
SBA
Research

SBA Research

Sicherheitsforschungszentrum.

Mission: Bindeglied zwischen **Forschung & Wirtschaft**

- Größtes Forschungszentrum in Österreich mit **ausschließlichem Fokus auf Informationssicherheit**
- 2006 gegründet – ca. 140 Mitarbeiter:innen

USP: 2 Welten unter 1 Dach

- Angewandte **Sicherheitsforschung**
  - **COMET** Kompetenzzentrum
- Kommerzielle **Sicherheitsdienstleistungen**

SBA Research
Professional Services

Security Governance

- Security Governance Lagebild
- ISMS / ISO 27001
- Compliance (NIS-2, CRA, DORA, etc.)
- Risikomanagement & Business-Impact
- Audit & Beratung

Cyber Defense

- Cyber Security Lagebild
- Penetrationstests (Infrastruktur, Cloud, Netzwerk)
- Red/Blue/Purple Teaming
- Social Engineering & Phishing
- SWIFT CSP Audit

Security Schulungen

- Security Awareness
- Hacking & Defense (Web, Windows, IoT)
- Secure Coding & Application Security
- Cloud & Cloud-Native Security
- Zertifizierungsvorbereitung

Software Security

- Sicherer Software-entwicklungsprozess
- Threat Modeling & Architekturreviews
- Application & Mobile App Pentesting
- Quellcode-Audit
- CI/CD Audit

https://www.sba-research.org/professional-services/

whoami

- **Stefan Jakoubi**
  Geschäftsleitung Professional Services, CISO

- 19 Jahre im **InfoSec** Umfeld tätig
  - Security Governance & Compliance
  - ISO27001 Lead Auditor, QuaSte Prüfer,…

- SBA Research **CISO**
  - Professional Services ISO27001 zertifiziert

whoami

- **Mathias Tausig**

- Technical **IT Security Consultant** at SBA Research
  - Penetration testing, SDLC, Cloud Security, Threat Modeling, …

- Formerly SysAdmin, Developer, Security Officer, University teacher

CRA, ASVS & SAMM

3 Abkürzungen mit Schlagkraft

Bundesministerium Innovation, Mobilität und Infrastruktur
Bundesministerium Wirtschaft, Energie und Tourismus
FFG Forschung wirkt.
wirtschaftsagentur wien
Für die Stadt Wien
European Commission
FWF Österreichischer Wissenschaftsfonds
netidee FÖRDERUNGEN

CRA

197415/EU XXVII. GP
Eingelangt am 25/09/24

EUROPÄISCHE UNION

DAS EUROPÄISCHE PARLAMENT — DER RAT

Brüssel, den 25. September 2024
(OR. en)

2022/0272(COD) — PE-CONS 100/23

CYBER 328
JAI 1731
DATAPROTECT 391
TELECOM 409
MI 1168
CSC 579
CSCI 215
CODEC 2601

GESETZGEBUNGSAKTE UND ANDERE RECHTSINSTRUMENTE

Betr.: VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung)

Erwägungsgrund 1 der VO

Dabei sollten **zwei große Probleme angegangen werden, die hohe Kosten für die Nutzer und die Gesellschaft** verursachen:

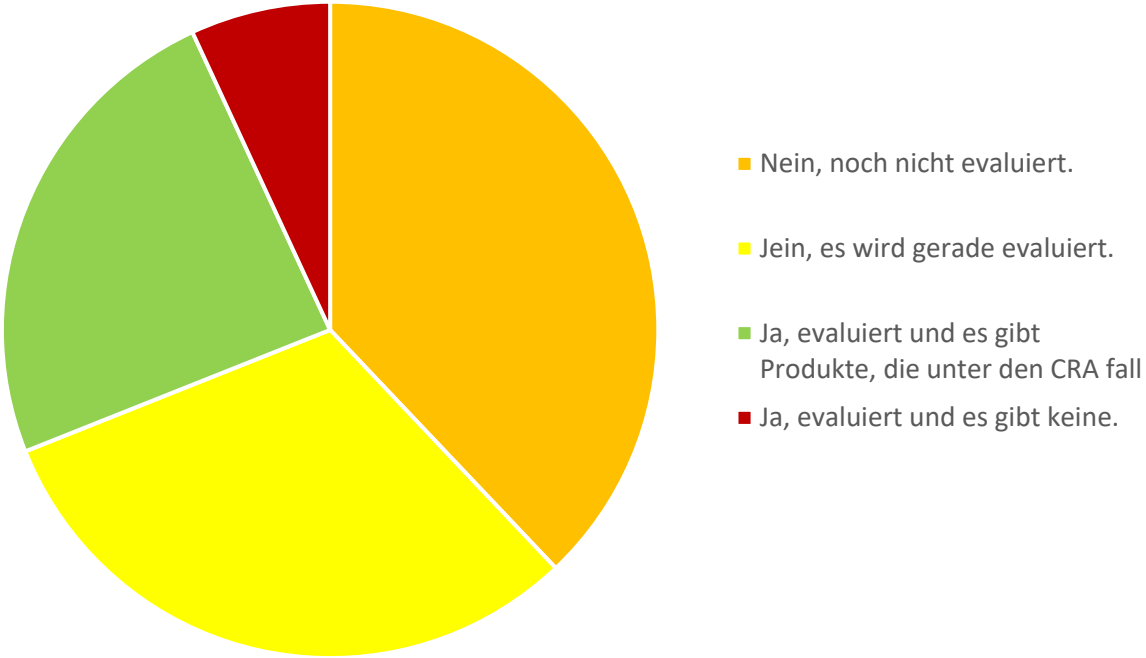
- ein **geringes Maß an Cybersicherheit von Produkten mit digitalen Elementen,** das sich in **weitverbreiteten** Schwachstellen und der unzureichenden und **inkohärenten Bereitstellung von Sicherheitsaktualisierungen** zu deren Behebung zeigt**,**
- sowie ein unzureichendes Verständnis und ein mangelnder Informationszugang der Nutzer, wodurch sie daran gehindert werden, **Produkte mit angemessenen Cybersicherheitsmerkmalen auszuwählen** oder sicher zu verwenden.

