# Unternehmenssicherheit – weit mehr als nur IT-Sicherheit

Namhaften Unternehmen, von denen zu vermuten ist, dass Datensicherheit fester Bestandteil ihrer Wertschöpfungskette ist, sind bekanntlich reihenweise sensible und personenbezogene Daten gestohlen worden. Gestohlen von zugriffsberechtigten Mitarbeitern oder von Personen, die sich Zugang zu den Daten verschafften. Die Täter konnten offensichtlich mühelos alle Sicherheitsvorkehrungen umgehen. Gleichgültig, ob Finanzbehörden, Marktforscher, Datenhändler oder der Wettbewerb Interesse an den Daten zeigen, es gibt offensichtlich einen Abnehmermarkt, der sich auch dubioser Quellen bedient. Der Anreiz ist groß, denn es geht in der Regel um viele Millionen Euro. Wenn ein Abnehmermarkt existiert, wenn der Preis stimmt und wenn der Aufwand gering ist, gibt es auch Täter und Nachahmungstäter.

## Datendiebstahl und kein Ende?

Zu den zahlreichen bekannt gewordenen Fällen gehört der Vorfall bei der Liechtensteiner LGT Bank (Liechtenstein-Steueraffäre). Es gab keinen Einbruch, kein Eindringen in das Datennetz und keine Gewaltanwendung. Es war die Tat eines Mitarbeiters, der mit der Digitalisierung von Papierunterlagen beauftragt wurde und nach eigenen Angaben die Brisanz der Daten von 3.929 „Stiftungen“ erkannt hatte. Er entwendete die erstellten Sicherungsbänder, die frei zugänglich auf einem Schreibtisch in der IT-Abteilung lagen. Zu Hause entschlüsselte er die Daten ohne weitere Spezialkenntnisse und bot den Finanzbehörden eine kleine Auswahl an. Dort wurde das Kosten-/Nutzenverhältnis hochgerechnet, rechtliche und moralische Bedenken über Bord geworfen und der Deal war perfekt.

Auch im Fall der Liechtensteinischen Landesbank (LLB) hatte ein Mitarbeiter die Daten von 2.325 Kunden kopiert und mitgenommen. Die genauen Einzelheiten sind nicht bekannt. Wie im Fall der LGT-Bank haben offensichtlich alle Sicherungsmaßnahmen versagt. Selbst der Deutschen Telekom wurden 17 Millionen sensible

Kundendaten entwendet. Das Ereignis hat kurzzeitig viel Staub aufgewirbelt, wurde aber schnell wieder aus dem Fokus der Nachrichtenwelt verbannt. Der Tathergang ist bis heute nicht aufgeklärt bzw. nicht veröffentlicht worden. Es ist zu vermuten, dass auch hier eine grobe Vernachlässigung bekannter Regeln der Datensicherheit vorlag oder es sich um die Tat einer privilegierten Person mit Zugriff auf die Daten handelte.

Die geschilderten Fälle machten nicht nur Schlagzeilen. Zusätzlich entstanden ein erheblicher wirtschaftlicher Schaden und ein nicht zu unterschätzender Imageverlust. Auch die straf- oder zivilrechtlichen Folgen sollten nicht unerwähnt bleiben. Damit sind nicht die Folgen für den eigentlichen Täter gemeint, sondern die Folgen für das Unternehmen und die verantwortlichen Personen. So ist bekannt, dass im Fall der Liechtensteiner Steueraffäre

mehrere Schadensersatzklagen zugunsten der betroffenen Bankkunden entschieden wurden. Die Folgen für die verantwortlichen Führungskräfte sind allerdings nur oberflächlich bekannt.

## Der Insider – das unterschätzte Risiko

In diesen oder vergleichbaren Fällen handelte sich nicht um Angriffe von außen, sondern von innen. Es waren Insider, die Lücken im Sicherheitssystem erkannt hatten und mit geringstem Aufwand und in einer sehr kurzen Realisierungszeit einen extrem hohen Schaden verursacht hatten. Die allgemein üblichen Sicherheitsmaßnahmen zur Abwehr dieser Form krimineller Handlungen hatten allein nicht ausgereicht. Firewalls, Intrusion-Detektion-Systeme, Rollen- und Berechtigungsmanagement, User-Monitoring, Vereinzelungsanlagen, Videoüberwachung, Zutrittskontrolle usw. hatten versagt. Bedenkt man, dass bei Daten- und Informationsdiebstahl und überhaupt Wirtschaftskriminalität die Dunkelziffer extrem hoch ist, müsste in Sachen Sicherheit und Datenschutz deutlich konsequenter gehandelt werden. Kurz gesagt: Die Sicherheitsmaßnahmen müssen verstärkt auf den Menschen und seinen Rucksack fokussiert werden.

