Universität der Bundeswehr München
Institut für Schutz und Zuverlässigkeit

LIONS

gefördert durch
dtec.bw

Innentäter – Risiko für die Supply Chain – Digitale Souveränität und Digitale Verantwortung

Ulrike Lechner und Manfred Hofmeier

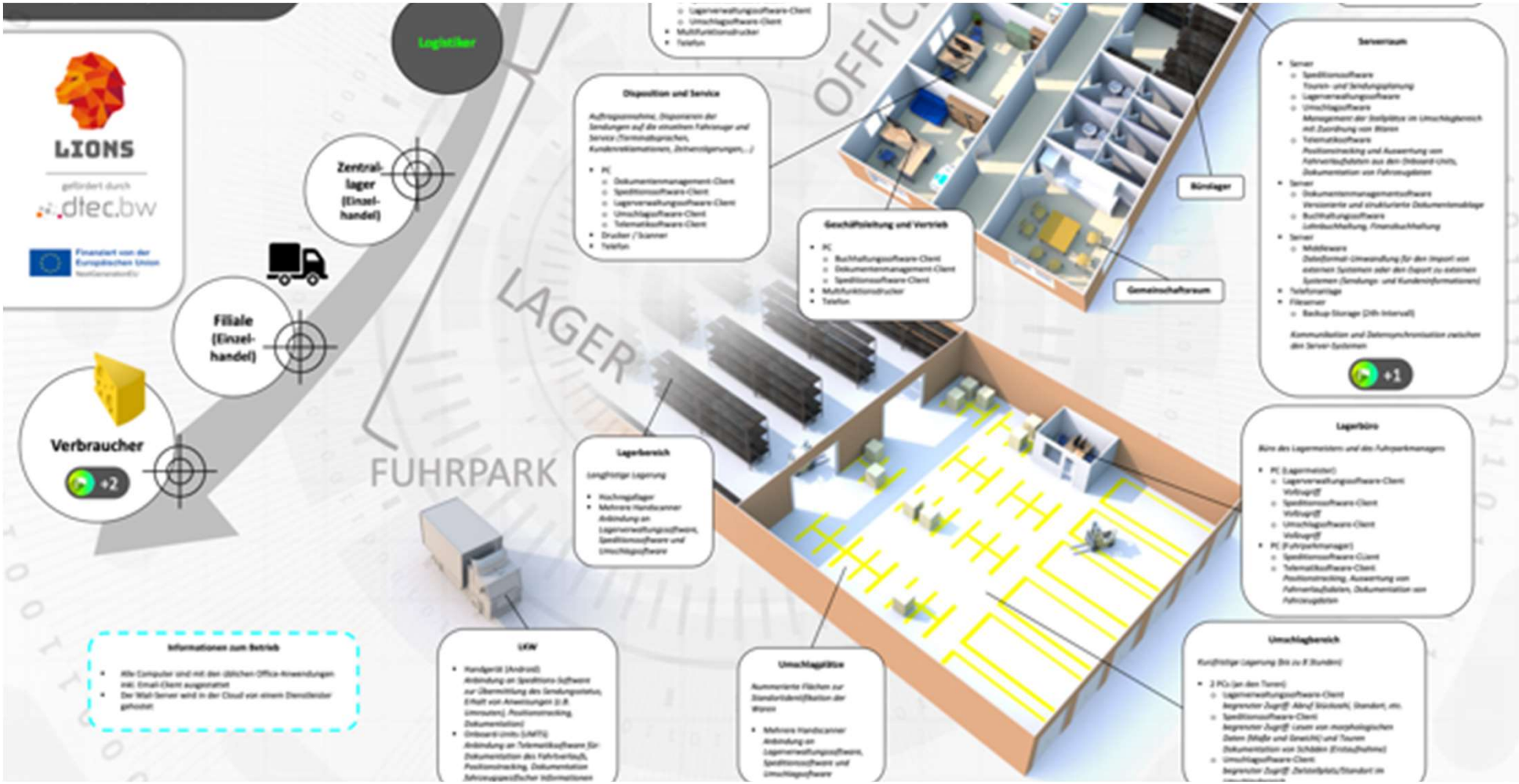
IKT-Sicherheitskonferenz 2023, Linz

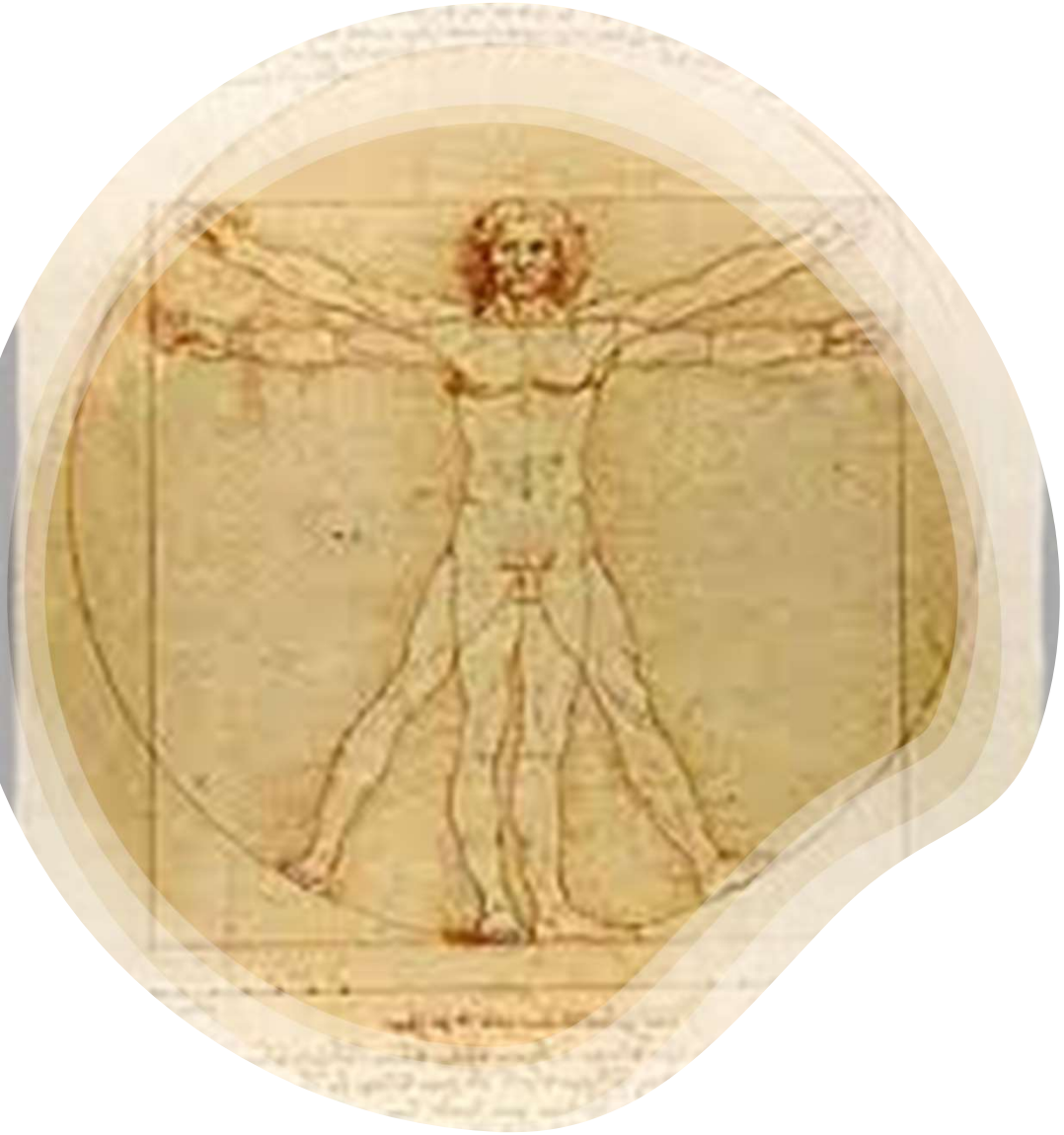
Finanziert von der Europäischen Union
NextGenerationEU