Timeline des Cyber Resilience Acts (CRA)

- **2024**: VO ist in Kraft getreten
  - Ergänzende Normen bis 2027 in Erarbeitung
- **Volle Geltung:** Winter 2027

- **Aktueller Stand der Unternehmen: „Findungsphase“**

Umfrage CRA-Webinar



Wer ist betroffen?

- **„Wirtschaftsakteure“ =** Hersteller; Bevollmächtigte; Einführer; Händler;
  Verwalter quelloffener Software

- **Keine Ausnahmen für KMU - lediglich „Erleichterungen“** (Leitfäden/Anleitungen, vereinfachte Dokumentationspflichten, …)

Was ist betroffen?

- **„Produkte mit digitalen Elementen“** = Software, Hardware – ohne Unterscheidung ob High-End System aus der Industrie, Heimelektronik oder Spielzeug
- **Wenn Datenverbindungen zu anderen Geräten oder zu Netzen/Informationssystemen technisch möglich** (auch wenn Produkte nur „offline“ betrieben werden)
- **Wenn Produkte innerhalb der EU** mit Gewinnerzielungsabsicht im Rahmen einer Geschäftstätigkeit am Markt **bereitgestellt werden (Open Source)**

- **Während des gesamten Lebenszyklus des Produkts** (idR 5 Jahre – oder auch länger)

Was ist nicht betroffen?

- **Open Source Software** (wenn keine Gewinnerzielungsabsicht)
- **SaaS, Cloudsysteme** (wenn nicht Bestandteil eines vernetzten Produktes)
- **Produktgruppen, die durch andere Vorschriften reguliert werden** (Zivile Luftfahrt, KfZ-Bauteile, Schiffsausrüstung, Medizinprodukte, In-Vitro-Diagnostika)
- **„Produkte“ mit Bezug zu nationaler Sicherheit/Verteidigung oder öffentlicher Verwaltung/Behörden**
- **Produkte, für die aufgrund sektorenspezifischer Rechtsakte** ein gleichwertiges oder höheres Sicherheitsniveau vorgeschrieben wird
- **Ersatzteile für Produkte**, die vor Gültigkeit der Verordnung in Verkehr sind

ANHANG I

GRUNDLEGENDE CYBERSECURITYANFORDERUNGEN

Teil I Cybersicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen

(1) Produkte mit digitalen Elementen werden so konzipiert, entwickelt und hergestellt, dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten.

(2) Auf der Grundlage der Bewertung [Risikobewertung/Threat Modelling] digitalen Elementen, soweit zutreffend,

a) ohne bekannte ausnutzbare Schwachstellen auf dem Markt bereitgestellt werden,

b) mit einer sicheren Standardkonfigur[„secure by default“] dem gewerblichen Nutzer in Bezug auf ein abgeschneidertes Produkt mit digitalen Elementen nichts anderes vereinbart wurde, und die Möglichkeit bieten, das Produkt in seinen ursprünglichen Zustand zurückzusetzen,

c) sicherstellen, dass Schwachstellen durch Sicherheitsaktualisierungen behoben werden können, gegebenenfalls auch durch automatische Sicherheitsaktualisierungen [Sicherheitsupdates] installiert werden sowie über einen klaren und benutzerfreundlichen Opt-out-Mechanismus verfügen, über dem die Nutzer über verfügbare Aktualisierungen informiert werden und sie vorübergehend verschieben können;

