunden)
- Beteiligte unterstützende Dritte betreffen **unterschiedliche Sicherheitsanforderungen**

Lösungsmechanismen (1)

Aufteilen der Supply Chain in disjunkte Blöcke:

- **Kategorisierung** der unterstützenden Dritten mit dem Ziel der Clusterung
 - **Ziel:** möglichst viele unterstützende Dritte mit möglichst einheitlichem Vorgehen adressieren können
 - **Grundlage:** Einheitlicher Schutzbedarf
- **Priorisierung** der unterstützenden Dritten nach Wichtigkeit / Risiko
 - **Ziel:** Wichtigstes zuerst adressieren
 - **Grundlage:** Höchster Schutzbedarf bzw. höchster Impact (inkl. Abhängigkeit!)
- **Handlungsbedarf für Überprüfung** festlegen
 - **Ziel:** möglichst wenig Aufwand für alle Beteiligten verursachen
 - **Grundlage:** getroffene Vereinbarung mit unterstützendem Dritten
 - nur vereinbaren, was ausreichend eindeutig überprüfbar ist
 - Informationspflichten festlegen (Selbstauskunft & Meldepflichten)
 - (Vor-Ort-) Kontrollen fokussiert durchführen, wenn Mehrwert daraus folgt

Lösungsmechanismen (2)

Standardisierung der Supply Chain Absicherung:

- **Zu erfüllende Pflichten zuerst**
 - **Ziel:** Compliance zu Anforderungen aus relevanten Standards (z.B. ISO/IEC 27001 i.V.m. ISO/IEC 27036) bzw. Regulatorien (z.B. KRITIS) mit Exception Handling
 - **Grundlage:** Präzise abgeleitete Anforderungen & sinnvolle Bewertungskriterien
- **Vereinheitlichung des Vorgehensmodells**
 - **Ziel:** möglichst viele identische und bereits durch fachfremde Stellen (z.B. Einkauf) möglichst einfach durchführbare Schritte
 - **Grundlage:** Checklisten in Abhängigkeit zu festgelegten Kriterien & standardisierte Verpflichtungserklärungen für den unterstützenden Dritten
- **Die Kür zuletzt**
 - **Ziel:** Effizienter Einsatz von Ressourcen für Absicherung der Supply Chain
 - **Grundlage:** getroffene Vereinbarung mit unterstützendem Dritten
→ Nur so viel Einzelkontrolle wie absolut nötig; 3rd Party Audits einbeziehen

Herzlichen Dank für Ihre Aufmerksamkeit!

it.sec

Ihre Ansprechperson

it.sec GmbH

Bernhard C. Witt

Head of IT GRC Management

Principal Consultant, eCISO, eISB,
eDSB und/oder Internal Auditor
sowie Prüfer nach § 8a III BSIG

bcwitt@it-sec.de

Tel. +49 (0) 731 205 89 11

www.it-sec.de