Unser Thema: Die Supply Chain, ihre Risiken und der Weg zu Digitaler Souveränität und Digitaler Verantwortung

Sicherheit – Die Burg

(Quelle: Martin Falbisoner, Digital Commons)


LIONS
gefördert durch
dtec.bw
Finanziert von der Europäischen Union
Logistiker
Zentral-lager (Einzel-handel)
Filiale (Einzel-handel)
Verbraucher
+2
LAGER
FUHRPARK
OFFICE
Disposition und Service
Aufträgsannahme, Disponieren der Sendungen auf die einzelnen Fahrzeuge und Service (Terminabsprachen, Kundenreklamationen, Zeitverzögerungen, ...)
PC
Dokumentenmanagement-Client
Speditionssoftware-Client
Lagerverwaltungssoftware-Client
Umschlagsoftware-Client
Telematiksoftware-Client
Drucker / Scanner
Telefon
Geschäftsleitung und Vertrieb
PC
Buchhaltungssoftware-Client
Dokumentenmanagement-Client
Speditionssoftware-Client
Multifunktionsdrucker
Telefon
Serverraum
Server
Speditionssoftware
Touren- und Sendungsplanung
Lagerverwaltungssoftware
Umschlagsoftware
Management der Stellplätze im Umschlagbereich mit Zuordnung von Waren
Telematiksoftware
Positionstracking und Auswertung von Fahrzeugdaten aus den Onboard-Units, Dokumentation von Fahrzeugdaten
Server
Dokumentenmanagementsoftware
Versionierte und strukturierte Dokumentenablage
Buchhaltungssoftware
Lohnbuchhaltung, Finanzbuchhaltung
Server
Middleware
Datenformat-Umwandlung für den Import von externen Systemen oder den Export zu externen Systemen (Sendungs- und Kundeninformationen)
Telefonanlage
Fileserver
Backup-Storage (24h Intervall)
Kommunikation und Datensynchronisation zwischen den Server-Systemen
+1
Büroläger
Gemeinschaftsraum
Lagerbereich
Langfristige Lagerung
Hochregallager
Mehrere Handscanner Anbindung an Lagerverwaltungssoftware, Speditionssoftware und Umschlagsoftware
Lagerbüro
Büro des Lagermeisters und des Fuhrparkmanagers
PC (Lagermeister)
Lagerverwaltungssoftware-Client
Vollzugriff
Speditionssoftware-Client
Vollzugriff
Umschlagsoftware-Client
Vollzugriff
PC (Fuhrparkmanager)
Speditionssoftware-Client
Telematiksoftware-Client
Positionstracking, Auswertung von Fahrzeugdaten, Dokumentation von Fahrzeugdaten
Informationen zum Betrieb
Alle Computer sind mit den üblichen Office-Anwendungen inkl. Email-Client ausgestattet
Der Mail-Server wird in der Cloud von einem Dienstleister gehostet
LKW
Handgerät (Android)
Anbindung an Speditions-Software zur Übermittlung des Sendungsstatus, Erhalt von Anweisungen (z.B. Umrouten), Positionstracking, Dokumentation)
Onboard-Units (LMTS)
Anbindung an Telematiksoftware für Dokumentation des Fahrtverlaufs, Positionstracking, Dokumentation fahrzeugspezifischer Informationen
Umschlagfläche
Nummerierte Flächen zur Standortidentifikation der Waren
Mehrere Handscanner Anbindung an Lagerverwaltungssoftware, Speditionssoftware und Umschlagsoftware
Umschlagbereich
Kurzfristige Lagerung (bis zu X Stunden)
2 PCs (an den Toren)
Lagerverwaltungssoftware-Client
Begrenzter Zugriff: Abruf Stückzahl, Standort, etc.
Speditionssoftware-Client
Begrenzter Zugriff: Lesen von morphologischen Daten (Maße und Gewicht) und Touren
Dokumentation von Schäden (Fotoaufnahme)
Umschlagsoftware-Client
Begrenzter Zugriff: Zielstellplatz/Standort im



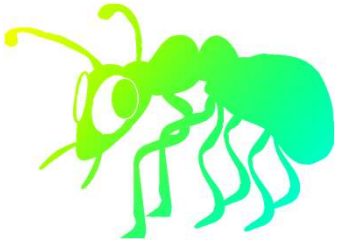
- Der Verantwortungsraum wird grösser und volatiler
- Digitale Souveränität: Handlungsoptionen angesichts von Ereignissen und Entwicklungen - - Digitale Verantwortung
- Informationssicherheitsmaßnahmen für Empowerment und Awareness
- Der Mensch im Zentrum

