Gefahren

- Elementar-Gefahren (Feuer, Wasser, Blitz, Lawine, Erdbeben, Sonnensturm, ...)
    Ad Feuer:
        Brandgase (chem. Aggressivität, Hitze, Ruß-Partikel, ...),
        besonders bei Kabelbränden!
        Löschmittel
    Ad Wasser:
        Rohrbruch und Lecks
            (Leitungswasser & Abwasser, Heizungs- und Kühlwasser)
        Hochwasser, Rückstau von Regenwasser, "Absaufen" von Kabelschächten, ...
        Offene Fenster
        Getränke!!!
- Strom-Ausfall, Überspannung, überlastete Leitungen, Kabel als Stolperfallen
- Ausfall der Klimatisierung, Klimaanlage zu schwach
- Bauarbeiten (Staub, Erschütterungen)
- Unterbrechung von Datenleitungen (Bagger)
- Einbruch, phys. Sabotage (Bombenanschlag), Diebstahl (Notebooks, Handies, ...)
- Techn. Defekte, SW-Fehler, fehlgeschlagene Updates
- Alterung (von Datenträgern, z.B. Band / CD)
- Verschmutzung (Staub)
- Ressourcen-Mangel (RAM, Storage)
- Nicht eingespielte Updates gegen veröffentlichte Fehler
- Menschliches Versagen:
    Dummheit & Schlamperei (auch Reinigungspersonal, ...)
    Verlust (von HW, von Keycards, ...)
- Fehlende Dokumentation, fehlende Regelungen
- Insolvenz von Lieferanten & Dienstleistern, Auslaufen von Lizenzen, ...
    (SW nicht mehr benutzbar, Daten nicht mehr erreichbar, ...)
- Ausfall wichtiger Mitarbeiter (Krankheit, Tod, ...)
- "Harte" Trennung von einem Dienstleister / einem Cloud-Anbieter
- Zugang mit entwendeten Zugangsdaten oder über Standard-Passwörter,
    HW und SW mit eingebauten Backdoors
- Datenverlust, Datenmanipulation, Datensabotage (z.B. Krypto-Virus)
- Programm-Manipulation (insbes. durch manipuliertes automatisches Update)
- Datendiebstahl (Know-How und Betriebsgeheimnisse,
    Kunden- oder Patientendaten, Passwörter & Schlüssel)
    -- via legalem Zugriff durch Berechtigte
    -- via Blick auf den Bildschirm & unbeaufsichtigte Arbeitsplätze
    -- via phys. Datenträger (Kopie auf USB-Stick,
        Diebstahl von Notebooks und Datenträgern,

ungelöschte ausrangierte Festplatten und Handies)
-- via SW-Lücken (unerlaubter Zugriff, ev. von extern via Netz)
-- via Anzapfen von Netz-Verbindungen, Abfangen von E-Mails,
Umleiten von Datenverbindungen,...
(WLAN? Phys. Zugriff auf Datenleitungen, ev. außerhalb des Gebäudes?
Zugriff beim Provider? IMSI-Catcher?)
- Eingriff in Steuerungssysteme (Industriesteuerungen, Schließanlagen,
Energie- und Datennetze, Autos, Flugzeuge und Verkehrsanlagen, med. Geräte ...)
- Viren und andere Schadprogramme
- Denial of Service
= provozierte Abstürze & Stillstände / Überlastung des Netzes und der Server
==› Erpressung
==› Umleitung des abgeblockten Datenverkehrs
- Keylogger, Aktivierung von Mikrofon und Kamera
- Password Brute Forcing
- Home Office & Handy
- Ressourcen-Missbrauch (z.B. Crypto Mining, exzessive private Nutzung, ...)
Ganz böse bei gesetzeswidrigen Aktivitäten / Daten!
- Nutzung zum Angriff auf Dritte (XSS-Attacken, Schadsoftware auf Webservern bzw.
in Werbeeinblendungen, Schadsoftware in SW-Download,
Mißbrauch des Mailservers als Spamschleuder)
- Social Engineering, Phishing Mails
(Herauslocken von Daten, Anstiften zu Überweisungen, ...)
- Web Defacement

Angreifer

- Hacker (aus Angeberei / aus finanziellen Motiven)
- Kriminelle mit finanziellen Interessen
- Terroristen
- Unzufriedene Kunden (vor allem bei Behörden!) und Geschäftspartner
- Aktive (Geldgier? Frust? Erpressung?) / ehemalige / gekündigte Mitarbeiter
- Mitarbeiter von Dienstleistern
- Die Konkurrenz
- Die Medien
- Geheimdienste und Strafverfolger
(Unterscheide berechtigte Zugriffe / unberechtigte Zugriffe)
- Ausgeuferte Massen-Angriffe, Angreifer ohne bestimmtes Ziel

Folgen

- Betriebsstillstand (Produktion, Dienstleistung, ...)
- Direkte finanzielle Verluste (z.B. Personal-Stillstands-Kosten), entgangene Einnahmen
- Schadenbehebungs-Kosten (HW & Personal)
- Permanenter Verlust wesentlicher Geschäftsdaten
  (==› Weiterführung des Betriebs nicht möglich, Insolvenz)
- Rechtl. Folgen: Strafen & Haft, Datenverarbeitungs-Verbot
- Gefahr für Leib und Leben (siehe z.B. bei Angriffen: Steuerungssysteme)
- Mechan. Schäden (an Maschinen)
- Erpressung (Rückerhalt der Daten, DoS, ...)
- Schadenersatz, Haftungsforderungen
- Ansehens-Verlust, Kunden-Verlust
- Abfluss des Betriebs-Know-Hows, Wettbewerbs-Nachteile
- Identitäts- und Zertifikats-Diebstahl und -Missbrauch
  (von Firmen-Zertifikaten / von einzelnen Mitarbeitern / von Kunden)
- Manipulation des Börsenwertes

Maßnahmen

- Baulich / Infrastruktur:
  Geografische Redundanz: 2 Standorte
  Räumliche Trennung: Sensibler Serverraum, normaler Serverraum,
  Raum für Backup, Raum für Drucker
  Einbruchs- und Zerstörungsschutz (notstromversorgte Alarmanlage, keine Fenster!)
  Zugangskontrolle, ev. Wachpersonal
  Schutz vor Explosion, Feuer, Wasser
  Klima & Notstrom (3-stufig)
- Schulung der Mitarbeiter, Richtlinien, Notfallpläne
- Redundanz auf allen Hardware-Ebenen (Storage, Netz, Server)
- Aufteilung und Isolierung von Systemen / von Netzen
- Backup (getestet!)
- Auswahl sicherer Software
- Sicherheits-SW (Virenscanner, Firewall, ...)
- Verschlüsselung, Signaturen, ...
- Gutes Authentifizierungsverfahren (Karte, Biometrie, ...), Passwort-Richtlinien
- Sichere Konfiguration & Administration (Benutzerrollen und Zugriffsrechte, ...)
- Protokollierung (der Zugriffe, der Anmeldungen, ...)
  automat. Überwachung der Protokolle,
  System- und Netzüberwachung, IDS/IPS ("atypisches Systemverhalten")
- Sichere Entsorgung von Datenträgern, sicheres Löschen
- Update der Systeme, Patches einspielen (zeitnah!)