FACHARTIKEL
E-SECURITY

von Reto Zbinden
Geschäftsführer Swiss Infosec AG

E-Security – Teil der Informationssicherheit?

Ziel aller Aktivitäten im Bereich Sicherheit ist es, schädigende Ereignisse für das Unternehmen, seine Mitarbeiter, Partner und die Umwelt in Häufigkeit und Auswirkung auf ein Minimum zu reduzieren. Wie kann dieses Ziel erreicht werden?

E-Security ist ein Teilbereich der Informationssicherheit (ISI). ISI wird definiert wird als das angemessene und dauernde Gewährleisten der Verfügbarkeit, Integrität und Vertraulichkeit der IT-Ressourcen und der damit bearbeiteten oder übertragenen Informationen. Die ISI dient dem Schutz sämtlicher Informationen, ungeachtet der Art ihrer Darstellung und Speicherung. Die Informatiksicherheit oder IT-Sicherheit befasst sich mit elektronisch bearbeiteten Informationen. Der Begriff des Informationsschutzes ist ein ursprünglich militärischer Begriff unter dem der Schutz der Vertraulichkeit von Informationen verstanden wird, unabhängig von der Art ihrer Darstellung und Speicherung.

Gesetzliche Anforderungen und Datenschutz

Sowohl Entwicklung als auch Betrieb und Verwendung von IT-Systemen, Applikationen und Informationen können gesetzlichen Anforderungen unterworfen sein. Sichere Informationsbearbeitung heisst auch gesetzeskonforme Informationsbearbeitung.
Ein Bestandteil der ISI bildet der Datenschutz, der sich mit dem Schutz der Persönlichkeit der von einer Datenbearbeitung betroffenen Personen beschäftigt. Das seit dem 1. Juli 1993 gültige Datenschutzgesetz des Bundes erfasst sowohl die automatisierte als auch die manuelle Bearbeitung von Personendaten. Diese Daten müssen aufgrund des Gesetzes angemessen

durch technische und organisatorische Massnahmen vor dem Zugriff Unbefugter geschützt werden (Art. 6 DSG). Am 6. März 2001 nahm der Bundesrat die Motion an, das Datenschutzgesetz einer Überarbeitung zu unterziehen. Nach einer ersten Rückweisung durch den Nationalrat, der der Ständerat und schliesslich auch die Rechtskommission des Nationalrates nicht folgten, wird die Revision nun in den nächsten Monaten in den Räten behandelt.

Geschäftsbücherverordnung, elektronische Signatur und Basel II

Aufgrund der seit dem 1. Juni 2002 in Kraft gesetzten Geschäftsbücherverordnung kann der gesamte Geschäftsverkehr eines Unternehmens (allg. Geschäftsbücher, Belege und weitere geschäftsrelevante Informationen) in elektronischer Form archiviert werden. Sollen elektronische Dokumente vor Gericht als Beweismittel zugelassen werden, so bedarf es hinsichtlich ihrer Beweiskraft der Einhaltung der sehr weit gehenden Geschäftsbücherverordnung. Sofern gewisse Sicherheitsanforderungen eingehalten werden, können die elektronischen Dokumente gemäss GeBüV auch auf veränderbaren Datenträgern gespeichert werden, was grundsätzlich die Kosten der Archivierung massiv verringern hilft.

Bei elektronischen Dokumenten ist immer die inhärente Gefahr der unberechtigten Veränderung zu berücksichtigen. Am 1.1.2005 tritt das Bundesgesetz über die elektronische Signatur, ZertES, in Kraft. Das ZertES soll den Weg für eine breite Akzeptanz und Nutzung der asymmetrischen Verschlüsselungstechnologie im Rahmen von Public-Key-Infrastrukturen (PKI) ebnen. Bis dato gibt es aber in der Schweiz keine Anbieter von Zertifizierungsdiensten im Bereich der elektronischen Signatur, was grundsätzlich die Akzeptanz und Nutzung in der Praxis in Frage stellt.

Starke Impulse werden vom Abkommen Basel II ausgehen. Ab voraussichtlich 2006 soll das Mass der Eigenkapitalunterlegung von Bankinstituten unter anderem auch davon abhängig sein, inwieweit operative Risiken nachhaltig bewältigt werden. Diese Abhängigkeit werden die Banken an ihre Kunden weitergeben und ihre Ratingverfahren um den Bereich operative Risiken erweitern. Wer zukünftig operative Risiken gut bewältigt, wird weniger Zinskosten zu gewärtigen haben.