Die betroffenen Unternehmen sehen sich stets unschuldig als „Opfer krimineller Handlungen“. Keine Frage, das sind sie auch. Aber sollten nicht gerade auch kriminelle Handlungen Gegenstand einer Bedrohungs- und Risikoanalyse sein? Hat man es den Tätern ganz einfach zu leicht gemacht? Wurde das Risiko „Mitarbeiter als Täter“ zwar erkannt, aber trotz dominierender Gefahr und hoher Schadenswahrscheinlichkeit, billigend in Kauf genommen? Wurde das Risiko einfach ausgeblendet, weil „nicht sein kann, was nicht sein darf“? Hat man sich vom Satz leiten lassen „So etwas hat es bei uns noch nicht gegeben“? Wenn ja, ähnelt die Risikobetrachtung der Unternehmen einem Autofahrer, der trotz beschlagener Windschutzscheibe vorwärts fährt und sich dabei im Rückspiegel orientiert.

## Sicherheit ist Chefsache!

Die Sprecher der Unternehmen sind sich nicht zu schade regelmäßig zu versichern, dass in ihren Unternehmen der Datenschutz ganz oben steht und Sicherheit Chefsache ist. In den betroffenen Unternehmen hat man sich vor den Diebstählen offensichtlich nicht konsequent genug mit den besonderen Gefahren im Risikokernbereich IT, Risikoprofile hoch privilegierter Mitarbeiter oder überhaupt Insiderkriminalität, beschäftigt.

Ein funktionierendes Sicherheits- und Notfallmanagement ist gesetzlich gefordert. Sowohl im Aktiengesetz (AktG), im GmbH-Gesetz (GmbHG), im Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) und in vielen weiteren Normen (ISO, BSI) ist die „Organisationspflicht zur Schadensabwehr“ verankert. Zitat KonTraG: *„Die Gefahr von Verlusten und Schäden, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder infolge externer Ereignisse eintreten, angemessen einzuschränken oder gar zu verhindern“*. Eine Forderung mit weitreichender Bedeutung,

die den Menschen als Schwachstelle - egal ob vorsätzliche Handlung oder Fahrlässigkeit vorliegt - bewusst einbezieht.

## Halbe Sicherheit ist keine Sicherheit

In der Regel sieht sich die IT zu Recht als wichtigster Geschäftsbereich eines Unternehmens. Sie tritt entsprechend selbstbewusst auf und handelt hinsichtlich Daten- und Informationsschutz auch sehr eigenverantwortlich. Dies betrifft grundsätzlich alle Unternehmen mit mittlerem und hohem Schutzbedarf. Dazu gehören der Finanz- und Energiebereich sowie alle Organisationen und Einrichtungen, die laut BSI den kritischen Infrastrukturen zuzuordnen sind. In diesen Branchen sind zertifizierte Hochsicherheitsrechenzentren, Sicherheitsstandards entsprechend BSI-Anforderungen, Rollen- und Berechtigungsmanagement, IT-Dienstleisterzertifizierungen, Datenverschlüsselung usw. ein absolutes Muss im Tagesgeschäft. Betrachtet man aber die extrem hohe Risikokonzentration in Bezug auf die Insiderkriminalität - gerade in Verbindung mit Themen wie Outsourcing, Cloud-Computing und Offshoring sowie die Beschäftigung externer Mitarbeiter - ist festzustellen, dass bei entsprechend privilegierten Mitarbeitern eine bemerkenswerte Nachlässigkeit hinsichtlich der Zuverlässigkeit, der Risikobewertung und der notwendigen Sicherheits- und Kontrollmaßnahmen festzustellen ist.

## Sicherheit fordert konsequentes Handeln

Es ist unabdingbar, vorsätzliche Handlungen durch Insider ins Bedrohungsbild einzubeziehen. Das bedeutet natürlich: zusätzliche organisatorische, technische, bauliche und personelle Sicherheitsmaßnahmen; permanente Kontrolle und Revision; Konfliktpotenzial mit langjährigen Mitarbeitern und mit Personalvertretungen und es bedeutet in der Regel auch höhere Investitions- und Betriebskosten. Gerade deshalb ist es nicht nur eine Angelegenheit der betroffenen sensiblen Unternehmensbereiche, sondern in erster Linie eine Angelegenheit der Unternehmensleitung, denn sie muss die konsequente Umsetzung der erforderlichen Sicherheitsmaßnahmen strategisch unterstützen. Allerdings fehlt in den meisten Fällen - aus Furcht vor den damit verbundenen Konsequenzen - dieser ganzheitliche Ansatz, fehlt der Wille zu ganzheitlichen Lösungen.

