CYBERSECURITY & REGULIERUNG

19.11.2025
SAQ REGION BERN

Umberto Annino

umbi@auseco.net

UMBERTO ANNINO

INFORMATION SECURITY SPECIALIST

- In der IT tätig seit 1992, Information Security seit ca. 2000
- Consultant und Security Officer
  mit Tendenz zu regulierten Branchen (v.a. Finanzindustrie)
- Vorstandstätigkeit
  in verschiedenen Fachverbänden und –Organisationen
- Nebenberuflich tätig
  als Kursleiter und Dozent für Governance, Risk Management, Compliance, Information- & Cyber Security
- Aus- und Weiterbildung
  als Wirtschaftsinformatiker, NDS FH in Qualitätsmanagement und Eidg. Dipl. ICT-Security Expert
    - Verschiedene Zertifizierungen in den Themen Cybersicherheit, IT Risikomanagement, GRC, Datenschutz, Cloud Security, KI Security

Erreichbar unter:

+41 79 679 0096
umbi@auseco.net
https://www.linkedin.com/in/umbertoannino/

EINFÜHRUNG UND ZIELSETZUNG

BEGRÜSSUNG UND AGENDA

- **Cybersecurity Regulierung – eine Übersicht**
- **Cybersecurity – wie geht das?**
- **Wie weiter?**

Maturität und Realität

CMM-I Level	Explanation
Initial	**Processes are unpredictable**, poorly controlled, and reactive. Success depends on individual heroics rather than proven processes.
Managed	Projects have **basic project management processes established**. Requirements, processes, work products, and services are managed.
Defined	**Processes are well characterized, understood, and described in standards**, procedures, tools, and methods. Organization has a standard set of processes.
Quantitatively Managed	Organization and projects establish **quantitative objectives for quality and process performance**. Statistical and other quantitative techniques are used.
Optimizing	Organization focuses on **continuous process improvement** through incremental and innovative technological improvements.

REALITY CHECK

CYBERSECURITY REGULIERUNG

basic.basics

- EDV / ICT Security
- Informationssicherheit
- Cybersecurity
- Datenschutz

Informationssicherheit: CIA(+N)

- **Vertraulichkeit** (C – Confidentiality)
- **Integrität** (I – Integrity)
  - **Nicht-Abstreitbarkeit** (N – non-repudiation)
- **Verfügbarkeit** (A – Availability)

- (Operative run/change) **Risiken**
  “im Griff” / **kontrolliert = Sicherheit**

- **Sicherheit ist**
  - Ein **Zyklus**, kein Zustand
  - **Objektiv** (messbar?), nicht Subjektiv
  - **Relativ**, nicht absolut

Cybersecurity Regulierung EUROPA

NIS2 (network and information systems)

- Nachfolge-Gesetz für NIS1 (2016)
- Nationale Umsetzung seit Oktober 2024
- Vergrösserte Abdeckung, erhöhte Anforderungen, persönliche Haftung der Leitung und Bussen für Nicht-Einhaltung
- Anwendbarkeit: >50 MA oder >10 MEUR jährlicher Umsatz
- **Essential Entities** EE: regelmässige Prüfung)
  - Energie, Transport, Gesundheit
  - Banking&Finance, Digitale Infrastruktur, Wasser, öffentliche Verwaltung
- **Important Entities** IE: reaktive Prüfung
  - Digital Providers, Post&Kurierdienste, Abfallverwertung, Herstellung, Chemie, Food

Anforderungen

Ex-territoriale Anwendbarkeit für CH (indirekt)

- Governance & Management Verantwortung
- Cybersecurity Risikomanagement
  - Inkl. Supply Chain Security
- Striktes Incident Reporting
- Strengere Aufsicht und Bussen
  - EE: Bis 10 MEUR oder 2% globaler Umsatz
  - IE: bis 7 MEUR oder 1.4% globaler Umsatz

Cybersecurity Regulierung EUROPA

EU CRA (cyber resilience act)

