Schritte zur Umsetzung

Autor(en): **Zbinden, Reto C.**

Objekttyp: **Article**

Zeitschrift: **Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology**

Band (Jahr): **80 (2002)**

Heft 5

PDF erstellt am: **28.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-877196

Informationssicherheit

Schritte zur Umsetzung

Die Sensibilisierung für die Notwendigkeit von Aktivitäten im Bereich der Informationssicherheit (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 Informationssicherheit gelegt wird.

Es wird oft davon ausgegangen, es treffe nur die Anderen. Die bekannt werdenden Sicherheitsvorfälle stellen nur die Spitze des Eisbergs dar, unter der Wasseroberfläche lauert eine hohe Dunkelziffer. Informationssicherheit wird dort ernst genommen, wo einschneidende Schäden oder Beinaheschäden eintraten. Doch aus Schaden klug zu werden, kann zu spät sein.

RETO C. ZBINDEN

Das 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.
Informationssicherheit wird definiert als das angemessene und dauernde Gewährleisten der Verfügbarkeit, der Integrität und der Vertraulichkeit der IT-Ressourcen und der damit bearbeiteten oder übertragenen Informationen. Die Informationssicherheit dient dem Schutz sämtlicher Informationen ungeachtet der Art ihrer Darstellung und Speicherung. Die Informatiksicherheit oder IT-Sicherheit befasst sich mit den elektronisch bearbeiteten Informationen.

Gesetzliche Anforderungen

Sowohl Entwicklung als auch Betrieb und Verwendung von IT-Systemen, Applikationen und Informationen können gesetzlichen Anforderungen unterworfen sein. Sichere Informationsbearbeitung heisst auch gesetzeskonforme Informationsbearbeitung.
Einen Bestandteil der Informationssicherheit 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). Die Massnahmen zur Gewährleistung der Informationssicherheit müssen grundsätzlich verhältnismässig sein. Sie tragen dem Zweck der Bearbeitung, der Art und dem Umfang der Bearbeitung, der Einschätzung der möglichen Risiken für die betroffenen Personen oder das Unternehmen und dem gegenwärtigen Stand der Technik Rechnung. Am 6. März 2001 nahm der Bundesrat die Motion an, das Datenschutzgesetz einer Überarbeitung zu unterziehen.
Neben dem Datenschutzgesetz sind im Rahmen des IT-Einsatzes auch die Anforderungen des Urheberrechts und der individuellen Geheimhaltungspflichten (Fernmelde-, Bank-, Arztgeheimnis) zu berücksichtigen. Zu erwähnen ist beispielsweise das Rundschreiben der Eidg. Bankenkommission «Auslagerung von Geschäftsbereichen (Outsourcing)» vom 26. August 1999, das konkrete Sicherheitsanforderungen aufstellt.
In Deutschland gilt seit Mai 1998 das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), das Unternehmen verpflichtet, ein internes Riskmanagement zu implementieren. Eine vergleichbare Anforderung fehlt in der Schweiz.

Informationssicherheit: Handlungsbedarf wird nicht erkannt

Der Wert eines Unternehmens ist heute in einem hohen Masse abhängig vom Wert oder vom Unwert seiner Informationen bzw. der Fähigkeit, auf diese Informationen zugreifen zu können. Die Abhängigkeit der Unternehmen und Anwender von der zeitgerechten Verarbeitung ihrer Informationen und der Verfügbarkeit der Kommunikationsmöglichkeiten wächst rasant.
Auch die allgemeine Verunsicherung aufgrund des krisengeschüttelten Jahrs 2001 und insbesondere des 11. September 2001 führte nicht zu einem nachhaltigen Umdenken im Bereich der unternehmensinternen Informationssicherheit. Auch nach dem 11. September finden mittel- und langfristige Konzeptionen und Massnahmen zur Verbesserung der integralen Sicherheit und der Informationssicherheit nur sehr schwer Akzeptanz beim Management. Die im Nachgang zum 11. September 2001 ergriffenen Massnahmen konzentrierten sich, wenn solche überhaupt konkret thematisiert und definiert wurden, auf physische Sicherheitsaspekte. Physische Sicherheitsmassnahmen haben den Vorteil des Handfesten und der Vordergründigkeit für sich.
Am Anfang steht die Erkenntnis, dass die Information einen zentralen Faktor der Wertschöpfung, einen zentralen Wertträger innerhalb des Unternehmens darstellt. Eine weitere Erkenntnis besteht darin, zu entdecken, dass angemessene Informationssicherheit zusätzlich bestellt bzw. speziell beauftragt werden muss: Es braucht zusätzliche Konzepte, zusätzliche Aufwände, zusätzliche Intervention seitens des Managements, ansonsten unsichere Systeme unsicher bleiben.

