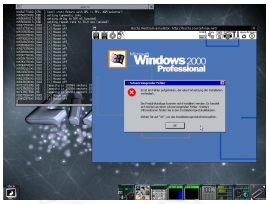



# Millionenschäden: Die Kosten eines Datenlecks - Best Practices der Data Security für Unternehmen

Cyberkriminelle haben es häufig auf lukrative Daten abgesehen – mit oft beträchtlichem finanziellem Schaden für das gehackte Unternehmen: In Deutschland kostet ein Datenverstoß eine Organisation durchschnittlich umgerechnet 4,32 Mio. Euro (4,78 Mio. US-Dollar), so das Ergebnis des aktuellen Cost of a Data Breach Report des Ponemon Institute und IBM. Deutschland besetzt damit Platz 3 nach den USA (8,19 Mio. US-Dollar) und dem Mittleren Osten (5,97 Mio. US-Dollar). Der globale Durchschnitt liegt bei 3,92 Mio. US-Dollar.

Der Report befragte weltweit 507 Unternehmen aus 17 Branchen und untersuchte unter anderem, wie durch Abwehrmaßnahmen die Kosten eines Datenlecks reduziert werden können. Beispielsweise trugen Unternehmen, die Security-Automation-Technologien eingesetzt hatten, nur etwa die Hälfte der Kosten einer Datensicherheitsverletzung, verglichen mit Unternehmen, die diese Technologien nicht eingesetzt hatten. Eine umfassende Data Security-Strategie ist für jedes Unternehmen deshalb heutzutage unumgänglich, um finanzielle Schäden durch Datenlecks einzudämmen.

Grundlegende Best Practices für die Data Security

**1. Data Discovery**
Heute befinden sich Daten nicht nur in Unternehmensnetzwerken, sondern auch in der Cloud, auf Mobilgeräten und an Homeoffice-Arbeitsplätzen. Das Aufspüren sensibler Daten sowie die Transparenz zu wissen, wohin Daten fließen, wer darauf Zugriff hat und sie weitergeben kann, ist grundlegend für die Datensicherheit. Ansonsten können Unternehmen nicht bewerten, welche Dateien, Dokumente oder geistiges Eigentum das größte Risiko bei einem Sicherheitsverstoß darstellen. Der erste Schritt ist deshalb die Entwicklung einer organisatorischen Sichtung und Strukturierung aller Daten.

Umfassende Data Loss Prevention-Lösungen (DLP) verfügen über Data Discovery-Appliances. Diese ermöglichen ein automatisches, konfigurierbares Scannen von lokalen und Netzwerk-Freigaben unter Verwendung von erkennungsspezifischen Inspektionsrichtlinien, um sensible Daten überall dort zu finden, wo sie sich befinden. Detaillierte Auditprotokolle und -berichte liefern zudem die erforderlichen Informationen, um die Einhaltung von Vorschriften nachzuweisen, vertrauliche Informationen zu schützen und das Risiko von Datenverlusten zu verringern.

**2. Datenklassifizierung**

Die Strategien zur Datenklassifizierung können von Unternehmen zu Unternehmen variieren, aber durch den Einsatz von DLP-Tools zur Analyse sensibler Daten und der Anwendung von Richtlinien können Unternehmen die dringend benötigte Struktur in ihre Sicherheitsstrategie implementieren. Üblicherweise werden Daten in folgende Kategorien eingeteilt:

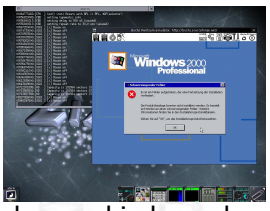
- Eingeschränkt: Daten, die bei einem Datenleck dauerhafte und schwere Konsequenzen für ein Unternehmen bedeuten
- Vertraulich: Daten, die vor unbefugtem Zugriff geschützt werden müssen und mäßig sensible Informationen enthalten
- Öffentlich: Daten, die geteilt werden dürfen

**3. Zugriffskontrollen und kontinuierliche Datenverfolgung**

Nachdem die Daten klassifiziert wurden, sollten Unternehmen sicherstellen, dass auf Benutzerebene geeignete Sicherheitskontrollen vorhanden sind, um Informationen vor Diebstahl zu schützen. Richtlinienkontrollen stellen sicher, dass Daten nicht durch böswillige oder fahrlässige Mitarbeiter verändert, verloren oder gestohlen werden können. Gerade unvorsichtige Mitarbeiter sind seit Jahren eine der Hauptursachen für den Verlust von Unternehmensdaten.

Um Risiken zu minimieren, entscheiden sich deshalb viele Unternehmen für Kontrollen, die den Datenzugriff für die Mitarbeiter einschränken. Dies stellt sicher, dass Angestellte nur Zugang auf für ihre Arbeit notwendige Daten haben. Data Loss Prevention-Tools bieten hier die Überwachung, Verfolgung und den Schutz sensibler Daten vor nicht autorisiertem Zugriff während des gesamten Verarbeitungszyklus, unabhängig davon, ob sie sich im Ruhezustand, Gebrauch oder in Übertragung befinden. Einige Lösungen verfügen über Richtlinien, die das Auffordern, Blockieren oder automatische Verschlüsseln ermöglichen, wenn ein Benutzer mit sensiblen Daten arbeitet. Andere können so konfiguriert werden, dass sie unbefugten Zugriff auf sensible Inhalte, Manipulationen oder die Synchronisierung mit Cloud-Umgebungen vollständig verhindern.

**4. Mitarbeiteraufklärung bei riskantem Verhalten**




Neben der Möglichkeit, kritische Daten zu überwachen und zu verfolgen, können Kontrollen zudem verhindern, dass Benutzer bestimmte Handlungen ausführen, wie etwa Daten zu verschieben, zu kopieren oder zu drucken. In diesen Szenarien können Administratoren DLP-Lösungen einsetzen, um Nutzern Benachrichtigungen anzuzeigen, die erklären, weshalb eine Handlung – sei es der Zugriff, das Verschieben oder das Verschicken bestimmter Daten per Mail – verboten ist. Dies trägt zur Aufklärung der Mitarbeiter bei und fördert die Optimierung im Umgang mit kritischen Informationen.

## 5. Einsatz verhaltensbasierter Erkennungswerkzeuge

Neben Data Loss Prevention, können zudem Lösungen wie Endpoint Detection and Response (EDR) oder Advanced Threat Protection (ATP) Bedrohungen in Echtzeit erkennen, bevor Daten gefährdet werden. EDR-Tools überwachen Endpunkt- und Netzwerkereignisse und speichern diese Informationen in einer zentralen Datenbank. Diese Daten werden auf Anomalien wie selten auftretende Prozesse, ungewöhnliche oder unbekannte Verbindungen und andere verdächtige Aktivitäten untersucht. Der Vorgang kann automatisiert werden, wobei Anomalien Alarme für sofortige Gegenmaßnahmen oder weiterführende Untersuchungen auslösen. Zudem bieten viele EDR-Tools auch eine manuelle oder nutzergesteuerte Datenanalyse.

Wenn Organisationen genau wissen, welche ihrer Daten besonders wertvoll sind, können sie diese zielgerichtet durch kontinuierliche Überwachung und Verschlüsselung gegen externe Angreifer und Insider-Bedrohungen verteidigen, selbst im Fall eines Sicherheitsverstoßes. Der Einsatz der obengenannten Data Security-Best Practices kann Unternehmen helfen, ihre sensiblen Informationen besser zu schützen und hohe Kosten durch einen Sicherheitsvorfall zu vermeiden.