MUG Science Day

Die größten Risiken unserer Zeit

Cyberrisiken

23. April 2022

Martin Kreuzer, Senior Risk Manager Cyber Risks

Munich RE

Image: [M] Munich Re / [P] Westend61 / Getty Images

Agenda

Munich RE

1
Die heutige Ausgangslage

2
Ransomware bleibt die Bedrohung Nummer 1

3
Angriffe auf Lieferketten werden zunehmen

4
“Internet of Things” als große Heraus-forderung

5
Alle geostrategischen Konflikte werden “digitalisiert”

6
Was können wir tun?

Die Risk Management Perspektive

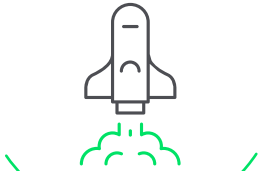
Image: [M] Munich Re / [P] Westend61 / Getty Images

Die heutige Ausgangslage

Munich RE

1 Billion
vernetzter Sensoren
(CISCO)

$6 Billion
Geschätzte globale Schäden durch Cyberkriminalität
(Cybersecurity Ventures)



5,3 Milliarden
Internetnutzer weltweit

16,4 Milliarden
vernetzter IoT Geräte (Statista)

19.170
Tage

Ransomware bleibt die Bedrohung Nummer 1

Munich RE

“The ransomware surge ruining lives”

BBC News
Apr. 30th 2021

Ransomware as a Service wird immer professioneller und arbeitsteiliger

Besonders kritisch: Angriffe auf Operational Technology (OT) und kritische Infrastrukturen

Multiple Erpressung wird zum neuen “Ransomware-Standard”

Nur **1%** der weltweiten Nationalstaaten hatten 2021 Gesetze zur Regulierung von Lösegeldzahlungen erlassen. Dieser Wert wird bis Ende 2025 auf ca. **30%** steigen (Gartner)

Ransomware bleibt die Bedrohung Nummer 1

Von 1.086 Organisationen, deren Daten verschlüsselt wurden, erhielten **96%** ihre Daten zurück.

(Sophos-survey: “The State of Ransomware 2021”)

Gesamtkosten zur Behebung eines Ransomware-Angriffs betrugen im Jahr 2021 **1,85 Mio. USD** (Vorjahr: 761.106 US-Dollar)

(ENISA Threat Landscape 2021)

Die durchschnittliche Lösegeldzahlung lag 2021 auf einem Rekordwert von **570.000 USD**

(Palo Alto Unit 42 Ransomware Threat Report, H1 2021)

„Es ist wahrscheinlich, dass wir 2022 die Obergrenze einer Lösegeldforderung von **100 Mio. USD** erreichen werden.“

(ENISA)

Angriffe auf Lieferketten nehmen weiter zu

Munich RE

> Ransomware is the why (money), and supply chain is the how (through third-party software)

Splunk
(2022 Prediction)

- Große Supply-Chain-Hacks wie bei SolarWinds werden an Häufigkeit zunehmen
- Open-Source-Software und Cloud-Dienstleister geraten zunehmend ins Visier
- Branchen, die viele unterschiedliche Hard- und Softwarekomponenten verwenden, sind bevorzugte Ziele - z.B. Gesundheitswesen, Energiesektor
- Bis 2025 werden **60%** der Unternehmen das Thema Cybersicherheit als Voraussetzung für geschäftliche Engagements verwenden (Gartner)
- Digitale Abhängigkeiten nehmen stark zu – z. B.: Marktanteil von Windows bei ca. **76%** (Statcounter, Stand Januar 2022)