Neben den obigen Anforderungen sind im Rahmen des IT-Einsatzes auch die Anforderungen des Urheberrechts und der individuellen Geheimhaltungspflichten (Fernmelde-, Bank-, Arztgeheimnis u. a. m.) zu berücksichtigen. Zu erwähnen ist etwa das Rundschreiben der Eidg. Bankenkommission «Auslagerung von Geschäftsbereichen (Outsourcing)» vom 26. August 1999, das konkrete Sicherheitsanforderungen aufstellt.

Generell lässt sich sagen, dass gesetzliche Anforderungen in der Schweiz zwar bestehen, jedoch die offen gelassenen Konkretisierungen gerade in Praxis zu oft unüberwindbaren Hürden werden. Es wäre wünschenswert, wenn der Gesetzgeber die Minimalanforderungen an die ISI in den jeweiligen Gesetzen konkreter und somit auch verständlicher fassen würde.

Regelwerk, Organisation und Awareness

Zum Schutz der Informationen sind technische, organisatorische und administrative Sicherheitsmassnahmen zu definieren, die in einem Regelwerk zusammengefasst werden können. Ein solches Regelwerk kann ungefähr 80 Prozent der Risiken abdecken. Um die verbleibenden Risiken zu erkennen, sind eigentliche Risikoanalysen durchzuführen, deren Resultate in das Regelwerk zurückfliessen.

Als Basis des Regelwerkes drängt sich der «Code of Practice for Information Security Management» (CoP), ISO 17799/BS 7799 auf. Im Rahmen dieser Anforderungen wird der Aufbau eines eigentlichen Information-Security-Management-Systems (ISMS) gefordert. Ein ISMS ist die Gesamtheit der organisatorischen und konzeptionellen Massnahmen zur Steuerung und Optimierung der ISI eines Unternehmens. Zu einem ISMS gehören: Owner Prinzip, formell in den Prozess Risikobehandlung eingebundenes Top-Management, Klassifizierung, unabhängige Audits u. v. a. m.

Zur technischen Konkretisierung kann auf das IT-Grundschutzhandbuch (GSHB) des Bundesamtes für Sicherheit in der Informationstechnik zu-

SENSIBILISIERUNG UNGENÜGEND

Die Sensibilisierung für die Notwendigkeit von Aktivitäten im Bereich der ISI ist aufgrund medienwirksamer Ereignisse stark gefördert worden. Nach wie vor ist aber festzustellen, dass in zu vielen Unternehmen zu wenig Wert auf einen angemessenen Stand der ISI gelegt wird. Es wird wohl davon ausgegangen, es treffe nur die Anderen. Die bekannt werdenden Sicherheitsvorfälle stellen nur die Spitze des Eisberges dar – unter der Wasseroberfläche lauert eine hohe Dunkelziffer. ISI wird dort ernst genommen, wo einschneidende Schäden oder Beinaheschäden eintraten: aus Schaden klug zu werden, kann zu spät sein.

