

1 Sofortmaßnahmen - nach einem (fiktiven) Datenleck bzw. Hacker-Angriff (Kompakt-Darstellung)?

1.1 Profidata-IT / Web-Link

<https://www.profidata-it.de/Szenario---Digitale-Bedrohung.html>

1.2 Kompakt-Darstellung / Hardcopy



[profidata-IT](#) | [Kontakt](#) | [IoT-Sensor-Daten](#) | [Recht und Orga](#) | [Internes](#)

<p style="text-align: center;">1</p> <p style="text-align: center;">SOFORTIGE REAKTION:</p> <p>Wir schalten (wenn nötig und möglich) alle betroffenen Systeme sofort ab, um den Schaden zu minimieren.</p> <p>Externer Info-Link...</p>	<p style="text-align: center;">2</p> <p style="text-align: center;">KRISENSTAB EINRICHTEN:</p> <p>Wir rufen einen fachkundigen, internen Krisenstab zusammen, um die Situation zu koordinieren.</p> <p>Externer Info-Link...</p>	<p style="text-align: center;">3</p> <p style="text-align: center;">EINDÄMMUNG:</p> <p>Wir identifizieren und isolieren den Angriff, um seine Ausbreitung zu verhindern.</p>
<p style="text-align: center;">4</p> <p style="text-align: center;">ANALYSE UNDDOKUMENTATION:</p> <p>Wir sammeln alle relevanten Informationen und Meldungen über den Vorfall und dokumentieren alles möglichst detailliert.</p>	<p style="text-align: center;">5</p> <p style="text-align: center;">WIEDERHERSTELLUNG:</p> <p>Wir rebooten und stellen die betroffenen Systeme und Daten wieder her und protokollieren, dass keine Schadsoftware mehr vorhanden ist.</p>	<p style="text-align: center;">6</p> <p style="text-align: center;">MELDEPFLICHT PRÜFEN:</p> <p>Wir müssen (in Absprache mit unseren Kunden) überprüfen, ob wir verpflichtet sind, den Vorfall offiziell zu melden. Weitere Details dazu enthält die DSGVO.</p> <p>Daten-Meldung gemäß DSGVO...</p>
<p style="text-align: center;">7</p> <p style="text-align: center;">UNTERSTÜTZUNG ANFORDERN :</p> <p>Wir identifizieren und isolieren den Angriff, um seine Ausbreitung zu verhindern.</p> <p>Externer Info-Link...</p>	<p style="text-align: center;">8</p> <p style="text-align: center;">REFLEXION UND ANPASSUNG:</p> <p>Wir identifizieren und isolieren den Angriff, um seine Ausbreitung zu verhindern.</p>	<p style="text-align: center;">9</p> <p style="text-align: center;">KONTINUIERLICHE VERBESSERUNG:</p> <p>Auch noch nach dem eigentlichen Cyber-Vorfall führen wir regelmäßige Sicherheits-Überprüfungen und Penetrations-Tests durch.</p>

2 Vorgaben und Arbeitsschritte unseres Teams zur Bekämpfung und Prävention von Cyberangriffen:

2.1 (1) Sofortige Reaktion und Erste Maßnahmen

- a. **Erkennung und Bewertung des Vorfalls**
 - **Bestätigung des Vorfalls:** Verifizieren Sie, dass es sich tatsächlich um einen Cyber-Angriff handelt.
 - **Vorläufige Bewertung:** Bestimmen Sie das Ausmaß und die Auswirkungen des Angriffs auf Ihre Systeme und Daten.
- b. **Aktivierung des Incident Response Teams**
 - **Team-Benachrichtigung:** Informieren Sie sofort alle Mitglieder des Incident Response Teams.
 - **Rollenverteilung:** Weisen Sie klare Verantwortlichkeiten zu, um eine koordinierte Reaktion sicherzustellen.
- c. **Eindämmung des Angriffs**
 - **Systemtrennung:** Trennen Sie betroffene Systeme vom Netzwerk, um die Ausbreitung des Angriffs zu verhindern.
 - **Temporäre Maßnahmen:** Implementieren Sie Sofortmaßnahmen wie das Blockieren verdächtiger IP-Adressen oder das Erhöhen der Zugangskontrollen.

2.2 (2) Krisenstab einrichten

- a. **Zusammenstellen des Teams**
 - **Vielfältige Expertise:** Wählen Sie Mitglieder mit unterschiedlichen Fachkenntnissen aus IT-Sicherheit, Recht, Kommunikation und Management.
 - **Rollen und Verantwortlichkeiten:** Definieren Sie klare Aufgaben und Verantwortlichkeiten für jedes Mitglied des Krisenstabs.
- b. **Etablierung der Kommunikationskanäle**
 - **Sichere Kommunikationswege:** Richten Sie sichere Kommunikationsmittel wie verschlüsselte E-Mails oder gesicherte Messenger ein.
 - **Regelmäßige Updates:** Planen Sie regelmäßige Briefings und Updates, um alle Mitglieder des Krisenstabs auf dem neuesten Stand zu halten.
- c. **Entwicklung eines Krisenplans**
 - **Notfallprotokolle:** Erstellen Sie detaillierte Notfallprotokolle und Checklisten für verschiedene Szenarien.
 - **Ressourcen und Werkzeuge:** Stellen Sie sicher, dass alle notwendigen Ressourcen und Werkzeuge für den Krisenstab verfügbar sind.

