



LOGISTIKUM
CHALLENGE ACCEPTED

Cyber Security aus der Supply Chain Perspektive

LSZ Kongress, Security & Risk Management
22.03.2023 – Loipersdorf
FH-Assistenz-Professor & Research Project Manager
Mag. Michael Herburger, BA MA PhD

Vorstellung



LOGISTIKUM
CHALLENGE ACCEPTED

Mag. Michael Herburger, BA MA PhD

- FH-Assistenz-Professor & Research Project Manager, Lektor (FH OÖ, Logistikum Steyr)
- Leiter Research Field „Supply Chain Risk Management, Resilience & Security“
- Seit 2016 Fokus auf Cyber Risiken in der Supply Chain
- Zahlreiche nationale und internationale Projekte mit IT-Security-ExpertInnen
- „All hazards-approach“ in diversen Projekten
- Mitglied in div. Gremien/Arbeitsgruppen
Plattform I4.0, Cyber Security Plattform (CSP), ISO/EN, ISCRiM
Associate von H2020-Projekten im Bereich Cyber Security (ECHO, CS4E)



PURCHASE

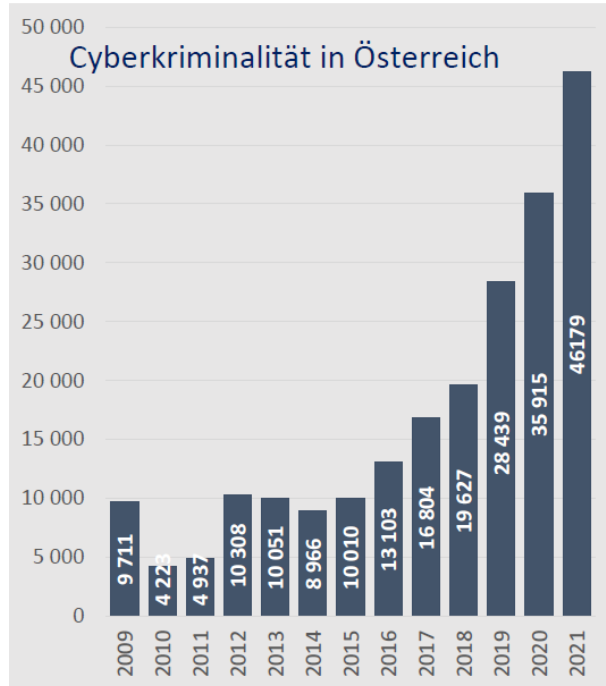


Supply Chain



CYBER SECURITY

Anstieg Cyber-Kriminalität



Quelle: Bundesministerium für Inneres (2022)

“80% der KMU von Cybercrime betroffen”

[APA-OTS, 2022]

“57% der KMU würden im Falle eines Sicherheitsvorfalles in Konkurs gehen”

[EU Agency for Cybersecurity (ENISA), 2021]

“90% sehen KMU als das schwächste Glied in der Lieferkette an - 40% der Befragten wurden durch einen Vorfall im Bereich der Cybersicherheit in der Lieferkette negativ beeinflusst”

[World Economic Forum, 2022]

“Unternehmen benötigen im Durchschnitt 280 Tage, um einen Cyberangriff zu erkennen und darauf zu reagieren”

[World Economic Forum, 2022]

Cyber Risiko – ein Vergleich



LOGISTIKUM
CHALLENGE ACCEPTED



Nr 1 der Unternehmensrisiken



LOGISTIKUM
CHALLENGE ACCEPTED

The most important global business risks for 2022



1
↑ 44%
2021: 3 (40%)

Cyber incidents
(e.g. cyber crime, IT failure/ outage, data breaches, fines and penalties)



2
↓ 42%
2021: 1 (41%)

Business interruption
(incl. supply chain disruption)



3
↑ 25%
2021: 4 (27%)

Natural catastrophes
(e.g. storm, flood, earthquake, wildfire, weather events)

Key

- ↑ Risk higher than in 2021
- ↓ Risk lower than in 2021
- No change from 2021

(5%) 2021 risk ranking %

Figures represent the number of risks selected as a percentage of all survey responses from 2,650 respondents. All respondents could select up to three risks per industry, which is why the figures do not add up to 100%.

