Was kostet eine Datensicherheitsverletzung

Martin Runde | Marketing Manager Security DACH | 17. September , 2020

IBM Security

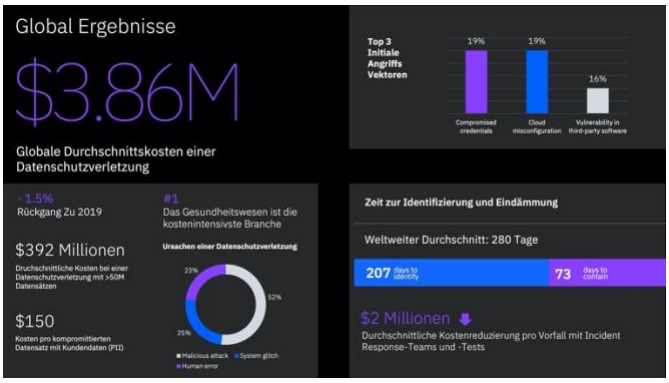
Die Frage ist nicht ob sondern wann ein Unternehmen Opfer einer Datensicherheitsverletzung wird. Welche Folgen drohen ist das Thema der „Cost of a Data Breach“ Studie.

Das Ponemon Institut hat im Auftrag der IBM zum 15mal in Folge die jährliche „Cost of a Data Breach“ Studie veröffentlicht. Die Studie versucht die Folgen von Datensicherheitsverletzungen zu quantifizieren. Also zu ermitteln welche Kosten in der Folge von Datensicherheitsverletzungen bei Unternehmen unterschiedlicher Größenordnungen und Industrien entstehen. Der Report ist fest im Markt etabliert und zeigt vor allem auch die historische Entwicklung der Kosten im Jahres- und Ländervergleich.

Der Aufwand, der getrieben wird, um belastbare Daten zu erzielen ist enorm. Für den Bericht 2020 hat das Ponemon Institute mehr als 500 Organisationen befragt, bei denen zwischen August 2019 und April 2020 Datensicherheitsverletzungen aufgetreten sind. Dabei handelt es sich um Unternehmen aus 17 Ländern, unterschiedlichen Größenordnungen und Branchen. Um die Daten zu erheben wurden mehr als 3.000 Einzelinterviews mit betroffenen Personen durchgerührt.

Die Daten haben damit eine hohe Aussagekraft und stellen für Unternehmen einen wichtigen Benchmark dar, um ihr eigenes finanzielles Risiko bewerten zu können. Im weltweiten Durchschnitt liegen die Kosten für eine Datensicherheitsverletzung bei 3.86 Millionen US Dollar. Die Spanne reicht dabei von mehr als 8 Millionen US Dollar bei US-amerikanische Unternehmen bis hin zu knapp über 1 Millionen US Dollar in Brasilien. Hier gibt es natürlich eine deutliche Korrelation zu der Wirtschaftsleistung eines Landes und des betroffenen Unternehmens.

Bemerkenswert ist die durchschnittliche Lebensdauer einer Datensicherheitsverletzung, die im Schnitt bei 270 Tagen bis zur Entdeckung und Beseitigung liegt. Viel Zeit für die Angreifer sich in Ruhe in einem Netzwerk einzurichten, Spuren zu verwischen, sich auszubreiten, Informationen zu sammeln, um dann zielgerichtet zuzuschlagen. Nicht überraschend ist hingegen die Korrelation zwischen dieser Lebensdauer und der entstehenden Schadenshöhe



Die Ursachen für Datensicherheitsverletzungen selbst sind vielfältig und reichen von menschlichem Versagen bis hin zu Systemfehlern. Allerdings sind in mehr als der Hälfte aller Fälle Cyber-Angriffe für die Vorfälle verantwortlich. Als Einfallstor für diese böswilligen Datensicherheitsverletzungen dienen in erster Linie kompromittierte Benutzerkennungen und Fehlkonfigurationen in der Cloud. Hier ist die Implementierung eines modernen Identitäts- und Zugriffsmanagements, sowie die Identifizierung, Lokalisierung und der Schutz kritischer Daten in hybriden Multi Cloud Umgebungen eine geeignete und wirkungsvolle Gegenmaßnahme.

Betroffen sind bei gut 80% aller Datensicherheitsverletzungen Personen bezogene Informationen. Hier haben wir dann auch den größten Einfluss auf die verursachten Kosten durch Meldepflichten, Vertrauens- und Reputationsverlust .

Die Studie hilft Unternehmen nicht nur zu verstehen mit welchen Kosten eine Datensicherheitsverletzung durchschnittlich verbunden ist. Sie können auch erkennen, welche Maßnahmen diese Kosten in welchem Maße reduzieren oder erhöhen. Dieses Wissen ermöglicht den Unternehmen dann Investitionen in Sicherheit gezielt und anhand des tatsächlichen Nutzens zu planen.

So ist die Fähigkeit eines Unternehmens zur Reaktion auf Zwischenfälle durch den Einsatz geschulter Incident Response Teams der größte Kostensenker.

Am effektivsten, um die Kosten von Datenverstößen zu senken sind hingegen Technologien wie erweiterte Analysefähigkeiten, der Einsatz von KI und Orchestrierung, um Risiken zu identifizieren und automatisiert auf Vorfälle reagieren zu können.

Auf der anderen Seite der Liste stehen komplexe Security Landschaften als der größte Kostentreiber bei Datensicherheitsverletzungen. Hier können Unternehmen durch Konsolidierung und Modernisierung Ihrer Sicherheitsinfrastruktur ihr Risiko deutlich reduzieren.

Die Studie zeigt viele auch regionale und branchenspezifische Zusammenhänge auf von denen wir hier nur einige darstellen konnten. Ein Blick in die Studie lohnt sich für jeden der Security Programme oder Investitionen verantwortet.

Unter dem folgenden Link kann die Studie kostenlos heruntergeladen werden.

https://www.ibm.com/downloads/cas/JPKPEA40