TeleTrusT-Konferenz 2025

Berlin, 02.07.2025

Gemeinsam stark: Kollaborative IT-Sicherheit in Partner- und Lieferantennetzwerken

Tim Koll, LocateRisk

Agenda & Einleitung · Warum sind Sie heute hier?

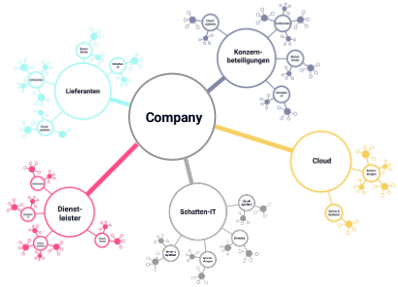
1. Warum kollaborative IT-Sicherheit?
2. Die neue Realität der Lieferketten
3. Typische Risiken und Schwachstellen
4. Der Wandel: Vom Perimeter zum Ökosystem
5. Lösungsansätze: VRM & EASM
6. Auswirkungen der NIS2-Richtlinie
7. Handlungsempfehlungen & Key Takeaways

Die alte Welt vs. Die neue Realität

Gestern: Das "Burg und Graben"-Modell

- Klar definierter Perimeter
- Fokus auf interner Netzwerksicherheit
- Sicherheit als rein internes Thema

Heute: Das vernetzte Ökosystem



- Aufgelöste Perimeter durch Cloud, APIs, IoT und Remote-Arbeit
- Tiefe Integration von hunderten Lieferanten und Partnern
- Ihre Sicherheit ist direkt von der Sicherheit Ihrer Partner abhängig

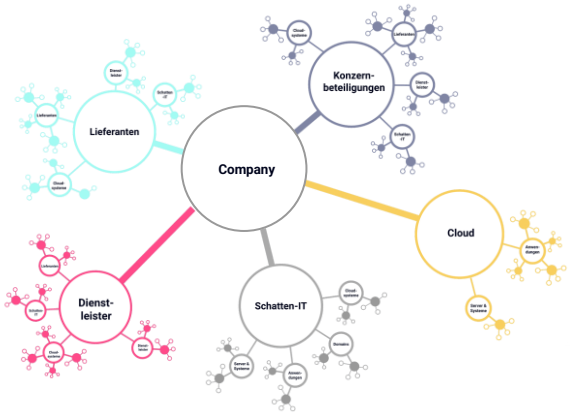
Das Dilemma: Ihre größte Stärke ist Ihre größte Schwachstelle

Effiziente Lieferketten erhöhen die Geschwindigkeit – **aber auch die Angreifbarkeit.**

Praxisbeispiele:

SolarWinds (2020):
Ein kompromittierter Software-Lieferant infizierte tausende hochkarätige Kunden

Log4j (2021):
Eine Schwachstelle in einer weit verbreiteten Open-Source-Komponente legte unzählige Systeme lahm



Die bittere Wahrheit: Angreifer attackieren nicht mehr nur die Festung, sondern die ungesicherten Versorgungsrouten

Das neue Paradigma: Kollaborative Stärke

Ein proaktiver, transparenter und gemeinsamer Ansatz zur Cybersicherheit über Unternehmensgrenzen hinweg

Ziel

- **Geteilter Verantwortung (Shared Responsibility):** Sicherheit ist eine gemeinsame Aufgabe
- **Kontinuierlicher Transparenz:** Einblick in die Sicherheitslage der Partner
- **Gemeinsamen Standards & Prozessen:** Etablierung einer gemeinsamen Sicherheitsbasis

Vendor Risk Management (VRM) · Traditionell vs. 2.0

Traditionelles VRM

- Excel-basierte Fragebögen
- Jährliche, zeitpunktbezogene Audits
- Oft nur ein "Papier-Tiger" ohne echte Aussagekraft

VRM 2.0

- Automatisierte Plattformen für Onboarding und Bewertung
- **Kontinuierliches Monitoring** von Risikosignalen
- Integration in Ihre eigenen Sicherheitsprozesse
- Fokus auf Risikobehandlung, nicht nur auf Risikofeststellung

Das neue Paradigma: Kollaborative Stärke

Ein proaktiver, transparenter und gemeinsamer Ansatz zur Cybersicherheit über Unternehmensgrenzen hinweg

Wichtig

- EASM beschränkt sich nicht auf Ihre eigene Infrastruktur
- EASM-Tool identifiziert auch exponierte Cloud-Speicher, unsichere APIs und unbeabsichtigt zugängliche Ressourcen Ihrer Lieferanten
- **EASM schließt die Lücke, die Fragebögen hinterlassen**

Der Game-Changer · Die NIS2-Richtlinie

Was ist NIS2?
Die neue EU-Richtlinie zur Netzwerk- und Informationssicherheit.

