Firewall für Mensch und Rucksack

IT-Sicherheit kann jeder – die eigentliche Herausforderung liegt in der geschickten Verknüpfung virtueller Maßnahmen mit physischem Objektschutz und Awareness zur lückenlose Sicherheitssynthese

Von Volker Kraiß und Walter Wilke

Namhaften Unternehmen, von denen zu vermuten steht, dass Datensicherheit fester Bestandteil ihrer Wertschöpfungskette ist, sind bekanntlich reihenweise sensible und personenbezogene Daten abhanden gekommen. Gestohlen haben sie zugriffsberechtigte Mitarbeiter oder Externe, die sich unberechtigt Datenzugang verschafften. Die Täter konnten offensichtlich mühelos alle Sicherheitsvorkehrungen umgehen. Gleichgültig, ob Finanzbehörden, Markforscher, 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 um viel Geld. Die Nachfrage bestimmt auch hier das Angebot.

Foto: Helder Almeida - Fotolia.com

Verluste, so weit das Auge reicht

Bekannt geworden ist unter anderem der Vorfall bei der Liechtensteiner LGT Bank („Liechtenstein-Steueraffäre"). Es gab keinen Einbruch, niemand war ins Datennetz eingedrungen, und keiner hatte Gewalt ausgeübt. Vielmehr war es die Tat eines Mitarbeiters, der mit der Digitalisierung von Papierunterlagen beauftragt worden war 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

Die SI-Autoren Walter Wilke und Volker Kraiß sind Inhaber des nach ihnen benannten Security-Consulting-Unternehmens Kraiß + Wilke (www.kraiss-consult.de).

eine kleine Auswahl an. Die verantwortlichen Beamten rechneten das Kosten-/Nutzen-Verhältnis hoch, warfen rechtliche und ethische Einwände über Bord – und der Deal war perfekt.
Auch der Deutschen Telekom wurden 17 Millionen sensible Kundendaten entwendet. Das Ereignis hat kurzzeitig viel Staub aufgewirbelt, verschwand aber schnell wieder aus dem Fokus der Nachrichten. Der Tathergang ist bis heute nicht aufgeklärt oder veröffentlicht. Es ist zu vermuten, dass auch hier banale Regeln der Datensicherheit verletzt wurden oder privilegierte Mitarbeiter, sprich: aus den oberen Etagen, mit Zugriff auf die Daten ihre Hände im Spiel hatten.
Es geht hier nicht nur um unschöne Schlagzeilen. Tatsächlich ist in jedem einzelnen Fall ein erheblicher wirtschaftlicher Schaden entstanden, vom immensen Imageverlust ganz zu schweigen. Auch die straf- oder zivilrechtlichen Folgen sollen nicht unerwähnt bleiben – nicht die für die Täter, sondern die für das Unternehmen und die organisatorisch Verantwortlichen. So ist bekannt, dass im Fall der Liechtensteiner Steueraffäre mehrere Schadensersatzklagen zu Gunsten der betroffenen Bankkunden entschieden wurden. Die Folgen für die verantwortlichen Führungskräfte sind allerdings nur oberflächlich bekannt.

Täter meist Insider

In diesen und vergleichbaren Fällen handelt sich nicht um Angriffe von außen. Es sind in der Regel Insider, die Lücken im Sicherheitssystem erkennen und mit geringstem Aufwand und in sehr kurzer Zeit einen extrem hohen Schaden verursachen. Die allgemein üblichen technischen Sicherheitsmaßnahmen zur Abwehr solch krimineller Handlungen reichen allein nicht aus. Firewalls, Intrusion-Detection-Systeme, Rollen- und Berechtigungsmanagement, User-Monitoring, Vereinzelungsanlagen, Videoüberwachung, Zutrittskontrolle hatten versagt. Bedenkt man, dass bei Daten- und Informationsdiebstahl und überhaupt Wirtschaftskriminalität die Dunkelziffer extrem hoch ist, müsste in Sachen Sicherheit und Datenschutz deutlich konse-

quenter gehandelt werden. Kurz gesagt: Die Sicherheitsmaßnahmen müssen verstärkt auf den Menschen fokussiert werden – und auf seinen Rucksack.

In all diesen Fällen sehen sich die betroffenen Unternehmen gebetsmühleartig als „Opfer krimineller Handlungen". Keine Frage, das sind sie auch. Aber sollten nicht gerade kriminelle Handlungen Gegenstand einer grundsätzlichen Bedrohungs- und Risikoanalyse sein? Hat man es den Tätern nicht einfach zu leicht gemacht? Wurde nicht das Risiko des Mitarbeiters als potenziellem Täter zwar erkannt, aber trotz dominierender Gefahr und hoher Schadenswahrscheinlichkeit billigend in Kauf genommen? Wurde das Risiko ausgeblendet, weil „nicht sein kann, was nicht sein darf"? Wenn ja, dann ähneln die Unternehmen bei der Risikobetrachtung einem Autofahrer, der trotz beschlagener Windschutzscheibe vorwärts fährt und sich dabei im Rückspiegel orientiert.

Die Unternehmenssprecher sind sich nicht dafür zu schade, regelmäßig zu versichern, dass in ihrem Betrieb der Datenschutz selbstverständlich ganz oben steht und Sicherheit – wir wollen es gar nicht mehr hören – natürlich „Chefsache" ist. Dann muss der Chef wohl kräftig Mist gebaut haben. Ganz sicher hat er sich nicht konsequent mit den besonderen Gefahren im Risikokernbereich IT, mit Risikoprofilen hoch privilegierter Mitarbeiter oder überhaupt der Insider-Kriminalität beschäftigt.

