
ISX2024
IT-Security Digital Conference
isxconference.de | #isxcon #isxconference
VOGEL IT AKADEMIE

VOM CHAOS-KRAXLER ZUM DIGITALEN GIPFELSTÜRMER – WIE UNTERNEHMEN DIE DIGITALE TRANSFORMATION UND CYBERSICHERHEIT MEISTERN

Florian Laumer | PASSION4IT | 14.11.2024

PASSION4IT GMBH
ÜBER UNS

Danke das wir uns vorstellen dürfen!

HAUSBERG. K2. MOUNT EVEREST. JEDE ERFOLGREICHE EXPEDITION FOLGT DEN GLEICHEN GRUNDSÄTZEN.

Ob Klettersteigpremiere oder die persönliche Erstbesteigung eines der Seven Summits: Steht man allein am Fuß des Berges, lässt der Blick nach oben unweigerlich Zweifel am Gelingen des Unterfangens aufkommen.

Was aber, wenn genau in dieser Situation ein erfahrener Bergführer dir beruhigend die Hand auf die Schulter legt? Mit dir dein Vorhaben minutiös plant, dich auf alle Eventualitäten vorbereitet? Und am Tag X als dein Seilgefährte voraus steigt?

WIR SIND DIGITALE BERGFÜHRER

Für deine IT-Vorhaben hast du mit PASSION4IT deinen Bergführer gefunden. Erfahre mehr, wie du durch digitalisierte Prozesse dein Business in ungeahnte Höhen bringen kannst!!

ZAHLEN, DATEN, FAKTEN

2019
Gegründet

9
Digitale Bergführer

90+
Kunden D-A-CH

4,0
Millionen € Umsatz

1%
Vom Umsatz an den Umweltschutz

VOM CHAOS-KRAXLER ZUM DIGITALEN GIPFELSTÜRMER – WIE UNTERNEHMEN DIE DIGITALE TRANSFORMATION UND CYBERSICHERHEIT MEISTERN

Florian Laumer | PASSION4IT | 14.11.2024

FLORIAN LAUMER

+49 151 11676 502

Florian.laumer@passion4it.de

https://www.linkedin.com/in/florianlaumer/

www.passion4it.de

- ✓ 25 Jahre Leidenschaft für IT, Digitalisierung, digitale Transformation und Innovation
- ✓ Hands On Mentalität
- ✓ LEAD Digital Transformation Analyst (LEADing Practice)
- ✓ ITQ-Auditor (Informationssicherheit)
- ✓ ICO ISMS Security Officer according to ISO/IEC 27001:2022
- ✓ CISM (Certified Information Security Manager)
- ✓ Certified SAFe 6 Agilist

KERNTHEMEN DER BERGTOUR

- Digitale Transformation:
  Wettbewerbsvorteil inkl. Sicherheitsstrategie
- Agilität und Cybersicherheit:
  Erfolgsmodell für die digitale Welt
- Künstliche Intelligenz:
  Der digitale Bergführer auch in der der Cybersicherheit

DIGITAL RISER REPORT

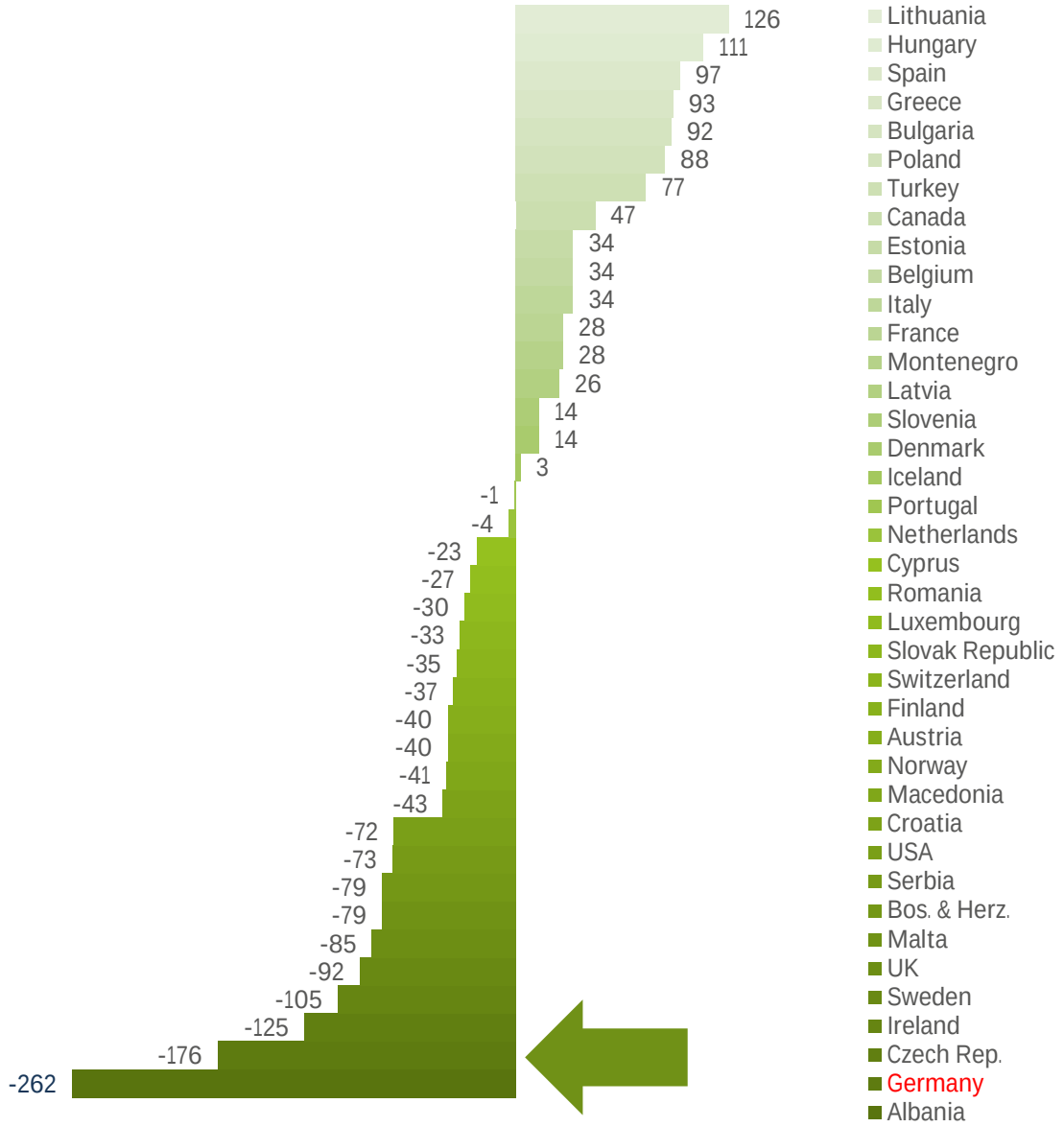
Quelle: European Center for Digital Competitiveness (Hrsg.), Digitalreport 2024, Berlin, 2024