E-Security als Teil der Integralen Sicherheit

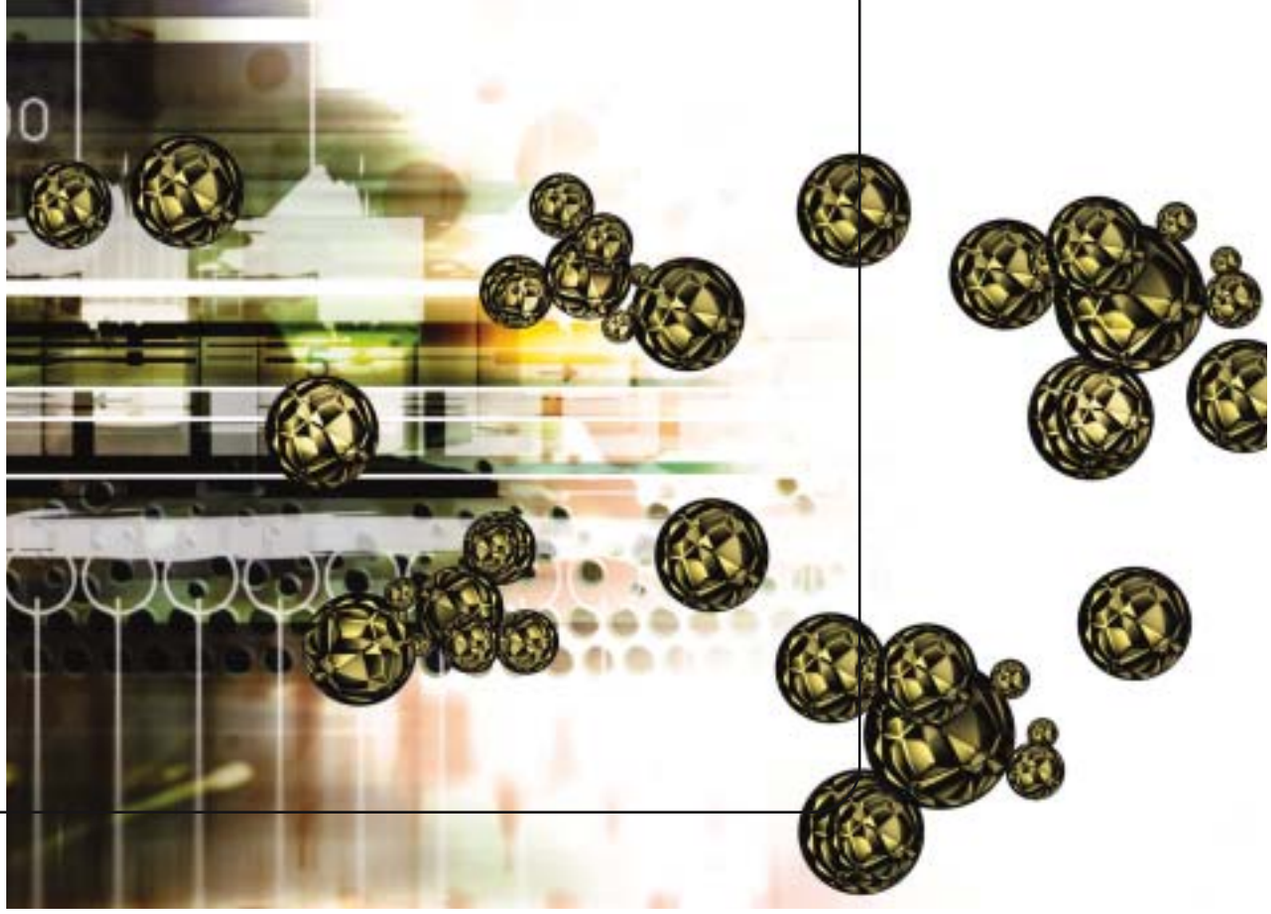
Unter Integraler Sicherheit wird verstanden, dass dem gesamten Bereich Sicherheit konsequent, umfassend, abgestimmt, geplant und effizient in ethisch, wirtschaftlich und rechtlich vertretbarem Rahmen unter Nutzung bestehender Synergien begegnet wird. Voraussetzungen dafür sind das Engagement der Unternehmensleitung, eine klar formulierte Politik, die die Verpflichtung der Organisation festlegt und dokumentiert, sowie eine effiziente Aufbau- und Ablauforganisation, die die weiteren Schritte zu bewältigen in der Lage ist.

Sicherheitspolitik

Das Management muss der Sicherheit einen umfassenden Stellenwert einräumen, die Sicherheitskultur vorzeichnen und im Unternehmen verbreiten, umsetzen und ständig kultivieren. Es muss Massnahmen im Bereich der ISI initiieren und aktiv tragen. Alle Vorgesetzten müssen sich ihrer Vorbildfunktion bewusst sein. Im Rahmen einer Politik sind die Sicherheitsziele zu definieren, die Grundsätze für die einzelnen Sicherheitsbereiche zu formulieren und der Ablauf der Risikoerkennung, -bewertung und -überprüfung festzulegen.

