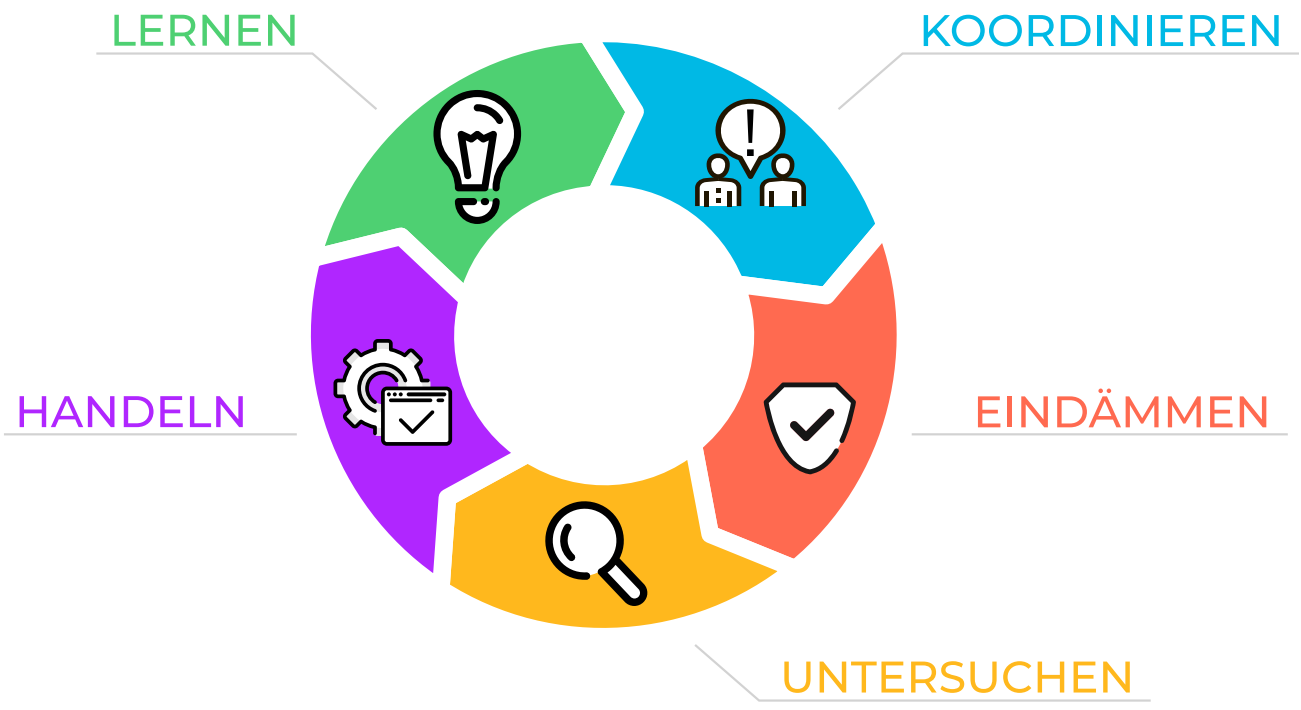
DATENLECK! UND NUN?



Ein Datenleck kann **verheerende finanzielle Folgen** haben, sei es durch den Verlust von Kunden, rechtliche Konsequenzen oder einen Reputationsschaden. Eine umfassende Aufarbeitung ist daher unerlässlich! Es sollten zügig **Sofortmaßnahmen** ergriffen werden, um die Ursachen zu ermitteln und die Sicherheitslücken zu schließen.

Im folgenden finden Sie einen kurzen **5-Punkte-Plan**, der die wichtigsten Maßnahmen enthält, die Sie jetzt treffen sollten. Zusätzlich finden Sie am Ende eine umfassende **Checkliste**, mit deren Hilfe Sie Ihren aktuellen Status festhalten können.

