Lieferantenrisikomanagement Blueprint

Lieferantenrisikomanagement-Prozess

- Die Bewertung des Lieferantenrisikos sollte integraler Bestandteil des unternehmensweiten Lieferanten- und Beschaffungsprozesses sein
- Viele Unternehmen haben aber dazu noch kein Konzept bzw. keine Policy
- Die vorliegende Konzeptvorlage soll einen Vorschlag darstellen, auf Basis dessen Unternehmen ihr individuelles Lieferantenrisikomanagement aufbauen können

Klassifikationsschema

Zunächst ist es wichtig, die eigenen Lieferanten zu kategorisieren, denn nicht jeder Lieferant stellt ein gleich großes Risiko für das Unternehmen dar.

Wir empfehlen die Kategorisierung der Lieferanten in zwei Dimensionen:

1. **Kritikalität des Systems/Services** für das Unternehmen
   - ⇨ aus Sicht der Wertschöpfung und Erbringung der Kernservices
   - ⇨ Kritikalität der verarbeiteten Daten
   - ⇨ Berücksichtigung der BIA
   - ⇨ Berücksichtigung industriespezifischer Anforderungen (zb. SRB-Relevanz im Banken-Sektor)
2. **Art des Einsatzes / Integrationsgrad**
   - ⇨ Art und Kritikalität der Schnittstellen (Provider, Internet, etc.)
   - ⇨ Auch „unkritische“ Systeme können zur Angriffsoberfläche beitragen!

Klassifikationsmatrix

	Kritikalität des Systems		
Art des Einsatz / Integrationsgrad	**Kritisch** Kernsysteme/services zur Unterstützung von Kernprozessen oder Kernprodukten des Unternehmens Systeme/Services mit RTO <= 4h Sektor Kritikalität (zB. SRB) sensible personenbezogene Daten	**Wesentlich** Wichtige Supportsysteme/services zur Unterstützung von nicht essenziellen Supportprozessen oder Nicht-Kernprodukten des Unternehmens Systeme/Services mit RTO <= 3d personenbezogene Daten oder unternehmenssensible Daten	**Unwesentlich** Sonstige Supportsysteme/services Systeme/Services mit RTO > 3d keine personenbezogenen Daten oder unternehmenssensible Daten
Hoch Betrieb oder Wartung von HW/SW oder Services mit Schnittstellen des Providers auf Netzwerk- oder Anwendungsebene System/Service aus dem Internet erreichbar	**Tier 1**	**Tier 2**	**Tier 2**
Mittel Bereitstellung von HW/SW oder Services ohne Schnittstellen des Providers auf Netzwerk- oder Anwendungsbene System/Service aus dem Internet erreichbar	**Tier 2**	**Tier 2**	**Tier 3**
Niedrig Bereitstellung von HW/SW oder Services ohne Schnittstellen des Providers auf Netzwerk- oder Anwendungsbene System/Service nicht aus dem Internet erreichbar	**Tier 2**	**Tier 3**	**Tier 4**

Bewertungsprozess

- ⇨ Im Rahmen des Onboarding-Prozesses wird ein Lieferantenrisikoprofil auf Basis der Klassifikationsmatrix errechnet
- ⇨ Dies kann durch Beantwortung definierter Fragen automatisiert erfolgen

Beliebig ergänzbar

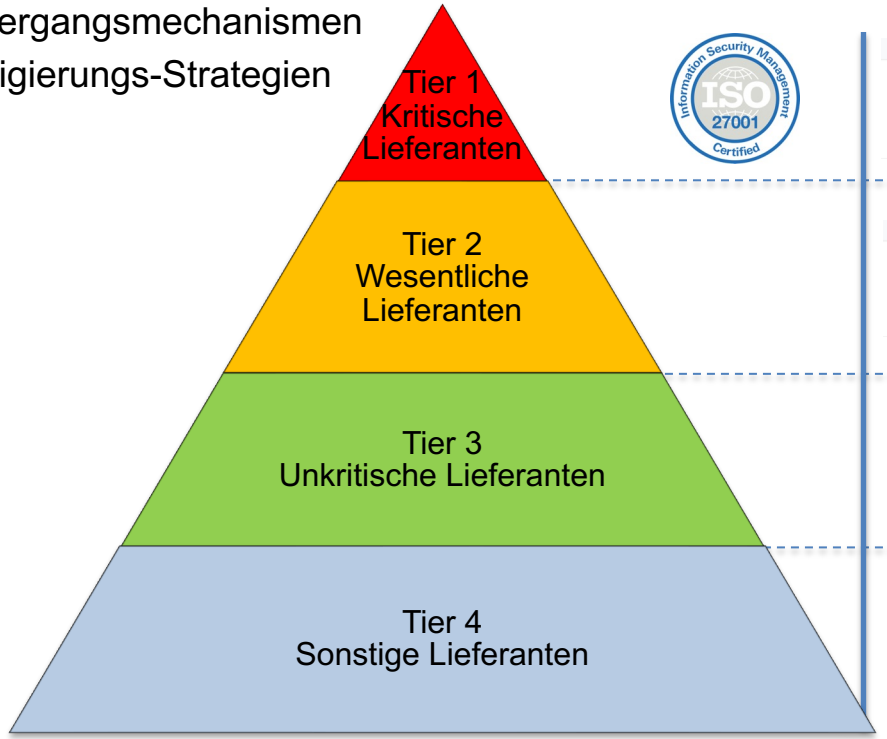
- Kernsystem / wesentliches Supportsystem / sonstiges Supportsystem
- Unterstützung von Kernprodukten/services / sonstige Produkte/Services
- Sektor Kritikalität ja/nein
- RTO <=4h / <= 3d / > 3d
- Sensible PBD / PBD / keine PBD
- Unternehmenssensible Daten / keine unternehmenssensiblen Daten
- Betrieb oder Wartung von HW/SW oder Services / Bereitstellung von HW/SW oder Services
- mit / ohne Schnittstellen des Providers auf Netzwerk- oder Anwendungsebene
- System/Service aus dem Internet erreichbar / nicht erreichbar

Beispiel: Softwarelieferant für Buchhaltungssoftware, der im Rahmen der Wartungsprozesse auch Zugriff auf die Buchhaltungsdaten hat

	Kritikalität des Systems		
Art des Einsatz / Integrationsgrad	**Kritisch**	**Wesentlich**	**Unwesentlich**
Hoch	**Tier 1**	**Tier 2**	**Tier 2**
Mittel	**Tier 2**	**Tier 2**	**Tier 3**
Niedrig	**Tier 2**	**Tier 3**	**Tier 4**

Lieferantenrisikopyramide

- ⇨ Definition von Sicherheitsanforderungen und Kontrollmechanismen auf Basis des Risikolevels
- ⇨ Verpflichtung der Lieferanten auf Basis von SLAs
- ⇨ Übergangsmechanismen
- ⇨ Mitigierungs-Strategien



DAS ÖSTERREICHISCHE CYBERRISK RATING by KSV1870

Exemplarisch

ISO 27001 Information Security Management Certified

A-Rating — A+ Rating mit Audit durch QuaSte — CYBER TRUST AUSTRIA

A-Rating — A Rating besser als 250 — CYBER TRUST AUSTRIA

B-Rating — B Rating besser als 250 — CYBER TRUST AUSTRIA

WebRisk Score — WebRisk Indikator als „Red Flag“