Fraunhofer AISEC

Fraunhofer Institute for Applied and Integrated Security AISEC

Entwicklungen im Bereich Cybersicherheit: Trends, Herausforderungen und Lösungsansätze

Claudia Eckert, Institutsleitung Fraunhofer AISEC, Technische Universität München

29.1.2025

Agenda

1. Cybersicherheit: ein Lagebild
2. Cybersicherheit: Entwicklung der Bedrohungslage
3. Cybersicherheit: Herausforderungen und Chancen
4. Lösungsansätze: Best Practices, um Mindeststandards zu etablieren
5. Anknüpfungspunkte für eine Automatisierung
6. Zusammenfassung

1. Cybersicherheit: ein Lagebild

Bitkom-Studie zur Cybersicherheitslage in Deutschland, 2024

- Gemeldete Vorfälle:
  - 91% der befragten Unternehmen waren betroffen.
  - Angriffsziele: Datendiebstahl, Spionage oder Sabotage
- Geschätzter Schaden:
  - ca. 266,6 Milliarden Euros in Deutschland in 12 Monaten
- Blick in die Zukunft:
  - 65% der befragten Unternehmen sehen ihre Existenz bedroht durch Cyberattacken,
  - Dramatischer Anstieg gegenüber 52% in 2023 und gegenüber lediglich 9% in 2021!

Schaden durch...	Schadenssummen in Mrd. Euro (2024)	Schadenssummen in Mrd. Euro (2023)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	54,5	35,0
Kosten für Rechtsstreitigkeiten	53,1	29,8
Umsatzeinbußen durch nachgemachte Produkte bzw. Plagiate	39,2	15,3
Kosten für Ermittlungen und Ersatzmaßnahmen	32,2	25,2
Datenschutzrechtliche Maßnahmen, z.B. durch Behörden	27,2	12,4
Imageschaden bei Kunden oder Lieferanten, Negative Medienberichterstattung	20,2	35,3
Patentrechtsverletzungen, auch vor Anmeldung	14,8	10,4
Erpressung mit gestohlenen Daten	13,4	16,1
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	11,2	21,5
Geldabfluss durch Betrugsversuche	0,8	3,9
Sonstige Schäden	0	1,1
Gesamtschaden pro Jahr	**266,6**	**205,9**

Quelle: Bitkom, 2024

Weltweite Bedrohungslage

- Cybercrime Angriffe kosten die Weltwirtschaft ca. 9.22 Billionen US Dollar in 2024. (Statista).
- Betroffen sind Unternehmen jeder Größe und aus allen Branchen:
  - Maschinenbau (stark ansteigend), Konsumgüter, Handel, Logistik, Gesundheitswesen, Energie, Finanzbereich

2. Cybersicherheit: Entwicklung der Bedrohungslage

Entwicklungs-Trends:

- Digitalisierung: funktionierende IT-Systeme, Anwendungen und IT-Services sind geschäftskritisch!
  - Eine Unterbrechung der Geschäftstätigkeit zieht hohe Kosten nach sich!

    z.B. Geschätzter durchschnittlicher Schaden eines Datendiebstahls $4.9 Million in 2024 (Quelle IBM).

- Software und Data sind die Basis für moderne, effiziente Geschäftsprozesse!
  - Die Angriffsmöglichkeiten durch Schwachstellen in der Software vergrößern sich rasant.

    z.B. Ransomeware: Big Business: im Durchschnitt wurden $1.5 Million in 2023 bezahlt. (SC Magazine)

- KI Einsatz
  - Unsichere KI: z.B. manipulierte Trainingsdaten, Abfangen von Eingaben (prompt) und Ausgaben, Datenschutz
  - KI als Angriffswerkzeug: z.B. automatisierte, personalisierte Angriffe, DeepFakes für Social Engineering

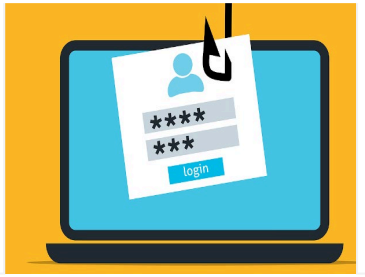
2. Cybersicherheit: Entwicklung der Bedrohungslage

Nach wie vor größte Bedrohungen für Unternehmen:

- Ransomware:
- Abwehr mit Standard Technologien und Maßnahmen:
  - U.a.: Backup, Netzwerk-Segmentierung, Notfallplanung

- Unautorisierter Zugriffe:
- Abwehr mit Standard Technologien und Maßnahmen:
  - U.a. : Aufgaben-orientierte Zugriffskontrolle, Verschlüsselung, Zero-Trust