d) durch geeignete Kontrollmechanismen Schutz vor unbefugtem Zugriff bieten, darunter u. a. zumindest Authentifizierungs-, Identitäts- oder Zugangsverwaltungssysteme, und einen möglicherweise unbefugten Zugriff melden,

e) die Vertraulichkeit gespeicherter, übermittelter oder anderweitig verarbeiteter personenbezogener oder sonstiger Daten schützen, z. B. durch Verschlüsselung relevanter Daten, die gespeichert sind oder gerade verwendet oder übermittelt werden, durch modernste Mechanismen und durch den Einsatz anderer technischer Mittel,

f) die Integrität gespeicherter, übermittelter oder anderweitig verarbeiteter Daten, ob personenbezogener oder sonstiger Daten, Befehle, Programme und Konfigurationen vor einer vom Nutzer nicht genehmigten Manipulation oder Veränderung schützen und deren Beschädigung melden,

g) die Verarbeitung personenbezogener oder sonstiger Daten auf solche, die angemessen und von Bedeutung sind, und auf das für die Zwe[Datenschutz/Datenminimierung] Maß beschränken („Datenminimierung“);

h) die Verfügbarkeit wesentlicher und grundlegender Funktionen, auch nach einem Sicherheitsvorfall, einschließlich über Abwehr- und Eindämmungsmaßnahmen gegen Überlastungsangriffe auf Server (Denial-of-Service-Angriffe), sicherstellen,

i) die negativen Auswirkungen von den Produkten selbst oder von vernetzten Geräten auf die Verfügbarkeit der von anderen Geräten oder Netzen bereitgestellten Dienste minimieren,

j) so konzipiert, entwickelt und hergestellt werden, dass sie — auch bei externen Schnittstellen — möglichst geringe Angriffsflächen bieten,

k) so konzipiert, entwickelt und hergestellt werden, dass die Auswirkungen eines Sicherheitsvorfalls durch geeignete Mechanismen und Techniken zur Minderung der möglichen Ausnutzung verringert werden,

l) sicherheitsbezogene Informationen durch Aufzeichnung und/oder Überwachung einschlägiger interner Vorgänge wie Zugang zu Daten, Diensten oder Funktionen und Änderungen daran bereitstellen und den Nutzern einen Opt-out-Mechanismus zur Verfügung stellen,

m) den Nutzern die Möglichkei[Datenschutz/Löschung/Portierbarkeit] wenn diese Daten auf andere Pro[illegible]Weise geschieht.

Teil II Anforderungen an die Behandlung von Schwachstellen

Die Hersteller von Produkten mit digitalen Elementen müssen

(1) Schwachstellen und [SBOM] digitalen Elementen ermitteln und dokumentieren, u. a. durch Erstellung einer Software-Stückliste[illegible]baren Format, aus der zumindest die obersten Abhängigkeiten der Produkte hervorgehen;

(2) im Hinblick auf die Risiken im Zusammenhang mit den Produkten mit digitalen Elementen unverzüglich Schwachstellen behandeln und beheben, unter anderem durch Bereitstellung von Sicherheitsaktualisierungen; soweit technisch machbar, müssen neue Sicherheitsaktualisierungen getrennt von den Funktionsaktualisierungen bereitgestellt werden;

(3) die Sicherheit des Produkts mit digitalen Elementen regelmäßig und wir[Pentests]

(4) sobald eine Sicherheitsaktualisierung bereitgestellt worden ist, Informationen über beseitigte Schwachstellen teilen und veröffentlichen, einschließlich einer Beschreibung der Schwachstellen mit Angaben, anhand deren die Nutzer das betroffene Produkt mit digitalen Eleme[Veröffentlichung]hen, sowie eindeutige und verständliche Informationen[illegible]ründeten Fällen, in denen die Hersteller der Auffassung sind, dass die Risiken der Veröffentlichung die Vorteile in Bezug auf die Sicherheit überwiegen, können sie die Veröffentlichung von Informationen über eine behobene Schwachstelle so lange aufschieben, bis den Nutzern die Möglichkeit gegeben wurde, den entsprechenden Patch anzuwenden;

(5) eine Strategie für die koordinierte Offenlegung von Schwachstellen aufstellen und umsetzen;

(6) Maßnahmen ergreifen, um den Austausch von Informationen über mögliche Schwachstellen in ihrem Produkt mit digitalen Elementen und darin enthaltenen Komponenten Dritter zu erleichtern, und dazu u. a. eine Kontaktadresse für die Meldung der in dem Produkt mit digitalen Elementen entdeckten Schwachstellen angeben;

(7) Mechanismen für die sichere Verbreitung von Aktualisierungen für P[mehr Sicherheitsupdates]mit digitalen Elementen bereitstellen, damit Schwachstellen rechtzeitig und im Falle von Sicherheitsaktualisierungen g[illegible]omatisch behoben oder eingedämmt werden;

(8) dafür sorgen, dass Sicherheitsaktualisierungen, die zur Bewältigung festgestellter Sicherheitsp[noch mehr Sicherheitsupdates]fügung stehen, unverzüglich u[illegible]Bezug auf ein mab[illegible]dukt mit digitalen [illegible]werden, zusammen mit Hin[illegible] einschlägigen Informationen, auch über zu treffende mögliche Maßnahmen.

