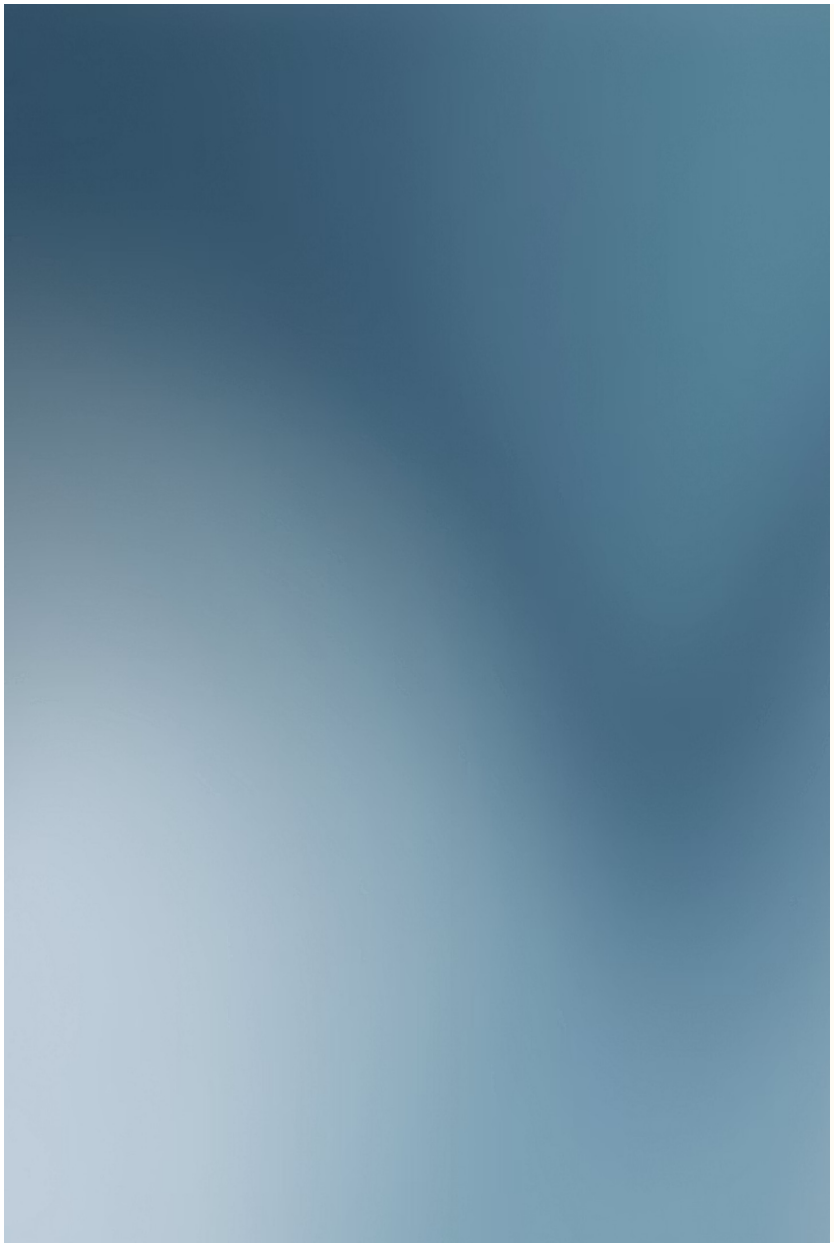

`Schutzbedarfsanalyse`

IT-Sicherheit auf Grundschutzniveau für kleine und mittlere Unternehmen – organisatorisch, technisch und nachweisbar umgesetzt.

GRUNDLAGEN

IT-Sicherheit auf Grundschutzniveau

Was bedeutet Grundschutz?

Grundschutz bedeutet Basis-Sicherheit, die in jedem Betrieb etabliert sein muss – organisatorisch, technisch und nachweisbar. Es ist die Mindestabsicherung gegen typische und realistische Bedrohungen durch bewährte Standardmaßnahmen.

***Der entscheidende Merksatz:** Ohne Regeln keine Sicherheit. Ohne Technik keine Wirkung. Ohne Nachweis keine Punkte.*

Informationssicherheit schützt drei zentrale Werte:
***Vertraulichkeit, Integrität und Verfügbarkeit (CIA-Triade)**.*
Organisation und Technik gehören untrennbar zusammen – eine Policy ohne Umsetzung ist lediglich Dekoration ohne Schutzwirkung.

