Checkliste

Welche Kostenfaktoren im Falle eines Datenverlustes zu berücksichtigen sind

Pauschale Angaben auf Basis von Durchschnittswerten sind wenig hilfreich, um die finanziellen Folgen des Verlusts geschäftskritischer Daten realistisch einschätzen zu können. Balabit empfiehlt Unternehmen deshalb eine individuelle Einschätzung vorzunehmen. Denn je nach Branche, in der ein Unternehmen tätig ist, Compliance-Vorgaben und Datenschutzregelungen können diese Werte stark variieren. In der folgenden Checkliste sind zentrale Punkte aufgeführt, die berücksichtigt werden sollten, um die Gesamtkosten von Datenlecks für ein Unternehmen zu erfassen.

1. **Informationspflicht**: Ist das Unternehmen gesetzlich verpflichtet, nach einem Datenleck betroffene Kunden zu informieren? Wenn ja, auf welchem Weg soll das erfolgen (Telefon, E-Mail, Briefpost)? Die Antworten auf diese Fragen erlauben es, die Kosten abzuschätzen, etwa Arbeitszeit, Material, Briefporto et cetera.
2. **Erweiterung der Kapazitäten in der Kundenbetreuung:** Selbst dann, wenn nur jeder zehnte betroffene Kunde oder Partner nach einem Datenleck mit Kundenbetreuern Kontakt aufnimmt, kann dies zu einer erheblichen Mehrbelastung der Abteilung führen. Zu klären ist, ob die Zahl der Betreuer zeitweilig erhöht werden muss, ob die Anfragen mit eigenem oder nur mithilfe von Fremdpersonal zu bewältigen sind und welche Mehrkosten (zusätzliches Personal, Überstunden) das verursacht. Hilfreich ist, mehrere Szenarien zu erarbeiten, etwa für den Fall, dass jeder fünfte oder fünfzehnte Kunde Kontakt zum Unternehmen aufnimmt.
3. **Schadenersatzforderungen:** Die Rechtsabteilung muss prüfen, ob das Unternehmen Kunden Schadenersatz leisten muss, wenn diese durch das Datenleck finanzielle Einbußen erlitten haben.
4. **Kreditkarten sperren:** Sollten Kreditkarteninformationen abhandengekommen sein, kann es notwendig sein, Karten zu sperren und Kunden neue Versionen zur Verfügung zu stellen. Auch das kostet Zeit und Geld.
5. **Kundenverluste:** Eine mögliche Folge von Datenverlusten ist, dass Kunden und Partnerfirmen das Vertrauen verlieren und die Zusammenarbeit mit einem Unternehmen beenden. Wichtig ist, die „Absprungrate“ von Kunden und die damit verbundenen Umsatz- und Gewinneinbußen zu ermitteln.
6. **Kosten der Neukunden-Akquise:** Um Kundenverluste zu kompensieren, müssen gegebenenfalls neue Kunden akquiriert werden. Auch in diesem Fall gilt es die entsprechenden Kosten aufzuschlüsseln. Meist verfügen Unternehmen bereits über entsprechende Daten, sprich wie viel Euro zu veranschlagen sind, um einen neuen Kunden zu gewinnen.
7. **Kompensationszahlungen:** Unabhängig davon, ob ein Unternehmen juristisch dazu verpflichtet ist, kann es betroffenen Kunden Rabatte oder Kompensationszahlungen anbieten. Zu klären ist, welche Arten von Entschädigungen in Frage kommen (Geld, Gutscheine) und wie hoch der finanzielle Aufwand dafür ist.

