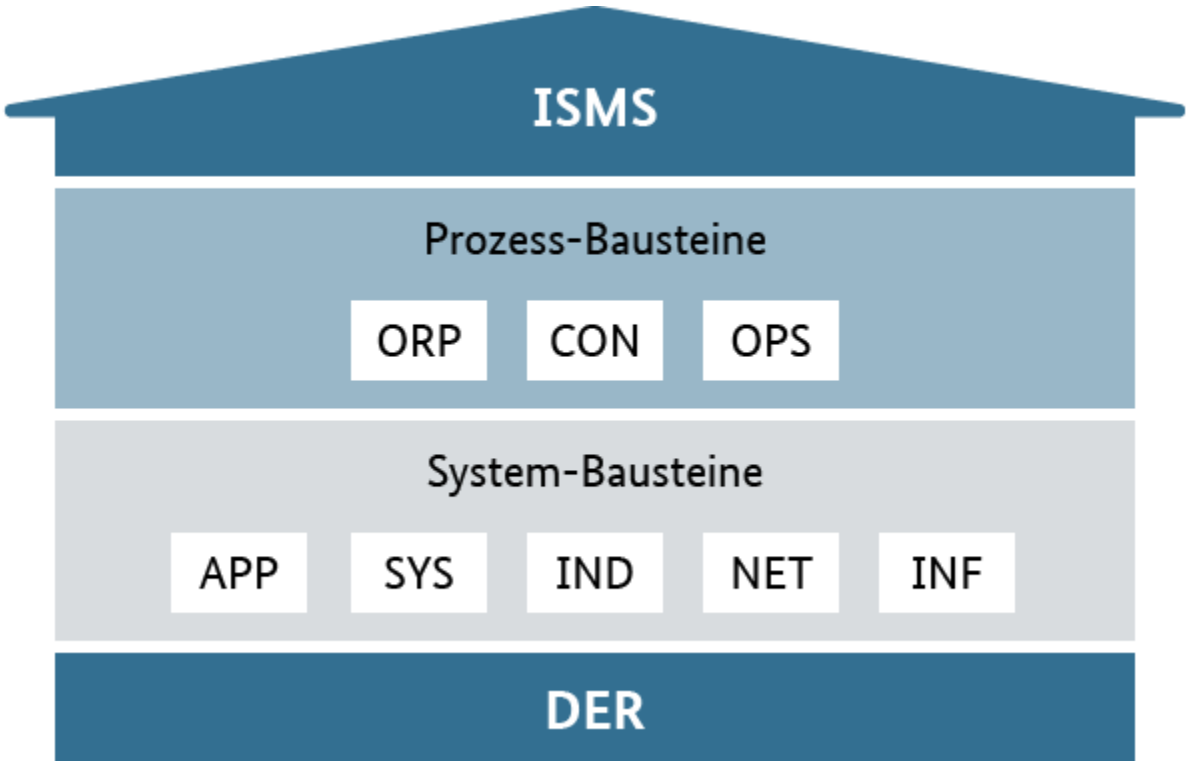
Gruppenarbeits-Szenarien mit realistischen Gefahrenszenarien für die wichtigsten IT-Grundschutz Themengebiete



Inhaltsverzeichnis

Grundschutzkompendium

Das **IT-Grundschutzkompendium** ist die zentrale Veröffentlichung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur systematischen Absicherung von IT-Infrastrukturen. Zusammen mit den BSI-Standards 200-1 bis 200-4 bildet es das Fundament für einen methodischen Aufbau der Informationssicherheit in deutschen Behörden und Unternehmen.

