8 Security by Design

Standard Warenkorb für Hardware benötigt

- Bei Abweichung vom Standard muss Genehmigungprozess (inkl. Security Check) druchgeführt werden

Strategie für Softwareentwicklung

- Interne Entwicklung
  - hohe Flexibilität
  - Volle Verantwortung für evtl. Risiken
- Outsourced Development
  - Ähnlich wie interne Entwicklung
  - Teilverantwortung kann ausgelagert werden
  - Risiko und Kosten bleiben erhalten
- Software Anpassung
  - Nutzung von Standard Produkten (gebunden an Produkte)
  - Verantwortlich für Sicherheitsqualität
  - Verantwortung für Risiko jeglicher Anpassung bleibt erhalten
- Stick to the Standards
  - Software Produkt definiert Funktionalität
  - Nutzung von Standard-Konfiguration

Secure Codig Guidelines

- OWASP
- .NET
- Java SE
- NIST

➡️ Test Tools

Ansätze nach OWASP:

- Input Validation
- Output Encoding
- Authentication and Password Management
- Session Management
- Access Contro
- Cryptographic Practices
- Error Handling and Logging
- Data Protection
- Communication Security
- System Configuration
- Database Security
- File Management
- Memory Management

Supplier Management und Auswirkung auf InfoSec (Outsourcing)

- Confidentiality
- Datenzugriff
  - Prozess Kenntnisse
- Integrity
  - Datenmanipulation
  - Falsche Verarbeitung
- Availability
  - Service nicht verfügbar
  - Auswirkung auch auf andere Services

Formen des Outsourcings

- Outtasking
  - Auslagerung einzelner konkreter Aufgaben
- Selektives Outsourcing
  - Spezielle Teile eines Bereichs auslagern
  - Ziel ist Wissenskompensation
- Übergangs-Outsourcing
  - temporäre Auslagerung
  - z.B. bei Prozess-/Technikwechsel
- Umfassendes Outsourcing
  - Auslagerung ganzer Unternehmensbereiche
  - beinhaltet auch Hardware
- End of Life Fertigung
  - Produkte/Dienstleistung mit wenig Nachfrage werden ausgelagert
- Application Service Providing
  - SaaS

Bewertung externer Dienstleister/Lieferanten

- Ratings
- Pentests
  - hoher Aufwand
- Audits
  - hoher Aufwand
- Quality Meetings