- **Sicherheit von Produkten** (Hardware, Software) “mit digitalen Elementen” durch Haftung der Hersteller
- Anwendbarkeit: alle Produkte, die **in der EU vertrieben** werden (verkauft, angeboten)
- **PDE** (products with digital elements): jedes System mit einer direkten oder indirekten Verbindung zu anderen Systemen oder Netzwerken
- **Kategorien** der Kritikalität
  - **Default** (grösster Teil der Produkte, not high-risk)
  - **Important** (Produkte mit kritischen Funktionen, zB Netzwerkgeräte, OS, SIEM)
  - **Critical** (Subset von “Important” mit höchstem Risiko, zB HSM)
- Nicht anwendbar auf bereits anderweitig abgedeckte Produktkategorie (zB medizinische Geräte, Automobile) oder SaaS
- Inkraftsetzung: Dezember 2024, Reporting Pflicht: September 2026, “full encorcement” Dezember 2027

Anforderungen

- Secure by Design & Default
- Mandatory Vulnerability Handling
- Strict 24-hour reporting duty
- Transparenz & Dokumentation
- Konformitäts-Assessment & CE Markierung
  - Self-assessment für “Default”
  - Unabhängige Prüfung für “Important” und “Critical”

- **Bussen**
  - High Tier: Bis 15 MEUR oder 2.5% globaler Jahresumsatz
  - Lower Tier: bis 10 MEUR oder 2% globaler Jahresumsatz, 5 MEUR oder 1% bei inkorrekter Information
  - Verkaufsverbot, Einschränkungen, verpflichtender Rückruf

Cybersecurity Regulierung SCHWEIZ

DSG (Datenschutzgesetz) und Verordnung

- Gilt für Bundesorgane und private Personen, schützt Persönlichkeitsrecht und Grundrecht via PII-Bearbeitung
  - Personendaten, besonders schützenswerte Personendaten; Profiling und Profiling mit hohem Risiko
- **Zweckbindung**, Richtigkeit,
  freiwillige Einwilligung (informed consent) – ausdrücklich bei Profiling (Behörde), Profiling mit hohem Risiko (Private) und Bearbeitung bes. schützenswerter PII
- **Datenschutz durch Technik** (privacy by design) und datenschutzfreundliche Voreinstellungen (privacy by default)
- **Datensicherheit**; **Auftragsdatenbearbeitung**
- Datenschutzberater (Private: optional)
- **Verzeichnis der Bearbeitungstätigkeiten** (ROPA records of processing activities)
  - **Datenschutz-Folgenabschätzung** (DPIA data privacy impact assessment)
- **Bekanntgabe ins Ausland** geregelt
- **Meldepflicht** von Verletzungen der Datensicherheit
- **Auskunftsrecht**, Recht auf Datenherausgabe, Lösch-recht (right to be forgotten)

ISG (Informationssicherheitsgesetz) und Verordnung

- Anwendbarkeit: kritische Infrastrukturen
- Pflicht zur **Meldung von Cyberattacken**: seit 01.04.2025
- Bussen werden ab 01.10.2025 durchgesetzt (bis 100k CHF)
- Anwendbarkeit neben KRITIS v.a. Bundesorgane, Armee, Kantonale Verwaltung und -Organisationen

Ferner / geplant:

- **FINMA** – Finanzmarktaufsicht: Rundschreiben
  - Operationelle Risiken, Outsourcing, Meldepflicht Cyberattacken
- Büpf/Vüpf (Bundesgesetz zur Überwachung Post/Fernmeldeverkehr)
- NDG (Nachrichtendienstgesetz)
- Geplant: CRA – **Sicherheitsanforderungen für Produkte** mit digitalen Elementen (Stand Oktober 2025)

AI Governance

EU AI Act

Risikobasierter Ansatz; teilt AI-Systeme in 4 Kategorien ein:

- Unacceptable risk (prohibited)
- High-risk (heavily regulated)
  - Conformity assessments
  - FRIA (fundamental rights impact assessment)
  - Inherent high-risk sectors: KRITIS, education, employment, law enforcement, border control
  - Incident reporting obligation
  - HITL human-in-the-loop
  - Input data quality; inform affected individuals
  - Technical documentation (training data, design choices, performance metrics, known limitations)
  - Accuracy, Robustness and Cybersecurity
- Limited risk (transparency obligation)
- Minimal risk (largely unregulated)