DIGITALISIERUNGS-LEVEL

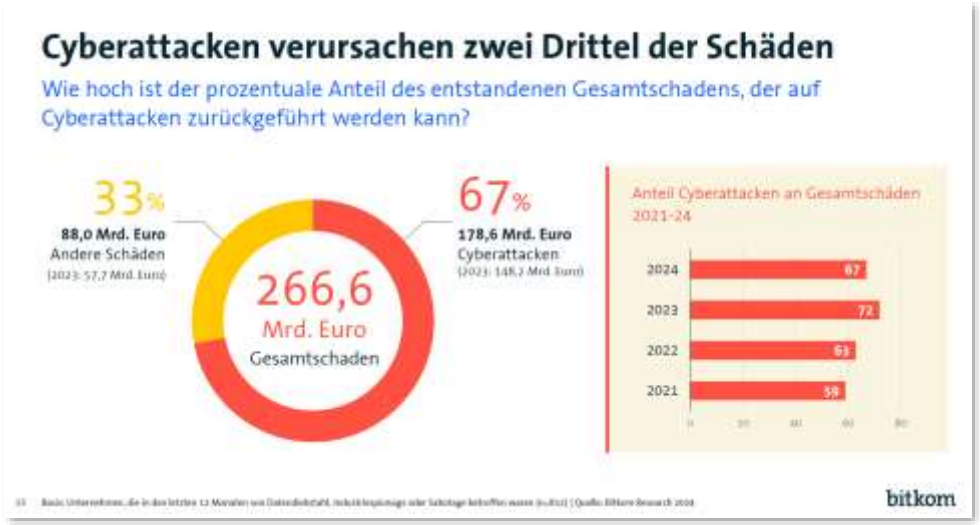
Innerhalb der EU inkl. Veränderung zum Vorjahr.

DEUTSCHLAND STABIL

Im hinteren Drittel.