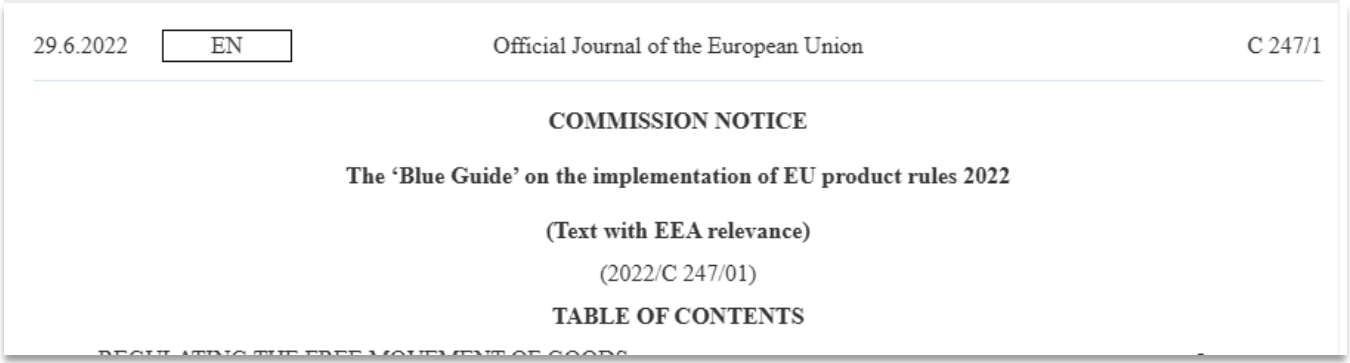
https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32024R2847

14 Requirements

8 Requirements

CRA = Konformitätsbewertung!

No CE-Mark – No EU-Market!



29.6.2022 EN Official Journal of the European Union C 247/1

COMMISSION NOTICE

The 'Blue Guide' on the implementation of EU product rules 2022

(Text with EEA relevance)

(2022/C 247/01)

TABLE OF CONTENTS

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022XC0629%2804%29&qid=1747224321757

90% aller Produkte

10% aller Produkte*

* https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-political-agreement-cyber-resilience-act

Selbstbewertung der Konformität in Eigenverantwortung über risiko-basierten Ansatz.

Standard	Wichtig Klasse I	Wichtig Klasse II	Kritisch
Interne Fertigungskontrolle in Eigenverantwortung auf Basis einer	Selbstbewertung möglich nach standardisiertem Verfahren, **harmonisierten Normen** oder Schemata Konformitätsbewertung unter Beteiligung Dritter	Konformitätsbewertung unter Beteiligung Dritter (EU-Baumusterprüfung, interne Fertigungskontrolle, umfassende Qualitätskontrolle)	Konformitätsbewertung unter Beteiligung Dritter (europäisches Schema für die Cybersicherheitszertifizierung oder eines der Verfahren für Kl. II)
Alle Produkte, die nicht unter eine höhere Kategorie fallen	19 Produktgruppen	4 Produktgruppen	dzt. 3 Produktgruppen
	zB Browser, Passwortmanager, SIEM, VPN, Router, Modems, Switches, Netzwerkmonitore, „Virtuelle Assistenten“, Smart-Home-Devices, Wearables	zB Firewalls/IDS/IPS, Virtualisierungsumgebungen	Hardwaregeräte mit Sicherheitsboxen; Smart-Meter-Gateways in intelligenten Messsystemen; Chipkarten oder ähnliche Geräte

SBA Research, 2025

Non-Compliance

- „Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein."

- **Mangelnde Sicherheit (zB wegen fehlender Updates) = mangelhaftes Produkt** = verschuldensunabhängige Haftung (vgl. PLD – Produkthaftungs-Richtline)