- Intentionale Sicherheitsvorfälle durch Innentäter und Innentäterinnen
- Wenig zugängliche Fälle

➢ Entwicklung eines Serious Games als

1) Erhebungsinstrument für Bedrohungsszenarien

2) Informationssicherheits-Maßnahme: Awareness & Empowerment



Operation Digitale Ameise

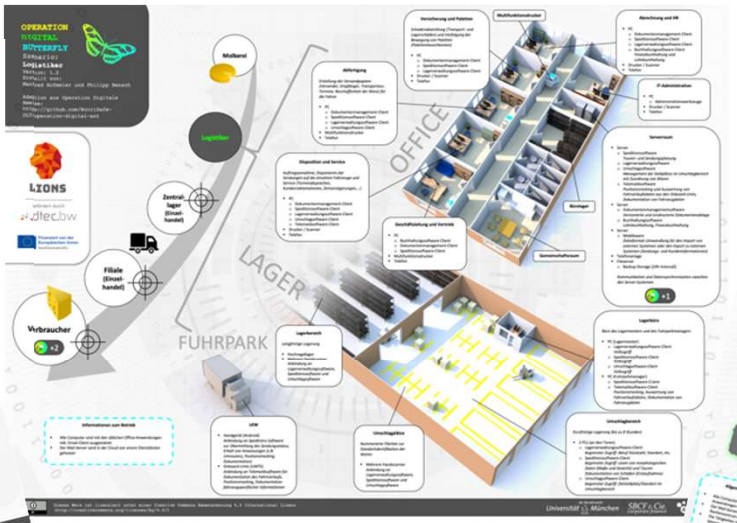
NutriSafe | GEFÖRDERT VOM Bundesministerium für Bildung und Forschung | Bundesministerium Landwirtschaft, Regionen und Tourismus | SIFO.de

Operation Digital Butterfly

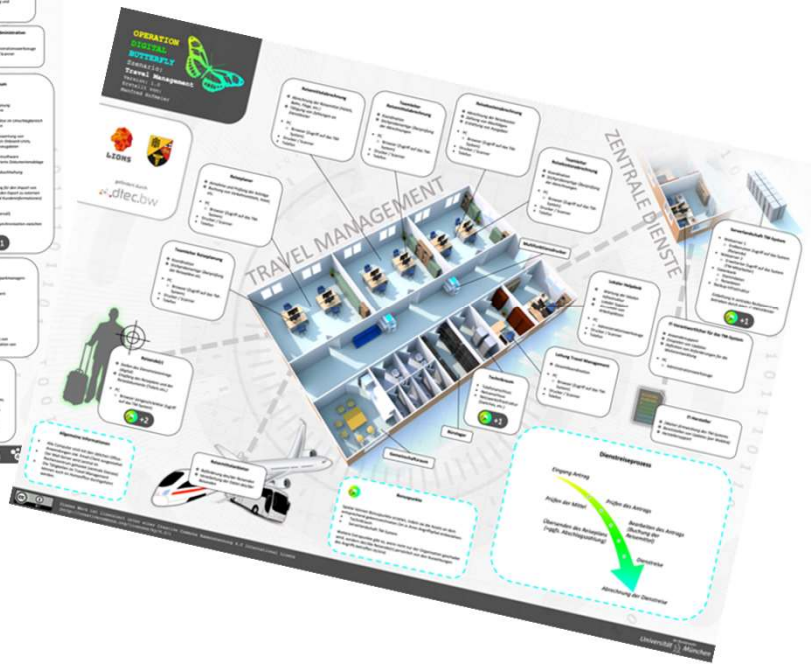
LIONS | gefördert durch dtec.bw Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr | Finanziert von der Europäischen Union NextGenerationEU

Operation Digital Butterfly

Schlacht- und Zerlegebetrieb



Logistik



Travel Management
(in einer Behörde)

Wer bin ich (Rolle / Position)?

Was möchte ich erreichen / Was ist mein Ziel?

Warum will ich das?

Wie rechtfertige ich das vor mir selbst?

Szene #:

Ort:

Sicherheitsmaßnahme

Eine für **alle Teams gültige** Maßnahme:

Plausibilität der Rolle

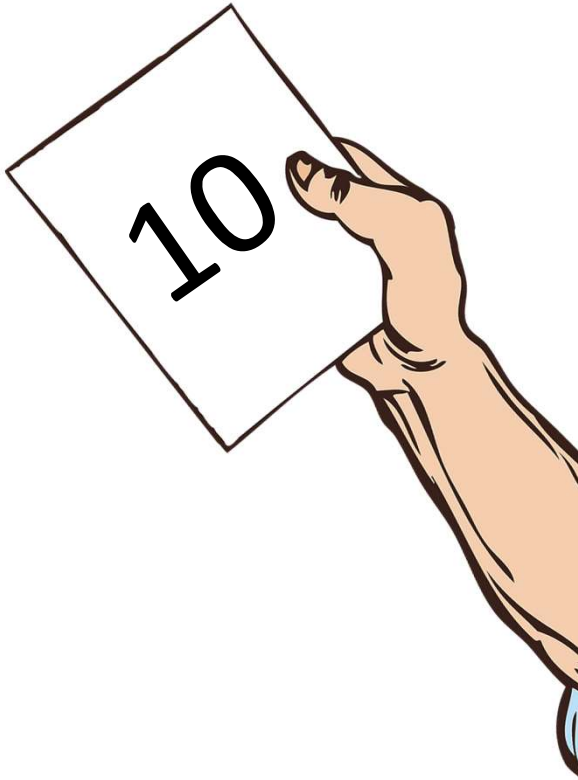
Wie plausibel ist die Rolle (z.B. Fähigkeiten des Innentäters, Motivation)?

Plausibilität der Story

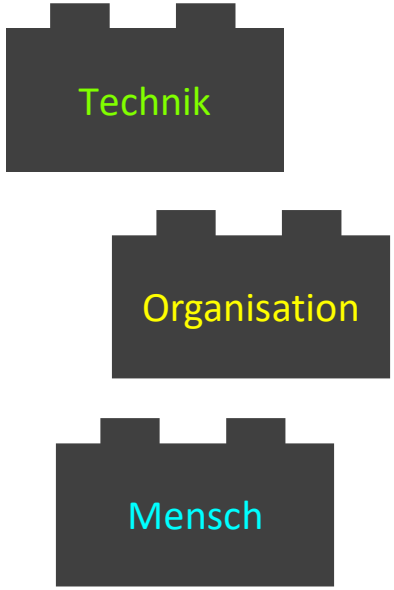
Wie plausibel ist die Story des Angriffs (z.B. vorhandene Gegenstände, Erfolg des Angriffs, getroffen Annahmen)?

