Was ist Cybersicherheit?

Cybersicherheit befasst sich mit dem Schutz der digitalen Abwicklung und Steuerung von Geschäftsprozessen. Durch die fortschreitende Vernetzung von IT-Infrastrukturen und dem Internet der Dinge (IoT) entstehen neue Risiken: Sowohl technische Systeme als auch deren Nutzer werden zunehmend zu potenziellen Angriffszielen. Auch Schatten-IT und Schatten-KI tragen zur Gefährdungslage bei und müssen in Sicherheitsstrategien berücksichtigt werden.

Unternehmen sind daher verpflichtet, ihre IT-Transaktionen sowie Kundendaten wirksam vor Sicherheitsverletzungen zu schützen. Dabei spielt das Pareto-Prinzip eine wichtige Rolle: Es besagt, dass bereits 20 % der Investitionen in Sicherheitsmaßnahmen bis zu 80 % der angestrebten Schutzwirkung erzielen können. So lässt sich ein wirtschaftlich effizienter Sicherheitsstandard realisieren

Zu den Kriterien, die es im Cyberraum zu schützen gilt, zählen:

- **Vertraulichkeit**: Nur Befugten den Zugang ermöglichen.

- **Integrität**: keine Veränderung der Nachrichten durch Dritte auf dem Transportweg.

- **Authentizität**: Nachweisbarkeit der Echtheit und Abstammung von Informationen.

- **Verfügbarkeit**: Gewährleistung der ständigen Verfügbarkeit des Netzwerks, bzw. der Leistungen.

Systematik der Bedrohungen:

- **Technische vs. nicht-technische**: Funkstörungen// Menschliche Fehler

- **beabsichtigte vs. nicht-beabsichtigte**: DOSA// Bedienungsfehler durch Mensch

- **aktive vs. passive**: Eingriff in ein Computersystem// Abhören der Kommunikation

Konkrete Sicherheitsmaßnahmen im Unternehmensumfeld?

- Aufbau eines VPN-Netzwerks
- Geeignete Firewall-Konfiguration (Paketfilter mit Firewall-Regeln)
- Verschlüsselung der Nachrichten durch gängige Sicherheitsprotokolle (SSH, RDP, TLS, ...)
- Mitarbeiterschulungen und Sensibilisierung

Welche Richtlinien sind von besonderer Relevanz?

Zur Unterstützung der Cybersicherheit und des Datenschutzes sind zahlreiche Gesetze und Richtlinien veröffentlicht worden. Dabei ist es wichtig zu berücksichtigen welche Institution deren Veröffentlichung verantwortet. Gesetze, die auf Ebene der europäischen Union veröffentlicht werden, sind bundesspezifischen Gesetzen übergeordnet. Gesetze, die auf Bundesebene verabschiedet werden, sind denen eines Bundeslandes vorzuziehen. Beispielsweise beschäftigen sich im Finanzwesen sowohl DORA (Digital Operational Resilience Act) als auch das IT-Sicherheitsgesetz 2.0 – zweiteres zumindest in seiner erweiterten Variante (UBI-Einstufung) – mit dem Thema Cybersicherheit. Da DORA auf europäischer Ebene gilt, müssen zunächst sämtliche Anforderungen dieser Verordnung umgesetzt sein.

- **Datenschutzrichtlinien**

DSGVO/ ISO-29100: Schutz von personenbezogenen Daten vor missbräuchlicher Verwendung und Verarbeitung im Unternehmensbereich. Regelungen zur Verwendung gelten unter Erlaubnisvorbehalt oder Gestattung. Anforderungen an Verantwortliche und Auftragsverarbeiter unter Festlegung von **TOMs** (technisch, organisatorische Maßnahmen)

- **Cybersicherheitsrichtlinien**

IT-Sicherheitsgesetz: Bundesgesetz zu Investitionen in Cybersicherheit. Verbesserung der IT-Sicherheit in Unternehmen und Bundesverwaltung. Mittels UBI-Einstufung werden betroffene Organisationen identifiziert und eingestuft (UBI-1 bis UBI-3).

DORA (Digital Operational Resilience Act): Europäische Gesetzgebung zu Verbesserung der IT-Sicherheitsstrategie für Finanzinstitutionen. Auch werden Vorgaben zur Beaufsichtigung von IT-Dienstleistern festgelegt.

BSI200er und ISO 27000-Familie: Normen zur Sicherung von Informationen in Organisationen. Eine Kern-Anforderung ist der Aufbau und die Verwaltung eines ISMS (Informationssicherheitsmanagementsystem).

Außerdem Cobit4: ...

Was ist ein ISMS?

Ein ISMS kann als Konzept verstanden werden, dass alle Maßnahmen zur Implementierung der Sicherheitsstandards eines Unternehmens umfasst. Dazu zählen Konzepte und Dokumente zur IT-Sicherheitsstrategie, Leitlinien der IT-Sicherheit, IT-

Sicherheitskonzepte, konkrete Sicherheitsmaßnahmen, u.v.m. Durch ISMS die Einführung von Sicherheitsstandards vereinfacht, aber auch die Einhaltung der Ressourceneffizienz (Pareto-Prinzip) gefördert.

Für die Umsetzung eines ISMS können diverse Richtlinien herangezogen werden: BSI200, ISO27000, ITIL, COBIT4, ...

Was sind die konkreten Maßnahmen bei der Umsetzung eines ISMS?

1. Organisatorische Maßnahmen: Regelungen, Richtlinien und Schulungen für Mitarbeiter des Unternehmens. (Schulung, Sensibilisierung, Rollenverteilung, ...)

2. Personelle Maßnahmen: Kommunikation von Sicherheitsrichtlinien bereits im Arbeitsvertrag, angemessene Betreuung bei unternehmensinternem Tätigkeitswechsel, ...

3. Technische Maßnahmen: Maßnahmen auf IT-Systeme (z.B. Patchmanagement, ...)

4. Infrastrukturmaßnahmen: Maßnahmen an der Unternehmensinfrastruktur (z.B. Zutrittskontrollen, ...)

➔ alle Maßnahmen werden durch Berechtigungskonzepte unterstützt (z.B. Zutrittsrechte auf Gebäude, Zugriffsrechte auf Daten, Zugangsrechte zu Anwendungen, ...)

Es werden zwei Herangehensweisen zur Umsetzung eines ISMS unterschieden:

- Risikoanalyse: wird über die ISO27000 Reihe umgesetzt

- Grundschutz: wird über die BSI200-Reihe umgesetzt, mit teilweisem Einbezug der Risikoanalyse. Das AWS **verinice** setzt ein ISMS nach Grundschutz um.

ENGELHARDT, Max, [2020]. ***Hacking & IT-Security für Einsteiger: der leichte Weg zum IT-Security-Experten*.** Landshut: BMU Verlag.