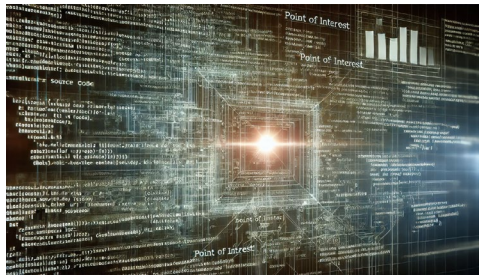
- Social Engineering, Phishing:
- Abwehr mit Standard Technologien und Maßnahmen:
  - U.a.: 2-Faktor-Authentisierung, Mitarbeiter-Schulung



3. Cybersicherheit: Herausforderungen und Chancen

Herausforderung KI: Birgt neben Risiken enorme Chancen für die Erhöhung der Cybersicherheit

1. KI-Assistenz für die Analyse von Software (z.B. von Software von Dienstleistern):
   Auffinden von Sicherheitsschwachstellen und Datenschutzverletzungen in Software
2. KI-Assistenz für die Entwicklung sicherer Software (z.B. inhouse entwickelter Code):
   Generierung von Programm-Code ohne Einfallstore für Angriffe
3. KI-Assistenz für ein kontinuierliches Schwachstellenmanagement (z.B. für CRA):
   Ähnlichkeitssuche, ob eine gemeldete Schwachstelle in eigenen Produkten vorliegt und beseitigt werden muss
4. KI-Assistenz für das IT Sicherheitsmanagement (z.B. für NIS2 Compliance-Nachweise):
   Anleitung zur sicheren System-Konfigurierung, Generierung von Dokumentationen



Herausforderung Regulatorik: Erzeugt Aufwand, sorgt aber auch für Mindeststandards an Schutzmaßnahmen

1. schützt vor Missbrauch, Datenabfluss, Spionage,
2. sichert Geschäftsbetrieb (Business Continuity),
3. sichert den Marktzugang (z.B. CE Kennzeichen erfordert ab 2027 die Einhaltung des CRA)

3. Cybersicherheit: Herausforderungen und Chancen

Einige weltweite Regularien im Überblick: Auffallend viele Gemeinsamkeiten!

Name, in Kraft	Land	Ziel
GDPR, 2018	EU	Rules for the protection of personal data in the EU; impact on companies doing business in Europe or serving European citizens.
NIS2, national law Oct. 2024	EU	Broadens the scope and increases the requirements for companies in critical sectors
Cyber resilience Act, CRA, 2024	EU	Securing products based on/containing digital elements, compliance is required to acquire the CE label for the EU market.
Cybersecurity Act, CSA, 2019	EU	Framework for certifying the cybersecurity of products, services and processes: 5G, Cloud
The Cybersecurity Improvement Act, 2020	US	requires federal agencies to consider security standards when procuring IoT devices.
Consumer Privacy Act (CCPA),	California	Similar to GDPR , sets high transparency and data security requirements for companies.
Proteção de Dados, 2020	Brazil	Regulation for the protection of personal data in Brazil. It is strongly based on the GDPR
Cybersecurity Law, 2017	China	Requirements for data storage and transmission; companies have to conduct regular security audits.
Cybersecurity Act, 2018	Singa-pore	Requires critical information infrastructures providers to implement cybersecurity measures and to report security incidents.
Basic Act on Cybersecurity, 2018	Japan	Law obliges the public and private sectors to implement comprehensive security measures

3. Cybersicherheit: Herausforderungen und Chancen

Lessons Learned

- Es ist nicht die Frage ob man angegriffen wird, sondern wie gut man gerüstet ist, resilient(er) ist!
- Standard Sicherheits-Maßnahmen können wirksam gegen eine Vielzahl von Standard Angriffen schützen!

  Aber: Was sind erforderliche Maßnahmen? Wie sind sie korrekt einzusetzen?

Viel, hilft nicht unbedingt auch viel!

Nur punktuelle Absicherung ist sinnlos!

Kontrollen müssen sinnvoll integriert werden!

These: Regulatorische Vorgaben liefern gute Leitplanken

4. Lösungsansätze: Best Practices, um Mindeststandards zu etablieren

Abgeleitet aus NIS2-Katalog Artikel 21 (2), BSI Gesetz §30 und CRA-Anforderungen

1) Risk Management
- Asset Management, Risk Analysis, Risk Assessments

2) Vulnerability Management
- Vulnerability Detection, Vulnerability Reporting (Customer, Authority, Partner)
- Secure Patching, Updating (product life cycle)

3) Business Continuity
- Backup-Management,
- Emergency Plan, Recovery Management,
- Crisis Management

4) Security of the digital Supply Chains
- Dependency Management
- Software bill of material (SBOM), Certification