Watch our short film about the top 10 risks for 2022

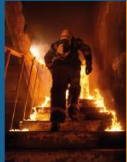
View the full Allianz Risk Barometer 2022 rankings here

ALLIANZ RISK BAROMETER 2022



4
↓ 22%
2021: 2 (40%)

Pandemic outbreak
(e.g. health and workforce issues, restrictions on movement)



7
→ 17%
2021: 7 (14%)

Fire, explosion



8
↓ 15%
2021: 4 (19%)

Market developments
(e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)



9
↑ 13%
2021: 13 (18%)

Shortage of skilled workforce



10
↓ 11%
2021: 8 (13%)

Macroeconomic developments
(e.g. monetary policies, austerity programs, commodity price increase, deflation, inflation)



6
↑ 17%
2021: 9 (13%)

Climate change¹
(e.g. physical, operational, financial and reputational risks as a result of global warming)

5
→ 19%
2021: 5 (19%)

Changes in legislation and regulation
(e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)



2017

Møller-Mærsk

Hackerangriff kostet Reederei Hunderte Millionen

Mit Erpressersoftware haben Angreifer die größte Container-Reederei der Welt zeitweise lahmgelegt. Die Unternehmensgruppe A.P. Møller-Mærsk schätzt den Schaden auf bis zu 300 Millionen Dollar.



2022

Cyber Threats Cyber Attack

Cyber Attack hits Maersk Group again

Maersk has made it official that its business subsidiary operating in Australia was hit by a second cyber attack early this month. Security analysts at Svitzer Australia have discovered that the email system of the company was under the control of hackers from past 10 months before the hack was discovered on March 1st this year.

STATE OF FREIGHT

Hackers can bring ships and planes to a grinding halt. And it could become much more common

PUBLISHED MON, JUN 27 2022-2:14 AM EDT | UPDATED MON, JUN 27 2022-2:14 AM EDT

Relevanz Supply Chain



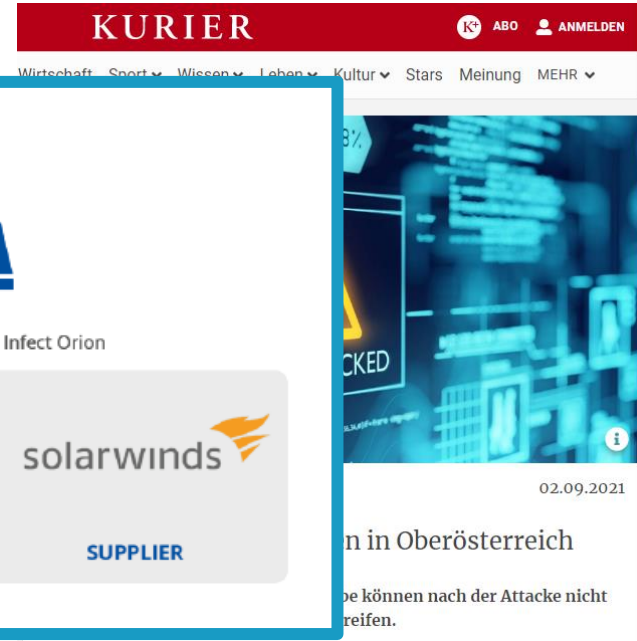
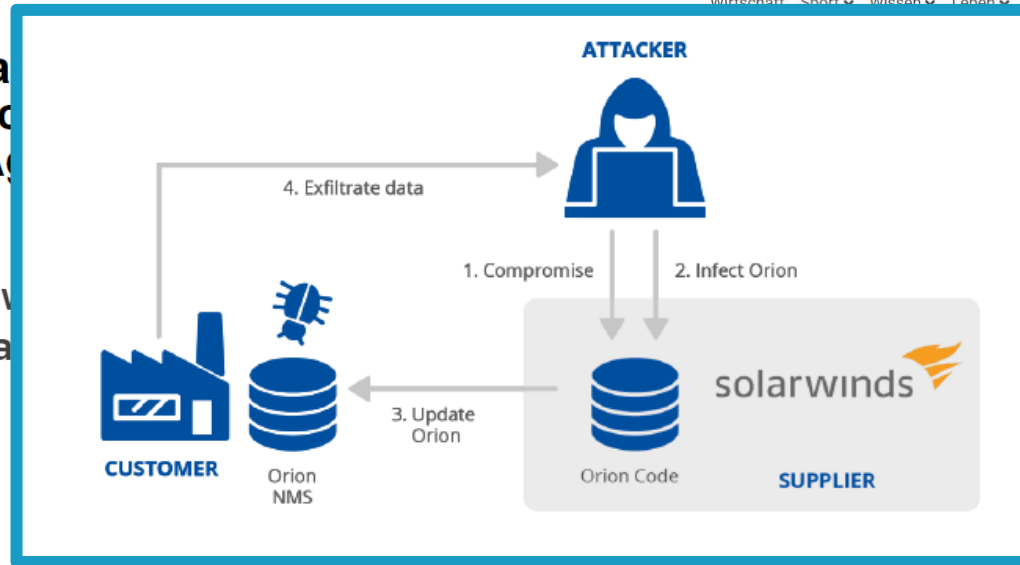
LOGISTIKUM
CHALLENGE ACCEPTED