Ziel

- Anhebung und Harmonisierung des Cybersicherheitsniveaus in der EU

Wen betrifft es?

- Deutlich erweiterter Anwendungsbereich

Kernbotschaft

- NIS2 macht Cybersicherheit zur Chefsache und
- Verhängt bei Verstößen empfindliche Strafen

NIS2 & die Lieferkette: Aus Empfehlung wird Pflicht

Artikel 21:
NIS2 verpflichtet Unternehmen explizit, die Sicherheit ihrer Lieferketten zu managen

Anforderung 1

- Unternehmen müssen die **spezifischen Cyber-Risiken** bewerten, die von jedem direkten Lieferanten oder Dienstleister ausgehen.

Anforderung 2

- Die **Qualität und Widerstandsfähigkeit** der Produkte und Dienstleistungen der Lieferanten muss bewertet werden.

Anforderung 3

- Es müssen angemessene **Sicherheitsmaßnahmen** zur Steuerung dieser Risiken umgesetzt werden.

NIS2 in der Praxis: Was heißt das konkret?

VRM wird zur Pflicht

- Sie benötigen einen nachweisbaren, systematischen Prozess zur Risikobewertung Ihrer Lieferanten. Einmalige Fragebögen reichen nicht mehr aus.
- Die Ergebnisse müssen dokumentiert und in Ihre Risiko-Management-Entscheidungen einfließen.

EASM wird zur Notwendigkeit

- Um die Risiken der Lieferkette zu bewerten (wie von NIS2 gefordert), müssen Sie deren externe Angriffsfläche kennen.
- EASM liefert die objektiven, technischen Daten, die ein modernes VRM benötigt, um über die reine Compliance hinauszugehen.

Synergie: VRM + EASM = echte Kollaborative Stärke

Vendor Risk Management (VRM)

… definiert den **organisatorischen Rahmen**: "Welche Sicherheitsanforderungen stellen wir an unsere Partner?"

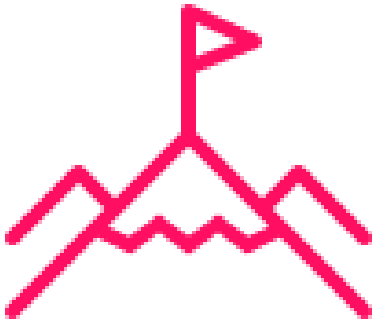
External Attack Surface Management (EASM)

… liefert die **technische Validierung**: "Halten unsere Partner diese Anforderungen in der Praxis ein?"

- **Risikobasierte Steuerung** der Lieferanten
- **Nachweis** der Sorgfaltspflicht gemäß NIS2
- Echte **Reduzierung der Angriffsfläche** des gesamten Ökosystems.

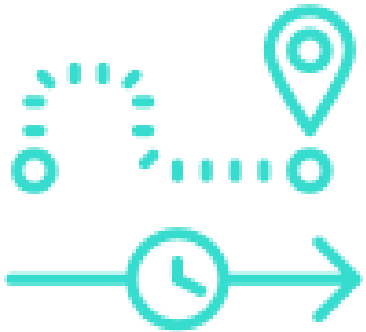
Kritische Betrachtung · Herausforderungen in der Praxis

1. Vertrauen vs. Kontrolle
2. Machtgefälle
3. Standardisierung
4. Kosten & Ressourcen



Erste Schritte zur Umsetzung · Wo fangen Sie an?

1. Transparenz schaffen (intern)
2. Standards definieren
3. Prozesse etablieren
4. Technologie nutzen
5. Verträge anpassen



Fazit & Key Takeaways

Ihre wahre Angriffsfläche ist das gesamte Ökosystem.

- Kollaborative Stärke durch Transparenz und geteilte Verantwortung der zukunftsfähige Weg.
- NIS2 macht das Management von Lieferkettenrisiken nicht nur empfehlenswert, sondern gesetzlich verpflichtend
- Die Kombination von VRM und EASM kann diese Herausforderung strategisch und technisch meistern.

Wie ist Ihr Sicherheitsstatus?

Gewinnen Sie einen Einblick
anhand Ihrer echten Daten!

tim.koll@LocateRisk.com