PRAXISBEISPIEL

Unser durchgängiger Mini-Fall

Betriebsgröße

60 Benutzer im aktiven Betrieb

IT-Infrastruktur

Microsoft 365, Fileserver, VPN-Zugang, Firewall

Zielsetzung

Grundschutz sauber und nachweisbar aufstellen

Dieser realistische Beispielbetrieb wird uns durch alle Maßnahmen begleiten und zeigt, wie Grundschutz in der Praxis funktioniert. Die Größe und Ausstattung entspricht vielen KMUs in Deutschland und macht die Anforderungen konkret greifbar.

Organisatorische Maßnahmen – Rollen & Verantwortlichkeiten

IT-Sicherheitsbeauftragter (ISB)

Koordiniert Sicherheitsregeln, Maßnahmen und Kontrollen im gesamten Betrieb

Datenschutzbeauftragter (DSB)

Verantwortlich für DSGVO, AV-Verträge, Löschkonzept und technisch-organisatorische Maßnahmen

Systemadmin / IT-Betrieb

Technische Umsetzung: Patchen, Logs, Backup und Wiederherstellung

IT-Management

Gibt Ziele frei, stellt Budget und Personal bereit, setzt strategische Prioritäten

Prüfungsfalle

„Niemand zuständig" ist eine Sicherheitslücke mit Ansage. Klare Verantwortlichkeiten sind die Grundlage jeder funktionierenden Sicherheitsorganisation.

Arbeitsauftrag zur Vertiefung

Ordnen Sie folgende sechs Aufgaben den korrekten Rollen zu:

- *Passwort-Policy erstellen*
- *Firewall-Regeln konfigurieren*
- *Löschfristen definieren*
- *Incident-Meldung koordinieren*
- *Awareness-Schulung durchführen*
- *Backup-Tests ausführen*

DOKUMENTATION

IT-Sicherheitsrichtlinie – Inhalte und Struktur

Minimum-Artefakte für AP1

- *Sicherheitsrichtlinie (1–2 Seiten)*
- *Asset-Liste (wichtigste Systeme)*
- *Incident-Prozess (Kurzablauf)*
- *Backup-/Restore-Regel (inkl. Test)*

Was gehört in die Richtlinie?

Eine wirksame IT-Sicherheitsrichtlinie enthält klar definierte Bereiche:

- ***Zweck und Geltungsbereich:*** *Wer und was fällt unter die Richtlinie*
- ***Mindestregeln:*** *Zugänge, Geräte, Updates, Daten, Cloud, Remote-Arbeit, Besucherregelung*
- ***Vorfallmanagement:*** *Wie werden Incidents gemeldet, dokumentiert und eskaliert*
- ***Verbindlichkeit:*** *Konsequenzen bei Verstößen müssen explizit genannt werden*

Arbeitsauftrag: Formulieren Sie acht prägnante Bulletpoints für eine praxistaugliche IT-Sicherheitsrichtlinie eines mittelständischen Betriebs.

Passwort-Policy – der AP1-Klassiker

Moderne Passwort-Anforderungen

*Eine zeitgemäße Passwort-Policy setzt auf **Multi-Faktor-Authentifizierung (MFA)** für alle Admin-Konten und Remote-Zugriffe. Ohne MFA ist selbst die beste Passwortpolitik nur halb so wirksam.*

Zentrale Prinzipien:

- *Passwörter sollten **lang** sein statt „kompliziert um jeden Preis" – Passphrasen sind oft besser merkbar und sicherer*
- *Keine Wiederverwendung über Systeme hinweg*
- *Kein Teilen von Zugangsdaten zwischen Personen*
- *Keine physischen Notizen (Post-its am Monitor)*
- *Technische Kontrollen: Sperre nach Fehlversuchen, Rate-Limiting*
- *Passwortmanager werden empfohlen oder sogar bereitgestellt*
- ***Strikte Trennung:** User-Account ≠ Admin-Account*

Prüfungsfalle

Eine Regel ohne technische Durchsetzung ist wirkungslos. Die beste Policy nützt nichts, wenn sie nicht im System verankert ist.

Arbeitsauftrag

Formulieren Sie eine vollständige Passwort-Policy mit sechs konkreten Regeln und zwei technischen Kontrollen, die die Einhaltung sicherstellen.

Awareness & Schulung – der menschliche Faktor

Phishing-Erkennung & Meldewege

Mitarbeiter müssen verdächtige E-Mails erkennen und wissen, wie sie diese melden – idealerweise über ein Ticketsystem oder eine dedizierte Hotline.

Sichere Arbeitsplatzpraktiken

Clean-Desk-Policy, automatische Bildschirmsperre, vorsichtiger Umgang mit USB-Sticks, Downloads und Makros sowie Besucherregelungen.