2.3 (3) Eindämmung

- a. **Betroffene Systeme isolieren**
 - **Netzwerkrennung:** Trennen Sie die betroffenen Systeme sofort vom Netzwerk, um die Ausbreitung des Angriffs zu stoppen.
 - **Sperrung von Benutzerkonten:** Deaktivieren Sie kompromittierte Benutzerkonten und erhöhen Sie die Sicherheitsvorkehrungen für noch aktive Konten.
- b. **Vorläufige Sicherheitsmaßnahmen einleiten**
 - **Blockierung verdächtiger IP-Adressen:** Identifizieren und blockieren Sie verdächtige IP-Adressen, die mit dem Angriff in Verbindung stehen.
 - **Erhöhte Zugangskontrollen:** Implementieren Sie vorübergehend strengere Zugangskontrollen, wie Multi-Faktor-Authentifizierung (MFA), um unbefugten Zugriff zu verhindern.
- c. **Schadensbegrenzung**
 - **Daten sichern und sichern:** Sichern Sie alle kritischen Daten und erstellen Sie Backups, um Datenverlust zu vermeiden.
 - **Temporäre Systemfixes:** Führen Sie vorläufige Patches oder Updates ein, um bekannte Sicherheitslücken zu schließen, bis eine umfassendere Lösung implementiert werden kann.

2.4 (4) Analyse und Dokumentation

- a. **Forensische Untersuchung**
 - **Vorfallanalyse:** Untersuchen Sie die Ursache des Angriffs, die angewandten Methoden und die betroffenen Daten.
 - **Beweismittelsicherung:** Sichern Sie alle relevanten Beweismittel wie Protokolldateien, Netzwerkverkehr und betroffene Dateien für eine detaillierte Analyse und mögliche rechtliche Schritte.
- b. **Schwachstellenanalyse**
 - **Identifikation von Sicherheitslücken:** Bestimmen Sie die Schwachstellen, die den Angriff ermöglicht haben.
 - **Risikobewertung:** Bewerten Sie das Risiko dieser Schwachstellen und priorisieren Sie die Behebung entsprechend ihrer Kritikalität.
- c. **Dokumentation des Vorfalls**
 - **Chronologische Aufzeichnung:** Erstellen Sie eine detaillierte, chronologische Dokumentation aller Ereignisse und Maßnahmen, die während des Vorfalls durchgeführt wurden.
 - **Erstellung eines Vorfallberichts:** Fassen Sie die Ergebnisse der Analyse und die ergriffenen Maßnahmen in einem umfassenden Vorfallbericht zusammen, der für interne Schulungen und zukünftige Referenzzwecke verwendet werden kann

2.5 (5) Wiederherstellung

a. System- und Datenwiederherstellung

- **Sichere Backups verwenden:** Stellen Sie die betroffenen Systeme und Daten aus zuvor erstellten sicheren Backups wieder her, um den Normalbetrieb schnellstmöglich wieder aufzunehmen.
- **Integritätsprüfung:** Überprüfen Sie die Integrität der wiederhergestellten Daten und Systeme, um sicherzustellen, dass keine Schadsoftware oder beschädigten Dateien vorhanden sind.

b. Überprüfung und Validierung

- **Funktionsprüfung:** Führen Sie umfassende Tests durch, um sicherzustellen, dass alle wiederhergestellten Systeme und Anwendungen ordnungsgemäß funktionieren.
- **Sicherheitsprüfung:** Stellen Sie sicher, dass alle bekannten Sicherheitslücken geschlossen wurden und keine weiteren Schwachstellen bestehen.

c. Kommunikation und Dokumentation

- **Interne Information:** Informieren Sie alle Mitarbeiter über den Abschluss der Wiederherstellungsmaßnahmen und geben Sie Anweisungen, wie weiter vorzugehen ist.
- **Berichterstattung:** Dokumentieren Sie den gesamten Wiederherstellungsprozess und erstellen Sie einen Bericht, der die durchgeführten Maßnahmen und die aktuellen Systemzustände beschreibt.