BEDROHUNGSLAGE



GDV Gesamtverband der Versicherer

Versicherer pochen auf Cyber-Prävention

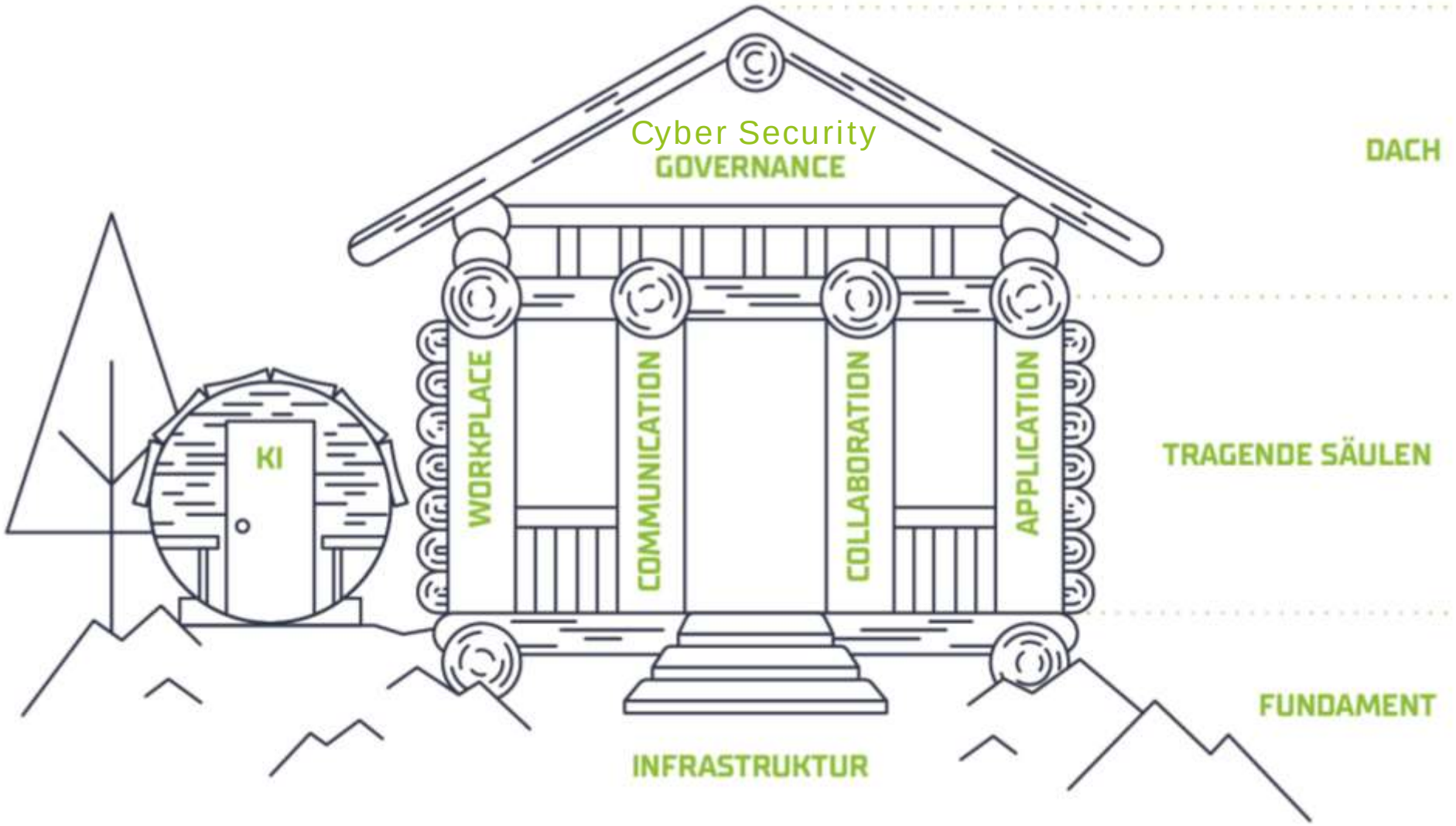
Die Entwicklung wirkt sich auf die Zeichnungspolitik der Unternehmen aus. Mit einem Anstieg um rund ein Viertel auf 309 Millionen Euro stiegen die Prämieneinnahmen in der Cyber-Sparte gegenüber 2022 zwar, das Plus lag aber deutlich unter dem Niveau der Vorjahre (2022: 56,3 Prozent; 2021: 49,2 Prozent). „Angesichts der wachsenden Gefahrenlage bestehen die Versicherer bei Neuabschlüssen auf wirksame Schutzmaßnahmen. Cyber-Prävention darf kein Lippenbekenntnis sein", betont Asmussen.