Datenschutz-Grundlagen

Umgang mit personenbezogenen Daten, Zweckbindung, Löschfristen und die Grundprinzipien der DSGVO im täglichen Arbeitskontext.

Arbeitsauftrag: Erstellen Sie fünf einfache Ja/Nein-Schulungsfragen zur Security Awareness für Azubis und neue Mitarbeiter.

PROZESSMANAGEMENT

Prozesse, die Sicherheit wirklich tragen

Patch-/Update-Prozess

Wer patcht wann? Kritische Sicherheitslücken werden sofort geschlossen

Berechtigungsprozess

Antrag → Freigabe → Umsetzung → regelmäßiges Review

Backup-Prozess

Backup-Plan plus regelmäßige Restore-Tests sind Pflicht

Incident-Management

Melden, Eindämmen, Beweissicherung, Wiederherstellung, Lessons Learned

Diese vier Kernprozesse bilden das Rückgrat der operativen IT-Sicherheit. Ohne dokumentierte und gelebte Prozesse bleibt Sicherheit eine Absichtserklärung ohne praktische Wirkung.

Arbeitsauftrag: *Schreiben Sie einen kompakten Incident-Kurzprozess mit sechs konkreten Schritten, einschließlich der Kommunikationswege („wer informiert wen wann").*

Technische Maßnahmen – Virenschutz & Endpoint Protection

Basis-Anforderungen Endpoint Security

Moderne Endpoint-Protection geht über klassischen Virenschutz hinaus. Die Mindestanforderungen umfassen:

Prüfungsfalle

Antivirus ist installiert, aber niemand schaut in die Management-Konsole – das ist Security-Theater ohne Wirkung.

Arbeitsauftrag: *Nennen Sie vier konkrete technische Mindestanforderungen an ein Virenschutzsystem im Betrieb mit jeweils einer Begründung.*

Virenschutz/EDR

Auf allen Clients und Servern installiert und aktiv

Mehrschichtige Erkennung

Echtzeitschutz, Signaturen und Verhaltenserkennung

Zentrale Verwaltung

Management-Konsole mit Reports als Nachweis

Quarantäne-Prozess

Automatische Isolation plus definierter Ablauf

Firewall & Netzwerksegmentierung

Eine saubere Netzwerksegmentierung trennt verschiedene Sicherheitszonen und reduziert die Angriffsfläche erheblich. Kritische Systeme werden vom normalen Benutzerverkehr isoliert.

Firewall-Grundprinzipien

Eine professionelle Firewall-Konfiguration basiert auf klaren Prinzipien:

- ***Stateful Firewall** mit klarer Regelbasis nach dem Prinzip „deny by default"*
- ***Segmentierung:** Servernetz, Clientnetz, Gäste-WLAN und Management-Netz getrennt*
- ***VPN mit MFA:** Starke Verschlüsselung, getrennte Admin-Zugänge*
- ***Umfassendes Logging:** Erlaubte und geblockte Events sowie alle Admin-Änderungen*

Arbeitsauftrag: Definieren Sie sechs Firewall-Regeln als Prinzipien (nicht als Port-Nummern), zum Beispiel: „Nur definierte Admin-IPs dürfen auf Management-Interfaces zugreifen".

E-Mail-Security & Anti-Spam

01

Mehrschichtiger Schutz

Spamfilter, Malware-Scan, URL- und Attachment-Filter arbeiten zusammen

02

Domain-Absicherung

SPF, DKIM und DMARC schützen vor Domain-Spoofing und Impersonation

03

Quarantäne-Management

Verdächtige Nachrichten werden isoliert, Freigabeprozess ist definiert

04

Phishing-Meldung

Einfacher Meldemechanismus per Button oder dedizierter E-Mail-Adresse

Phishing-Anzeichen erkennen

- *Dringlichkeit und Drohungen in der Betreffzeile*
- *Absenderadresse stimmt nicht mit angegebener Organisation überein*
- *Links führen zu abweichenden Domains (Hover-Check)*

Sofortmaßnahmen im Betrieb

1. *Verdächtige E-Mail nicht öffnen, Links nicht anklicken*
2. *An IT-Sicherheit/Helpdesk melden*
3. *Bei versehentlichem Klick: Passwort sofort ändern, IT informieren*

Arbeitsauftrag: *Nennen Sie drei konkrete Anzeichen für Phishing-Mails und drei unmittelbare Handlungsschritte im Verdachtsfall.*

Updates, Hardening, MFA & Backup – das Grundschutz-Brett

Patchmanagement

Betriebssysteme, Anwendungen und Firmware (Firewall, Switches, Access Points) werden regelmäßig aktualisiert