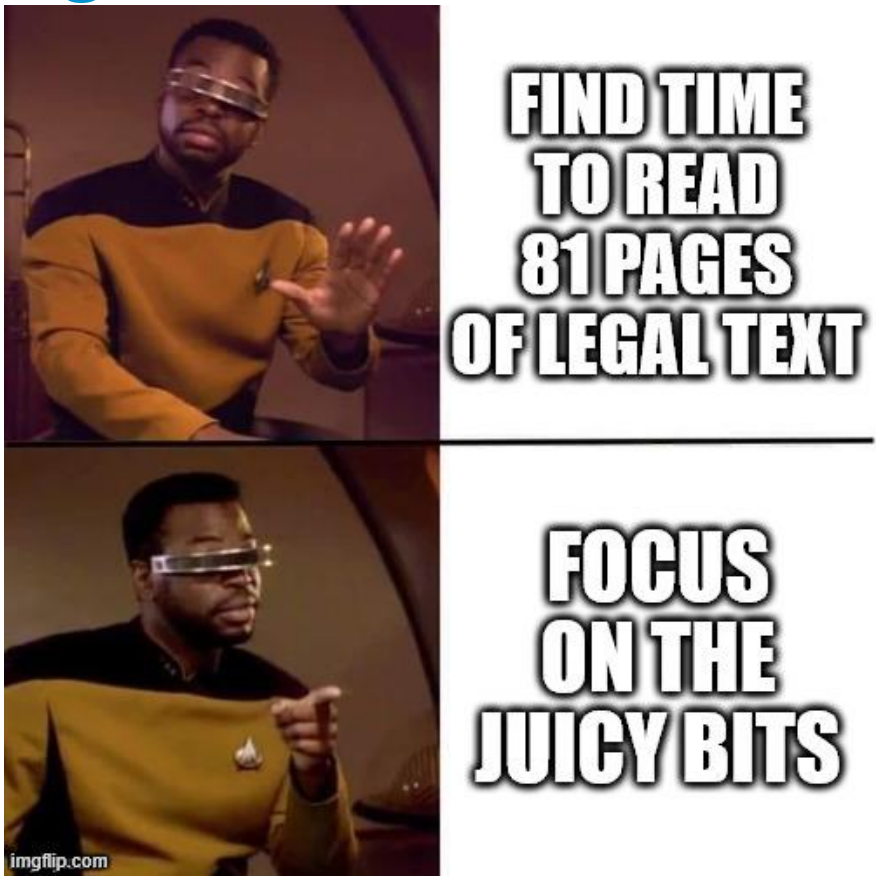
- Je nach Verstoß - Geldbußen von bis zu 15 000 000 EUR oder von bis zu 2,5 % des gesamten weltweiten Jahresumsatzes – je nachdem was höher ist.
  - Bemessung der Strafhöhe nach: Schwere des Verstoßes; ob es bereits Strafen wegen eines ähnlichen Verstoßes gegeben hat; nach Größe und Marktanteil des Unternehmens (als Erleichterung für KMU)

Was tun?

Umsetzung

(Sie haben den rechtlichen Teil vorerst überstanden)