Sofortmaßnahmen

1. KOORDINIEREN: Überprüfen Sie die gemeldeten Informationen und stellen Sie sicher, dass es sich tatsächlich um ein Datenleck handelt. Stellen Sie außerdem sicher, dass alle relevanten Personen (z. B. Management, Systemadministrator, Datenschutzbeauftragter) über den Vorfall informiert sind und die Verantwortlichkeiten für alle nächsten Schritte geklärt sind.
2. EINDÄMMEN: Wird Ihnen ein Datenleck bekannt, dann heißt es: Schnell handeln! Um den Schaden möglichst gering zu halten, sollten sie sofort passende Gegenmaßnahmen ergreifen. Konkret bedeutet dies: Beheben Sie das Datenleck indem Sie den Zugriff auf die Daten unterbinden (z. B. durch geeignete Firewallregeln).
3. UNTERSUCHEN: Um das genaue Ausmaß des Vorfalls einschätzen zu können, sollten Sie einige Fragen beantworten: Welche Daten sind betroffen (z. B. personenbezogene Daten, Geschäftsdaten, Zugangsdaten ...)? Wer ist betroffen? Wer hat auf die Daten zugegriffen (z. B. über eine Analyse der Serverlogs)?
4. HANDELN: Sobald das genaue Ausmaß des Vorfalls bekannt ist, müssen in der Regel weitere Maßnahmen ergriffen werden:
    1. INFORMIEREN: Für den Fall, dass personenbezogene Daten betroffen sind und nicht ausgeschlossen werden kann, dass dies zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, muss binnen 72 Stunden die zuständige Aufsichtsbehörde benachrichtigt werden (siehe Art. 33 DSGVO).
    2. ABSICHERN: Sind Account- oder Zugangsdaten kompromittiert worden (z. B. Passwörter), müssen diese geändert werden. Alle betroffenen Accountinhaber müssen in diesem Fall informiert werden, um auch eventuell weitere betroffene Accounts absichern zu können.
    3. SCHÜTZEN: Sind sensible Daten (z. B. Daten vulnerabler Gruppen oder kritischer Systeme) betroffen, müssen eventuell zusätzliche Maßnahmen ergriffen werden, um eine spätere Gefährdung auszuschließen und einen dauerhaften Schutz gewährleisten zu können.
5. LERNEN: Ist der Vorfall aufgearbeitet, stellt sich die Frage: Wie lassen sich solche Schwachstellen zukünftig vermeiden? Fehler passieren und lassen sich auch nie ganz ausschließen. Allerdings lassen sich z. B. Maßnahmen einführen, um Fehler früher oder sogar automatisch zu erkennen. Durch geeignete Prozesse und Automatismen können viele Probleme effizient abgefangen werden, bevor sie überhaupt entstehen. Falls Sie hierbei Hilfe benötigen oder Fragen haben, können Sie gerne ein kostenloses Erstgespräch mit uns vereinbaren.

Checkliste

1. ☐ Unautorisierten Zugriff auf die Quelle des Datenlecks unterbinden z. B. durch:
    1. ☐ Zugriff auf Datenbank über Firewall einschränken
    2. ☐ unabsichtlich exponierte Datenbank vom Netz nehmen
    3. ☐ unabsichtlich exponierte Dateien vom Server entfernen
    4. ☐ Achtung: Die Daten sollten nicht direkt komplett gelöscht werden, um eine spätere Aufarbeitung zu ermöglichen!
2. ☐ Ausmaß des Datenlecks untersuchen:
    1. ☐ Sind im Datenleck Account- oder Zugangsdaten enthalten? (z. B. Passwörter oder Passworthashes)
        1. ☐ Accountinhaber informieren
        2. ☐ Falls möglich, betroffene Zugangsdaten ändern
        3. ☐ Andernfalls, Passwortänderungsprozess anstoßen
    2. ☐ Sind im Datenleck Kundendaten/personenbezogene Daten enthalten?
        1. ☐ Falls nötig, Datenschutzvorfall an Aufsichtsbehörde melden (72h Frist; siehe Art. 33 DSGVO)
        2. ☐ Falls nötig, Betroffene informieren (siehe Art. 34 DSGVO)
    3. ☐ Wer hat auf die Daten zugegriffen?
        1. ☐ Ist eine lückenlose Dokumentation aller Zugriffe auf die Daten möglich? (vom Ursprung des Datenlecks bis zur Meldung durch Lutra Security)
        2. ☐ Sind alle Zugriffe auf autorisierte/vertrauenswürdige Parteien zurückzuführen? (zur vollständigen Aufarbeitung können wir gerne die IP-Adressen von Lutra Security zur Verfügung stellen)
3. ☐ Nächste Schritte definieren, dabei können beispielsweise folgende Fragen helfen:
    1. ☐ Wie kam es zu dem Vorfall?
    2. ☐ Ist sichergestellt, dass ich Vorfälle dieser Art zukünftig vermeiden oder erkennen kann?
    3. ☐ Welche Maßnahmen kann ich ergreifen, um ähnliche Vorfälle zu vermeiden?

https://lutrasecurity.com
hello@lutrasecurity.com
+49 89 2152 5883-0

lutra security

NACHHALTIG SICHERER