“Internet of Things” als große Herausforderung

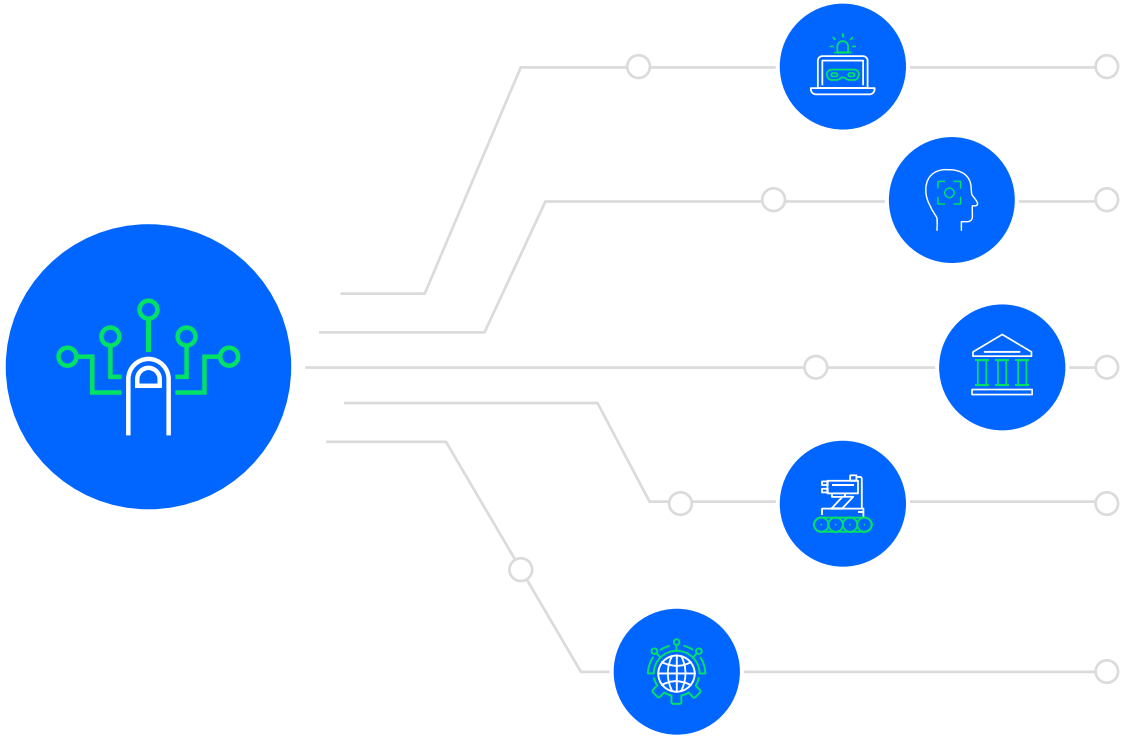
Munich RE

“By 2025, threat actors will have weaponized operational technology environments successfully enough to cause human casualties”

Gartner

- Risiko für Betriebsunterbrechungen und physische Schäden steigt
- Konvergenz von IT und OT sowie Schwachstellen müssen besser adressiert werden
- Bis 2025 wird es mehr als **30 Milliarden** IoT-Verbindungen geben plus Billionen von Sensoren, die sich mit diesen Geräten verbinden. (iot-analytics.com). Zwei Beispiele:
  - Der Wert von Smart Car-Informationen wird 2030 voraussichtlich bei **450** bis **750 Milliarden** US-Dollar liegen. Bis 2025 sollen monatlich **10 Exabyte** an Daten von vernetzten Autos stammen (Forbes)
  - Mangelnde Sicherheit von IoT-Geräten im Gesundheitswesen: **53%** der vernetzten medizinischen und anderer IoT-Geräte in Krankenhäusern weisen eine bekannte kritische Schwachstelle auf (Cynerio)

Alle geostrategischen Konflikte werden “digitalisiert”