Weitere Instrumente für AI Governance

- NIST AI RMF risk management framework
- ISO 42001
- MITRE ATLAS (Adversarial Threat Landscape for AI Systems)
- OWASP Top10 LLM

OWASP Top10 LLM

LLM01:2025 Prompt Injection

LLM02:2025 Sensitive Information Disclosure

LLM03:2025 Supply Chain

LLM04:2025 Data and Model Poisoning

LLM05:2025 Improper Output Handling

LLM06:2025 Excessive Agency

LLM07:2025 System Prompt Leakage

LLM08:2025 Vector and Embedding Weaknesses

LLM09:2025 Misinformation

LLM10:2025 Unbounded Consumption

CYBERSECURITY

BASICS.INTERMEDIATE.EXPERT

Security Lifecycle™

PLAN	1	**Asset Inventory** HW, SW, Daten, IoT; Cloud Services, 3rd party AI Bonus-item: DFD Datenflussdiagramm(e)	Daten bestimmen den “Schutzbedarf” in Schritt 2 >> Rest ist “Mittel zum Zweck”
	2	**Schutzbedarf** CIA+N Anforderungen: legal/regulatory/contractual; betrieblich (Gewinn/Kosten)	Schutzbedarf wird beim “data owner” erhoben >> Aufgabe des Business (security requirements)
	3	**Risikoanalyse** – quantitative oder qualitative; Bonus: Threat Modeling	Cyber-Risiken schwer zu quantifizieren (und schwer zu kommunizieren)
	4	**Sicherheitskonzept** – PPT / organisatorisch + technisch	Und wieviel kostet das???
DO	5	**Umsetzen** des Sicherheitskonzept	Lückenlose Umsetzung >> Asymmetrie der virtuellen Welt (1 Lücke = mögliche Katastrophe)
CHECK	6	**Prüfen** der Sicherheit	Scoping für Fortgeschrittene: Pentest oder Attack Sim?
ACT	7	Kontinuierliche Verbesserung – **KVP**	Die Findings aus dem security assessment erledigen sich nicht von selber

Cloud Security – Shared Responsibility (?)