01
BASECAMP

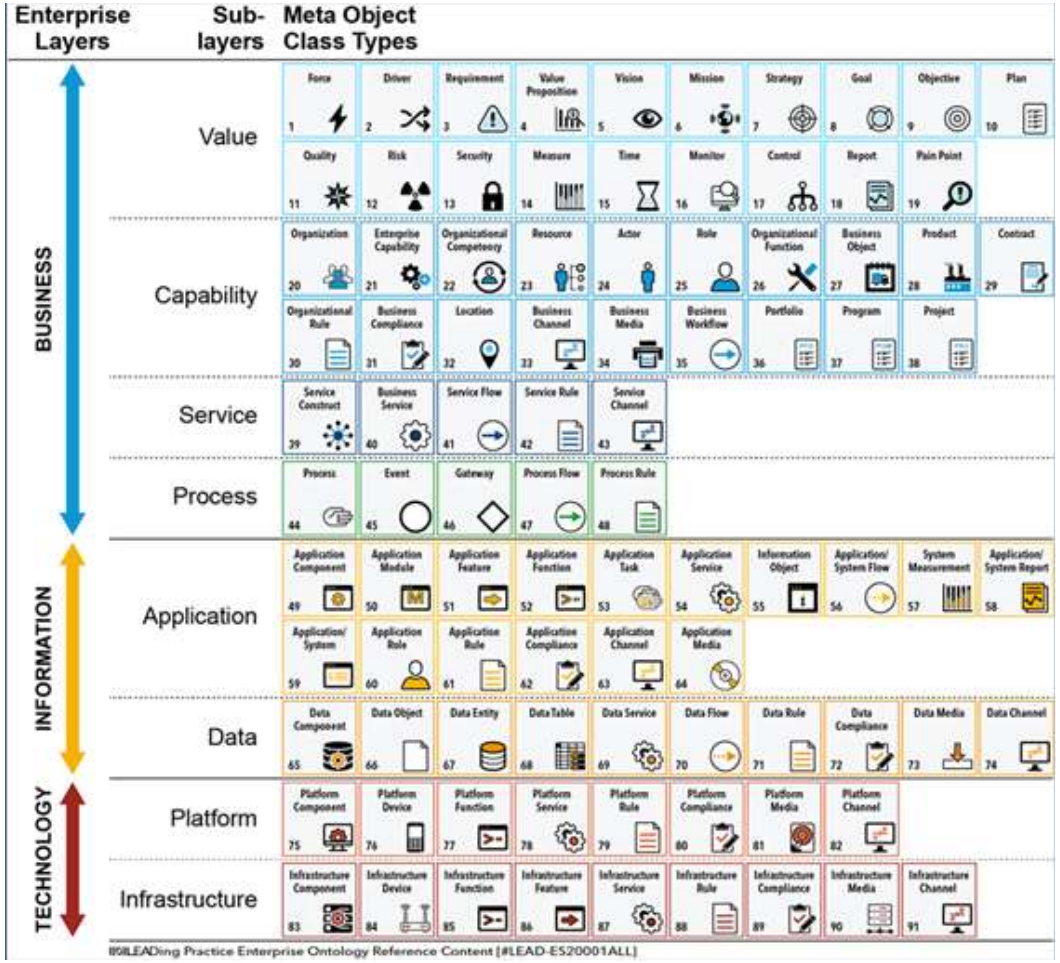
BASECAMP

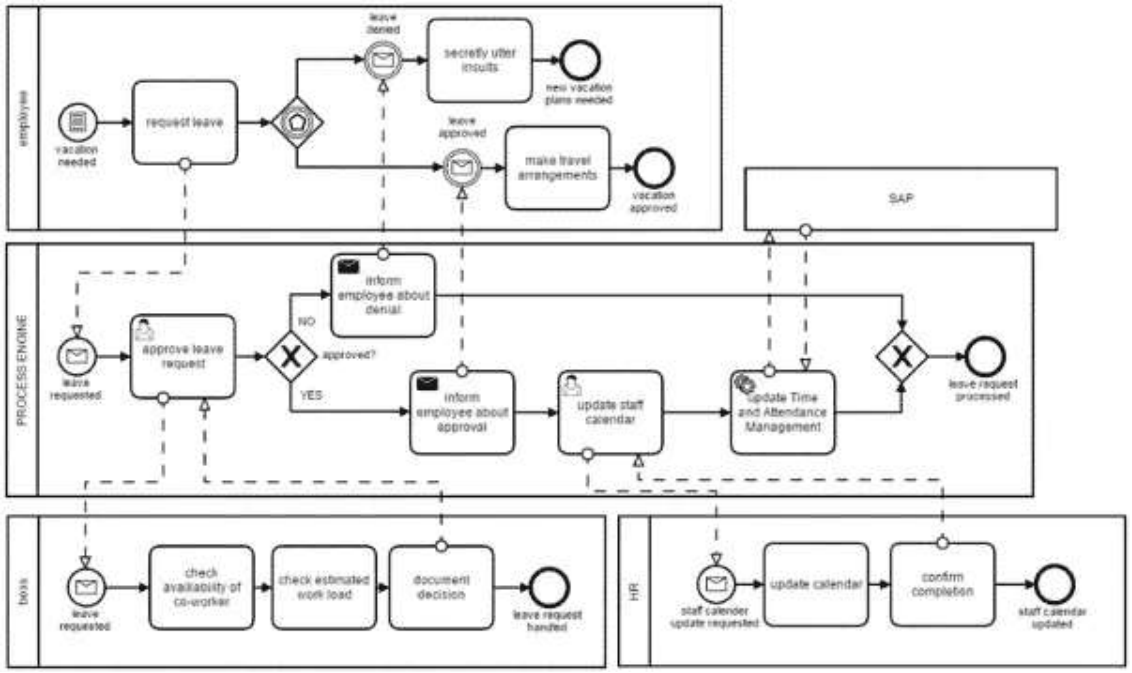
- Ausgangslage: Herausforderungen ohne klare Strategie
- Erkenntnis: Vereinzelte Tools reichen nicht, um konkurrenzfähig zu bleiben
- Lösungsansatz: Vom blinden Aktionismus zur strategischen Planung für die Wertschöpfenden Prozesse. Stabilisieren der Kernprozesse.
- Ergebnis: Klare Zielsetzung, Roadmap und langfristige Wettbewerbsfähigkeit

DIE BAUSTEINE...