2.6 (6) Meldepflicht prüfen

a. Risikobewertung des Datenvorfalles

- **Schweregrad des Vorfalls bewerten:** Bestimmen Sie, ob der Datenverlust oder der Cyber-Angriff ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt.
- **Betroffene Datenarten analysieren:** Prüfen Sie, welche Arten von personenbezogenen Daten betroffen sind (z. B. Finanzdaten, Gesundheitsinformationen, Identitätsdaten).

b. Relevante rechtliche Anforderungen überprüfen

- **Gesetzliche Meldepflichten identifizieren:** Ermitteln Sie, welche spezifischen gesetzlichen Meldepflichten in Ihrem Land oder Ihrer Region gelten (z. B. DSGVO in der EU, BDSG in Deutschland).
- **Behördliche Anforderungen erfüllen:** Stellen Sie sicher, dass alle Anforderungen der zuständigen Datenschutzbehörde, wie die Meldung innerhalb von 72 Stunden, eingehalten werden.

c. Informationsumfang und Verantwortlichkeiten festlegen

- **Erforderliche Informationen zusammenstellen:** Sammeln Sie alle notwendigen Details, die in der Meldung enthalten sein müssen, wie die Art des Vorfalls, die betroffenen Daten und die ergriffenen Maßnahmen.
- **Verantwortliche Person benennen:** Bestimmen Sie, wer für die Durchführung der Meldung an die Datenschutzbehörde und die Kommunikation mit den betroffenen Personen verantwortlich ist.

2.7 (7) Unterstützung anfordern

- a. **Interne Unterstützung mobilisieren**
 - **Kollegen und Fachabteilungen:** Informieren Sie relevante Fachabteilungen und Kollegen, um schnelle interne Hilfe und Ressourcen zu mobilisieren.
 - **Schlüsselpersonen benennen:** Identifizieren Sie Schlüsselpersonen, die spezifische Expertise oder Verantwortung in der Krisenbewältigung haben.
- b. **Externe Experten hinzuziehen**
 - **IT-Sicherheitsexperten:** Engagieren Sie externe IT-Sicherheitsexperten oder Dienstleister, die auf die Reaktion und Bewältigung von Cyber-Angriffen spezialisiert sind.
 - **Rechtliche Beratung:** Ziehen Sie rechtliche Berater hinzu, um sicherzustellen, dass alle rechtlichen Anforderungen eingehalten werden und rechtliche Schritte korrekt eingeleitet werden.
- c. **Behördliche Unterstützung**
 - **Kontaktaufnahme zu Behörden:** Melden Sie den Vorfall bei den zuständigen Datenschutzbehörden und bitten Sie gegebenenfalls um Unterstützung oder Anleitung.
 - **Zusammenarbeit mit Strafverfolgungsbehörden:** Bei schwerwiegenden Vorfällen arbeiten Sie eng mit den Strafverfolgungsbehörden zusammen, um die Täter zu identifizieren und rechtlich zu verfolgen.

2.8 (8) Reflexion und Anpassung

- a. **Erfahrungsbewertung**
 - **Lehren aus dem Vorfall:** Analysieren Sie den gesamten Vorfall und identifizieren Sie, welche Maßnahmen gut funktioniert haben, und welche verbessert werden müssen.
 - **Feedback sammeln:** Holen Sie Feedback von allen Beteiligten ein, um verschiedene Perspektiven und Erfahrungen zu berücksichtigen.
- b. **Prozessoptimierung**
 - **Anpassung der Notfallpläne:** Aktualisieren und optimieren Sie Ihre Notfall- und Wiederherstellungspläne basierend auf den Erkenntnissen aus der Reflexion.
 - **Sicherheitsrichtlinien verbessern:** Überprüfen und verstärken Sie Ihre Sicherheitsrichtlinien und -protokolle, um ähnliche Vorfälle in Zukunft zu verhindern.
- c. **Technologische Verbesserungen**
 - **Neue Sicherheitsmaßnahmen implementieren:** Evaluieren und implementieren Sie neue Technologien und Tools, die Ihre Sicherheitsinfrastruktur stärken.
 - **System-Updates und Patching:** Stellen Sie sicher, dass alle Systeme auf dem neuesten Stand sind und regelmäßige Sicherheitsupdates und Patches eingespielt werden.

2.9 (9) Kontinuierliche Verbesserung

- a. **Regelmäßige Überprüfungen und Audits**
 - **Sicherheitsaudits:** Führen Sie regelmäßige Sicherheitsaudits und Penetrationstests durch, um mögliche Schwachstellen zu identifizieren und zu beheben.
 - **Prozessbewertungen:** Überprüfen Sie regelmäßig Ihre Sicherheitsprozesse und -richtlinien, um sicherzustellen, dass sie aktuell und effektiv sind.
- b. **Feedbackschleifen und Optimierungen**
 - **Feedbackintegration:** Integrieren Sie Feedback aus Vorfällen und Übungen in Ihre Sicherheitsstrategie, um kontinuierliche Verbesserungen vorzunehmen.
 - **Optimierungsmaßnahmen:** Entwickeln und implementieren Sie Maßnahmen zur Optimierung Ihrer Sicherheitsinfrastruktur basierend auf den Ergebnissen der Feedbackschleifen.
- c. **Einsatz von KI-gestützten Lösungen**
 - **KI-basierte Bedrohungserkennung:** Nutzen Sie Künstliche Intelligenz, um Bedrohungen in Echtzeit zu erkennen und darauf zu reagieren.
 - **Automatisierte Analyse:** Implementieren Sie KI-gestützte Analysewerkzeuge, um große Mengen an Sicherheitsdaten effizient zu verarbeiten und potenzielle Schwachstellen schneller zu identifizieren.