Mit Sicherheit sicher!

Richtlinien für die Schadensbegrenzung nach einer Verletzung der Datensicherheit

Sie gehen vermutlich davon aus, dass Ihre Unternehmensdaten sicher sind – aber der schlimmste aller Fälle kann auch bei Ihnen eintreten. Aktuell geschieht genau das so oft wie nie zuvor. Die gemeinnützige Organisation Privacy Rights Clearinghouse fand heraus, dass es 2011 in Unternehmen zu 313 Datenschutzverletzungen kam. Rund 23 Millionen Akten mit sensiblen Daten waren davon betroffen. Zum Vergleich: 2010 war die Sicherheit von 12 Millionen Akten gefährdet.[2 1] Die Wahrheit ist: Datenmissbrauch stellt heutzutage eine der besorgniserregendsten Angelegenheiten jedes Unternehmens dar.

Nachfolgend haben wir für Sie einige einfache Richtlinien aufgeführt, die Sie beachten sollten, wenn es in Ihrem Unternehmen zum Missbrauch von elektronischen Daten oder Papierdokumenten kommt. Auch wenn einige dieser Hinweise Sie vielleicht überraschen – sie alle basieren auf Ratschlägen von Experten und Erfahrungen von Unternehmen, die bereits mit solchen Sicherheitsverletzungen zu tun hatten.*

Holen Sie sich umgehend einen Rechtsbeistand.

- Bevor Sie außenstehende Experten ins Boot holen, sollten Sie zunächst Ihren Rechtsanwalt auf den neuesten Stand der Dinge bringen, rät Forensiker Kevin Mandia, der als Ermittler für den Online-Broker TD Ameritrade arbeitete.[3]

- Es ist nicht immer notwendig, ein externes Forensikerteam zu engagieren.

- Erstellen Sie eine Liste der betreffenden Daten. Sie können sich auch dafür entscheiden, den Datenmissbrauch nicht zu melden – das hängt ganz von den Daten ab, die gestohlen wurden oder vermisst werden (Beispiele von Datenverlusten, die unbedingt gemeldet werden müssen, finden Sie auf der nächsten Seite).

Gehen Sie nicht davon aus, dass es jemand aus der Firma war.

- Sie sollten sich zu Beginn nicht nur auf diese Möglichkeit konzentrieren, auch wenn die meisten Unternehmen automatisch davon ausgehen, so Mandia.

- Ermittlungen innerhalb eines Unternehmens kosten 10 Mal mehr als außerhalb des Unternehmens. Der Grund: Sie müssen zum Teil verdeckt durchgeführt werden, was oft monatelang dauern kann.

- Innerhalb der ersten fünf Tage nach einem Datenmissbrauch sollten Sie so schnell wie möglich aktiv werden, um festzustellen, was genau geschehen ist und wer involviert war.

Bestimmen Sie jemanden, der die Untersuchungen durchführen soll und erstellen Sie einen Aktionsplan.

- Nachdem ein Datenmissbrauch aufgedeckt wurde, gibt es in vielen Unternehmen oft keine klare Ermittlungsrichtung, weil innerhalb der Firma kein verantwortlicher Ansprechpartner für solche Vorfälle vorhanden ist.

Wir über uns

Shred-it ist auf die Bereitstellung eines auf den Kunden zugeschnittenen Aktenvernichtungsservice spezialisiert, der Unternehmen die Einhaltung von Gesetzen ermöglicht und gewährleistet, dass ihre Kunden, Mitarbeiter und vertraulichen Geschäftsinformationen zu jeder Zeit sicher sind. Wir bieten in der Branche den sichersten und effizientesten Vernichtungsservice von vertraulichen Daten.

Rufen Sie Ihre nächstgelegene Filiale an:
0800 028 1160

Besuchen Sie unsere Webseite:
shredit.de

Mit Sicherheit sicher!

Richtlinien für die Schadensbegrenzung nach einer Verletzung der Datensicherheit

„Was für Unternehmen anfänglich ein zweitrangiges Thema war, wurde später zu einer Methode der Risikoverringerung. Wer als Vorstandschef, Geschäftsführer, Verantwortlicher für die Informationssicherheit oder Geschäftsinhaber die Rolle des Schutzes der Privatsphäre und der Daten im Unternehmen nicht ernst nimmt, dessen Tage sind gezählt“,

so Eduard Goodman, leitender Datenschutzbeauftrager des Unternehmens IDT 911.