Legalese for Engineers

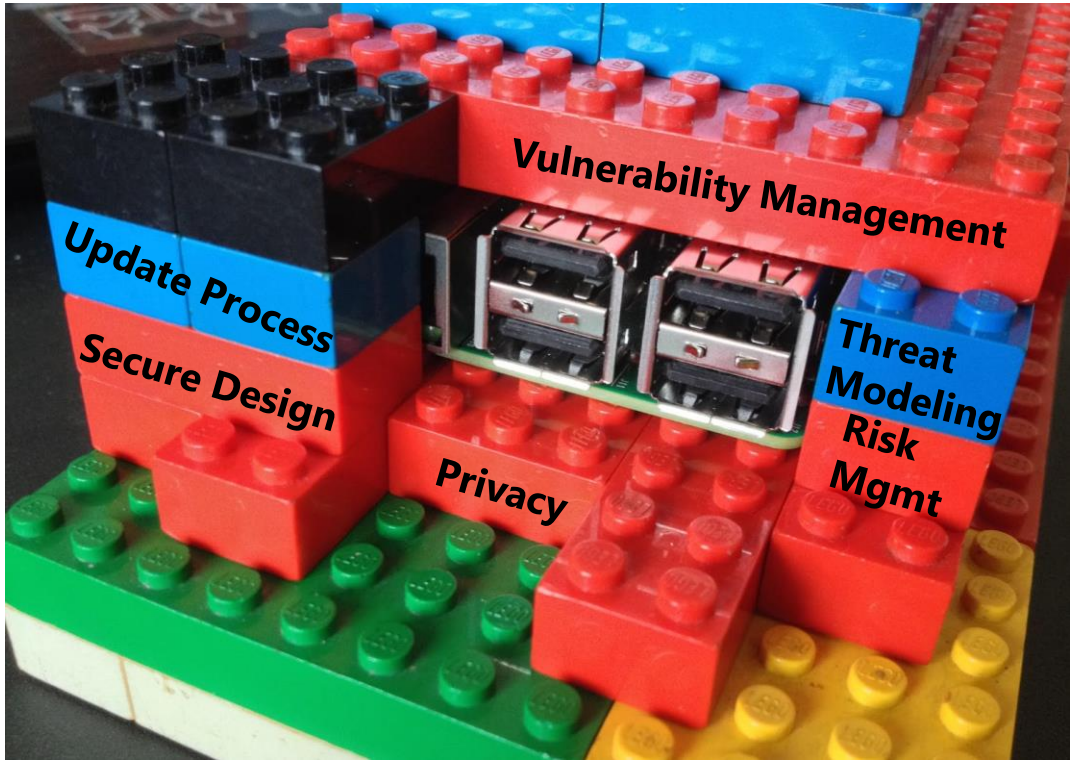


Legalese for Engineers

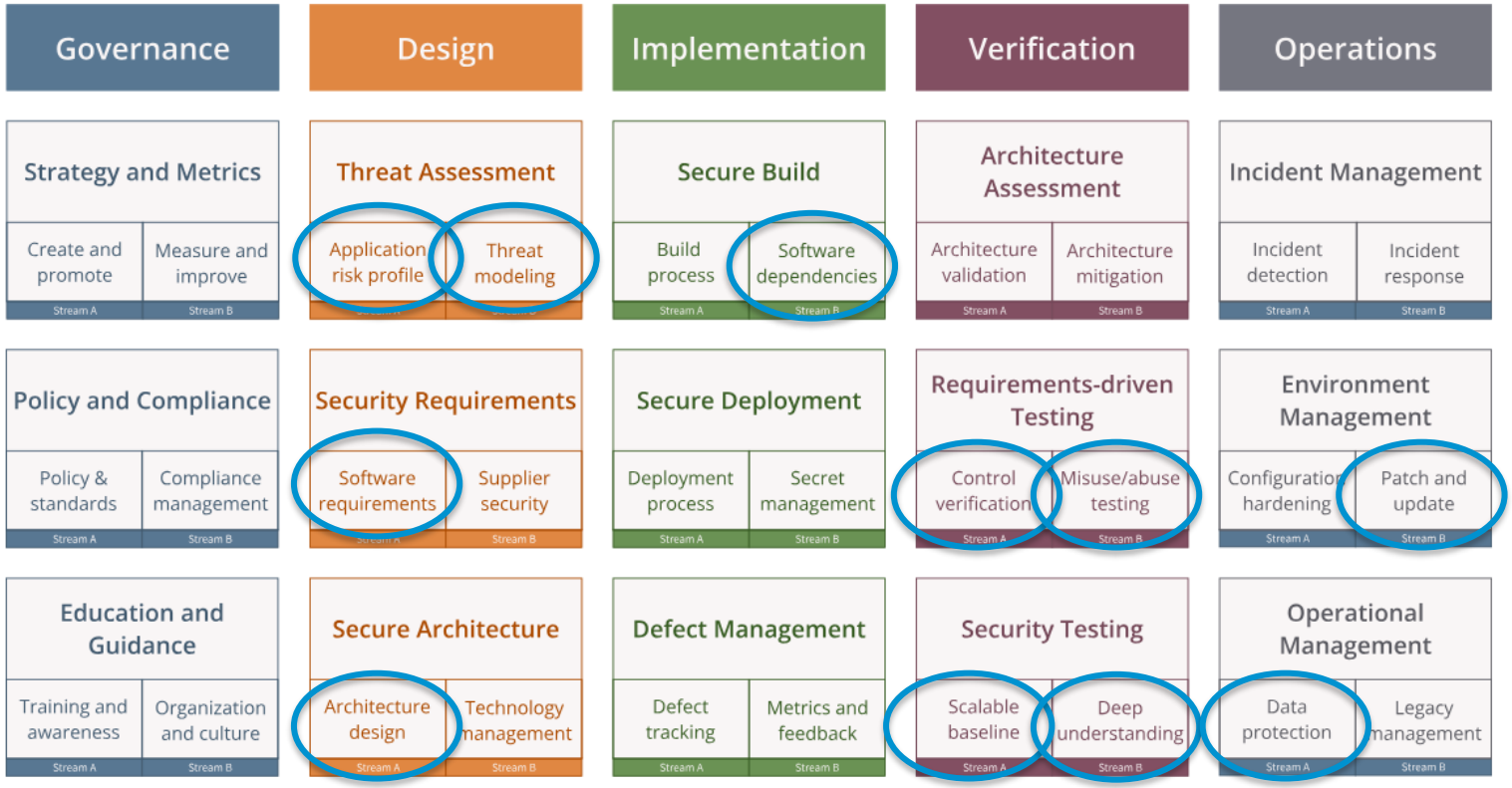
Wo beginnen?

- Am besten direkt zum Anhang springen
  - ANNEX I: ESSENTIAL CYBERSECURITY REQUIREMENTS
  - ANNEX II: INFORMATION AND INSTRUCTIONS TO THE USER
- Das sind 3 Seiten, statt 81

Was macht ein sicheres Produkt aus?



