Elementare Gefährdungen in der IT-Sicherheit

IT-Sicherheit

ITT-Net-IS

17. März 2025

1 Einleitung

Elementare Gefährdungen stellen eine ernsthafte Bedrohung für IT-Systeme, deren Infrastruktur und Daten dar. Diese Gefährdungen umfassen physikalische, klimatische, menschliche und technologische Risiken, die die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen gefährden können.

2 Definition und Bedeutung

Elementare Gefährdungen sind oft nicht gezielte, sondern durch Umwelteinflüsse oder unbeabsichtigte Handlungen entstehende Risiken für IT-Systeme. Beispiele sind Naturkatastrophen, Stromausfälle oder Fahrlässigkeit im Umgang mit IT-Komponenten. Diese Gefahren können erhebliche wirtschaftliche und sicherheitstechnische Folgen haben, weshalb eine systematische Risikoanalyse und Schutzmaßnahmen erforderlich sind.

3 Arten von elementaren Gefährdungen

- **Physikalische Gefahren:** Brand, Wasser, Staub, Korrosion
- **Klimatische Bedingungen:** Hitze, Kälte, Luftfeuchtigkeit
- **Technische Risiken:** Stromausfall, Netzwerkausfall, Hardware-Defekte
- **Menschliche Faktoren:** Fehlbedienung, Fahrlässigkeit, Sabotage
- **Externe Ereignisse:** Naturkatastrophen, Großereignisse, Terroranschläge

Notes

- **Korrosion:** Allmähliche Zerstörung von Materialien durch chemische Reaktionen, z. B. Rostbildung bei Metallen.
- **Netzausfall:** Unterbrechung der Stromversorgung oder Netzwerkverbindungen, die den Betrieb von IT-Systemen beeinträchtigen.
- **Sabotage:** Gezielte Schädigung von Systemen oder Prozessen durch interne oder externe Personen.

4 Liste der elementaren Gefährdungen

- G 0.1 Feuer
- G 0.2 Ungünstige klimatische Bedingungen
- G 0.3 Wasser
- G 0.4 Verschmutzung, Staub, Korrosion
- G 0.5 Naturkatastrophen
- G 0.6 Katastrophen im Umfeld
- G 0.7 Großereignisse im Umfeld
- G 0.8 Ausfall oder Störung der Stromversorgung
- G 0.9 Ausfall oder Störung von Kommunikationsnetzen
- G 0.10 Ausfall oder Störung von Versorgungsnetzen
- G 0.11 Ausfall oder Störung von Dienstleistungsunternehmen
- G 0.12 Elektromagnetische Störstrahlung
- G 0.13 Abfangen kompromittierender Strahlung
- G 0.14 Ausspähen von Informationen (Spionage)
- G 0.15 Abhören
- G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten
- G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

- G 0.18 Fehlplanung oder fehlende Anpassung
- G 0.19 Offenlegung schützenswerter Informationen

Notes

- **Spionage:** Illegale oder unerlaubte Informationsbeschaffung durch unbefugte Dritte.
- **Elektromagnetische Störstrahlung:** Unbeabsichtigte oder gezielte elektromagnetische Signale, die elektronische Geräte beeinflussen oder auslesen können.
- **Versorgungsnetze:** Infrastrukturen für Wasser, Gas, Internet, Strom, die bei Ausfall wirtschaftliche oder gesellschaftliche Schäden verursachen können.

- G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle
- G 0.21 Manipulation von Hard- oder Software
- G 0.22 Manipulation von Informationen
- G 0.23 Unbefugtes Eindringen in IT-Systeme
- G 0.24 Zerstörung von Geräten oder Datenträgern
- G 0.25 Ausfall von Geräten oder Systemen
- G 0.26 Fehlfunktion von Geräten oder Systemen
- G 0.27 Ressourcenmangel
- G 0.28 Software-Schwachstellen oder -Fehler
- G 0.29 Verstoß gegen Gesetze oder Regelungen
- G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

Notes

- **Manipulation von Hard- oder Software:** Gezielte Veränderung von IT-Systemen, um Fehlfunktionen oder Sicherheitslücken zu erzeugen.
- **Software-Schwachstellen:** Fehler in Programmen, die Angreifer für unerlaubte Zugriffe oder Manipulationen nutzen können.
- **Ressourcenmangel:** Fehlende technische, personelle oder finanzielle Mittel für den sicheren IT-Betrieb.