Schadenspotential

Wie groß ist der Schaden für das Produkt oder die Lieferkette?



Identify	Wie könnte man im Vorhinein erkennen, dass eine solche Gefahr besteht?
Protect	Wie könnte man den Angriff verhindern oder abwehren?
Detect	Wie könnte man den Angriff erkennen, wenn er passiert?
Respond	Wie könnte man auf den Angriff reagieren?
Recover	Wie könnte man schnell wieder zum Normalbetrieb zurückkehren?



National Institute of Standards and Technology (2018): Framework for Improving Critical Infrastructure Cybersecurity - Version 1.1.

#	Datum	Szenario	Fokus	Teams	Teilnehmer
1	24.04.2019	Praxis für Neurologie und Psychiatrie	Erster Test des Spielprinzips (noch ohne Supply Chain)	5	5
2	27.05.2020	Schlacht- und Zerlegebetrieb	Interner Testdurchlauf (mit Supply Chain)	2	6
3	06.07.2020	Schlacht- und Zerlegebetrieb	Durchführung im NutriSafe-Konsortium	4	15
4	29.10.2020	Logistik	Test des neuen Spielfeldes	3	7
5	26.11.2020	Logistik	Durchführung mit NutriSafe-Konsortium und Praxispartnern	4	15
6	01.03.2021	Logistik	Durchführung mit dem LIONS-Konsortium und Praxispartnern	3	12
7	27.09.2021	Travel Management	Test des neuen Spielfeldes	3	12
8	09.02.2022	Travel Management	Durchführung mit dem BAIUDBw	3	10
9	16.02.2022	Travel Management	Durchführung mit dem BAIUDBw	3	9
10	23.02.2022	Travel Management	Durchführung mit dem BAIUDBw	3	9
11	06.07.2022	Logistik	Durchführung mit dem Bayerischen Landesamt für Gesundheit und Lebensmittelsicherheit (LGL)	3	13

#	Datum	Szenario	Fokus	Teams	Teilnehmer
1	24.04.2019	Praxis für Neurologie und Psychiatrie	Erster Test des Spielprinzips (noch ohne Supply Chain)	5	5
2	27.05.2020	Schlacht- und Zerlegebetrieb	Interner Testdurchlauf (mit Supply Chain)	2	6
3	06.07.2020	Schlacht- und Zerlegebetrieb	Durchführung im NutriSafe-Konsortium	4	15
4	29.10.2020	Logistik	Test des neuen Spielf	3	7
5	26.11.2020	Logistik		4	15
6	01.03.2021	Logist	LIONS-Konsortium …spartnern	3	12
7	27.09.2021	Travel	Test des neuen Spielfeldes	3	12
8	09.02.2022	Travel Management	Durchführung mit dem BAIUDBw	3	10
9	16.02.2022	Travel Management	Durchführung mit dem BAIUDBw	3	9
10	23.02.2022	Travel Management	Durchführung mit dem BAIUDBw	3	9
11	06.07.2022	Logistik	Durchführung mit dem Bayerischen Landesamt für Gesundheit und Lebensmittelsicherheit (LGL)	3	13