Managementaufgabe

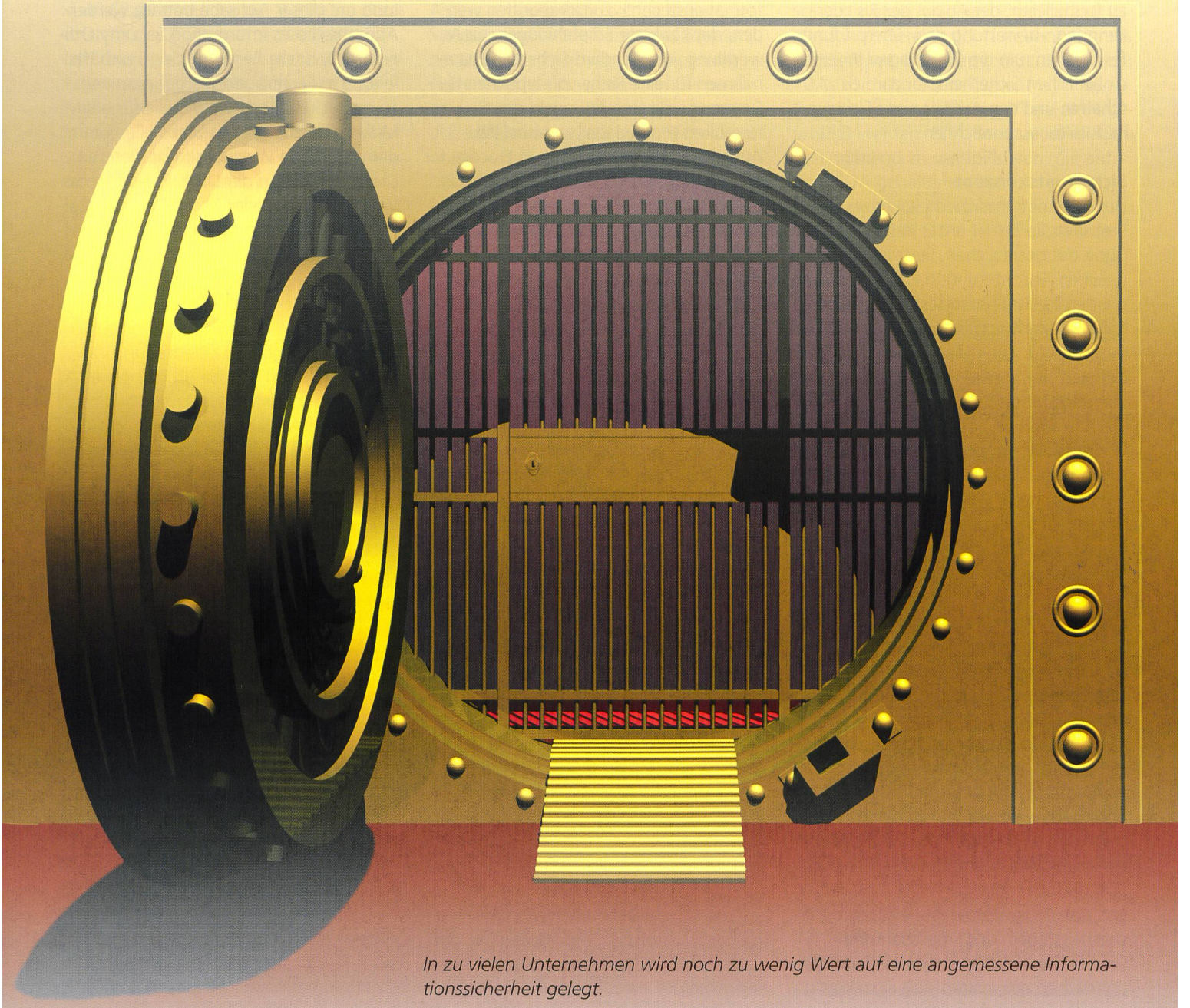
Es ist die Aufgabe der Geschäftsleitung, Massnahmen im Bereich der IT-Sicherheit zu initiieren und aktiv zu tragen. Alle Vorgesetzten müssen sich ihrer Vorbildfunktion bewusst sein. Im Bereich der IT-Sicherheit ist es keinesfalls damit getan, in Hard- oder Software zu investieren. Die Mehrheit der Massnahmen im Bereich IT-Sicherheit sind rein organisatorischer und konzeptioneller Natur. Daneben sind im Einzelfall technische Massnahmen und somit auch Investitionen zu prüfen.