- G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen
- G 0.32 Missbrauch von Berechtigungen
- G 0.33 Personalausfall
- G 0.34 Anschlag
- G 0.35 Nötigung, Erpressung oder Korruption
- G 0.36 Identitätsdiebstahl
- G 0.37 Abstreiten von Handlungen

- G 0.38 Missbrauch personenbezogener Daten
- G 0.39 Schadprogramme
- G 0.40 Verhinderung von Diensten (Denial of Service)

Notes

- **Identitätsdiebstahl:** Unbefugte Nutzung persönlicher Daten zur Täuschung oder für Betrugszwecke.
- **Denial of Service (DoS):** Überlastung von IT-Systemen durch gezielte Anfragen, um Dienste unbrauchbar zu machen.
- **Schadprogramme:** Bösartige Software wie Viren, Trojaner oder Ransomware, die Daten stehlen oder Systeme lahmlegen.

- G 0.41 Sabotage
- G 0.42 Social Engineering
- G 0.43 Einspielen von Nachrichten
- G 0.44 Unbefugtes Eindringen in Räumlichkeiten
- G 0.45 Datenverlust
- G 0.46 Integritätsverlust schützenswerter Informationen
- G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe

Notes

- **Social Engineering:** Psychologische Manipulation von Menschen, um vertrauliche Informationen zu erlangen.
- **Datenverlust:** Unwiderrufliches Löschen oder Zerstören von Daten, z. B. durch Hardware-Defekte oder Angriffe.
- **Integritätsverlust:** Veränderung von Daten, sodass deren ursprüngliche Bedeutung oder Verlässlichkeit verloren geht.

5 Schutzmaßnahmen und Risikomanagement

Zur Minimierung elementarer Gefährdungen ist ein mehrstufiges Sicherheitskonzept notwendig:

- ***TOM: Technisch-organisatorische Maßnahmen.***
  - ***Technische Maßnahmen: Brandschutzsysteme, Notstromaggregate, redundante Netzwerke***
  - ***Organisatorische Maßnahmen: Notfallpläne, Mitarbeiterschulungen, Zutrittskontrollen***
  - ***Prozessuale Maßnahmen: Regelmäßige Backups, Wartungsarbeiten, Sicherheitsrichtlinien***

6 Übung: Schutzbedarfsanalyse für den eigenen Computerarbeitsplatz

6.1 Aufgabenstellung

Führen Sie eine Schutzbedarfsanalyse für Ihren Computerarbeitsplatz durch. Gehen Sie dabei wie folgt vor:

1. **Inventarisierung**:
   - Listen Sie alle wichtigen Komponenten auf (Hardware, Software, Daten)
   - Beschreiben Sie kurz ihre Funktion und Bedeutung
2. **Schutzbedarfsfeststellung**:
   - Bewerten Sie für jede Komponente den Schutzbedarf bezüglich Vertraulichkeit, Integrität und Verfügbarkeit
   - Verwenden Sie die Kategorien NIEDRIG, MITTEL, HOCH
   - Begründen Sie Ihre Einschätzung
3. **Bedrohungsanalyse**:
   - Identifizieren Sie mindestens 5 relevante Bedrohungen
   - Beschreiben Sie potenzielle Auswirkungen
4. **Maßnahmenplanung**:
   - Leiten Sie konkrete Schutzmaßnahmen ab
   - Priorisieren Sie diese nach Wichtigkeit und Aufwand
5. **Dokumentation**:
   - Erstellen Sie ein kurzes Dokument (2-3 Seiten), das Ihre Ergebnisse zusammenfasst
   - Fügen Sie einen Maßnahmenplan mit Zeitschiene bei

6.2 Hilfsmittel

Nutzen Sie zur Orientierung folgende Bausteine aus dem IT-Grundschutz-Kompendium:

- SYS.2.1: Allgemeiner Client
- APP.1.1: Office-Produkte
- NET.2.2: WLAN-Nutzung
- ORP.1: Organisation
- CON.2: Datenschutz

6.3 Bewertungsgrundlage

Die Schutzbedarfsanalyse wird anhand folgender Kriterien bewertet:

- Vollständigkeit der Inventarisierung
- Nachvollziehbarkeit der Schutzbedarfsbewertungen
- Relevanz der identifizierten Bedrohungen
- Angemessenheit der vorgeschlagenen Maßnahmen
- Qualität der Dokumentation