40 Bedrohungsszenare (Rollen und Angriffe)

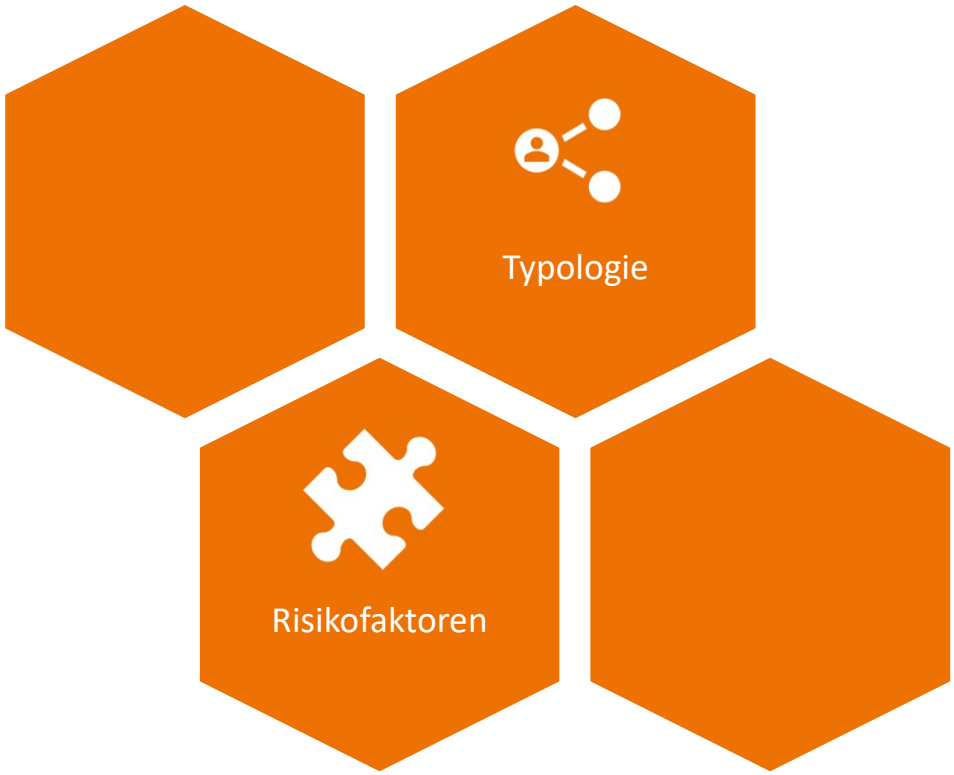
Interviewstudie

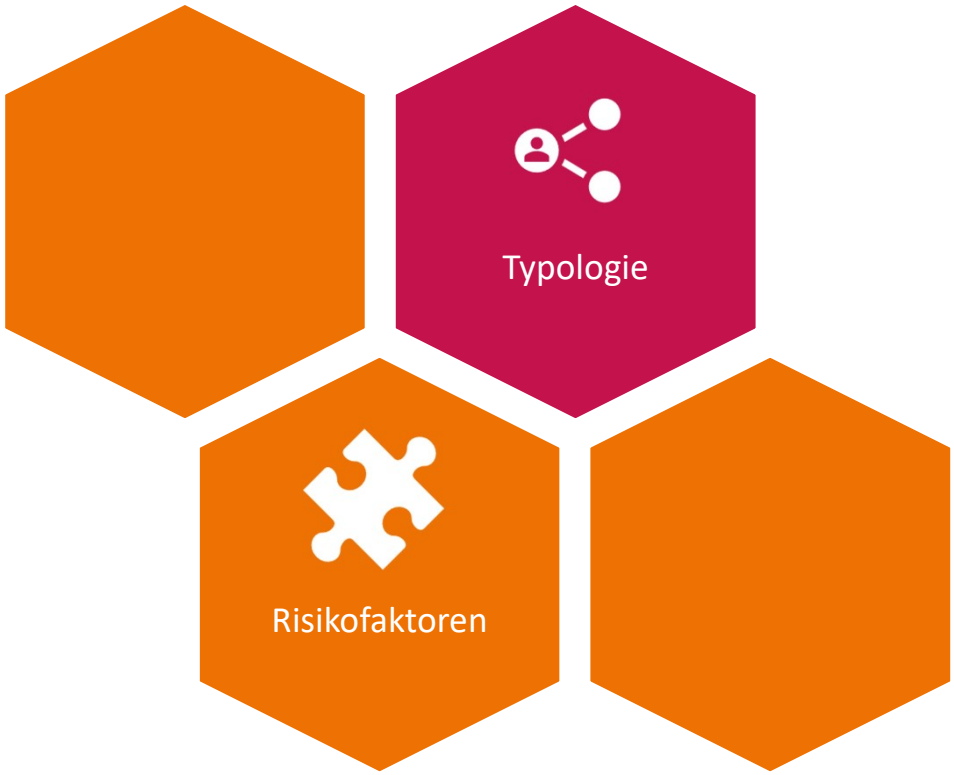
#	Datum	Organisation	Interviewpartner
1	12.12.2021	Beratungsgesellschaft im Logistikbereich	Director
2	15.12.2021	Energiekonzern	Senior Expert PenTesting
3	15.12.2021	Energiekonzern	Senior Expert Cyber Forensics Senior Expert Cyber Forensics Compliance Investigations
4	17.12.2021	Energieversorgungsunternehmen	Information Security Manager
5	12.01.2022	Ingenieurbüro	Leiter Softwareentwicklung
6	16.01.2022	Hersteller von Sicherheitstechnologie	Information Security Officer
7	03.06.2022	-	Informationssicherheitsexperte
8	23.06.2022	-	People Manager
9	07.07.2022	Hersteller von Spezialsoftware für die Industrie	Managing Director
10	25.07.2022	Behörde	Leiter Informationstechnik
11	04.08.2022	Hersteller von Security-Softwareprodukten	Geschäftsführer

Interviewstudie

#	Datum	Organisation	Interviewpartner
1	12.12.2021	Beratungsgesellschaft im Logistikbereich	Director
2	15.12.2021	Energiekonzern	Senior Expert PenTesting
3	15.12.2021	Energiekonzern	Senior Expert Cyber Forensics Senior Expert Cyber Forensics Complian[illegible]ations
4	17.12.2021	Energieversorgungsunternehmen	[illegible] Manager
5	12.01.2022	Ingeni[illegible]	[illegible]sklung
6	16.01.2022		Information Security Officer
7	03.06.2022		Informationssicherheitsexperte
8	23.06.2022	-	People Manager
9	07.07.2022	Hersteller von Spezialsoftware für die Industrie	Managing Director
10	25.07.2022	Behörde	Leiter Informationstechnik
11	04.08.2022	Hersteller von Security-Softwareprodukten	Geschäftsführer

20 Instanzen / Gruppen von Innentätervorfällen

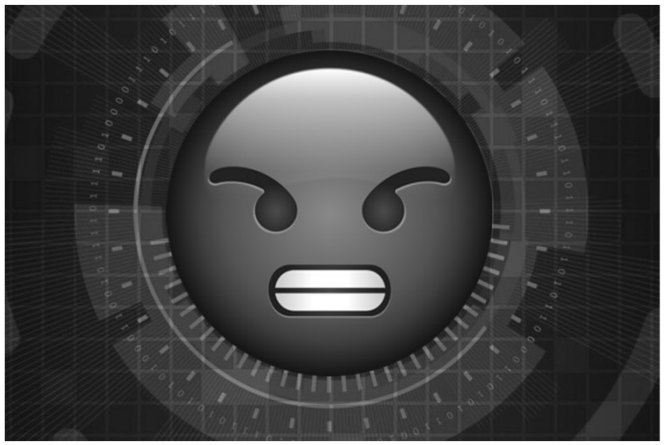

Typologie
Risikofaktoren


Typologie
Risikofaktoren

Typen von Innentätern

- Disgruntled Employee (Leaver)
- Datenmitnahme zur Konkurrenz
- Industriespionage
- Staatliche Spionage
- Ausnutzen von Privilegien
- Unautorisierter Zugriff auf persönliche Daten
- Verkauf von geistigem Eigentum
- Whistleblower
- Politisch motivierte Sabotage
- Erpressung
- Illegale Nutzung von IT-Infrastruktur

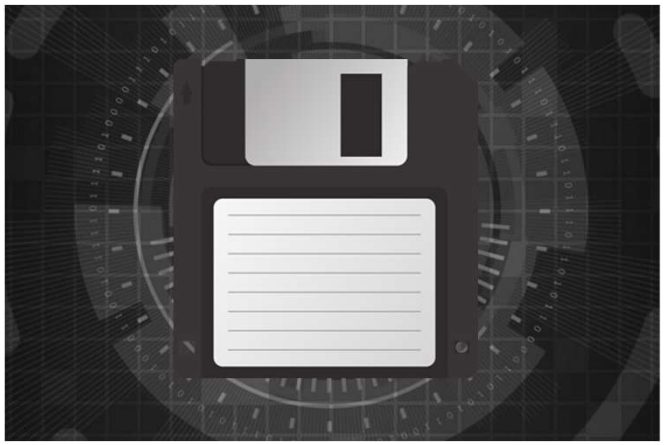
Disgruntled Employee / Leaver



- Vertragliche Bindung zur Organisation (z.B. MA)