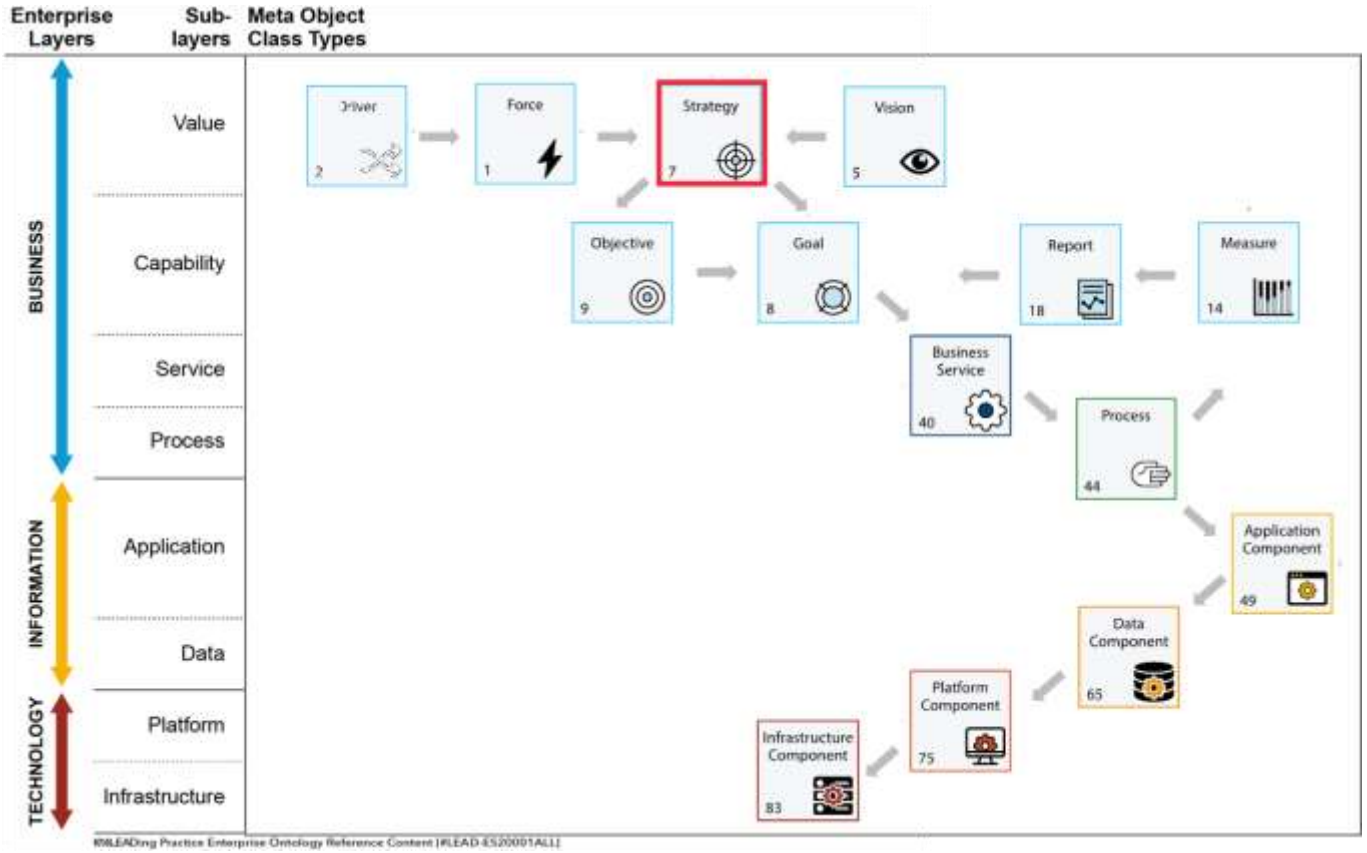


DIE BAUSTEINE...



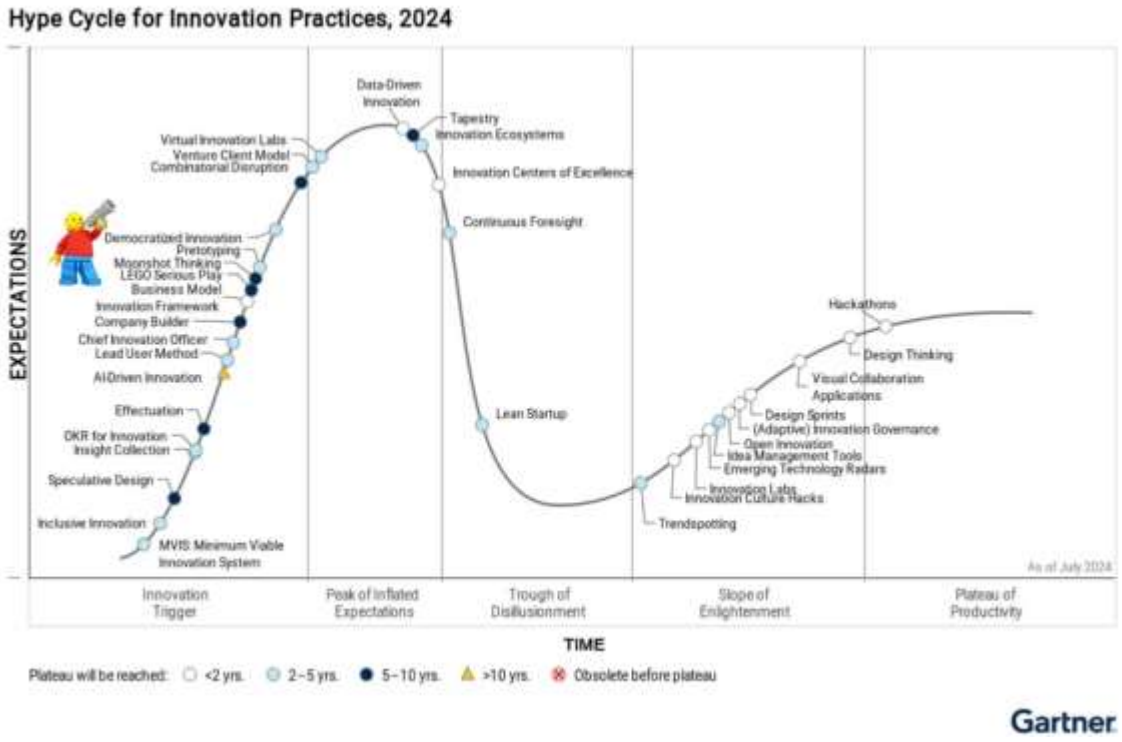


ALLE ELEMENTE SIND MITEINANDER VERBUNDEN




6 Steine-Party
915.103.765

LEGO SERIOUS PLAY



02

DER RISIKOBASIERTE KLETTERPLAN (Z.B. FÜR NIS2)

„Vom Feeling her habe ich ein gutes Gefühl“

DER RISIKOBASIERTE KLETTERPLAN (Z.B. FÜR NIS2)

- Digitalisierung bedeutet, gezielte Herausforderungen strategisch anzugehen.
- Risikomanagement ist unerlässlich, um die größten Hürden zu bewältigen.
- Kein planloses Herumklettern mehr, sondern gezielter Fortschritt.
- Ein strukturierter Ansatz verleiht Flexibilität und Effizienz.