Struktur und Inhalt des IT-Grundschutzkompendiums

Aktuelle Version

- **Edition 2023** (Stand: Februar 2023)
- **111 Bausteine** in 10 thematischen Schichten
- **Umfang:** Über 2.000 Seiten
- **Format:** PDF und maschinenlesbare JSON-Objekte (ab 2026)

Die 10 Schichten des IT-Grundschutzes

Das Kompendium ist nach einem **Schichtenmodell** organisiert:

Prozessorientierte Bausteine:

1. **ISMS** - Sicherheitsmanagement
2. **ORP** - Organisation und Personal
3. **CON** - Konzepte und Vorgehensweisen
4. **OPS** - Betrieb
5. **DER** - Detektion und Reaktion

Systemorientierte Bausteine:

6. **INF** - Infrastruktur
7. **NET** - Netze und Kommunikation
8. **SYS** - IT-Systeme
9. **APP** - Anwendungen
10. **IND** - Industrielle IT

Aufbau der Bausteine

Jeder Baustein enthält:

- **Beschreibung und Zielsetzung**
- **Abgrenzung** zu anderen Bausteinen
- **Gefährdungsübersicht**
- **Anforderungen** in drei Kategorien:
    - Basis-Anforderungen
    - Standard-Anforderungen
    - Anforderungen bei erhöhtem Schutzbedarf

BSI-Standards (Begleitdokumente)

BSI-Standard 200-1: ISMS-Grundlagen

- **Titel:** "Managementsysteme für Informationssicherheit (ISMS)"
- **Umfang:** 48 Seiten
- **Inhalt:** Allgemeine Anforderungen an ein ISMS
- **Kompatibilität:** ISO/IEC 27001:2013

BSI-Standard 200-2: IT-Grundschutz-Methodik

- **Titel:** "IT-Grundschutz-Methodik"
- **Umfang:** 180 Seiten
- **Inhalt:** Drei Vorgehensweisen:
  - **Basis-Absicherung:** Schneller Einstieg
  - **Standard-Absicherung:** Vollständiger Schutz
  - **Kern-Absicherung:** Fokus auf kritische Bereiche

BSI-Standard 200-3: Risikoanalyse

- **Titel:** "Risikoanalyse auf Basis von IT-Grundschutz"
- **Umfang:** 54 Seiten
- **Inhalt:** Methodisches Vorgehen bei individueller Risikoanalyse

BSI-Standard 200-4: Business Continuity Management

- **Titel:** "Business Continuity Management"
- **Umfang:** 310 Seiten
- **Inhalt:** Systematischer Aufbau eines BCMS
- **Kompatibilität:** ISO/IEC 22301:2019

Download-Links und offizielle Quellen

Hauptquellen (BSI-Website)

IT-Grundschutzkompendium Edition 2023:

- **URL:** https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html
- **Direkter PDF-Download:** https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf

BSI-Standards Download-Bereich:

- **Übersichtsseite:** https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html

Einzelne Standards:

- **BSI-Standard 200-1:** https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.pdf
- **BSI-Standard 200-2:** https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf
- **BSI-Standard 200-3:** https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf
- **BSI-Standard 200-4:** https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf

Ergänzende Materialien

IT-Grundschutz-Profile:

- **URL:** https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Profile/it-grundschutz-profile_node.html
- **Inhalt:** Branchenspezifische Musterimplementierungen

Umsetzungshinweise:

- **URL:** https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Umsetzungshinweise/umsetzungshinweise_node.html
- **Inhalt:** Detaillierte Implementierungsanleitungen für ausgewählte Bausteine

Online-Kurs IT-Grundschutz:

- **URL:** https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Online-Kurs-IT-Grundschutz/online-kurs-it-grundschutz_node.html
- **Inhalt:** Interaktiver Einstiegskurs in die IT-Grundschutz-Methodik

Wichtige Neuerungen und Entwicklungen

Edition 2023 Highlights

- **10 neue Bausteine** hinzugefügt
- **21 Bausteine** grundlegend überarbeitet
- **Strukturelle und sprachliche** Überarbeitung aller Bausteine
- **Gendergerechte** Formulierungen
- **Ergänzung:** Baustein CON.11.1 "Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH"

IT-Grundschutz++ (ab 2026)

Das BSI entwickelt derzeit eine **grundlegende Revision** des IT-Grundschutzes:

Neue Merkmale:

- **Maschinenlesbare JSON-Syntax** statt PDF-Dokumente
- **Objektorienterter Ansatz** zur Reduzierung von Redundanzen
- **Punktebewertung** für messbare Sicherheitsniveaus
- **Reduzierung** von 111 auf 67 Bausteine in 19 Checklisten
- **Git-basierte Verteilung** für einfachere Updates

Stichtag: 1. Januar 2026

Praktische Anwendung und Tools

Zertifizierungsmöglichkeiten

- **ISO 27001 auf Basis IT-Grundschutz:** Internationale Anerkennung
- **BSI-Grundschutz-Testat:** Nationale Bestätigung
- **Gültigkeitsdauer:** 3 Jahre (ISO 27001) / 2 Jahre (Testat)

Software-Tools zur Umsetzung

Kommerzielle Lösungen:

- **verinice.PRO:** https://verinice.com/
- **INDITOR® BSI:** https://www.contechnet.de/produkte/grundschutz
- **SecuPedia Risk:** Verschiedene Anbieter

Open Source:

- **verinice Community Edition:** Kostenlose Basis-Version

Aufwandsschätzung

- **Basis-Absicherung:** 3-6 Monate (kleines Unternehmen)
- **Standard-Absicherung:** 6-18 Monate (je nach Größe)
- **Zertifizierungsvorbereitung:** Zusätzlich 3-6 Monate

Zielgruppen und Anwendungsbereiche

Primäre Zielgruppen

- **Kritische Infrastrukturen** (KRITIS-Betreiber)
- **Bundesbehörden und Länder**
- **Kommunale Verwaltungen**
- **Unternehmen** aller Größenordnungen
- **Dienstleister** im IT-Bereich

Branchen-spezifische Profile

- **Hochschulen und Forschungseinrichtungen**
- **Kommunale Verwaltung**
- **Gesundheitswesen**
- **Energieversorgung**
- **Kleine und mittlere Unternehmen (KMU)**

Integration in die Datenschutz- und Backup-Strategie

Relevante Bausteine für Backup-Konzepte

- **CON.3:** Datensicherungskonzept
- **OPS.1.2.2:** Archivierung
- **CON.6:** Löschen und Vernichten
- **CON.2:** Datenschutz
- **OPS.1.1.3:** Patch- und Änderungsmanagement

DSGVO-Integration

- **Artikel 32 DSGVO:** Sicherheit der Verarbeitung
- **Technische und organisatorische Maßnahmen (TOMs)**
- **Dokumentationspflichten** nach DSGVO
- **Privacy by Design/Default** in Bausteinen verankert

Fazit und Ausblick

Das BSI IT-Grundschutzkompendium stellt einen **de-facto Standard** für IT-Sicherheit in Deutschland dar. Mit seiner strukturierten Herangehensweise, der modularen Aufbauweise und der kontinuierlichen Weiterentwicklung bietet es Organisationen aller Größenordnungen eine **praxiserprobte Methodik** zur systematischen Absicherung ihrer IT-Landschaft.

Die **kostenlose Verfügbarkeit** aller Materialien, kombiniert mit umfangreichen Schulungsangeboten und einer aktiven Community, macht den IT-Grundschutz zu einem **zugänglichen und bewährten Instrument** für den Aufbau eines robusten Informationssicherheitsmanagementsystems.

Empfehlung: Beginnen Sie mit dem **Online-Kurs** und der **BSI-Standard 200-1**, um sich einen Überblick zu verschaffen, bevor Sie in die detaillierte Anwendung der Bausteine aus dem Kompendium einsteigen.