Zunehmende Vermischung von Cyberkriminalität und nationalstaatlichen Aktivitäten

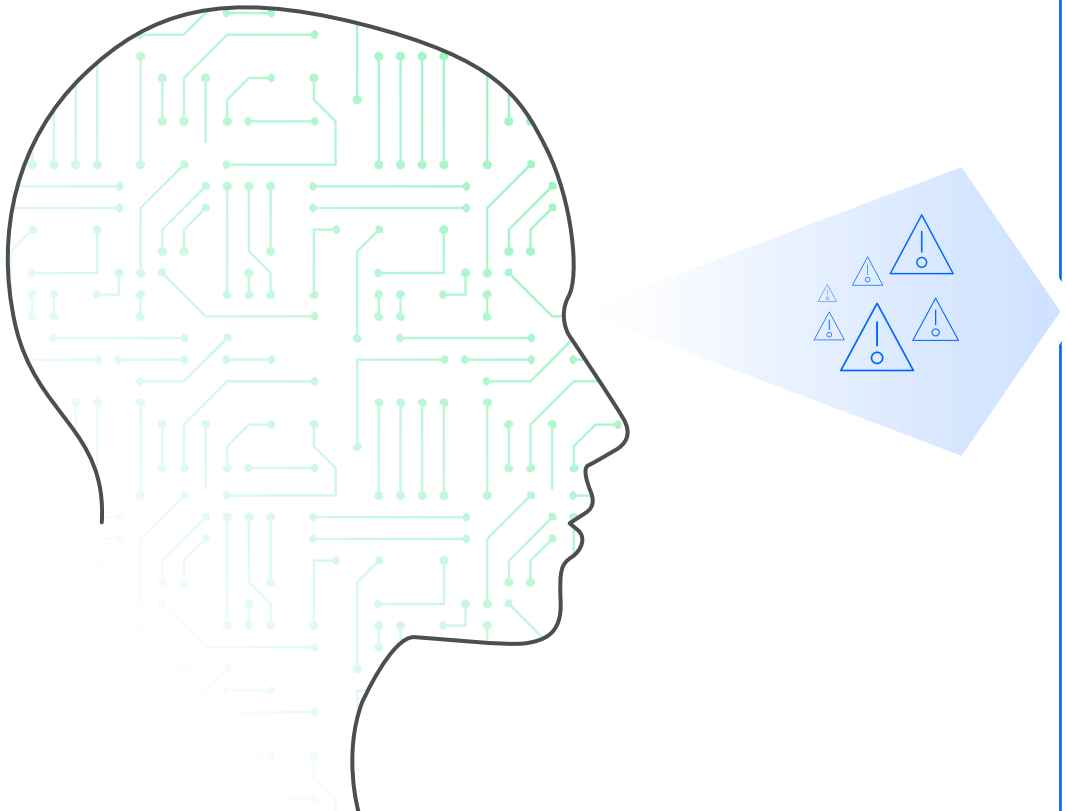
Schwerpunkte: Geopolitische Spannungen, Kriege, Pandemie, US-Midterms, Kryptowährungen, geistiges Eigentum, kritische Infrastrukturen…

Politische Systeme und Gesellschaften werden digitalisiert, wenn Staaten, Konflike und Kriege, Medien, Währungen, Identitäten usw. online gehen

Cyber als Teil der militärischen „Showrooms“

Satelliten und Weltrauminfrastruktur werden zum Ziel von Cyberangriffen.
Ein „Hack in Space“ ist keine Utopie

Was können wir tun?
Die Risk Management Perspektive



Auswirkungen der Pandemie bleiben bestehen:
95,3 % der Unternehmen sagen, dass sie seit Beginn der Pandemie stärker auf Technologie angewiesen sind.
(NTT 2021 Global Workplace Report)

Ein Trend ist die zunehmende Cybersicherheitslücke zwischen großen Unternehmen und KMU.
(Munich Re Global Cyber Risk and Insurance Survey 2022)

Erhöhte regulatorische Anforderungen.

Cloudumgebungen und KI werden zum Treiber von Cybersicherheit.

Weltweiter Fachkräftemangel: Ca. **3 Mio.** Cybersicherheits-Experten fehlen (WEC).

Versicherung als wesentlicher Teil der Lösung!

Ein letztes Statement

Munich RE

“

In 2022, the transition from an internet that is a reflection of the world, to a world that is a reflection of the internet, will radically accelerate.

Christopher Ahlberg
CEO at Recorded Future

Image: [M] Munich Re / [P] Westend61 / Getty Images

Vielen Dank für Ihre Aufmerksamkeit!

Martin Kreuzer
mkreuzer@munichre.com

Munich RE

Image: [M] Munich Re / [P] Westend61 / Getty Images