- BSI-Grundschutz, ISO-27001 - 27005, NIST2 CSF2.0 etc.

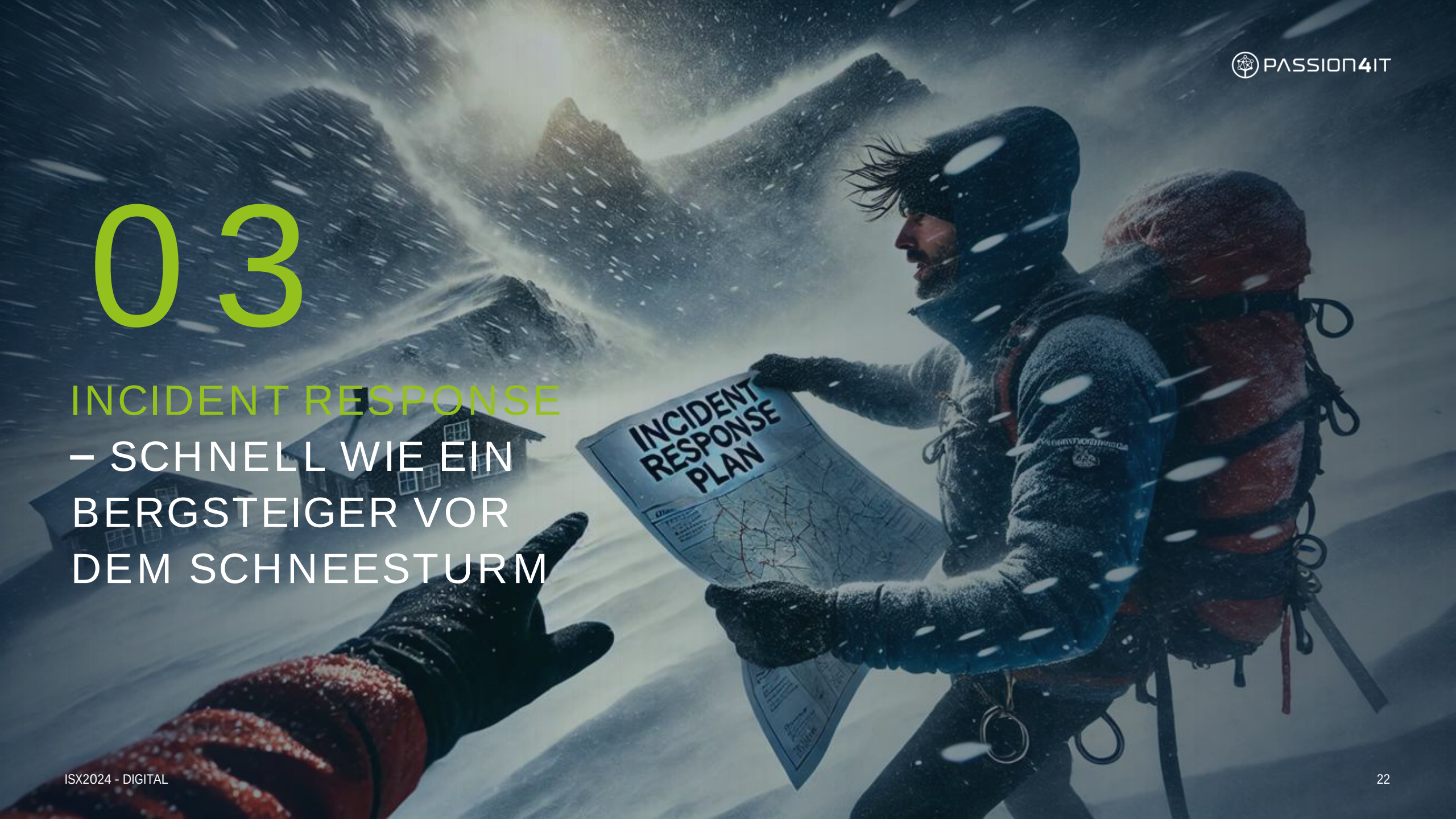
DER RISIKOBASIERTE KLETTERPLAN (Z.B. FÜR NIS2)