Sicherheitskonzept

Das ISI-Konzept konkretisiert die Politik unter Berücksichtigung der gesetzlichen, vertraglichen und internen Anforderungen. Im Konzept werden Massnahmen festgelegt, Aufgaben, Verantwortlichkeiten und Kompetenzen für Funktionen und Gremien definiert. Beschrieben werden einheitliche und standardisierte Methoden zur Identifikation und der regelmässigen Überprüfung von Risiken sowie zur Festlegung von Sicherheitsregeln und -massnahmen.



rückgegriffen werden (www.bsi.de). Sowohl für BS7799 wie auch GSHB existiert die Möglichkeit der Zertifizierung durch eine unabhängige Stelle. Die Bedeutung von Zertifizierungen im Bereich der Informationssicherheit wird in den kommenden Jahren massiv zunehmen.
Ein Mitglied der Geschäftsleitung ist als Delegierter für Sicherheit zu bestimmen. Ihm zur Seite zu stellen ist ein Fachgremium, das sich aus allen Fachbeauftragten der Sicherheitsteilbereiche zusammensetzt. Das Ziel dieses Gremiums ist es, die Sicherheitsaktivitäten zu koordinieren, zu lenken und Synergien zu erkennen und zu nutzen.
Die frühe Einsetzung eines internen Fachbeauftragten für ISI (Information Security Officer; ISO) wird dringend empfohlen. Soweit es die Grösse des Unternehmens zulässt, sollten aufgrund möglicher Interessenkonflikte keine Mitarbeiter der IT-Abteilung mit dieser Aufgabe betraut werden.
Die überwiegende Zahl von Schäden im IT-Bereich entsteht durch Nachlässigkeit, unzureichende Akzeptanz von Sicherheitsmassnahmen und aus mangelnder Kenntnis. Ein hohes Mass an Sicherheit kann auch im Bereich der IT nur erreicht und beibehalten werden, wenn sämtliche Mitarbeitenden die Bedeutung von Massnahmen für die Sicherung der Existenz des Unternehmens erkannt haben und bereit sind, entsprechend dieser Erkenntnis zu handeln.

Aktuelle technische Entwicklungen und Herausforderungen

Die Labilität der IT-Ressourcen wächst. Daneben wächst die Abhängigkeit der Unternehmen und Anwender von der zeitgerechten Verarbeitung ihrer Informationen und der Verfügbarkeit der Kommunikationsmöglichkeiten. Die steigende Labilität ist u. a. auf die laufend und rapide zunehmende Komplexität und Vernetzung der IT-Ressourcen zurückzuführen.
Heute fallen IT-Services aus, ohne dass Heerscharen von Spezialisten die leiseste Chance hätten, die Ursache des Ausfalls eindeutig festzustellen. Der Druck der Lieferanten, Produkte in immer schnelleren Zyklen zur Marktreife zu führen, trägt nicht direkt zur Steigerung eben dieser Reife im Einzelfall bei. Der Kostendruck verhindert profunde Tests vor der Auslieferung des Produktes. Diese Faktoren haben deshalb auch zukünftig zur Folge, dass erkannte, aber noch nicht behobene Sicherheitslücken von Angreifern erfolgreich ausgenutzt werden können.
Die Schnelligkeit der Wissensverbreitung zu Sicherheitslücken zwingt zu organisatorischen und konzeptionellen Massnahmen. Es muss sichergestellt werden, dass in der Öffentlichkeit bekannt werdende Sicherheitslücken auf ihre Relevanz untersucht werden und gegebenenfalls zeitgerecht behoben werden. Werden hier nicht spezielle Prozesse erarbeitet und etabliert, öffnen sich für die Angreifer zu lange Tür und Tor. Jegliche Verbindung zum Internet erfordert spezifische Schutzmechanismen, die unter dem Begriff Firewall zusammengefasst werden. Es muss einem externen Angreifer nachhaltig verunmöglicht werden, auf interne Systeme oder interne Informationen zuzugreifen. Eine einmal installierte Firewall muss aktiv gewartet werden – eine sehr zeitintensive Arbeit.