Einführung und Grundlagen der Informationssicherheit

Gruppenarbeit 1: Grundwerte-Bedrohungsanalyse

Szenario: Ihr mittelständisches Unternehmen "TechnoServ GmbH" (180 Mitarbeiter) plant den Aufbau eines ISMS (Informationssicherheits-Managementsystem) nach IT-Grundschutz. Analysieren Sie folgende Gefährdungsszenarien hinsichtlich der drei Grundwerte:

Gefahrenszenario A: Ein Ransomware-Angriff verschlüsselt alle Serverdaten, einschließlich der Kundendatenbank und ERP-Systems. Der Angreifer fordert 250.000 € Lösegeld.

- Welche Grundwerte sind betroffen? Bewerten Sie die Auswirkungen (niedrig/mittel/hoch)
- Entwickeln Sie präventive Maßnahmen für jeden Grundwert

Gefahrenszenario B: Ein Mitarbeiter verliert sein Laptop mit sensiblen Konstruktionsdaten für ein neues Produkt. Das Gerät ist nicht verschlüsselt.

- Analysieren Sie potenzielle Schadensfolgen über 12 Monate
- Erstellen Sie eine Stakeholder-Betroffenheitsmatrix

Aufgabe: Präsentieren Sie Ihre Analyse in 15 Minuten mit konkreten Schutzmaßnahmen und Kostenschätzungen.

Gruppenarbeit 2: Cyber-Kill-Chain Simulation

Szenario: Als IT-Sicherheitsbeauftragte analysieren Sie einen fortgeschrittenen Angriff auf Ihr Unternehmen.

Gefahrenszenario: Advanced Persistent Threat (APT) gegen Automobilzulieferer

1. **Reconnaissance:** Angreifer sammeln über LinkedIn und Unternehmenswebsite Informationen über IT-Struktur
2. **Initial Access:** Spear-Phishing E-Mail an Einkaufsleiter mit gefälschter Lieferantenanfrage
3. **Persistence:** Installation einer Backdoor über PowerShell-Skript
4. **Privilege Escalation:** Ausnutzung einer ungepatchten Windows-Schwachstelle
5. **Defense Evasion:** Verwendung von Living-off-the-Land-Techniken
6. **Lateral Movement:** Bewegung über das Netzwerk zu CAD-Servern
7. **Data Exfiltration:** Diebstahl von Konstruktionsplänen über verschlüsselte Kanäle

Aufgaben:

- Identifizieren Sie für jede Phase mögliche Erkennungsmaßnahmen
- Entwickeln Sie ein Incident Response Konzept
- Bewerten Sie, welche IT-Grundschutz-Bausteine relevant sind

Gruppenarbeit 3: Business Impact Analyse

Szenario: Stromausfall in Ihrem Rechenzentrum für unterschiedliche Dauer

Gefahrenszenario Stufe 1: 2-Stunden Stromausfall (USV-Überbrückung erschöpft)

Gefahrenszenario Stufe 2: 8-Stunden Stromausfall (Notstromgenerator ausgefallen)

Gefahrenszenario Stufe 3: 48-Stunden Stromausfall (Regional-Blackout)

Betroffene Systeme:

- E-Mail-Server und Groupware
- ERP-System (SAP)
- Produktionssteuerung
- Webshop und Kundenportale
- Telefonanlage und VoIP

Aufgaben:

- Erstellen Sie eine RTO/RPO-Tabelle für alle Systeme
- Kalkulieren Sie finanzielle Ausfallkosten pro Stunde
- Entwickeln Sie Notfallmaßnahmen nach Priorität
- Planen Sie Kommunikationsstrategien für Kunden/Lieferanten

Gruppenarbeit 4: Social Engineering Workshop

Szenario: Sie führen einen autorisierten Social Engineering Test durch

Gefahrenszenario A - CEO Fraud:

Ein Angreifer gibt sich als Geschäftsführer aus und fordert per E-Mail eine dringende Überweisung von 85.000 € an einen "strategischen Partner" in Hongkong. Die Buchhaltung soll "absolute Diskretion wahren".

Gefahrenszenario B - IT-Support Vortäuschung:

Anrufer gibt sich als Microsoft-Support aus und behauptet, schädliche Aktivitäten auf dem Computer entdeckt zu haben. Er fordert Fernzugriff zur "Bereinigung".