PASSION4IT

Risiko Szenario (Beschreibung eines möglichen Vorfalls)	Beschreibung des Schadens ("...führt zu")	Ursache / Grund für das Eintreten des Szenarios (= Schwachstelle)	Schadens-klasse	Schaden-summe	Eintritts-wahrschein-lichkeit	Zukunft	Risiko		[redacted]	Schadens-klasse (neu)	Schadenssumme (neu)	Eintritts-wahrscheinlich-keit (neu)	Zukunft	Risiko	Status Zusatzmaßnahme	Verantwortlich für Zusatzmaßnahme
		Sicherheitsrichtlinien.							Sicherheitsrichtlinien und regelmäßige Schulungen.				Jahren oder später ein			
Fehlende oder unzureichende Schulung	Führt zu erhöhter Anfälligkeit für Sicherheitsvorfälle.	Fehlende Sensibilisierung und Schulung der Mitarbeiter.	gering	<20.000 €	gering	Vorfall tritt frühestens in 6 Jahren oder später ein			Regelmäßige und umfassende Schulungsprogramme zur IT-Sicherheit für alle Mitarbeiter.	gering	<20.000 €	gering	Vorfall tritt frühestens in 6 Jahren oder		abgeschlossen	IT-Leiter (CIO - Chief Information Officer)
Technisches Versagen:																
Fehler in Software oder Firmware (z. B. Bugs, Konfigurationsfehler)	Führt zu Sicherheitslücken und möglichen Datenverlusten.	Unzureichende Testverfahren und Qualitätskontrollen bei der Softwareentwicklung/Implementierung strenger Testverfahren und regelmäßige Updates und Patches.	hoch	200.000 € und 1.000.000 €	mittel	Vorfall tritt in den nächsten 4-6 Jahren ein			Implementierung strenger Testverfahren und regelmäßige Updates und Patche (mittels EMPIRIUM).	hoch	200.000 € und 1.000.00	mittel	Vorfall trit in den nächsten 4-6 Jahren ein		abgeschlossen	IT-Leiter (CIO - Chief Information Officer)
Hardware-Ausfälle (z. B. Festplatten, Netzwerkkarten)	Führt zu Datenverlust und möglichen Betriebsunterbrechungen.	Alternde oder minderwertige Hardware und unzureichende Wartung.	mittel	20.000 € und 200.000 €	hoch	Vorfall tritt in den nächsten 1-3 Jahren ein			Regelmäßige Wartung und Austausch von Hardware sowie Implementierung von Backup-Lösungen.	mittel	20.000 € und 200.000 €	hoch	Vorfall tritt in den nächsten 1-3 Jahren ein		abgeschlossen	IT-Leiter (CIO - Chief Information Officer)
Stromausfälle	Führt zu Datenverlust und Betriebsunterbrechungen.	Fehlende Notstromversorgung und unzureichende Notfallpläne.	mittel	20.000 € und 200.000 €	mittel	Vorfall tritt in den nächsten 4-6 Jahren ein			Installation von unterbrechungsfreien Stromversorgungen (USV) und Notstromaggregaten.	mittel	20.000 € und 200.000 €	mittel	Vorfall tritt in den nächsten 4-6 Jahren ein		abgeschlossen	IT-Leiter (CIO - Chief Information Officer)
Technische Inkompatibilitäten	Führt zu Systemausfällen und Betriebsunterbrechungen.	Fehlende Kompatibilitätstests und unzureichende Planungen bei Systemänderungen.	mittel	20.000 € und 200.000 €	mittel	Vorfall tritt in den nächsten 4-6 Jahren ein			Durchführung umfassender Kompatibilitätstests vor Implementierung neuer Systeme oder Updates.	mittel	20.000 € und 200.000 €	mittel	Vorfall tritt in den nächsten 4-6 Jahren ein		abgeschlossen	IT-Leiter (CIO - Chief Information Officer)
Vorsätzliche Handlungen:																
Hacking (unerlaubter Zugriff auf Systeme)	Führt zu Datenverlust, finanziellen Verlusten und Rufschädigung.	Unzureichende Sicherheitsmaßnahmen wie fehlende Firewalls und Anti-Malware-Software.	hoch	200.000 € und 1.000.000 €	hoch	Vorfall tritt in den nächsten 1-3 Jahren ein			Implementierung umfassender Sicherheitslösungen und regelmäßige Sicherheitsüberprüfungen.	hoch	200.000 € und 1.000.00	hoch	Vorfall tritt in den nächsten 1-3 Jahren ein		abgeschlossen	IT-Leiter (CIO - Chief Information Officer)
Sabotage (gezielte Zerstörung oder Manipulation von Daten und Systemen)	Führt zu Datenverlust und Betriebsunterbrechungen.	Fehlende Überwachung und Sicherheitskontrollen für interne Benutzer.	hoch	200.000 € und 1.000.000 €	gering	Vorfall tritt frühestens in 6 Jahren oder später ein			Implementierung strenger Zugriffskontrollen und Überwachungssysteme sowie Etablierung von Kontrollmechanismen beim Verlassen des Unternehmens.	hoch	200.000 € und 1.000.00	gering	Vorfall tritt frühestens in 6 Jahren oder später ein		abgeschlossen	IT-Leiter (CIO - Chief Information Officer)

03

INCIDENT RESPONSE – SCHNELL WIE EIN BERGSTEIGER VOR DEM SCHNEESTURM



INCIDENT RESPONSE

- Vorbereitung allein reicht nicht; schnelle Reaktion in Krisensituationen ist entscheidend.
- Ohne Plan besteht die Gefahr, von der Krise überrascht zu werden.
- Anforderungen der Stakeholder gerecht werden
- Vermeiden eines Reputationsschaden, Imageverlust