Angreifer nutzen Schwachstellen in Lieferketten für deren Angriffe

U.S.

SolarWinds Sa
Customers, Inc
Government A

SolarWinds hack v
sophisticated atta



Cyber Security Awareness Supply Chain



LOGISTIKUM
CHALLENGE ACCEPTED

1. Niedrige Awareness

- Keine Erfahrung mit Cyber-Vorfall
- Awareness aus Medien, etc.

2. Höchste eigene Awareness

- Cyber-Vorfall selbst erlitten
- Impact auf Supply Chain - Verfügbarkeit

3. Höchste Awareness Richtung Supply Chain

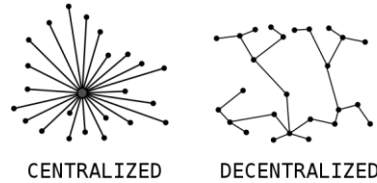
- Supply Chain Cyber-Vorfall erlitten
- Impact auf Supply Chain – Verfügbarkeit, Integrität und Vertraulichkeit



Supply Chain Cyber Security/Resilienz



LOGISTIKUM
CHALLENGE ACCEPTED



Forschungsprojekte und deren Outputs

SSCCS (Secure Supply Chains for Critical Systems) mit FH St. Pölten (IT Sicherheitsforschung), 07/21 – 06/25

- Vorgehensmodell Analyse Cyber Risiken in der Supply Chain
- Supply Chain Cyber Risk Canvas & Cards auf Basis „Business Model Canvas“
- 2 Teaching Cases zu „Supply Chain Cyber Security“ und „Supply Chain Incident Response“

CySeReS-KMU mit Uni Innsbruck, Uni Passau, TH Deggendorf, FH Salzburg, 01/23 – 12/25

- Cyber Security und Resilienz in Supply Chains mit Fokus auf KMUs

InduSec – IT/OT-Security-Schulungen mit SBA research, FH St. Pölten

DeNaLog – Schulungen zu Supply Chain Risikomanagement, Resilienz und Cyber Security

Sucredi – Supply Chain Cyber Resilience – Reifegradmodell (www.logistikum.at/sccr), mit 4 Konzernen in OÖ

- Projekte zu NIS2 in Österreich und Dänemark
- Projekte zu Supply Chain Resilienz/“all hazards-approach“ mit AIT (ReaGtSion) und Complexity Science Hub (SYRI)
- Teil von ASCII (Supply Chain Intelligence Institute Austria) mit Complexity Science Hub und WIFO

**Suche nach interessierten Unternehmen für weitere Projekte zu
Cyber Risiken in der Supply Chain (zahlreiche Kooperationsmöglichkeiten)**



LOGISTIKUM
CHALLENGE ACCEPTED

Logistikum Steyr

Mag. Michael Herburger, BA MA PhD

FH-Assistenz-Professor & Research Project Manager

Head of research field "Supply Chain Risk Management,
Resilience & Security"

tel: +43 5 0804 33255

mobile: +43 676 44 55 860

e-mail: michael.herburger@fh-steyr.at

Logistikum – Department of Logistics at the
University of Applied Sciences Upper Austria
FH OÖ Forschungs & Entwicklungs GmbH
Wehrgrabengasse 1-3 , 4400 Steyr

web:

www.logistikum.at

www.fh-ooe.at