FFHS
Fernfachhochschule Schweiz
Mitglied der SUPSI

Basics.Baseline.Security

Without a foundation, every house collapses.

Umberto Annino, Security Evangelist

GoHack 2025, 08.11.2025, FFHS Gleisarena, Zürich

Maturity Levels of Information Security

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

The Chaos

Baseline Security

Risk-Based Security

Resilient Security

HowTo Information/ICT/Cyber Security

PLAN	1	**Asset Inventory** HW, SW, Daten, IoT; Cloud Services, 3rd party AI	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
ACT	7	Kontinuierliche Verbesserung – **KVP**	Die Findings aus dem security assessment erledigen sich nicht von selber

Basics.Baseline.Security

- Good Governance → CISO
  - Risk Management
  - ISMS
  - Exception Management
- PPT – People (first), Process, Technology
- (PR)MFA – no exceptions!
- Asset Inventory
  - Including: Cloud Services, AI Tools, TPRM/SCS, DFD, SBOM
- VuMa/PaMa
- Baseline Security (ISO, NIST, IKT-Minimalstandard, SoGP, CIS; just do it.)
- Test ALL THE THINGS
  - Applications, Endpoints, Networks, Companies, 3rd parties
- Plan, Do, Check, Act (!)
- BCM, DR, (DF)IR
  - Just have a plan ready!
- Mindset: “towards Zero Trust”

The 4 Horsemen of the Cyber Apocalypse

- Lacking Comprehensive and up-to-date asset inventory
  - Because it's super boring
  - Details missing, and what's in it for me, anyway?
- Inadequate Identity and Access Management
  - Including PIM/PAM/PUM Privileged Identity/Access/User Management
- No or superficial 3rd party risk/security management, control and oversight
  - SDLC and SBOM? It's from <insert renowned companyname here>, so it will surely be safe?
  - (3rd party) AI Governance, anyone?
- Compliance-only security
  check the box, remove the blox!

Thank You!

Umberto Annino, Security Evangelist; Eidg. Dipl. ICT-Security Expert

NDS FH Exec. Quality Management, CISSP, ISSAP, ISSMP, ISSEP, CSSLP, CCSP, HCISPP, CCSK v5, CCZT, CCAK, CISA, AAIA, CISM, AAISM, CRISC, CGEIT, CIPP/E, CIPT, CIPM, CDPSE, GRCP, GRCA, IDPP, IPMP, IAAP, IRMP, ICEP, IAIP

Dozent FFHS

umberto.annino@ffhs.ch

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