

Aktuell. Detailliert. Fundiert.

Wirtschaft Konkret Nr. 301



EULER HERMES
Kreditversicherung

Ein sicheres Netz

Computerrisiken sind Chefsache

Inhalt

301 Ein sicheres Netz

3	Editorial	10	Sicherheit ist Chefsache	18	Was zu tun ist
4	Mangelnde Computer-Sicherheit	11	Vom Gesetz verpflichtet	18	Die wichtigsten Schritte
4	Die verkannte Gefahr	12	Worauf es wirklich ankommt	18	Hilfe im Notfall
5	Der Kern einer Krise	13	Checkliste: Fragen zur allgemeinen Organisation	19	Checkliste: Fragen zur zentralen Informationsverarbeitung
5	Mängel in den Unternehmen	14	Wie ein Konzept entsteht	20	Die häufigsten Fehler
6	Gefährliche Computer-Kriminalität	15	Checkliste: Fragen zur technischen Sicherheit des Rechenzentrums	21	Glossar der IT-Sicherheit
6	Risiken der Datenverarbeitung	16	Risiken bei Rationalisierung	22	Weiterführende Links
7	Zugriff für intelligente Täter	16	Ausweitung der EDV		
8	Erschreckende Sicherheitslücken	16	Richtig für jedes Unternehmen		
9	Checkliste: Fragen zur individuellen Informa- tionsverarbeitung	17	Checkliste: Fragen zur Organisation und Software-Entwicklung		
9	Checkliste: Fragen zu Mitarbeitern				

Impressum

„Wirtschaft Konkret“ ist eine Veröffentlichung der Euler Hermes Kreditversicherungs-AG, Friedensallee 254, 22763 Hamburg.

Verantwortlich: Hans Joachim Kasperski, Euler Hermes Kreditversicherungs-AG. **Redaktion:** Rainer Hupe Kommunikation, Hochallee 77, 20149 Hamburg.

Layout: Type Art Team Detlef Rögner GmbH, Kieler Straße 1, 25451 Quickborn.

Informationen nach bestem Wissen, jedoch ohne Gewähr. Nachdruck (auch auszugsweise) nur mit Genehmigung des Herausgebers.

Stand: Februar 2008

Editorial



Computer-Sicherheit

Bewährung für das Management

Computer sind das Nervenzentrum der Unternehmen, an Ihnen hängt alles. Sie vernetzen die Mitarbeiter untereinander, die Firmen miteinander und immer stärker die gesamte globalisierte Welt. Ohne Computer wären Unternehmen und Wirtschaft längst gelähmt. Und was heute schon eine schlichte Selbstverständlichkeit ist, wird in Zukunft noch dramatisch an Bedeutung gewinnen. Denn die verschiedenen Nutzungen unter dem Stichwort eBusiness stecken noch in den Kinderschuhen, sie werden sich in den nächsten Jahren rasant verbreiten.

Doch mit zunehmender Bedeutung wachsen nicht nur die ökonomischen Chancen, sondern auch die Risiken – bis hin zur Existenzgefährdung bei kleinen und mittleren Firmen. Spektakuläre Angriffe von außen durch Hacker und Viren, medienwirksam in Szene gesetzt, sind die eine Seite. Sie erreichen große Aufmerksamkeit und verursachen immer häufiger immensen Schaden. Doch es gibt noch eine andere Seite, „Angriffe“ von innen: ausfallende Systeme, mangelnde Kontrollen, Mitarbeiter, die Daten klauen oder manipulieren und so Millionen veruntreuen. Rund 80 Prozent aller Delikte im EDV-Bereich, so die Statistik, werden von den eigenen Mitarbeitern begangen.

Das Risikomanagement steckt dagegen noch in den Kinderschuhen. In vielen Firmen wird es als Spezialaufgabe für EDV-Leiter und Sicherheitsexperten angesehen. Dabei ist es längst Chefsache, geht es darum, eine Sicherheitskultur im gesamten Unternehmen zu entwickeln und zu kommunizieren. Das Bewusstsein für die besonderen Risiken moderner Informationstechnologie und die speziellen Anforderungen im Umgang damit muss bei jedem Mitarbeiter präsent sein.

Die vorliegende Broschüre gibt deshalb ganz konkrete Hinweise für den Aufbau und die Perfektionierung eines funktionierenden Sicherheitssystems, besonders in mittelständischen Unternehmen. Sie behandelt die grundlegenden Fragen: Was gehört zu einem effizienten Sicherheitsmanagement? Welche Schritte sind dazu nötig? Wie analysiert man Existenzgefährdende Sicherheitslücken? Welche Fehler machen die Unternehmen meistens? Wo bekommt man die entscheidenden Informationen?