Was bedeutet ganzheitliche Lösungen? Worauf ist der Fokus zusätzlich zu richten?

### 1. Das „Risiko Mensch“ konsequent einbeziehen

Das hohe Risikopotenzial „Insiderkriminalität“ muss berücksichtigt werden. Dazu gehören alle internen und externen Mitarbeiter und Dienstleister mit risikobehafteten Autorisierungen und Privilegien (Programmierer, Security- und Server-Administratoren, Systemverwalter, Operateure, Forscher, Entwickler, Geheimnisträger, Trainees usw.). Nicht zu vergessen sind Personengruppen, die nur indirekt mit sensiblen Daten in Verbindung gebracht wer-

den, aber denen aber ein Zugriff auf Datenträger oder Dokumente möglich ist. Dazu gehören Reinigungskräfte, Mitarbeiter von Fremdfirmen für Instandhaltung und Service, Trainees usw.

## 2. Durch ungetrübten Blick Risikoverzerrungen ausschließen

Befindlichkeiten und Voreingenommenheit müssen ausgeschlossen werden. Der ungetrübte Blick des externen Betrachters garantiert eine unvoreingenommene, neutrale und ganzheitliche Analyse. So können Bedrohungsbild, Schwachstellen und Risikopotenzial konsequent identifiziert werden. Die darauf abgestimmten Sicherheitsmaßnahmen können unbelastet entwickelt und umgesetzt werden.

## 3. Risikopotenzial entsprechend der Rollen, Tätigkeiten und Berechtigungen bewerten

Das Risiko- und Gefahrenpotenzial aller betroffenen Personen - bezogen auf Tätigkeiten, Rollen und Berechtigung - muss identifiziert und realistisch bewertet werden. Jede Überbewertung bedeutet Kosten und Aufwand. Jede Unterbewertung bedeutet vermeidbares Restrisiko.

## 4. Das Risiko auf möglichst wenig Personen konzentrieren

Tätigkeiten und damit verbundene Rollen und Berechtigungen so weit wie möglich einschränken und auf möglichst wenig Personen konzentrieren. Die Machtfülle der Personen - gerade bei langjährigen internen und externen Mitarbeitern - richtig bewerten und einstufen. Externe Mitarbeiter besonders kritisch betrachten.

## 5. Die Zuverlässigkeit der Personen konsequent prüfen

Alle Möglichkeiten einer Zuverlässigkeitsprüfung müssen anwendet werden. Zitat Dr. Stephan Fedtke (Quelle: kes, Ausgabe 12/2010 – Epische Macht): „Ohne Zweifel bestreitet der Mensch in der IT eine Doppelrolle. Er ist elementarer Erfolgsfaktor und höchstes Risiko zugleich. Bei solchen Mitarbeitern liegt eine exzessiv nachteilige und einseitige Risiko-Charakteristik vor. Diese ergibt sich aus dem Verhältnis der Höhe des potenziell angerichteten Schadens (Mio. Euro) zur Realisierungsdauer (ggf. nur Sekundenbruchteile).

Bezogen auf Unternehmen mit entsprechendem Schutzbedarf ist eine Zuverlässigkeitsprüfung analog zur Überprüfungstiefe gemäß Luftsicherheitsgesetz LuftSiG, §7 oder zu den Sicherheitsüberprüfungen des Bundes gemäß Sicherheitsüberprüfungsgesetz SÜG, § 9 (Ü2) oder §10 (Ü3) denkbar (Anmerkung: Jeder Mitwirkende am Bau einer Justizvollzugsanstalt muss eine Sicherheitsüberprüfung gemäß SÜG durchlaufen). Da aber für die Privatwirtschaft eine gesetzliche Grundlage für derartige Überprüfungen derzeit noch fehlt, sollte sich die Zuverlässigkeitsüberprüfung zumindest an den dort definierten Prüfkriterien orientieren und durch entsprechende Experten durchgeführt werden. Wie Dr. Fedtke anführt,

wäre es natürlich wünschenswert eine gesetzliche Grundlage für die Privatwirtschaft, z. B. unter Federführung des BSI, zu schaffen.

## 6. Arbeitsplätze in Sicherheitszonen konzentrieren

Auch wenn das „Risiko Mensch“ durch qualifizierte Zuverlässigkeits- oder Sicherheitsüberprüfungen minimiert wird, bleibt immer noch ein erhebliches Restrisiko. Entsprechend dem Motto „Vertrauen ist gut, Kontrolle ist besser“ sollten die Personen - nach Rollen und Berechtigungen geordnet - in besonderen Sicherheitszonen zusammengefasst werden. Konsequente Kontrollmaßnahmen können sich dann auf einen oder mehrere kleine Sicherheitszonen konzentrieren und mit geringstem Aufwand umgesetzt werden.