Hardening

Unnötige Dienste werden deaktiviert, sichere Defaults konfiguriert, Admin-Ports geschützt

Multi-Faktor-Authentifizierung

MFA für Admin-Konten, VPN, Cloud-Dienste und alle kritischen Systeme ist Pflicht

Backup-Strategie

3-2-1-Prinzip: 3 Kopien, 2 verschiedene Medien, 1 Kopie offline. Restore-Tests sind obligatorisch

Prüfungsfalle

Ein Backup ohne regelmäßige Restore-Tests ist Hoffnung, kein belastbares Konzept. Nur getestete Backups sind echte Backups.

Das 3-2-1-Prinzip in einem Satz: *Drei Kopien der Daten auf zwei verschiedenen Medientypen, wobei eine Kopie offline oder an einem anderen Standort liegt.*

Arbeitsauftrag: *Nennen Sie zwei verschiedene Varianten für Restore-Tests und erklären Sie deren jeweilige Vor- und Nachteile.*

Protokollierung & Monitoring – Nachweisbarkeit schaffen

Zentralisierte Log-Verwaltung

Effektives Monitoring erfordert die zentrale Sammlung und Auswertung von Logs aus allen relevanten Quellen:

- *Firewall-Logs (erlaubte und geblockte Verbindungen)*
- *Server-Logs (Systemereignisse, Fehler, Warnungen)*
- *Admin-Aktionen (alle privilegierten Zugriffe und Änderungen)*
- *VPN-Verbindungen (erfolgreiche und fehlgeschlagene Anmeldungen)*
- *Authentifizierungs-Events (Logins, Fehlversuche, Sperrungen)*

Aufbewahrungsfristen

Die Speicherdauer muss sowohl Audit-Anforderungen als auch datenschutzrechtliche Vorgaben berücksichtigen. Typisch sind 90 Tage bis 12 Monate, abhängig vom Log-Typ.

Kritische Events für Alarme

***Arbeitsauftrag:** Definieren Sie fünf „kritische Events" für unser Firewall-Szenario, die sofortiges Monitoring und Alerting erfordern.*

Admin-Login außerhalb der Geschäftszeiten

Mehrere Fehlversuche bei der Anmeldung (Brute-Force-Indikator)

Malware-Fund durch Endpoint-Protection

VPN-Anomalien (neue Geolocations, ungewöhnliche Zeiten)

Ungewöhnliche Firewall-Blockierungen in hoher Frequenz

Normen & Standards – ISO 27001 vs. BSI IT-Grundschutz

Die beiden wichtigsten Standards

ISO/IEC 2700x (insbesondere 27001/27002) *ist eine internationale Norm für Informationssicherheits-Managementsysteme (ISMS). Der Fokus liegt auf dem Plan-Do-Check-Act-Zyklus, umfassenden Nachweisen und kontinuierlicher Verbesserung. ISO 27001 ist zertifizierbar.*

BSI IT-Grundschutz *bietet konkrete Basismaßnahmen über strukturierte Bausteine. Die Methodik umfasst Schutzbedarfsfeststellung und darauf basierende Maßnahmenableitung für ein definiertes Grundschutz-Level. Sehr praxisorientiert für deutsche Verhältnisse.*

Prüfungsmerker

- *ISO 27001 = Management & Zertifizierung*
- *BSI Grundschutz = konkrete Basismaßnahmen & Bausteine*

Arbeitsauftrag: *Nennen Sie drei konkrete Gründe, warum Standards im Betrieb helfen – ohne „weil es Pflicht ist" als Argument.*

ZUSAMMENFASSUNG

Grundschutz im Betrieb – 5-Schritte-Methode

Mini-Prüfung – 5 Aufgaben im AP1-Stil

1. *Nennen Sie drei organisatorische Maßnahmen mit je einem konkreten Nutzen*
2. *Nennen Sie drei technische Maßnahmen mit je einem Risiko, das sie senken*
3. *Erklären Sie den Unterschied zwischen ISB und DSB in maximal zwei Sätzen*
4. *Nennen Sie vier unverzichtbare Inhalte einer Passwort-Policy*
5. *ISO 27001 vs. BSI Grundschutz: Nennen Sie einen Unterschied und eine Gemeinsamkeit*

Arbeitsauftrag zur Vertiefung: *Wenden Sie die 5-Schritte-Methode auf ein konkretes Projekt an – zum Beispiel „Firewall-Tausch mit High-Availability-Setup". Formulieren Sie für jeden Schritt einen prägnanten Satz.*