- Rache
- Suche nach „Gerechtigkeit“
  - Kündigung durch AG
  - Streit (mit Vorgesetzten oder der GF)
  - Fehlende Wertschätzung
  - Ungleiche Lohnstruktur
  - Übergangenwerden bei Gehaltserhöhungen
- Ziel: der Organisation schaden -> Sabotage / Reputationsschaden

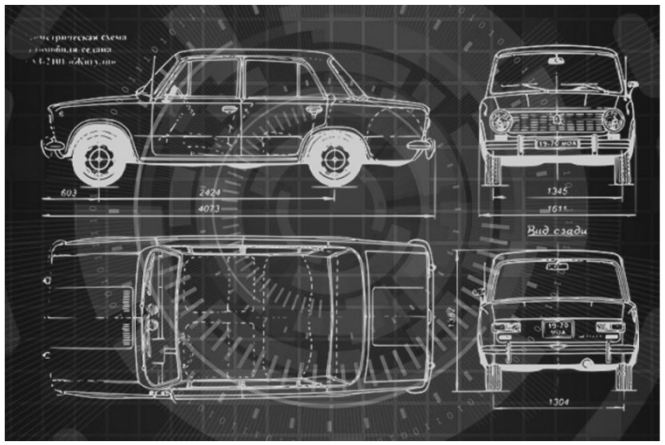
Datenmitnahme zur Konkurrenz



- Personen mit Zugang zu relevanten Daten (z.B. Dateien, Datenbanken)

- Mitnahme von Daten wie geistiges Eigentum oder anderer wertvoller Daten beim Wechsel zur Konkurrenz
- Persönlicher Vorteil
- Möglicherweise zusätzlich durch Rache motiviert

Industriespionage



- Jede Position mit Zugang zu relevanten Daten

- Ausnutzen von Privilegien zum Stehlen von wertvollen Informationen (z.B. geistiges Eigentum)
- Rekrutiert durch externe Aktoren, Bestechung
- Bereitschaft, Bestechung anzunehmen kann durch zusätzliche Faktoren beeinflusst sein (z.B. Zufriedenheit im Job, finanzielle Situation)

Staatliche Spionage

- Jede Position mit Zugang zu relevanten Daten

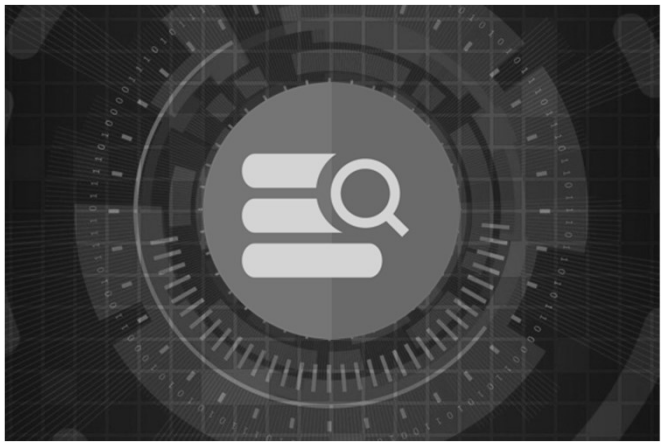
- Ausnutzen von Privilegien zum Stehlen von kritischen Informationen
- Rekrutiert durch externe Aktoren, Bestechung oder Erpressung
- Bereitschaft, Bestechung anzunehmen kann durch zusätzliche Faktoren beeinflusst sein (z.B. Zufriedenheit im Job, finanzielle Situation, familiäre Situation)

Ausnutzen von Privilegien

- Jede Position mit Zugang zu Material oder Systemen

- Ausnutzen von Privilegien zum persönlichen Vorteil
- Vielfältige Motivationen (finanziell, zu hoher Lebensstandard, Glaube es zu verdienen, Neid auf Kunden)
- Stehlen von Eigentum oder nutzen von Systemen für Betrug
- Start small and grow tall

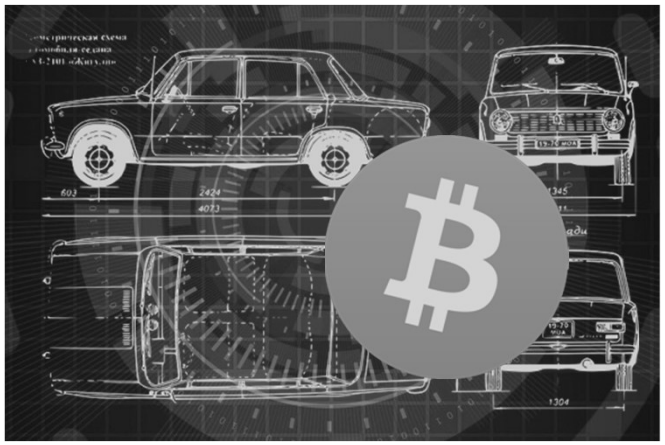
Unautorisierter Zugriff auf persönliche Daten



- Jede Position mit Zugriff auf persönliche Daten (User oder Admin)

- Inspektion von persönlichen Daten ohne dienstl. Grund
- Persönliche Gründe (Neugier, Zuneigung)
- Politische Gründe (Ausspähen von Feinden)

Verkauf von geistigem Eigentum



- Personen mit technischem Know-how (z.B. Administratoren oder Entwickler)

- Verkauf von Produktplänen oder Quellcode auf dem Schwarzmarkt (z.B. Darknet)
- Persönlicher finanzieller Vorteil
- Geringes Commitment
- Ethisch „flexibel“

Whistleblower

- Personen mit Zugang zu relevanten Daten

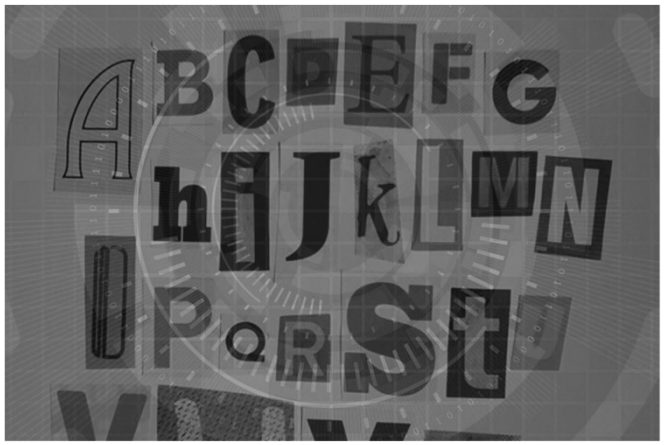
- Folgen ihren der politischen oder moralischen Vorstellungen
- Offenlegung von kritischen Informationen (z.B. Beweise des Unmoralischen
- Sehen sich selbst als Whistleblower (auch wenn sie es nicht sind)
- Ggfs. motiviert durch externe Akteure