TL;DR: SDLC FTW



https://owaspsamm.org

SDLC Maturity

Model | Design | Threat Assessment

The Threat Assessment (TA) practice focuses on identifying and understanding of project-level risks based on the functionality of the software being developed and characteristics of the runtime environment. From details about threats and likely attacks against each project, the organization as a whole operates more effectively through better decisions about prioritization of initiatives for security. Additionally, decisions for risk acceptance are more informed, therefore better aligned to the business.

By starting with simple threat models and building application risk profiles, an organization improves over time. Ultimately, a sophisticated organization would maintain this information in a way that is tightly coupled to the compensating factors and pass-through risks from external entities. This provides greater breadth of understanding for potential downstream impacts from security issues while keeping a close watch on the organization's current performance against known threats.

Maturity level		Stream A Application Risk Profile	Stream B Threat Modeling
1	Best-effort identification of high-level threats to the organization and individual projects.	A basic assessment of the application risk is performed to understand likelihood and impact of an attack.	Perform best-effort, risk-based threat modeling using brainstorming and existing diagrams with simple threat checklists.
2	Standardization and enterprise-wide analysis of software-related threats within the organization.	Understand the risk for all applications in the organization by centralizing the risk profile inventory for stakeholders.	Standardize threat modeling training, processes, and tools to scale across the organization.
3	Proactive improvement of threat coverage throughout the organization.	Periodically review application risk profiles at regular intervals to ensure accuracy and reflect current state.	Continuously optimization and automation of your threat modeling methodology.

https://owaspsamm.org/model/design/threat-assessment/

Output
Scoring

- **Was bekommt man?**
  - Eine quantitative Bewertung für alle Bereiche
  - Blinde Flecken so leicht zu identifizieren
- **Schlüsselergebnisse eines Assessment**
  - Status quo
  - Roadmap & Motivation für kurz- und langfristige Entwicklung
  - Wo soll ich anfangen?
  - Einfache Verbesserungen

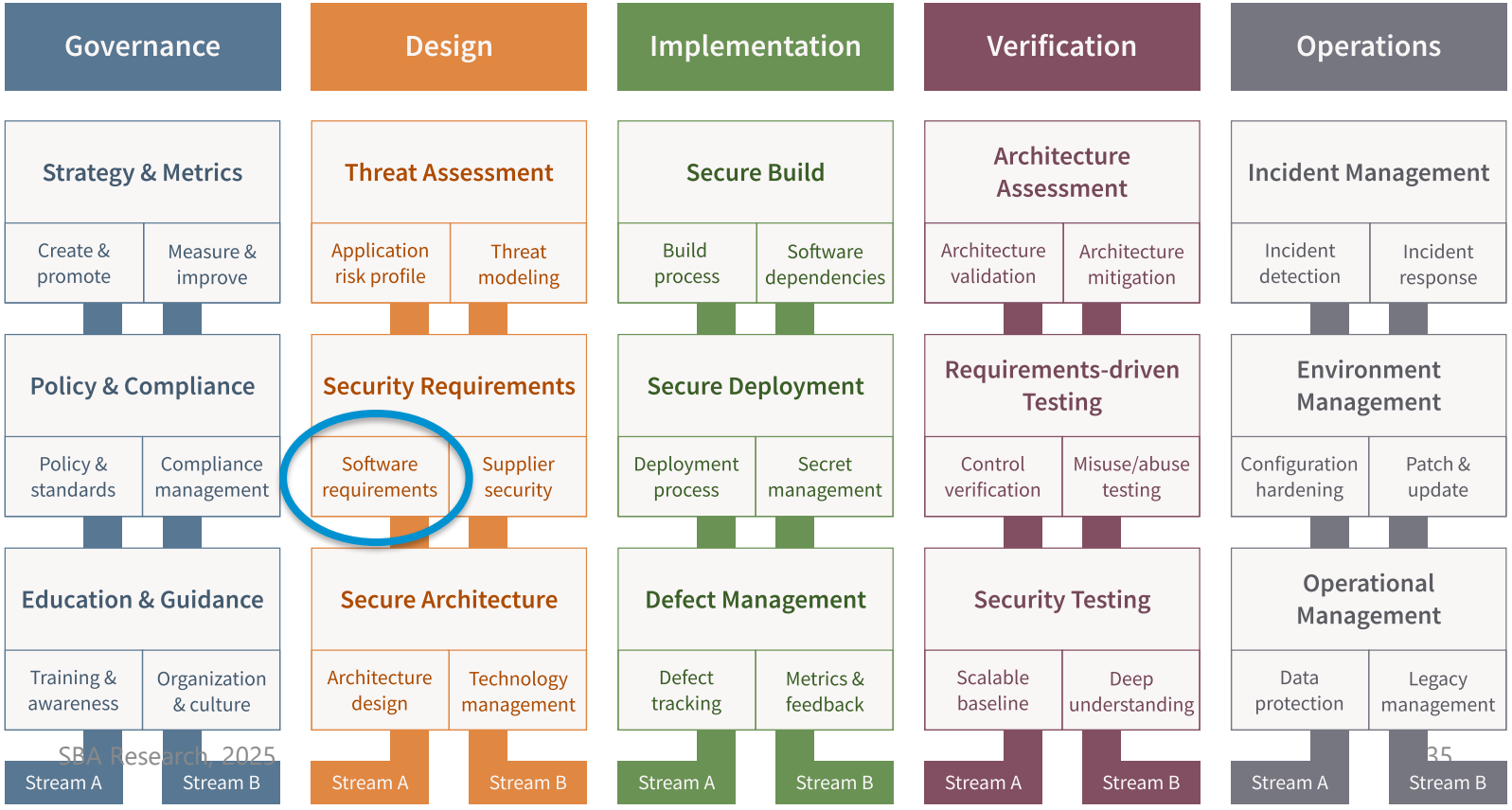
		Current Maturity Score			
			Maturity		
Functions	Security Practices	Current	1	2	3
Governance	Strategy & Metrics	0,63	0,25	0,25	0,13
Governance	Policy & Compliance	0,63	0,50	0,13	0,00
Governance	Education & Guidance	0,75	0,38	0,13	0,25
Design	Threat Assessment	0,50	0,25	0,25	0,00
Design	Security Requirements	0,25	0,25	0,00	0,00
Design	Secure Architecture	0,88	0,50	0,13	0,25
Implementation	Secure Build	1,88	1,00	0,63	0,25
Implementation	Secure Deployment	1,13	0,75	0,38	0,00
Implementation	Defect Management	0,63	0,63	0,00	0,00
Verification	Architecture Assessment	0,88	0,75	0,00	0,13
Verification	Requirements Testing	0,75	0,25	0,25	0,25
Verification	Security Testing	1,50	0,75	0,50	0,25
Operations	Incident Management	0,13	0,13	0,00	0,00
Operations	Environment Management	0,50	0,38	0,13	0,00
Operations	Operational Management	1,25	1,00	0,13	0,13

