Elementare Gefährdungen in der IT-Sicherheit

IT-Sicherheit

ITT-Net-IS

11. 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

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
- 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
- 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)
- 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

5 Schutzmaßnahmen und Risikomanagement

Zur Minimierung elementarer Gefährdungen ist ein mehrstufiges Sicherheitskonzept notwendig:

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