🛡️ Cyberangriff – Was tun, wenn es passiert ist?

Und wie Sie sich im Vorfeld wirksam schützen

Cyberangriffe sind längst keine Seltenheit mehr. Ob Ransomware, Phishing oder gezielte Attacken – auch kleine und mittlere Unternehmen geraten zunehmend ins Visier. Die Folgen sind oft dramatisch: Produktionsstillstand, Datenverlust, Reputationsschäden. Doch was ist zu tun, wenn der Ernstfall eintritt? Und: Wie kann man sich davor schützen?

Dieser Leitfaden bietet einen kompakten Überblick, natürlich ohne einen Anspruch auf Vollständigkeit zu haben – aber mit Empfehlungen führender Behörden wie dem **BSI**, der **Polizei**, **Datenschutzaufsichtsbehörden** sowie praxiserprobten Tipps aus der Wirtschaft.

🔐 Vor dem Angriff: Prävention ist der beste Schutz

Ein professionelles Sicherheitsniveau entsteht nicht über Nacht – aber mit den richtigen Maßnahmen lässt sich das Risiko eines erfolgreichen Angriffs deutlich senken.

✅ Technische Schutzmaßnahmen

- **Regelmäßige Sicherheitsupdates** (Patchmanagement) für Systeme und Anwendungen
- **Firewalls, Antivirenlösungen, Endpoint Detection & Response (EDR/XDR)**
- **Starke Zugangskontrollen:** Mehrstufige Authentifizierung (MFA), VPN für Remote-Zugriffe
- **Backups:** Getrennt, verschlüsselt und regelmäßig getestet

🧠 Organisatorische Maßnahmen

- **IT-Notfallplan erstellen:** Wer tut was im Ernstfall?
- **Zugriffsrechte nach dem Need-to-know-Prinzip**
- **Regelmäßige Awareness-Schulungen** für alle Mitarbeitenden
- **Simulationen & Krisenübungen**: Um Abläufe realistisch zu testen

---

🚨 Wenn es passiert ist: Reagieren – schnell und koordiniert

1. Interne Eskalation & Lageeinschätzung

- **IT-Sicherheitsverantwortliche kontaktieren:** Erste Analyse des Vorfalls
- **Krisenteam aktivieren:** Geschäftsführung, IT, Datenschutz, Kommunikation
- **Datenschutzbeauftragte einbinden:** Prüfung auf meldepflichtige Datenpanne nach DSGVO

2. Ausbreitung stoppen & Systeme sichern

- Betroffene Systeme **sofort vom Netz trennen**
- **Backups sichern**, laufende Backup-Vorgänge stoppen
- **Systemprotokolle, Screenshots und Speicherdaten sichern** – für spätere Analyse
- **Identifikation aller betroffenen Systeme** (auch versteckte Nebenwirkungen!)

3. Externe Stellen informieren

- **BSI – Bundesamt für Sicherheit in der Informationstechnik**
  → Unterstützung & Krisenhilfe: bsi.bund.de
- **Polizei – Zentrale Ansprechstellen Cybercrime (ZAC)**
  → Ermittlungen einleiten, Beweise sichern: polizei.de/zac
- **Landesdatenschutzbehörden:**
  → Meldung binnen 72 Stunden bei Datenpannen erforderlich.
  Beispiel MV: datenschutz-mv.de

🔄 Nach dem Vorfall: Lernen & stärken

1. Ursachenanalyse

- **Forensische Untersuchung:** Welche Schwachstellen wurden ausgenutzt?
- **Schwachstellen schließen** und Systeme härten

2. Wiederherstellung

- Systeme aus Backups **wiederherstellen oder neu aufsetzen**
- **Zugriffsrechte und Passwörter überprüfen** (inkl. 2FA einführen oder verstärken)

3. Dokumentation & Kommunikation

- Alle Schritte **dokumentieren** – für Behörden, Versicherungen, interne Auswertung
- Klare **interne Kommunikation** zur Stärkung des Sicherheitsbewusstseins
- Optional: **externe Kommunikation**, um Transparenz zu zeigen

---

🧭 Fazit: Vorbereitung entscheidet

Ein Cyberangriff kann jedes Unternehmen treffen – entscheidend ist, wie gut man darauf vorbereitet ist. Wer technische Schutzmaßnahmen trifft, seine Mitarbeitenden schult und für den Notfall klare Abläufe definiert, schützt nicht nur seine Daten, sondern auch seine Zukunftsfähigkeit.

💡 Extra-Tipp:

Nutzen Sie die **„TOP 12 Maßnahmen bei Cyber-Angriffen“** der Allianz für Cyber-Sicherheit als Checkliste zur Vorbereitung:

(Verlinkung zum PDF oder als Download einbinden)