Intrusion Detection und Firewall

Sogenannte Intrusion-Detection-Systeme ergänzen den Schutz der Firewalls. Sie sollen in Echtzeit das Verhaltensmuster eines Angreifers erkennen und Alarm auslösen.
Es ist eine Tendenz erkennbar, auch einzelne Segmente und Systeme des internen Netzes mittels Firewallfunktionalitäten zu schützen. Firewallfunktionen stellen dort eine Notwendigkeit dar, wo eigene firmeninterne Systeme und Netze mit so genannten nicht vertrauenswürdigen Netzen verbunden werden sollen. Als vertrauenswürdig sollten dabei nur Systeme und Netze bezeichnet werden, die unter der firmeneigenen Kontrolle stehen. Vermehrt werden nun firmeninterne Netze aufgrund ihrer Grösse und der unbekannten Zahl berechtigter und unberechtigter Benutzer als nicht vertrauenswürdig eingestuft.
Bei der privaten Verwendung des Internets wird sich zukünftig die Ver-

wendung einer so genannten Personal Firewall durchsetzen. Deren Verwendung ist besonders dringend empfohlen, wenn das System mittels Breitbandtechnologie dauernd mit dem Internet verbunden bleibt.
Unternehmen testen die Sicherheit ihrer Systeme und der Firewalls immer häufiger aktiv. Hier spricht man in Fachkreisen von sogenannten Penetration Tests. Im Rahmen solcher Überprüfungen werden allfällige Sicherheitslücken mittels automatisierter Verfahren und manueller Angriffe gesucht.
Eine Schlüsseltechnologie für die Informationssicherheit stellt die Verschlüsselung dar. Die Vertraulichkeit von Informationen lässt sich vielfach nur mittels kryptologischer Verfahren nachhaltig gewährleisten. Als Beispiel hierfür seien Virtual Private Networks (VPN) angeführt. VPNs dienen der sicheren Verbindung zweier oder mehrerer Partner über nicht vertrauenswürdige Netze. Die Sicherheit wird durch die Verschlüsselung erreicht. Damit erhöhen VPNs nicht nur die Sicherheit, sondern senken auch die Verbindungskosten – ein bei Sicherheitsmassnahmen leider nur seltener Nebeneffekt.

Sicherheitsrisiko PDA

Vor eine erst teilweise erkannte Sicherheitsproblematik werden die Unternehmung durch die Verbreitung der sogenannten Personal Data Assistants (PDA) und Smart Phones gestellt. Die Möglichkeiten dieser mobilen Geräte steigen laufend. Dateien können in Windeseile von Firmensystemen auf die PDAs transferiert werden. Der Schutz der PDAs entspricht jedoch in den wenigstens Fällen den Anforderungen wohl verstandener ISI. Daneben steigt die Zahl PDA-spezifischer Gefährdungen aufgrund der Standardisierung der eingesetzten Betriebsplattformen. Generell ist festzuhalten, dass Standards in erster Linie Angriffe erleichtern und erst in zweiter Linie die Entwicklung kompatibler und marktfähiger Sicherheitslösungen ermöglichen. Die Sicherheit hinkt also dauernd der technologischen Entwicklung hinterher. Im Falle von PDAs und Smart Phones wird zukünftig zu fordern sein, dass die darauf gespeicherten Daten mittels Verschlüsselung nachhaltig vor dem Zugriff Unberechtigter geschützt werden müssen. Eine Forderung, die sich im Bereich der Notebooks bereits etabliert hat. Daneben müssen auch PDAs vor bösartigem Code (Malicious Code), wie beispielsweise Viren, aktiv geschützt werden. PDA-Benutzer sind auch dahingehend zu sensibilisieren, die auf dem PDA gehaltenen Daten regelmässig zu sichern – eine minimale, jedoch häufig vernachlässigte Sicherheitsmassnahme.
Eine weitere Angriffsform, die sich neben den Viren und Würmern in den letzten Monaten entwickelt hat, ist das Phishing: Ein Angreifer versucht mittels eines gefälschten E-Mail-Massenversands als Köder möglichst viele Benutzer auf eine gefälschte, vom Erscheinungsbild her möglichst realistische Website zu locken, um den Benutzer dort Authentisierungsinformationen eingeben zu lassen. Diese Informationen (User ID, Passwort, Strichlistencode) werden anschliessend für Angriffe verwendet. Gerade die Verbreitung des Phänomens Phishing zeigt die wichtige Rolle des Benutzers und die Wichtigkeit von Sensibilisierungsmassnahmen auf.
Die Zukunft wird neue Herausforderungen im Bereich der Informationssicherheit mit sich bringen. Die technologische Entwicklung wird aber ihren Vorsprung gegenüber der Sicherheit immer bewahren. ◆