Zu Beginn der Aktivitäten sollte eine klare Formulierung der Zielsetzung, eine pointierte Darstellung der Wichtigkeit, die Einsetzung der verantwortlichen Funktionen und der Aufruf an sämtliche Mitarbeiter stehen, diese Aktivitäten zu unterstützen. Dies kann im Rahmen einer so genannten IT-Sicherheitspolitik, in der Ausführlichkeit und Tiefe vergleichbar mit einer QM-Politik, erfolgen.
Diese Politik oder Strategie ist anschliessend zu konkretisieren, Verfahren sind festzulegen, Verantwortlichkeiten sind zu definieren und gegebenenfalls notwendige Weisungen sind zu erstellen.
Die Durchführung einer umfassenden unternehmensweiten Risikoanalyse drängt sich nicht direkt auf. Die Erfahrung zeigt, dass Risikoanalysen in verschiedenen Unternehmen zu 60 bis 90% identische Massnahmen und Empfehlungen zur Folge haben. Deshalb wird in Abstimmung mit den international anerkannten Standards empfohlen, das Verfahren umzukehren und zu Beginn die Massnahmen, die dem State of the Art entsprechen, zu formulieren.

Informationssicherheit als Teil der integralen Sicherheit

Unter integraler Sicherheit wird im Folgenden verstanden, dass dem gesamten Bereich Sicherheit konsequent, umfassend, abgestimmt, geplant und effizient in ethisch, wirtschaftlich und rechtlich vertretbarem Rahmen unter Ausnutzung bestehender Synergien begegnet wird.

Voraussetzungen dafür sind das Engagement der Unternehmensleitung, eine klar formulierte Politik, welche die Verpflichtung der Organisation festlegt und dokumentiert sowie eine effiziente Aufbau- und Ablauforganisation, welche die weiteren Schritte zu bewältigen in der Lage ist.
Erst wenn das Unternehmen als System gewährleisten kann, dass verschiedene Stellen die verschiedenen Risiken methodisch identisch angehen und die Aktivitäten kommuniziert sowie koordiniert werden können, kann im Ansatz von einem verantwortungsbewussten und integralen Risk-Management gesprochen werden.
Der Nutzen solcher Massnahmen, der diese gleichzeitig auch unternehmerisch



In zu vielen Unternehmen wird noch zu wenig Wert auf eine angemessene Informationssicherheit gelegt.

rechtfertigt, stellt sich dar als Differenz zwischen Kosten der jeweiligen Massnahme und den dadurch vermiedenen Auswirkungen des Risikoeintritts. Besonders wichtig ist der Einbezug der potenziellen immateriellen Schäden in die Berechnung der Auswirkungen.

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 Informationssicherheit 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, der Ablauf der Risikoerkennung, -bewertung und -überprüfung festzulegen, um die Grundlagen für einen einheitlichen Sicherheitsstandard zu schaffen und den Aufbau einer Sicherheitskultur vorzuzeichnen.