Dabei ist ein funktionierendes Sicherheits- und Notfallmanagement gesetzlich gefordert. Sowohl im Aktiengesetz (AktG), im GmbH-Gesetz (GmbHG) und im Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) ist die „Organisationspflicht zur Schadensabwehr" verankert. Laut KonTraG ist 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 durch Vorsatz oder Fahrlässigkeit – bewusst einbezieht.

Mut zur Ganzheitlichkeit

Die IT-Abteilung sieht sich zu Recht als einer der zentralen Organisationen eines Unternehmens. Sie tritt entsprechend selbstbewusst auf und handelt hinsichtlich Daten- und Informationsschutz in der Regel sehr eigenverantwortlich. Dies betrifft grundsätzlich alle Unternehmen mit mittlerem und hohem Schutzbedarf. Dazu gehört der Finanz- und Energiesektor sowie alle Organisationen und Einrichtungen, die laut Bundesamt für Sicherheit in der Informationstechnik (BSI) den Kritischen Infrastrukturen zuzuordnen sind. Hier sind zertifizierte Hochsicherheitsrechenzentren, Sicherheitsstandards entsprechend BSI-Anforderungen, Rollen- und Berechtigungsmanagement, IT-Dienstleister-Zertifizierungen, Datenverschlüsselung usw. ein absolutes Muss im Tagesgeschäft. Betrachtet man aber die extrem hohe Risikokonzentration in Bezug auf die Insider-Kriminalität – gerade in Verbindung mit Outsourcing, Cloud-Computing und Offshoring sowie die Beschäftigung externer Mitarbeiter – ist festzustellen, dass beim Umgang gerade mit privilegierten Mitarbeitern eine bemerkenswerte Nachlässigkeit hinsichtlich Zuverlässigkeit, Risikobewertung und notwendigen Sicherheits- und Kontrollmaßnahmen herrscht.

10 Schritte zur Sicherheit

1. Das „Risiko Mensch" konsequent einbeziehen

Das hohe Risikopotenzial durch „Insider-Kriminalität" muss berücksichtigt werden. Dazu gehören alle internen und externen Mitarbeiter, Dienstleister mit risikobehafteten Autorisierungen und Privilegien (Programmierer, Sicherheits- und Server-Administratoren, Systemverwalter, Operateure, Forscher, Entwickler, Geheimnisträger, Trainees). Nicht zu vergessen sind Personengruppen, die nur indirekt mit sensiblen Daten in Verbindung gebracht werden, 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 ihre 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 wenige Personen konzentrieren

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

5. Zuverlässigkeit konsequent prüfen

Alle Möglichkeiten einer Zuverlässigkeitsprüfung müssen anwendet werden. 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 Risikocharakteristik vor. Diese ergibt sich aus dem Verhältnis der Höhe des potenziell ange-

Nachrichten über Datenklau sind inzwischen an der Tagesordnung.

Foto: ArTo - Fotolia.com

Wenn Sicherheit „Chefsache" ist, wie uns viele Pressesprecher gerne glauben machen wollen, dann bauen Chefs ganz offensichtlich kräftig Mist.

richteten Schadens (in Millionen Euro) zur Realisierungsdauer (gegebenenfalls nur Sekundenbruchteile)."
Bezogen auf Unternehmen mit entsprechendem Schutzbedarf ist eine Zuverlässigkeitsprüfung analog zur Überprüfungstiefe gemäß § 7 Luftsicherheitsgesetz (LuftSiG) oder zu den Sicherheitsüberprüfungen des Bundes gemäß § 9 (Ü2) oder § 10 (Ü3) Sicherheitsüberprüfungsgesetz (SÜG) denkbar. (Anmerkung: Jeder Mitwirkende am Bau einer Justizvollzugsanstalt muss eine Sicherheitsüberprüfung gemäß SÜG durchlaufen). Da aber für die Privatwirtschaft eine gesetzliche Grundlage für solche Überprüfungen derzeit noch fehlt, sollte sich die Zuverlässigkeitsüberprüfung zumindest an den dort definierten Prüfkriterien orientieren und durch entsprechende Experten durchgeführt werden. Wie Fedtke anführt, wäre es natürlich wünschenswert, eine gesetzliche Grundlage für die Privatwirtschaft, zum Beispiel 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. Personen sollten – 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 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. Keine unerwünschten Gegenstände

Es muss eindeutig geregelt werden, welche Gegenstände beim Zu- oder Abgang mitgeführt werden dürfen – hier sind wir beim schon zitierten Rucksack, für den eine Firewall zu gelten hat. Die durchaus unpopuläre Maßnahme sollte alle speicher- und kommunikationsfähigen Geräte mit Internetzugang einbeziehen und sich derzeit an der Größe von 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 beispielsweise „Clean Desk", Aufsicht von Reinigungs- und Instandhaltungspersonal, besondere Kontrolle externer Mitarbeiter.

9. Ständige Kontrolle, Revision und Optimierung

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 bei vorsätzlichen Handlungen auch erfolgversprechende Möglichkeiten entwickelt, diese zu umgehen. Getreu dem Motto des Arztes und Schriftstellters Curt

Foto: IrisArt – Fotolia.com

Datendieb oder loyale Mitarbeiterin? Es muss eindeutig geregelt werden, welche Gegenstände beim Zu- oder Abgang mitgeführt werden dürfen – Handtasche ja, Rucksack nein? An Handgepäck- und Personenkontrollen führt kein Weg vorbei.

Emmerich – „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 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 ihren 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 hohem 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 Insider-Kriminalität 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.