Politisch motivierte Sabotage

- Angriffsvektor bedingt durch Position und Skills

- Meinung, dass die Organisation den Schaden verdient und man im Sinne höherer Ziele handelt
- Ziel: der Organisation schaden (physisch oder digital)
  -> Sabotage oder Reputationsschaden
- Betrifft primär staatliche Organisationen oder Unternehmen bei denen die Moralität der Ziele oder Methoden infrage steht

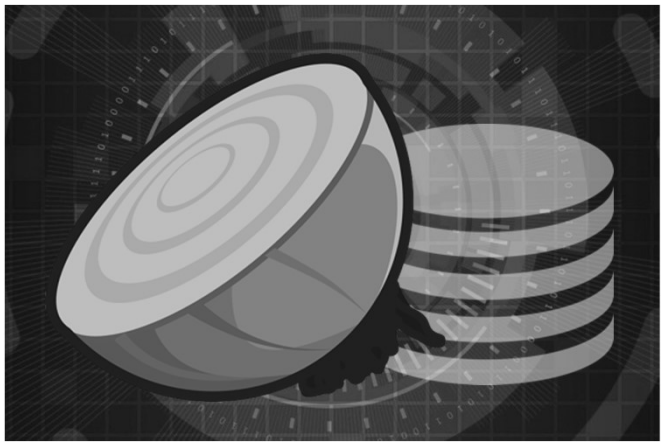
Erpressung



- Angriffsvektor bedingt durch Position und Skills

- Erpressung der Organisation
- Physisch (Güter)
- Digital (Daten, z.B. Verschlüsselung)
- Finanziell motiviert (z.B. finanzielle Probleme)
- Ggfs. krimineller Hintergrund oder psychologische Probleme
- Fehleinschätzung der Folgen

Illegale Nutzung von IT-Infrastruktur



- IT, besonders Sysadmins

- Nutzung von IT-Infrastruktur der Organisation für eigene (illegale) Zwecke
  - Nutzung von Datenträgern für Aufbewahrung oder Bereitstellung von illegalen Daten
  - Nutzung von Infrastruktur für illegale Transaktionen (z.B. Geldwäsche)


Typologie
Risikofaktoren

Risikofaktoren

Technologische Faktoren	Technische Sicherheitsmaßnahmen
	Technische Infrastruktur und Techologienutzung
Organisatorische Faktoren	Organisatorische Sicherheitsmaßnahmen und Richtlinien
	Prozesse des Personalmanagements
	Organisation der IT
	Organisationskultur
Menschliche Faktoren	Individuelle Sicherheitsfaktoren
	Psychologische Faktoren
	Soziale Faktoren
	Soziodemografische Faktoren
Infrastrukturelle Faktoren	Infrastrukturelle Sicherheitsmaßnahmen
	Beschaffenheit der (physischen) Infrastruktur

Technische Sicherheitsmaßnahmen

- Detektion von Änderungsmustern in Informationssystemen (z.B. Warnung bei Änderung von großen Datenmengen)
- Zutrittskontrollsysteme (z.B. bei Server- oder Technikräumen)
- Videoüberwachung in kritischen Bereichen und Korridoren
- 2FA / MFA
- Blacklisting von Hacking Tools
- Deaktivieren von USB-Ports

Technische Infrastruktur und Technologienutzung

- ▼ Rechtemanagement (wer kann was sehen / ändern?)
- ▲ Generische Accounts
- ▼ Logging von Interaktionen mit Informationssystemen
- ▲ Löschbarkeit von Logs
- ▲ Offener Zugang zu Technikräumen oder Verkabelung

Organisatorische Sicherheitsmaßnahmen und Richtlinien

- Awarenesskampagnen und Mitarbeitertrainings (Konsequenzen; Achtsamkeit z.B. bei radikalem Sprachgebrauch)
- Trainings für Führungskräfte (Korrekter Umgang mit MA; Antennen für Probleme; Unterstützung von MA)
- Maßnahmen zur politischen Bildung (besonders in staatl. Org.)
- Zeitnahe Aufklärung ungewöhnlicher Ereignisse (Vorboten/Indikatoren)
- Regelmäßiges Ändern u. Verteilung von Verantwortlichkeiten
- Raumreinigung in Abwesenheit
- Generalschlüssel
- Bewertung der Kritikalität von Kunden oder Partnern

Prozesse des Personalmanagements

- Aktives Fördern und Monitoren von Mitarbeiterzufriedenheit und Arbeitsatmosphäre
- Fördern interpersonaler Kontakte (soziale Kontrolle -> Bindungselemente „attachment“ und „involvement“)
- Angemessene Prozesse beim Onboarding (z.B. Sicherheitschecks)
- Angemessene Prozesse beim Offboarding (z.B. Überprüfung von Zugangsdaten; Freistellen bei Kündigung durch AG)

Organisation der IT

- Verteilung von Verantwortlichkeiten (z.B. Rechtemanagement vs. operative Administration)
- Management von Zutritts- und Zugriffsrechten (z.B. zu Serverräumen; Einsehbarkeit von Daten durch Admins)

Organisationskultur

- Arbeitsatmosphäre und Bindung an die Organisation
- Arbeitsbedingungen u. vertragliche Bedingungen
- Schlechte oder ungleiche Bezahlung
- Fehlende Wertschätzung oder unangemessener Umgang mit MA
- Externe MitarbeiterInnen (wenig Einfluss auf Zufriedenheitsfaktoren, wenig Bindung)
- Kollision der Organisationsziele mit den Werten der Individuen

Individuelle Sicherheitsfaktoren

- Wahrnehmung verdächtiger Ereignisse
- Ernstnehmen von Äußerungen und ungewöhnlichen Ereignissen
- Meldeverhalten
- Sicherung der Arbeitsplätze (z.B. Sperren von PCs)
- Allg. Informationssicherheits-Awareness