Sicherheitskonzept
Das Informationssicherheitskonzept 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 zur regelmässigen Überprüfung von Risiken sowie zur Festlegung von Sicherheitsregeln und -massnahmen.
Das Hauptziel eines Informationssicherheitskonzepts ist die betriebliche Organisation der Sicherheit aller Informationen im Rahmen der gesetzlichen, vertraglichen und internen Anforderungen. Mit der Festlegung von Massnahmen, der Definition von Aufgaben, Verantwortlichkeiten und Kompetenzen für Funktionen und Gremien sollen die Informationen und damit auch die für ihre Bearbeitung benötigten IT-Systeme so geschützt werden, dass die Informationssicherheit unternehmensweit gewährleistet wird.
Das Konzept beschreibt einheitliche und standardisierte Methoden zur Identifikation und zur regelmässigen Überprüfung von Risiken sowie zur Festlegung von Sicherheitsregeln und -massnahmen.
Spezifische Anforderungen des Informationssicherheitskonzepts zu einzelnen wichtigen Themenbereichen könnten bei Bedarf wiederum in separaten Bereichskonzepten weiter ausgeführt werden (Datensicherungskonzept, Zugriffsschutzkonzept).

Regelwerk
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% der Risiken abdecken. Um die verbleibenden Risiken zu erkennen, sind eigentliche Risikoanalysen durchzuführen, deren Resultate in das Regelwerk zurückfliessen.
Als Basis des Regelwerks kann einerseits auf das IT-Grundschutzhandbuch (GSHB) des Bundesamtes für Sicherheit in der Informationstechnik zurückgegriffen werden, das konkrete Empfehlungen zur Anwendung von Standard-Sicherheitsmassnahmen für eine Reihe von typischen IT-Systemen und Einsatzumgebungen formuliert (Homepage: www.bsi.de).
Andererseits kann der Code of Practice for Information Security Management (CoP), ISO 17799/BS 7799 zugezogen werden, der in Kürze auch zu einer schweizerischen Norm erhoben wird. Für beide Grundwerke sind Zertifizierungen möglich bzw. im Falle GSHB in Vorbereitung.

Organisation
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 auszunutzen.
Die frühe Einsetzung eines internen Fachbeauftragten für Informationssicherheit wird dringend empfohlen. Soweit es die Grösse des Unternehmens zulässt, sollten aufgrund möglicher Interessenkonflikte keine Mitarbeiter der IT-Abteilung mit dieser Aufgabe betraut werden.
Aufgabe dieses Information Security Officers (ISO) ist die Beratung der Geschäftsleitung in Fachfragen, Vorgehenspläne zu entwickeln und Anlaufstelle für alle Mitarbeiter zu sein. Als Stabstelle kommt dem ISO keine Weisungskompetenz zu. Diese verbleibt in der Linie. Es liegt in der Verantwortung jedes Mitarbeiters und aller Vorgesetzten in ihrem Führungs-

Vertraulichkeit

bedeutet, dass Informationen und die zu ihrer Bearbeitung und Übertragung verwendeten Schutzobjekte nur Berechtigten zugänglich sind (nur befugter Informationsbezug). Die Vertraulichkeit ist gewährleistet, wenn die als schutzwürdig definierten Objekte nur berechtigten Subjekten offenbart werden.

Integrität

bedeutet, dass Informationen oder Teile eines IT-Systemes nur durch Berechtigte verändert werden können. Die Integrität ist dann gewährleistet, wenn nur berechtigte Subjekte (Mensch, System oder Funktion) Schutzobjekte (System, Funktion oder Informationsbestände) zu berechtigten Zwecken korrekt bearbeiten, die Schutzobjekte spezifiziert sind und die Bearbeitung nachvollziehbar ist. Korrekt arbeitende Funktionen sind dann gewährleistet, wenn sie integre Schutzobjekte (System, Funktion oder Informationsbestände) in diesem Zustand belassen und/oder neue Schutzobjekte den Anforderungen entsprechend in einer als integer beschriebenen Form erzeugen.

