- Sind Sie über die Cyber-Security Ihrer Lieferanten und Sublieferanten informiert?
- Managen Sie diese aktiv?
- Sind Sie auf den Fall vorbereitet, dass eines Ihrer Lieferanten gehackt wird?
- Wissen Sie, was dann zu tun ist?

Risikofaktor Supply Chain

Der kompetente Umgang mit Supply-Chain-Risiken ist in unserer globalisierten Welt (Produktion auf Abruf, steigende Abhängigkeit von langen, komplexen Lieferketten) von enormer Wichtigkeit, um potenzielle Schäden minimieren zu können. SBA Research adressiert essenzielle Fragenstellungen in diesem Bereich, um die Resilienz Ihres Unternehmens zu kräftigen.

> Ein Cyber-Angriff auf den weltweit größten Aluminiumhersteller Norsk Hydro führt 2019 zu massiven Problemen in dessen Supply Chain und verursacht Schäden in Millionenhöhe. Die „NotPetya"-Attacke spielt 2017 ein bösartiges Update in eine ukrainische Steuerverwaltungssoftware ein, weltweit sind tausende Unternehmen betroffen (z. B. Maersk, der Logistikdienstleister TNT und der Ölproduzent Rosneft); im selben Jahr wird die „Cloud Hopper"-Kampagne bekannt, bei der staatliche Angreifende große Dienstleistungsunternehmen wie IBM und Hewlett Packard kompromittierten, um so deren KundInnen angreifen zu können.

Digitale und Cyber-Risiken werden mittlerweile als Top-Risiken für Unternehmen betrachtet[1]; aktuelle Entwicklungen wie Industrie 4.0, Digitalisierung oder Internet of Things werden diesen Trend weiter verstärken. Weltweit gibt es vermehrt Hacking-Angriffe auf Unternehmen und Unternehmen in deren Supply Chain, bei denen entweder sensible Daten von KundInnen gestohlen oder die Produktionsabläufe beeinträchtigt werden – in manchen Fällen bis hin zum Produktionsstopp.

Oft fühlt sich bei solchen „abteilungsübergreifenden" Herausforderungen jedoch niemand explizit zuständig, bzw. wird die alleinige Verantwortung bei der IT gesehen.

Unser Angebot

Genau hier setzt SBA Research an: Digitale und Cyber-Risiken werden unternehmensweit betrachtet, Supply-Chain-Risiken rücken in den Fokus.

- Begleitung bei der Einführung eines strukturierten Supply-Risk-Managements mit Fokus auf Cyber-Security
- Gap-Analyse: Abdeckung essenzieller Supply-Chain-Sicherheitsaspekte im Unternehmen
- Ableitung konkreter Maßnahmen für die Supply Chain Ihres Unternehmens
- Fragebogen zum „initialen Assessment" von Lieferanten (Auswahlprozess bzw. vor Vertragsabschluss)
- Business-Impact-Analyse zur Identifikation kritischer Lieferanten
- Entwicklung eines Audit-Konzeptes für Lieferanten/Dienstleistungsunternehmen (z. B. für die interne Revision)
- Durchführung von Lieferantenaudits

[1] Allianz Risk Barometer 2018

Anhand grundlegender Fragestellungen lässt sich sowohl der IST- wie auch SOLL-Zustand in Ihrem Unternehmen erheben, um davon abgeleitet ein individuelles Konzept zu erstellen.

Governance und Sichtbarkeit

- Ist eine Methodologie für Supply-Chain-Risk-Management mit Fokus auf Cyber-Security etabliert?
- Gibt es Transparenz bzw. Kennzahlen, um das Sicherheitsniveau zu bewerten und zu steuern?
- Gibt es eine Person, die bei Ihnen im Unternehmen für dieses Thema verantwortlich ist?
- Haben Sie Alternativen für kritische Lieferanten vorgesehen bzw. gibt es Pläne für deren Ausfall?
- Wird die Supply Chain im Rahmen eines etablierten Threat-Intelligence-Monitoring auf relevante Ereignisse von Liefer- oder Dienstleistungsunternehmen überwacht (z. B. Sicherheitsvorfälle, Unternehmens-übernahmen)?

Sicherheit bei Partner- und Dienstleistungsunternehmen

- Wissen Sie über das Sicherheitsniveau Ihrer Partner- und Dienstleistungsunternehmen Bescheid?
- Wer sind die „kritischen" Lieferanten im Hinblick auf Cyber-Security, und wie identifizieren Sie diese?
- Werden Sicherheitsanforderungen in Liefer- und Dienstleistungsverträgen berücksichtigt?
- Fordern Sie Zertifizierungen und/oder führen Sie Lieferantenaudits durch?
- Wie bewerten, entwickeln und auditieren Sie Lieferanten im Hinblick auf Cyber-Security?
- Wird im Rahmen von Akquisitionen bzw. strategischen Partnerschaften eine klassischer Due-Diligence-Prüfung um das Thema Cyber-Security erweitert?
- Ein Unternehmen in der Supply-Chain wurde gehackt – wie können Sie die Situation erfolgreich managen und auf welche Aspekte kommt es dabei an?

Schutz von Daten und IP

- Werden vertrauliche Informationen in der Supply Chain weitergegeben?
- Ab wann kann nicht mehr sichergestellt werden, dass vertrauliche Informationen unter Kontrolle sind?
- Sind die potenziellen Auswirkungen (auf Produktion, Geschäftsabläufe etc.) bei Verletzungen der Vertraulichkeit, Integrität und/oder Verfügbarkeit dieser vertraulichen Informationen bekannt?

Ihr Partner

SBA Research ist ein COMET-Exzellenzzentrum für Informationssicherheit mit Standort Wien. In Zusammenarbeit mit TU Wien, Universität Wien, WU Wien, TU Graz, AIT und FH St. Pölten sowie internationalen Institutionen betreiben wir Spitzenforschung auf internationalem Niveau. Zusätzlich etablierten wir einen Dienstleistungsbereich, der seit Jahren als verlässlicher Partner von Ministerien, Behörden, Großunternehmen und KMUs geschätzt wird. Dieser duale Ansatz der wissenschaftlichen Forschung und der praxisorientierten Umsetzung ermöglicht ein einzigartiges Leistungsangebot, das von Forschungskooperationen bis zu Penetrationstests reicht und Sicherheitsaspekte zukünftiger Schlüsselbereiche wie AI, IoT/Industrie 4.0, sichere Softwareentwicklung und Sicherheit in der Digitalisierung abdeckt. Ergänzt wird dies durch ein umfassendes Schulungsangebot.

SBA legt Wert darauf, Brücken von hochwertiger Forschung zu praktisch nutzbaren Ergebnissen zu schlagen und versteht sich – dank des umfassenden nationalen und internationalen Netzwerks – als Bindeglied zwischen Wissenschaft und Industrie.

Kontakt

Stefan Jakoubi
Geschäftsleiter Professional Services
sjakoubi@sba-research.org

Yvonne Poul
Geschäftsleiterin Strategic Innovation & Communication
ypoul@sba-research.org