Psychologische Faktoren

- Fehleinschätzung von möglichen Folgen
- Frustration (z.B. durch fehlende Wertschätzung, Bezahlung)
- Radikale politische oder religiöse Einstellungen (besonders bei staatl. Institutionen)
- Streben nach Aufmerksamkeit
- Suche nach Erregung (Kicks)
- Neid auf Kunden (z.B. bei teuren Produkten/Dienstleistungen)

Soziale Faktoren

- ▼ Interpersonale Kontakte in der Organisation (soziale Kontrolle)
- ▲ Kontakte zu extremistischen oder kriminellen Milieus

Soziodemografische Faktoren

- Finanzielle Schwierigkeiten
- Herkunft aus einem feindlich gesinnten Land (bei staatl. Institutionen)

Infrastrukturelle Faktoren

- Zutrittsmöglichkeiten (Technikräume, Produktionsbereiche)
- Sensible Infrastruktur in oder neben offen zugänglichen Bereichen

Weitere Informationen

Operation Digital Butterfly

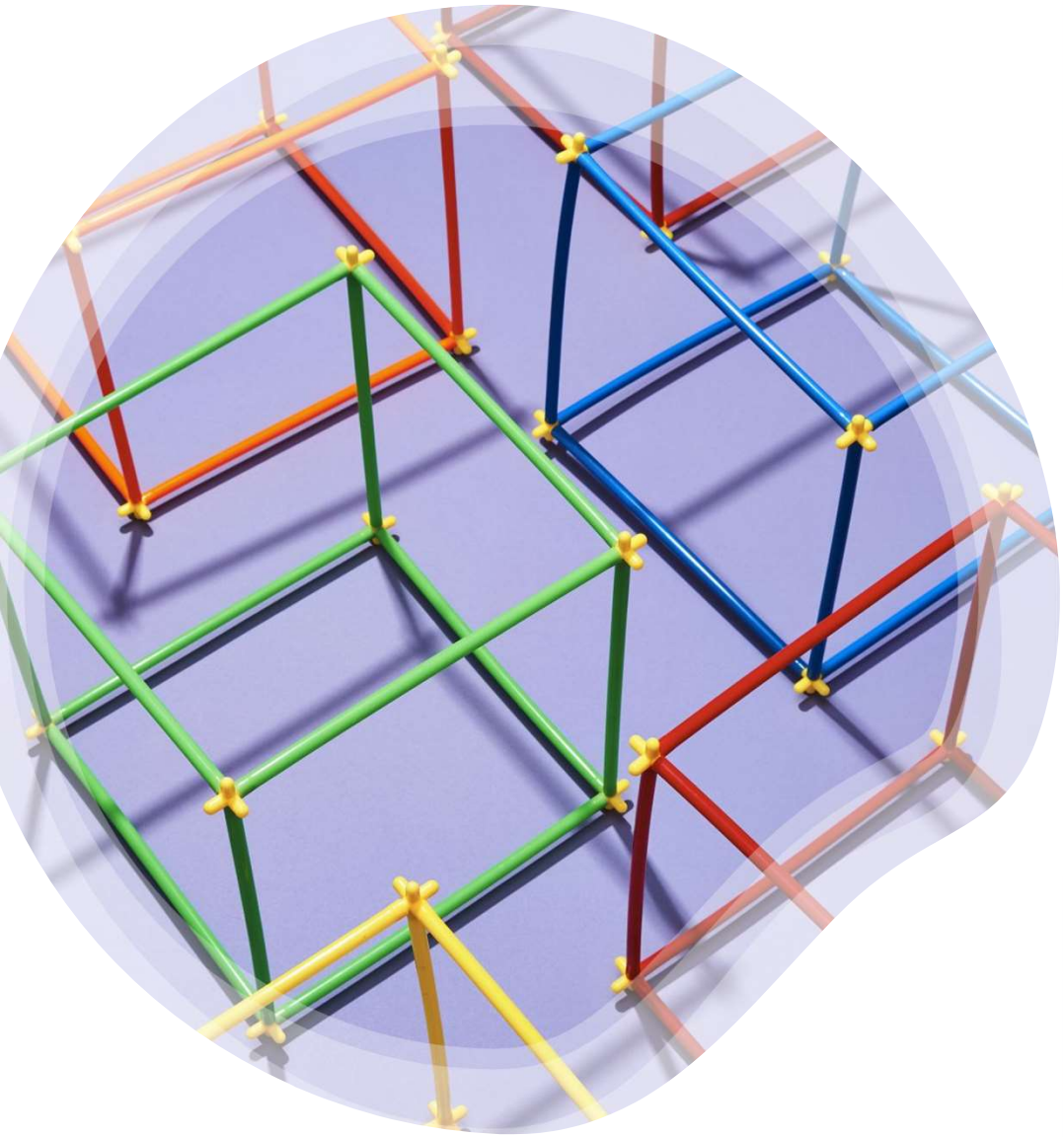
- GitHub: https://github.com/LIONS-DLT/operation-digital-butterfly

Typologie

- Hofmeier, M., Haunschild, I., Lechner, U. (2023): Malicious Insider Threat Types – An Empirical Analysis. 36th Bled eConference Digital Economy and Society, Bled.

Risikofaktoren

- Hofmeier, M., Seidenfad, K., Rieb, A., Lechner, U. (2023): Risk Factors for Malicious Insider Threats – An Analysis of Attack Scenarios. 29th Americas Conference on Information Systems, Panama City.



Unsere Serious Games zur Informationssicherheit

- CONTAIN – Die Ransomware meldet sich. Was dann?.

- CyberSecurity Challenges – Awareness für Secure Coding
  - Kooperation von LIONS, SIEMENS
- CATS – Awareness für Sicherheit im Betrieb Cloud-Diensten
  - Kooperation von LIONS, SIEMENS
- The Hidden Threat – Supply Chain Angriffe
  - Forschungsergebnis von LIONS (ab Mitte 2024)
- Operation Digitales Chamäleon – Ein Wargame für Kritische Infrastrukturen
  - Forschungsergebnis von VeSiKi

contain

Universität der Bundeswehr München
Institut für Schutz und Zuverlässigkeit

LIONS

Vielen Dank für die Aufmerksamkeit

Ansprechpartner

Ulrike Lechner & Manfred Hofmeier
ulrike.lechner@unibw.de. manfred.hofmeier@unibw.de