Verfügbarkeit

bedeutet, dass das IT-System und die damit bearbeiteten Informationen den Berechtigten in voller Funktionalität zur Verfügung stehen. Ein berechtigter Benutzer soll nicht abgewiesen werden. Die Verfügbarkeit ist dann gewährleistet, wenn die berechtigten Subjekte dauernd innerhalb der gemeinsam als notwendig definierten Frist auf die zur Durchführung ihrer Aufgaben benötigten Schutzobjekte zugreifen können, die notwendigen Massnahmen erarbeitet, durchgesetzt und eingeübt sind, die es bei Störungen erlauben, die Verfügbarkeit fristgerecht wieder herzustellen bzw. zu sichern.

bereich, die Informationssicherheit im Rahmen der Vorgaben umzusetzen. ISOs in Kleinunternehmen können diese Funktion auch im Nebenamt ausüben.

Awareness

Sicherheit lässt sich alleine durch technische Massnahmen nicht realisieren. Die Technik kann den Menschen in seinem Bemühen um Sicherheit zwar unterstützen. Sie kann jedoch keinen Ersatz für ein fehlendes Risikobewusstsein darstellen. Die überwiegende Zahl von Schäden im IT-Bereich entsteht durch Nachlässigkeit, unzureichender 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. Erst wenn dem Mitarbeiter der Sinn einer Handlung einleuchtet, die er auszuführen hat, wird er sie zuverlässig befolgen.
Information und Kommunikation über Informationssicherheit dürfen nicht isolierte Einzelereignisse sein. Die Mitarbeiter sind mit genügend Hintergrundinformationen zu versorgen, um verstehen zu können, wozu die Sicherheitsmassnahmen dienen, die sie auszuführen haben.

Aktuelle technische Entwicklungen und Herausforderungen

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 Produkts. 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 bzw. interne Informationen zuzugreifen. Eine einmal installierte Firewall muss aktiv gewartet werden, was eine sehr zeitintensive Arbeit ist.
So genannte Intrusion Detection Systems 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 Verwendung einer so genannten Personal Firewall durchsetzen. Deren Verwendung ist besonders dringend, 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 von Penetrationtests. Im Rahmen solcher Überprüfungen werden allfällige Sicherheitslücken mittels automatisierter Verfahren und/oder manueller Angriffe gesucht.
Die Verschlüsselung stellt für die Informationssicherheit eine Schlüsseltechnologie dar. Die Vertraulichkeit von Informationen lässt sich vielfach nur mittels kryptologischer Verfahren nachhaltig gewährleisten. Als Beispiel seien hier Virtual Private Networks (VPN) angeführt. VPNs dienen der sicheren, weil verschlüsselten Verbindung zweier oder mehrerer Partner über nicht vertrauenswürdige Netze. So erhöhen VPNs nicht nur die Sicherheit, sondern senken auch die Verbindungskosten, ein bei Sicherheitsmassnahmen leider nur seltener Nebeneffekt.
Vor eine erst teilweise erkannte Sicherheitsproblematik werden die Unternehmung durch die Verbreitung der so genannten Personal Data Assistants (PDA) 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 wenigsten Fällen den Anforderungen wohl verstandener Informationssicherheit. 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 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. 4

Quelle: Referat, gehalten anlässlich des FAEL-Seminars vom 3. Mai 2002 in Zürich.

***Reto C. Zbinden** ist seit zwölf Jahren CEO der Swiss Infosec AG. Als Fürsprecher beschäftigt er sich neben seiner Beratungstätigkeit in den Bereichen Integrale Sicherheit, Informationssicherheit und IT-Sicherheit. Ausserdem setzt er sich speziell mit den Themen Informatikrecht, insbesondere Datenschutz auseinander. Er ist Mitglied des wissenschaftlichen Beirats der Stiftung Infosurance, der ISACA, der Schweizer Informatiker Gesellschaft SI, des CLUSIS und der ISSA. E-Mail: zbinden@infosec.ch*

*Die Swiss Infosec AG besteht seit 1989 als unabhängiges Beratungs- und Ausbildungsunternehmen und ist ausschliesslich in den Bereichen Integrale Sicherheit, Informationssicherheit und IT-Sicherheit tätig. Newsletter erhältlich über infosec@infosec.ch.
Homepage: www.infosec.ch*