Gefahrenszenario C - Dumpster Diving + Tailgating:

Angreifer sammeln Informationen aus Mülltonnen und nutzen diese für glaubwürdige Gespräche beim unbefugten Betreten der Büroräume.

Aufgaben:

- Entwickeln Sie Erkennungsmerkmale für jeden Angriffstyp
- Erstellen Sie Verhaltensrichtlinien für Mitarbeiter
- Planen Sie ein Awareness-Training-Programm
- Simulieren Sie die Angriffe gegenseitig

Gruppenarbeit 5: Lieferketten-Sicherheit

Szenario: Supply-Chain-Angriff auf Ihr Softwareunternehmen

Gefahrenszenario: Ein Angreifer kompromittiert einen Ihrer Software-Bibliothek-Anbieter und schleust Schadcode in ein Update ein, das Sie an 10.000 Kunden weitergeben.

Betroffene Assets:

- Ihre Entwicklungsumgebung
- Build-Pipeline und CI/CD
- Code-Repositories
- Kundensysteme
- Vertrauen und Reputation

Aufgaben:

- Analysieren Sie die Angriffsvektoren in Ihrer Supply Chain
- Entwickeln Sie Kontrollmaßnahmen für Software-Dependencies
- Erstellen Sie ein Incident Response Plan für Supply-Chain-Vorfälle
- Planen Sie Kommunikation mit betroffenen Kunden
- Bewerten Sie rechtliche und finanzielle Risiken

Technische Sicherheitsmaßnahmen & Systemhärtung

Gruppenarbeit 1: Windows-Client Härtung

Szenario: Sicherheitsvorfälle durch kompromittierte Arbeitsplätze

Gefahrenszenario: Mehrere Windows-Clients wurden über Drive-by-Download-Angriffe mit Banking-Trojaner infiziert. Der Schädling sammelt Anmeldedaten und verschlüsselt Dateien.

Betroffene Umgebung:

- 150 Windows 11 Clients
- Domain-Umgebung mit Active Directory
- Office 365 Integration
- VPN-Zugang für Homeoffice

Aufgaben:

- Erstellen Sie eine Härtungs-Checkliste basierend auf IT-Grundschutz
- Konfigurieren Sie Group Policy Objects (GPOs) für Sicherheit
- Implementieren Sie Application Control (Windows Defender Application Control)
- Entwickeln Sie ein Monitoring-Konzept für verdächtige Aktivitäten
- Planen Sie sichere Browser-Konfigurationen

Erwartete Deliverables:

- Dokumentierte Härtungsmaßnahmen mit Begründung
- PowerShell-Skripte für automatisierte Konfiguration
- Test- und Validierungsverfahren

Gruppenarbeit 2: Netzwerksegmentierung

Szenario: Lateral Movement nach Kompromittierung

Gefahrenszenario: Ein Angreifer hat sich über eine kompromittierte Workstation Zugang zu Ihrem Netzwerk verschafft und bewegt sich lateral durch das Netz, um kritische Systeme zu erreichen.

Netzwerk-Topologie:

- DMZ mit Webservern und Mail-Gateway
- Intranet mit Clients und File-Servern
- Server-VLAN mit Domain Controllern und Datenbank-Servern
- Management-VLAN für Infrastruktur-Geräte
- WLAN für Gäste und Mitarbeiter

Aufgaben:

- Entwerfen Sie eine Mikrosegmentierung nach Zero-Trust-Prinzipien
- Definieren Sie Firewall-Regeln zwischen den Segmenten
- Implementieren Sie Network Access Control (802.1X)
- Planen Sie Monitoring und Anomalie-Erkennung
- Entwickeln Sie Quarantäne-Verfahren für kompromittierte Systeme

Gruppenarbeit 3: Cloud-Security Assessment

Szenario: Migration kritischer Anwendungen in die Cloud

Gefahrenszenario: Bei der Migration von SAP ERP und Kundendatenbank zu Azure sind Sicherheitslücken entstanden:

- Falsch konfigurierte Storage Accounts mit öffentlichem Zugriff
- Schwache Authentifizierung ohne Multi-Faktor
- Unverschlüsselte Datenübertragung
- Fehlende Monitoring und Logging-Konfiguration
- Unklare Backup- und Disaster Recovery-Prozesse

Aufgaben:

- Führen Sie ein Cloud Security Assessment durch
- Implementieren Sie Azure Security Center/Microsoft Defender
- Konfigurieren Sie Identity and Access Management (Azure AD)
- Entwickeln Sie Cloud-spezifische Backup-Strategien
- Erstellen Sie Compliance-Reports (DSGVO, SOX, etc.)

Gruppenarbeit 4: Mobile Device Management

Szenario: BYOD-Sicherheitsvorfälle

Gefahrenszenario: Mehrere private Smartphones von Führungskräften wurden mit Spyware infiziert, die E-Mails, Kontakte und Standortdaten abgreift. Die Geräte haben Zugriff auf Unternehmens-E-Mail und Cloud-Dienste.

Mobile-Umgebung:

- 200 iOS/Android Geräte
- Microsoft Exchange Online
- SharePoint/OneDrive Zugriff
- VPN-Verbindungen
- WLAN-Zugang im Büro

Aufgaben:

- Implementieren Sie Mobile Device Management (Intune/VMware Workspace ONE)
- Konfigurieren Sie Conditional Access Policies
- Entwickeln Sie Mobile Application Management (MAM) Strategien
- Erstellen Sie BYOD-Richtlinien und -Vereinbarungen
- Planen Sie Incident Response für mobile Sicherheitsvorfälle

Gruppenarbeit 5: Verschlüsselungskonzept

Szenario: Datendiebstahl durch Insider-Bedrohung

Gefahrenszenario: Ein Administrator mit privilegierten Zugriffen hat vertrauliche Kundendaten kopiert und an Wettbewerber verkauft. Der Vorfall wurde erst nach 8 Monaten entdeckt.

Betroffene Daten:

- Kundendatenbank mit Verträgen und Konditionen
- Finanzberichte und Budgetplanung
- Personalakten und Gehaltsdaten
- Entwicklungsprojekte und Patente
- E-Mail-Archive mit Geschäftskorrespondenz

Aufgaben:

- Entwickeln Sie ein umfassendes Verschlüsselungskonzept
- Implementieren Sie Database Encryption (TDE, Column-Level)
- Konfigurieren Sie File-Level Verschlüsselung (BitLocker, EFS)
- Planen Sie Key Management und Certificate Services
- Erstellen Sie Data Loss Prevention (DLP) Strategien

Organisatorische Sicherheitsmaßnahmen

Gruppenarbeit 1: Incident Response Simulation

Szenario: Ransomware-Angriff auf Produktionsumgebung

Gefahrenszenario: Freitag 14:30 Uhr: Ihre Produktionssteuerung (SCADA) wird von Ransomware befallen. 3 Produktionslinien stehen still, 200 Mitarbeiter können nicht arbeiten. Kundentermine sind gefährdet.

Timeline:

- **14:30:** Erste Meldungen über langsame Systeme
- **14:45:** Verschlüsselungsaktivität auf File-Servern erkannt
- **15:00:** Produktionsstopp, Ransomware-Note erscheint
- **15:15:** Backup-Systeme ebenfalls betroffen
- **15:30:** Erpresser-E-Mail mit 2 Mio. € Forderung

Aufgaben:

- Aktivieren Sie Ihren Incident Response Plan
- Koordinieren Sie die Krisenkommunikation (intern/extern)
- Treffen Sie Entscheidungen über Systemabschaltungen
- Bewerten Sie Wiederherstellungsoptionen
- Verhandeln Sie mit Stakeholdern über Ausfallzeiten
- Dokumentieren Sie alle Maßnahmen für forensische Analyse

Gruppenarbeit 2: Business Continuity Planning

Szenario: Naturkatastrophe zerstört Hauptstandort

Gefahrenszenario: Ein Hochwasser hat Ihr Hauptgebäude überflutet. Rechenzentrum, Büros und Produktionshallen sind nicht nutzbar. Wiederherstellung dauert minimum 6 Monate.