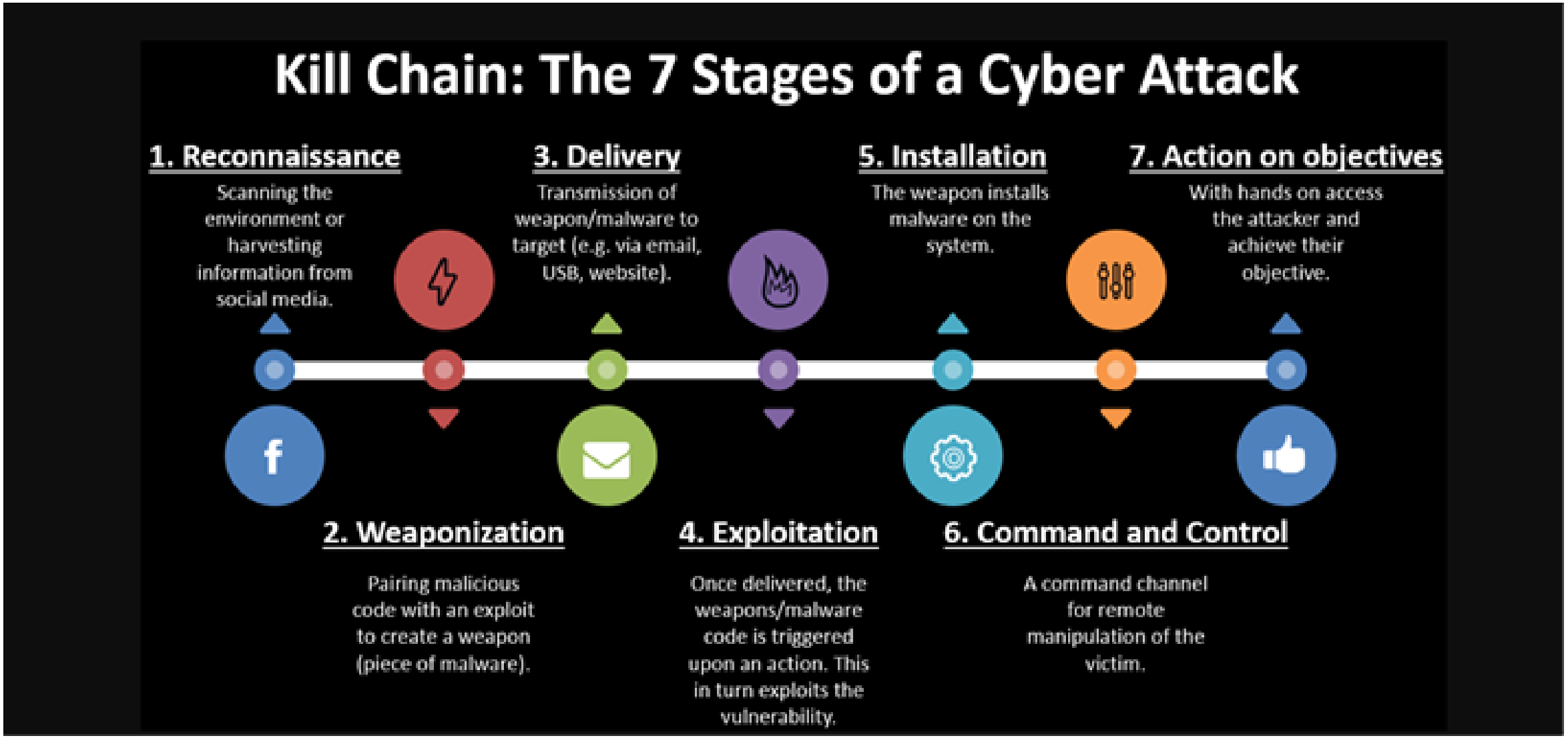
	IaaS	PaaS	SaaS
GRC			
Data Security			
Application Security			
Platform Security			
Infrastructure Security			
Physical Security			

Enterprise Responsibility

Shared Responsibility…

CSP Responsibility

Cyber Attacke – cyber kill chain



SECURITY INCIDENT RESPONSE

Vorbereitung

- Planung, Konzeption, Team-Aufbau (Training!)
- Tool-Bereitstellung, ggf. Externe Unterstützung (retainer)
- Baseline-Erstellung: Normalzustand definieren

Identifizierung

- Monitoring und Analyse von Events
- Triage, Bewertung und ggf. Alarmierung (trigger → playbook)