5) Information Security Management Processes

Security Policies; e.g.
- Password policy (lenght, life time, …)
- Access rights (need-to-know principle, role-based)
- On-Off-boarding policy: deactivation of accounts
- Mail policy, mobile device policy, messenger policy

6) Technical Measures e.g.
- Network segmentation, isolation (guest, company)
- Zero Trust Architecture: continous access controls
- Disk encryption, mail encryption
- Multi factor authentication
- (Security)-Updates/patches

7) Conformance attestation
- Documentation, testing, attestation

5. Anknüpfungspunkte für eine Automatisierung

Einige aktuelle Forschungsarbeiten am AISEC

Tool-Unterstützung für	AISEC-Tool-Entwicklungen (Auswahl)
• Risikoanalyse (1) Risk-Mgmt	QuBA
• Asset Management (1) Risk-Mgmt	ANMAD
• Vulnerability-Management: (2) Vulnerability-Mgmt	
◦ Prüfung von Cloud-Infrastrukturen/Software-Schwachstellen	Analyse-Werkzeug Clouditor
◦ Abgleich auf CVEs:	LLM-basierte Checks
◦ Vulnerability Reporting:	Prüfung der SBOMs
• Erstellung von SBOMs (4) Supply Chain Mgmt:	Werkzeug zur Erstellung und Analyse
• Erkennung der Betroffenheit von CVE-Meldungen:	KI-basierte CVE Checks
• Überwachung der Einhaltung von Policies: (5) Policy Mgmt	Analyse Werkzeug Clouditor
• Prüfung korrekter Krypto-Nutzung/Implementierung (6) Technology	Software-Analyse Werkzeug Codyze
• Erstellung von Konformitäts-Nachweise (7) Conformity	KI-basierte Tools, Tests
• Testen der Sicherheit von 3rd Komponenten (7) Conformity	Test-Werkzeuge, AISEC-Laborumgebung

Beispiel 1: Risikoanalyse: AISEC-Questionnaire-Based Assessment (QuBA)

Leichtgewichtiges Risk Assessment für IoT Geräte, die CRA unterliegen

Creating security risk assessments for all CRA-relevant products is extremely time-consuming.
The QuBA offers **quick assessments** to cover simple[1] products with low effort and appropriate quality.

The center piece of the method is a **questionnaire**.

The risk assessment is constructed from the answers and from a **knowledge base** (catalogs).

Risk treatment is based on
(1) selecting **proposed** assumptions and countermeasures (→ catalogs)
(2) **individual decisions** (typically for remaining risks above threshold).

[1]Simple from a security point of view, regarding the product's decomposition and interactions with its operational environment.

Beispiel 2: Baukasten an Compliance-Tools: CONFIRMATE

Modularer Aufbau, erweiterbar, unternehmensspezifisch anpassbar

1. Modul für Asset Discovery
   - Zusammenführen von Daten aus verschiedenen Quellen (Infrastruktur, Netzwerk, Cloud)
2. Modul für Cloud-Sicherheit
   - Prüfung von Cloud-Ressourcen auf Schwachstellen
3. Modul für Code-Sicherheit
   - Analyse von Programmcode, Schwachstellenanalyse
4. Modul zur Erstellung und Überwachung von SBOMs
   - Schwachstellenmanagement für die Software-Lieferkette

Unterstützte Regelwerke

In Arbeit: Unterstützung für CRA, NIS2, EUCS und BSI C5

6. Zusammenfassung

Leidensdruck 1: Starke Vergrößerung der Angriffsfläche, Angriffszahlen werden weiter steigen!

→ Umsetzen von angemessenen Schutzmaßnahmen ist alternativlos!

Leidensdruck 2: Vielzahl an verpflichtend umzusetzenden, regulatorischen Anforderungen

→ Umsetzen von Mindeststandards ist alternativlos!

Lichtblick 1: Umsetzung von Sicherheits-Mindeststandards

→ Abdeckung vieler überlappender Anforderungen **und gleichzeitig** wirksamer Schutz gegen Standard-Angriffe

Lichtblick 2: Viele Ansatzpunkte für Automatisierung, z.B.

→ AISEC-Software-Werkzeuge Risiko-, Schwachstellen-, Code-Analysen, SBOMs, Compliance-Checks, …

Vielen Dank

Claudia Eckert
Institutsleitung Fraunhofer AISEC
TU München, Lehrstuhl für Sicherheit in der Informatik
claudia.eckert@fraunhofer.de

Fraunhofer AISEC
Lichtenbergstraße 11
85748 Garching b. München
www.aisec.fraunhofer.de

Fraunhofer
AISEC

Fraunhofer Institute for Applied
and Integrated Security AISEC