## 7. Sicherungslinien konsequent überwachen

Zu- und Abgänge zu den Sicherheitszonen sollten - auch wenn längere Wege oder Unbequemlichkeiten entstehen - auf ein Minimum reduziert, aber dafür konsequent geregelt und überwacht werden. Sicherheitsschleusen, Personenvereinzelung, elektronische Zu- und Abgangskontrolle in Kombination mit Biometrie und Türzustandsüberwachung, Videoüberwachung, Einbruchmeldetechnik usw. sind natürlich obligatorisch. Die Sicherungslinien müssen klar und deutlich signalisieren: Hier beginnt ein besonderer Sicherheitsbereich, hier gelten besondere Sicherheitsmaßstäbe und Sicherheitsmaßnahmen.

## 8. Das Mitführen unerwünschte Gegenstände verhindern

Es muss eindeutig geregelt werden, welche Gegenstände beim Zugang oder Abgang mitgeführt werden dürfen. Die durchaus unpopuläre Maßnahme sollte alle speicher- und kommunikationsfähigen Geräte mit Internetzugang einbeziehen und sich derzeit an der Größe der USB-Sticks orientieren. An Handgepäck- und Personenkontrollen führt kein Weg vorbei. Es muss individuell entschieden werden, ob ständig oder unregelmäßig kontrolliert wird. Der Fokus der Kontrollen muss auf den Abgang gelegt werden. Ein Umgehen der Kontrollstellen muss zwingend vermieden werden. Ergänzende Maßnahmen innerhalb der Sicherheitszonen sind obligatorisch. Dazu gehören z. B.: Clean Desk, Aufsicht von Reinigungs- und Instandhaltungspersonal, besondere Kontrolle der externer Mitarbeiter.

## 9. Ständige Kontrollen, Revisionen und Optimierungen durchführen

Das in der IT übliche User-Monitoring ist dem Risikopotenzial entsprechend anzupassen, zu verschärfen oder überhaupt einzurichten. Dabei darf nicht vergessen werden, dass der fachlich versierte Insider schnell Sicherheitslücken erkennt und im Fall vorsätzlicher Handlungen auch erfolgsversprechende Möglichkeiten entwickelt, diese zu umgehen. Getreu dem Motto von Curt Emmerich, deutscher Arzt und Schriftsteller **„Ich war mir meiner Sache so sicher und gerade diese Sicherheit war es, der alle Zweifel entsprangen“**, sind alle Sicherheitsmaßnahmen einer ständigen Revision, möglichst durch neutrale Externe, zu unterwerfen und entsprechend zu optimieren.

### 10. Vertrauen und Mitwirkung fördern

Werden Sicherheitsmaßnahmen klar begründet und kommuniziert, werden sie auch als erforderlich wahrgenommen. Durch die frühzeitige Einbeziehung der betroffenen Personen und Personalvertretungen kann das entstehende Konfliktpotenzial deutlich reduziert und Investitionssicherheit geschaffen werden. Regelmäßige Informationen über das Thema Sicherheit und Unternehmensschutz, Erkenntnisse der Sicherheitsbehörden hinsichtlich Wirtschaftskriminalität und -Spionage schärfen das Sicherheitsbewusstsein der Mitarbeiter und deren Willen, die eingeführten Sicherheitsmaßnahmen zu unterstützen. Ganz gleich ob Safety oder Security - die Mitwirkung der Mitarbeiter ist unabdingbar.

## Fazit

Daten- und Informationsschutz ist für Unternehmen mit entsprechendem Schutzbedarf von existenzieller Bedeutung. Im Umgang mit Daten und Informationen stellt die Gruppe hoch privilegierter Mitarbeiter ein extrem hohes Risikopotenzial dar. Die dominierende Gefahr der Insiderkriminalität darf nicht ignoriert werden. Die Vorsorge- und Sicherheitsmaßnahmen müssen verstärkt wie eine Firewall auf den Menschen und seinen Rucksack fokussiert werden. Die vielfältigen Maßnahmen der virtuellen Sicherheit müssen mit den Maßnahmen des Objektschutzes stärker zusammenwachsen und eine konsequente und lückenlose Synthese bilden.

*Dieser Beitrag ist auch als Fachbeitrag in der Fachzeitschrift SecurityInsight unter dem Titel „Firewall für den Rucksack - Viel Sicherheit für LAN und WAN – was ist mit dem Rest?“ erschienen. Autoren: Volker Kraiss und Walter Wilke*