Einige Beispiele von Daten, die im Falle von Datenmissbrauch gemeldet werden müssen:

- Daten, die unter den Intellectual Property Attachè Act (IPAA), den Sarbanes-Oxley Act (SOX), den Payment Card Industry Data Security Standard (PCI) oder die Vorgaben der Federal Trade Commission (FTC) fallen **Beispiel:** Wenn nur ein Computer betroffen ist, müssen Sie dies nicht melden, solange die Rechte der betroffenen Personen geschützt bleiben.

- Persönliche Daten, wie Sozialversicherungsnummern, Persönliche Identifikationsnummern, Kreditkarteninformationen und Kontonummern. Beachten Sie dazu auch Ihre lokalen Vorschriften zu gesetzlich geschützten Daten.*

Banken sind gemäß den Bundesgesetzen dazu verpflichtet, Kunden über Datenmissbräuche zu informieren; in 46 Staaten gelten darüber hinaus Gesetze, die fordern, dass dies auch für andere Unternehmen gilt.

- Vermeiden Sie es, voreilige Schlüsse zu ziehen, bevor Sie genügend Informationen über die näheren Umstände des Datenmissbrauchs besitzen. Schon kurz nach seiner Entdeckung können sich Informationen über den Tathergang und betroffene Personen schnell ändern.

- Gestalten Sie die Ermittlungen effizienter, indem Sie eine Person auswählen (nicht mehr als zwei führende Mitarbeiter Ihres Unternehmens), die zur Durchführung solcher Untersuchungen geeignet ist.

- Koordinieren Sie die Ermittlungen unbedingt nach dem Need-to-Know-Prinzip und pflegen Sie eine regelmäßig Berichterstattung, so Forensikexperte Mandia.

Bewerten Sie den Vorfall in Bezug auf die Einhaltung der gesetzlichen Datenschutzbestimmungen.

- Sollte Ihr Unternehmen bereits eine Strategie zur Dokumentenverwaltung umsetzen und regelmäßige Revisionen durchgeführt haben, verfügen Sie sicher über Protokolle, welche die Einhaltung der Gesetze bestätigen; dies könnte Ihnen dabei helfen, herauszufinden, wie und wo es zum Datenmissbrauch kam.

- Beachten Sie die branchenspezifischen Gesetze. Mehr Einzelheiten zu Ihrer Branche und Ihrem Ort (Bundesland, Land) finden Sie in unserem Mediencenter im Abschnitt „Informationen zur Gesetzgebung“.

Schaffen Sie Abhilfe und verhindern Sie, dass es zu einem erneuten Datenmissbrauch kommt.

- Sorgen Sie dafür, dass - gemäß den gesetzlichen Bestimmungen - eventuell vom Datenmissbrauch betroffene Kunden, Verkäufer und andere externe Parteien benachrichtigt werden. So können diese die notwendigen Schritte einleiten, um sich vor Identitätsdiebstählen zu schützen

- Arbeiten Sie mit Ihrem Rechtsanwalt und einem erfahrenen PR-Agenten ein Kommuniqué für die Medien aus, wenn dies gesetzlich gefordert wird.

- Konsultieren Sie bei Bedarf externe Fachleute zur Einführung neuer Schutzmaßnahmen, neuer Softwares oder Dienstleistungen, um in Zukunft Datenschutzverletzungen zu verhindern.

- Überprüfen Sie Ihre aktuellen Sicherheitsvorkehrungen: Sind sie noch angemessen? Kennt sie jeder – und werden sie von jedermann befolgt?

- Ihre Sicherheitsrevision erfordert womöglich neue Verfahren und Prozesse, die kommuniziert werden müssen und eine Weiterbildung Ihres gesamten Personals nötig machen könnten.

Quellen:
1 Privacy Rights Clearinghouse, https://www.privacyrights.org/fs/fs17b-SecurityBreach.htm
2 CNN Money, http://money.cnn.com/2011/09/07/pf/identity_theft_protection.moneymag/index.htm
3 Security Dark Reading, http://www.darkreading.com/security/perimeter-security/208804800/what-not-to-do-after-a-security-breach.html

* Dieses Dokument stellt keinen Ersatz für eine Rechtsauskunft dar. Wenn Sie Maßnahmen hinsichtlich einer Datenschutzverletzung ergreifen möchten, sollten Sie umgehend Ihren Rechtsanwalt einschalten.