8. **Folgen eines Identitätsdiebstahls prüfen:** Sollte es Angreifern gelungen sein, die „digitale Identität“ von Kunden oder Mitarbeitern zu stehlen, kann ein „Credit Monitoring“ angebracht sein, also eine Kontrolle der Zahlungen, die vom Konto eines Kunden aus vorgenommen werden. Diese Serviceleistungen kosten Geld.
9. **Höhe von Strafen ermitteln:** Die IT- und Rechtsabteilung sollten ermitteln, ob Aufsichtsbehörden und Gerichte Strafen verhängen können, etwa wegen des Verstoßes gegen die EU-Datenschutz-Grundverordnung.
10. **Haftung von Führungskräften prüfen:** Bei schwerwiegenden Verstößen gegen Datenschutzbestimmungen können IT-Leiter oder Geschäftsführer vor Gericht gezogen und sogar zu Haftstrafen verurteilt werden. Neben den Anwalts- und Gerichtskosten müssen in solchen Fällen auch Ausgaben für Ersatzpersonal einkalkuliert werden, etwa für Interims-Manager.
11. **Vertragsstrafen**: Verträge mit Geschäftspartnern, Kunden und Zulieferfirmen können einen Passus enthalten, der Vertragsstrafen im Fall von Datenverlusten vorsieht. Kommt es zu einem solchen Vorfall, ist zu prüfen, welche Vertragspartner Ansprüche haben und wie hoch diese sind.
12. **Einschaltung externer IT-Sicherheitsfachleute:** Ein Kostenfaktor sind externe IT-Security-Spezialisten, etwa Fachleute für Forensik. Ihr Einsatz kann notwendig sein, um Details eines Datenverlustes oder Angriffs auf IT-Systeme zu ermitteln.
13. **Kosten durch den Ausfall von IT-Systemen:** Ein erfolgreicher Angriff auf IT-Systeme und Datenbestände hat möglicherweise zur Folge, dass diese Systeme eine Zeit lang nicht verfügbar sind und Ersatzkomponenten eingesetzt werden müssen. Die IT-Abteilung muss in jedem Fall prüfen, welche Systeme und IT-Dienste betroffen sind und welche heruntergefahren oder über andere Rechenzentren beziehungsweise IT-Komponenten bereitgestellt werden können. Einzurechnen sind zudem Umsatzeinbußen (Euro pro Tag), etwa wenn ein Online-Marktplatz zeitweilig nicht verfügbar ist.
14. **IT-Systeme und Datenbeständige überprüfen und gegebenenfalls neu aufsetzen:** Nach Erfahrungswerten von Balabit ist es nach einem „Data Breach“ meist unvermeidbar, die betroffenen IT- und Netzwerkkomponenten zu überprüfen und neu einzurichten. Zudem muss die Integrität der Daten überprüft werden. Damit sind beispielsweise folgende Aufwendungen verbunden: Test und Neukonfiguration von Systemen, die Überprüfung durch ein externes Labor und die dafür erforderliche Arbeitszeit von IT-Fachleuten.
15. **Unterstützung durch Rechtsexperten:** Ein Unternehmen muss gegebenenfalls einen externen Rechtsexperten engagieren, etwa einen Spezialisten auf dem Gebiet Datenschutzrecht.
16. **Hilfe durch externe PR-Fachkräfte:** Wird ein Datenleck publik, bedeutet dies in der Regel einen Image-Schaden. Daher kann es notwendig sein, externe PR-Fachleute für die Krisenkommunikation zu engagieren und mithilfe zusätzlicher PR-Maßnahmen den Schaden zu begrenzen.
17. **Auswirkungen auf den Unternehmenswert:** Bei börsennotierten Unternehmen können IT-Sicherheitsvorfälle und Datenverluste den Aktienkurs tangieren. Dies ist vor allem dann problematisch, wenn Übernahmegespräche anstehen.
18. **Spezialfall Finanzunternehmen – Folgen für die Liquidität:** Zwar gelten für Banken und Finanzdienstleister verschärfte Datenschutzvorgaben, etwa PCI-DSS. Allerdings sind solche Unternehmen auch besonders beliebte Ziele von Hacker-

Angriffen. Kommen bei solchen Attacken vertrauliche Daten abhanden, ziehen Kunden möglicherweise in großem Stil Einlagen und Depots ab. Im Extremfall führt dies zu Liquiditätsengpässen bei dem betreffenden Unternehmen. Damit verbunden sind erhöhte Kosten, etwa durch die kurzfristige Aufnahme von Krediten, um die Liquidität wiederherzustellen.

Fazit

Die genannten Beispiele machen deutlich, dass der unzureichende Schutz kundenbezogener Daten Kosten in Bereichen verursachen kann, die viele IT- und Geschäftsentscheider nicht auf dem Radar haben. Wer diese Aufwendungen summiert, erkennt schnell, dass sich die Ausgaben für IT-Sicherheitslösungen bezahlt machen. Kernelemente einer Sicherheitsarchitektur sind vor allem ein effektives Log-Management und ein Monitoring der Aktivitäten von Nutzern mit privilegierten Zugriffsrechten (Privileged Access Management). Solche Lösungen ermöglichen es, proaktiv Angriffe und Sicherheitsschwachstellen zu identifizieren und somit bereits im Vorfeld Datenverluste zu verhindern.

Pressekontakt
punktgenau PR
Christiane Schlayer
Fon +49 (0)911 9644332
Mobil +49 (0)179 5053522
christiane.schlayer@punktgenau-pr.de
www.punktgenau-pr.de

Kontakt zu Balabit
Balabit IT Security GmbH
Dara Nolan
Stefan-George-Ring 29
81929 München
Fon +49 (0)89 9308-6477
dara.nolan@balabit.com
www.balabit.com