Eindämmung

- Kurzfristige Eindämmung
- Langfristige Eindämmung

Beseitigung

- Ursachen-Analyse
- Entfernung und Härtung

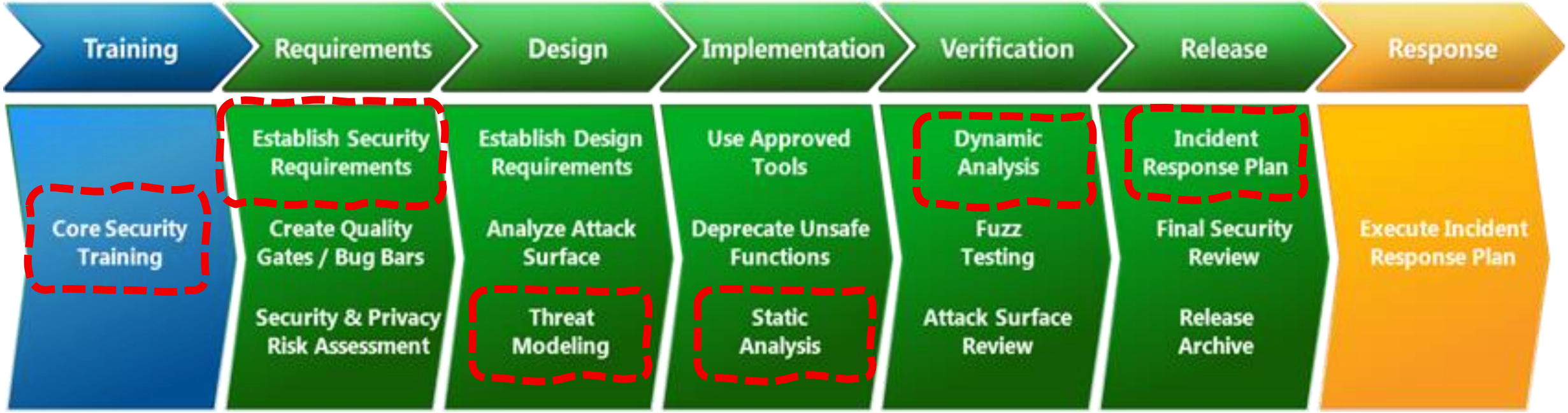
Wiederherstellung

- Validierung (ist wirklich alles “sauber”?)
- Wiederinbetriebnahme
- Ggf. Intensives Monitoring

Nachbereitung

- Post Incident Review (lessons learned)
- Dokumentation, Berichterstattung
- Optimierungsmassnahmen einleiten

SDL – secure development lifecycle



expert.level

Security by Design

Access & Control Principles

- Least Privilege
- Separation of Duties
- Complete Mediation (Zero Trust)

Architecture & Structure

- Defense in Depth
- Minimize Attack Surface → Threat Modeling
- Economy of mechanism (keep it simple)

Resilience & Defaults

- Secure defaults
- Fail safe (open), fail secure (closed)

Philosophy & Usability

- Open design (Kerckhoff's Principle)
- Psychological Acceptability

→ shift left: security requirements before security testing

Privacy by Design

7 Foundational Principles

- Proactive not reactive, preventative not remedial
- Privacy as the default setting
- Privacy embedded into design
- Full functionality – positive-sum, not zero-sum
- End-to-end security – full lifecycle protection
- Visibility and transparency – keep it open
- Respect for user privacy – keep it user-centric

WIE WEITER?

IKT MINIMALSTANDARD → NIST CSF V2.0

GOVERN

- Organizational Context
- Risk Management Strategy
- Roles, Responsibilities, and Authorities
- Policy
- Oversight
- Cybersecurity Supply Chain Risk Management

IDENTIFY

- Asset Management
- Risk Assessment
- Improvement

PROTECT

- Identity Management, Authentication, and Access Control
- Awareness and Training
- Data Security
- Platform Security
- Technology Infrastructure Resilience

DETECT

- Continuous Monitoring
- Adverse Event Analysis

RESPOND

- Incident Management
- Incident Analysis
- Incident Response Reporting and Communication
- Incident Mitigation

RECOVER

- Incident Recovery Plan Execution
- Incident Recovery Communication

KEY TAKEAWAYS

- **Good Governance**
  - Govern = Riskmanagement + Compliance
  - Compliance = treat as any other risk
    - Monitor legislative developments!
  - Board-level engagement and governance
- **PPT** People, Process, Technology
- **PRMFA** phishing-resistant MFA
- Asset **Inventory**
- **Vulnerability Management**, Patch Management, **Exception Management**
  - **Incident-Response** Fähigkeiten
- Adäquates **Risikomanagement**
  - Auf Basis eines _lückenlosen_ Grundschutzes!
- **Mindset** und Kultur
  - Rollenvorbilder, tone from the top
  - Regelmässige und aktuelle Awareness-Trainings
- **Testen der Sicherheit**
  - Applikationen und Systeme (Prio1: alles, was exponiert ist oder eine Schnittstelle hat)
  - Mitarbeitende
  - Kunden, Lieferanten, Geschäftspartner: TPRM third-party risk management, SCS supply-chain security
  - Gesamtes Unternehmen, Infrastruktur: attack simulation, red team exercise

Danke!

Umberto Annino

Security Evangelist

umbi@umbi.com