DATENSICHERHEIT IM UNTERNEHMEN

TATORT: „ARBEITSPLATZ“

von Guido Kerbsties

Wer heutzutage mit sensiblen, unternehmenskritischen Daten arbeitet, dürfte nicht mehr ruhig schlafen können. Denn das Spektrum an Delikten reicht von Datenklau, Betrug, Sabotage oder Spionage über Korruption bis hin zur Internet-Kriminalität (sog. Cyber-Crime). Selbst vermeintlich kleinere Datenpannen bescheren einem Unternehmen schnell einen wirtschaftlichen Schaden in astronomischer Höhe.

Meldepflicht bei Datenlecks

Seit der umfangreichen Novellierung des Bundesdatenschutzgesetzes (BDSG) 2009 ist ein Verschweigen von „Datenlecks“, die personenbezogene Daten betreffen, nicht mehr möglich. Im Gegenteil: Durch eine Meldepflicht kann ein Vertuschen zum Erhalt des Images sehr teuer werden. Ein Vorfall ist nach den Vorgaben des § 42a BDSG nunmehr unverzüglich der örtlich zuständigen Datenschutz-Aufsichtsbehörde sowie den Betroffenen selbst zu melden. Ein Unterlassen dieser Schritte kann ein Bußgeld von bis zu 300.000,00 bedeuten (§ 43 Abs. 3 i.V.m § 43 Abs. 2 Nr. 7 BDSG)! Zudem: Wer Kenntnis unrechtmäßig erlangter Daten hat, ist künftig zur Meldung des Vorfalls verpflichtet.

„Kompetentes Dreieck“ hilft

Um einen drohenden Schaden möglichst schnell und effizient begrenzen zu können, sind als erste „Notmaßnahme“ Experten aus nachfolgenden Fachbereichen unbedingt einzuschalten, unabhängig ob diese aus internen oder externen Bereichen kommen.

In seinem internen Arbeitsfeld betroffen von solchen Vorfällen ist immer der betriebliche Datenschutzbeauftragte, soweit er vom Unternehmen freiwillig oder nach den Vorgaben des § 4f BDSG pflichtgemäß bestellt worden ist. Hier (§ 4g Abs. 1, S. 1 BDSG) heißt es pauschal: „Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin.“ Seine Verantwortung liegt also auch im Schutz dieser Daten vor dem Zugriff Unbefugter oder sonstigem Datenverlust. Tritt ein solcher Fall ein, muss er zusammen mit der Unternehmensleitung die relevanten Hintergründe recherchieren und künftige Vorsorgemaßnahmen empfehlen.

Ein interner oder externer IT-Forensiker sollte ebenfalls rasch beteiligt werden, da meist die IT eines Unternehmens vom „Datenleck“ betroffen ist. Der IT-Forensiker ist speziell dafür ausgebildet, Informationen zu sammeln, aufzubereiten und auszuwerten. Nicht immer ist ein Verdächtiger auch gleichsam für die Entstehung eines „Datenlecks“ verantwortlich, im Rahmen einer Untersuchung in diesem Sinne sollte daher prinzipiell nach Spuren geforscht werden, welche einen Verdacht sowohl untermauern als auch widerlegen können. Im Falle eines Strafverfolgungsprozesses liefert ein unabhängiger IT-Forensiker gerichtsverwertbare Stellungnahmen oder Gutachten.

Mehr und mehr Unternehmungen bestellen inzwischen einen sogenannten Compliance-Beauftragten. Finanzdienstleister sind beispielsweise sogar zur Bestellung eines Compliance-Officers verpflichtet (§ 33 Abs. 1 Satz 2 WpHG i. Verbindung mit § 12 Abs. 4 WpDVerOV).

Die Ausgestaltung und die Aufgaben des Compliance-Officers sind im Rundschreiben „Mindestanforderungen Compliance-Funktion ...“ der BaFin detailliert aufgeführt (BT 1 ff. der gem. Rundschreiben 4/2010 (WA) veröffentlichten „Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten nach §§ 31 ff. WpHG für Wertpapierdienstleistungsunternehmen (MaComp)“ (zuletzt geändert am 07.12.2012)).

Kommt es zu einem „Datenleck“ im Unternehmen, liegen regelmäßig Rechtsverstöße vor, deren Aufklärung und Vermeidung auch in der Verantwortung des „Compliance-Beauftragten“ liegt.

Unter dem Begriff „Social Engineering“, spionieren sogenannte Social Engineers beispielsweise das persönliche Umfeld ihres Opfers aus. Sie versuchen Personen durch zwischenmenschliche Beeinflussung zur Preisgabe von vertraulichen Informationen zu bewegen. Neben der technischen Schwachstelle „IT“ ist daher das Augenmerk des Compliance-Beauftragten ebenso auf die Schwachstelle „Mensch“ zu richten.

Guido Kerbsties

Beispiel E-Mail-Accounts

Insbesondere das Datenschutzrecht verbietet Schritte, die technisch möglich und wünschenswert sind, aber einen unzulässigen Eingriff in das sogenannte informationelle Selbstbestimmungsrecht bedeuten. Ein nicht selten vorkommendes Beispiel ist die Betrachtung von dienstlichen E-Mail-Accounts mit privater Nutzung. Darf ein Beschäftigter ausdrücklich den dienstlichen E-Mail-Account auch für private Zwecke nutzen, ist das Einsehen dieses Accounts (auch zur Aufklärung eines Sachverhaltes) nicht ohne Weiteres erlaubt!

Fazit

Um die Hintergründe von „Datenklau“ aufzuklären, müssen die vorgenannten Experten sehr effizient zusammenarbeiten. Diese Zusammenarbeit ist geprägt vom aktuellen Stand der Technik und den verschiedenen Rechtsvorschriften, die neue Möglichkeiten, aber auch Grenzen des Handelns aufzeigen.

Eine – auch nach §15 FAO für Fachanwälte IT-Recht und Strafrecht anerkannte – Fachtagung beleuchtet am 23.09.2013 in Wiesbaden Details der vorgenannten Fachbereiche „Datenschutz“, „IT-Forensik“, „Compliance“ und hilft Ihnen wieder einen ruhigen Schlaf zu finden. **(http://www.update-bdsg.com)**

Kontakt: Guido.Kerbsties@conturn.com

Guido Kerbsties ist Head of Customer Services bei der CONTURN Analytical Intelligence Group. Der Artikel ist erstellt in Abstimmung mit dem ehemaligen Hessischen Datenschutzbeauftragten Manfred Weitz