Durchführung

- Interview
- Fertiger Fragebogen
- ~ 1 Tag
- Externe Experten führen das Interview
- Oder interne Security Champions etc.
    - Hoher Selbstlerneffekt

OWASP SAMM

Königsdisziplin: Requirements



Quellen für Security Requirements

- Verträge
- Compliance Anforderungen
- Interne Policies
- Ergebnisse von Pentest, Threat Modeling, …
- Standards (ASVS)
- Vergangene Incidents
- Erfahrungen aus anderen Teams

OWASP ASVS

- V1 Encoding and Sanitization
- V2 Validation and Business Logic
- V3 Web Frontend Security
- V4 API and Web Service
- V5 File Handling
- V6 Authentication
- V7 Session Management
- V8 Authorization
- V9 Self-contained Tokens
- V10 OAuth and OIDC
- V11 Cryptography
- V12 Secure Communication
- V13 Configuration
- V14 Data Protection
- V15 Secure Coding and Architecture
- V16 Security Logging and Error Handling
- V17 WebRTC

https://raw.githubusercontent.com/OWASP/ASVS/v5.0.0/5.0/OWASP_Application_Security_Verification_Standard_5.0.0_en.pdf

OWASP ASVS

V6.2 Password Security

The requirements in this section mostly relate to § 5.1.1.2 of NIST's Guidance.

#	Description	Level
6.2.7	Verify that "paste" functionality, browser password helpers, and external password managers are permitted.	1
6.2.8	Verify that the application verifies the user's password exactly as received from the user, without any modifications such as truncation or case transformation.	1
6.2.9	Verify that passwords of at least 64 characters are permitted.	2
6.2.10	Verify that a user's password stays valid until it is discovered to be compromised or the user rotates it. The application must not require periodic credential rotation.	2

DIE 3 zum Mitnehmen

1. **Produktklassen erheben** – (CRA ANHANG III) inkl. Bonusfrage: „ist es ein Produkt??“

2. **SDLC etablieren / SAMM Assessment durchführen** – Best Practices folgen

3. **Vorbereitet sein** – für alle Eventualitäten

Stefan Jakoubi
Mathias Tausig

SBA Research
Floragasse 7, 1040 Wien
sjakoubi@sba-research.org
mtausig@sba-research.org

Bundesministerium Innovation, Mobilität und Infrastruktur
Bundesministerium Wirtschaft, Energie und Tourismus
FFG Forschung wirkt.
wirtschaftsagentur wien
Für die Stadt Wien
European Commission
FWF Österreichischer Wissenschaftsfonds
netidee FÖRDERUNGEN