- Notfallplan, Richtlinien , Schutzbedarfskategorisierung

04

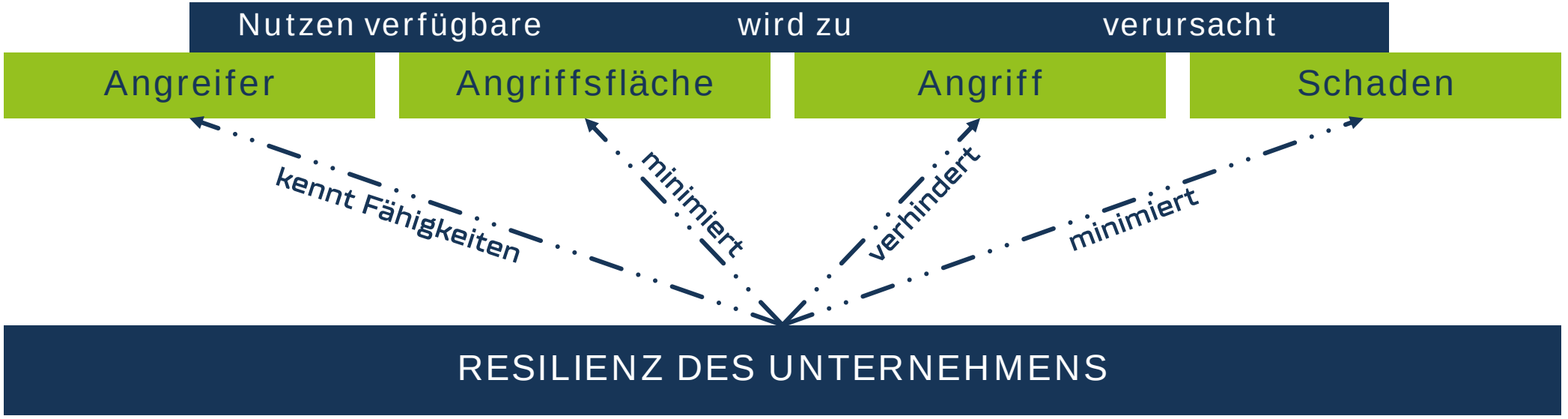
ECHTZEITÜBERWACHUNG – WIE ICH ZUM KLETTERPROFI MIT HÖHENRADAR WURDE

ECHTZEITÜBERWACHUNG

- Alte Strategie basierte darauf, erst zu reagieren, wenn Gefahr sichtbar wird.
- Ständige Wachsamkeit erforderlich, um Bedrohungen frühzeitig zu erkennen, wie ein Bergsteiger das Wetter beobachtet.
- Von reaktiver zu proaktiver Problemlösung.
- Prozesse und Risiken in Echtzeit überwachen und optimieren.

- IDR, XDR, SOC, SIEM, SOAR

ECHTZEITÜBERWACHUNG UND RESILIENZ



05

LIEFERKETTEN-SICHERHEIT – JEDER IM SEIL IST WICHTIG

LIEFERKETTEN-SICHERHEIT

- Sicherheit in Lieferketten ist so wichtig wie jedes Mitglied in der Seilschaft.
- Sicherstellung, dass alle Partner auf der Reise die richtige Ausrüstung haben.
- Gemeinsame Absicherung stärkt die Sicherheit, damit niemand den Weg allein gehen muss.
- Digitalisierte und sichere Lieferketten verschaffen Wettbewerbsvorteile.

- Kritische, Wichtige, Standard, Strategische Lieferanten

06

MITARBEITERSCHULUNGEN – MEIN TEAM WIRD ZUR SEILSCHAFT

MITARBEITERSCHULUNGEN

- Ein starkes Team ist essenziell, wie eine gut ausgebildete Klettergruppe.
- **Mitarbeiter wurden zu „Cyber-Helden“, die auf Gefahren vorbereitet sind.**
- Gemeinsam meistert das Team den Gipfel der Cybersicherheit.
- Digital geschulte Teams sind agiler und erfolgreicher.

- Awarenesstrainings, Phishingkampganen

07

DIGITAL MINDSET


Die Loorbeeren von heute
sind der Kompost von morgen.


Einfach mal
Machen.


PASSION4IT
Q&A

KONTAKT

FLORIAN LAUMER

+49 (0) 151 11676502

florian.laumer@passion4it.de

www.flolaumer.de

SCAN ME

- ✓ Exklusiver 1:1 und kostenloser Cyber Security Quick Check


PASSION4IT
CYBER SECURITIY IST EINE FORTLAUFENDE STRATEGIE UND MESSBAR – KEIN EINMALIGES PROJEKT

DER WEG ZUM ZIEL.

Unser gemeinsamer Aufstieg auf die digitalen Gipfel.

STEP 6
Digitalisierung Wertschöpfung

STEP 5
Digitalisierung Service Prozesse

STEP 4
Digitaler Arbeitsplatz

STEP 3
Quick Wins
Cyber Security Offensive

STEP 2
Digital Roadmap erarbeiten

STEP 1
Standortbestimmung
(Mitarbeiter, Kunden, Lieferanten, Geschäftsmodell, IT Landschaft)

Die Umsetzung der IT Strategie gleicht einer Bergtour. Dies bedeutet man braucht einen guten Plan, einen erfahrenen Bergführer, ein starkes, vertrauensvolles Team und etwas Glück.