Betroffene Bereiche:

- 300 Arbeitsplätze
- Primäres Rechenzentrum
- Produktionsanlagen
- Lager mit Rohstoffen/Fertigprodukten
- Parkplätze und Infrastruktur

Aufgaben:

- Entwickeln Sie einen 48h-Notfallplan
- Organisieren Sie alternative Arbeitsplätze
- Aktivieren Sie Disaster Recovery für IT-Systeme
- Koordinieren Sie Lieferanten und Produktionspartner
- Managen Sie Versicherungsabwicklung
- Planen Sie temporäre Geschäftsprozesse

Gruppenarbeit 3: Compliance Management

Szenario: Datenschutz-Audit mit kritischen Befunden

Gefahrenszenario: Eine Aufsichtsbehörde führt eine DSGVO-Prüfung durch und findet schwerwiegende Verstöße:

- Personendaten ohne Rechtsgrundlage gespeichert
- Fehlende Einwilligungserklärungen
- Unzureichende technische und organisatorische Maßnahmen
- Keine Auftragsverarbeitungsverträge mit Dienstleistern
- Versäumte Meldung von Datenpannen

Aufgaben:

- Erstellen Sie einen Maßnahmenplan zur Behebung
- Implementieren Sie Datenschutz-Management-Prozesse
- Führen Sie Privacy Impact Assessments durch
- Schulen Sie Mitarbeiter zu DSGVO-Anforderungen
- Entwickeln Sie Monitoring für Compliance-Verstöße

Gruppenarbeit 4: Vendor Risk Management

Szenario: Sicherheitsvorfall bei kritischem Dienstleister

Gefahrenszenario: Ihr Cloud-Hosting-Provider wurde Opfer eines Cyberangriffs. Angreifer haben Zugang zu Verwaltungsschnittstellen und könnten auf Kundendaten zugreifen.

Betroffene Services:

- Webshop und E-Commerce-Plattform
- Kundendatenbank und CRM
- E-Mail-Hosting und Collaboration
- Backup und Archivierung
- DNS und CDN-Services

Aufgaben:

- Bewerten Sie das Risiko für Ihr Unternehmen
- Aktivieren Sie alternative Dienstleister/Services
- Koordinieren Sie Kommunikation mit dem Provider
- Prüfen Sie Vertragsbedingungen und SLAs
- Entwickeln Sie langfristige Abhängigkeitsstrategien
- Verbessern Sie Ihr Vendor Assessment Verfahren

Gruppenarbeit 5: Mitarbeitersensibilisierung

Szenario: Erfolgreiche Phishing-Kampagne

Gefahrenszenario: 30% Ihrer Mitarbeiter sind auf eine Phishing-E-Mail hereingefallen und haben Anmeldedaten auf einer gefälschten Office 365-Seite eingegeben. Die Angreifer nutzen die Zugänge für Business Email Compromise.

Schadensszenario:

- Kompromittierte E-Mail-Konten versenden weitere Phishing-Mails
- Angreifer leiten Rechnungen an geänderte Bankverbindungen um
- Vertrauliche E-Mails werden an Wettbewerber weitergeleiteten
- Malware wird über E-Mail-Anhänge verbreitet

Aufgaben:

- Entwickeln Sie eine Sofortmaßnahmen-Strategie
- Erstellen Sie ein umfassendes Awareness-Programm
- Implementieren Sie Phishing-Simulation und -Tests
- Konzipieren Sie rollenspezifische Schulungen
- Messen Sie die Wirksamkeit Ihrer Maßnahmen
- Integrieren Sie Security Awareness in HR-Prozesse