*Rainer Hupe
Chefredakteur*



Mangelnde Computer-Sicherheit

Die verkannte Gefahr

Mit dem Begriff Computer-Sicherheit verbinden viele Nutzer die Bedrohung durch Hacker und Viren – also mehr oder weniger zufällige Angriffe von außen. Kein Wunder, gehen doch in fast regelmäßigen Abständen die Meldungen von Viren mit geheimnisvollen Namen durch die Medien, die ganze Server von Großorganisationen lahm legen oder von Hackern, die sich auf spektakuläre Weise Zugang zu geheimen Daten von Unternehmen oder sogar militärischen Datennetzen verschaffen. Die Gefahr durch unbefugte Zugriffe von außen auf sensible Unternehmensdaten lauert überall – das zumindest suggeriert die breite Medienresonanz.

Natürlich sind diese Gefahren groß und nehmen ständig zu – und dennoch sind sie nur eine Facette eines viel größeren Problems. In deutschen Firmen entstehen Jahr für Jahr Millionen-, wenn nicht Milliardenverluste durch Datenklau. So genau weiß das niemand, denn die Dunkelziffer ist beträchtlich. Klar ist aber, dass die größte Gefahr nicht von außen kommt, sondern in den Firmen selbst existiert. Rund 80 Prozent aller bekannt gewordenen Fälle von Datenverlust oder Datendiebstahl gehen von Mitarbeitern des eigenen Unternehmens aus. Zufällige Angriffe von Hackern und Viren oder gezielte Fälle von Wirtschaftsspionage sind (abgesehen von gravierenden Einzelfällen) im Ganzen gesehen jedoch eher von geringerer Bedeutung im Vergleich zu den Folgen vermeintlich banaler Dinge:

- Datenverluste durch Stromausfall und Fehlbedienung sind eine große Gefahr. Doch häufig genug bekommt ein ergebnisverantwortlicher Manager davon nichts mit. Er wundert sich höchstens über mangelnde Produktivität und schwindenden Profit, ohne dies mit mangelnder Computersicherheit in Verbindung zu bringen.
- Computer werden immer häufiger zu Komplizen bei wirtschaftskriminellen Handlungen in den Unternehmen (siehe Wirtschaft Konkret Nr. 300: „Wirtschaftskriminalität – das diskrete Risiko“). Mitarbeiter verschaffen sich Zugang zu vertraulichen Daten, nutzen elektronische Formulare oder fälschen Unterschriften auf Knopfdruck.



- Über Computernetze wickeln Firmen zunehmend nicht nur administrative Details, sondern wichtige Geschäftsprozesse ab, Schlagworte wie „Electronic Business“ oder „Electronic Commerce“ stehen dafür. Nach einer Umfrage des Fraunhofer-Instituts für Arbeitswirtschaft und Organisation (IAO) bei 13.000 Industrie- und Dienstleistungsunternehmen in Deutschland wird das so genannte eBusiness bei 80 Prozent der Befragten im Jahre 2006 eine hohe bis sehr hohe Bedeutung haben.

Der Kern einer Krise

In der dynamischen Entwicklung steckt nicht nur ein erhebliches ökonomisches Potential, sondern auch der Kern eines potenziellen Krisenszenarios, das die Existenz von Unternehmen und damit auch viele Arbeitsplätze

kosten kann. Denn einerseits steigt und fällt die Wettbewerbsfähigkeit gerade kleiner Unternehmen mit ihrer Fähigkeit, größtmöglichen Nutzen aus der EDV zu ziehen. Zeitgewinn, Kostensenkung und höhere Produktivität sind Vorteile, auf die niemand verzichten kann. Andererseits aber werden die Konsequenzen mangelnder IT-Sicherheit häufig gar nicht oder zu spät erkannt.

Jeder gute Manager versucht heute, vielfältige Risiken – ob bei den Wechselkursen oder in der Lagerhaltung – durch intelligentes Risikomanagement möglichst klein zu halten. Die Informationssicherheit, also der Schutz von Computersystemen vor Ausfall oder Angriff, gilt aber immer noch vornehmlich als Aufgabe der EDV-Abteilung. Gerade in mittelständischen Unternehmen wird das Thema oft vernachlässigt oder gar ignoriert – personell wie finanziell.

Mängel in den Unternehmen

So stellte etwa die KPMG Deutsche Treuhandgesellschaft erhebliche Mängel im Sicherheitsbewusstsein fest. Eine Studie der Wirtschaftsprüfer ergab, dass jeder zweite Top-Manager und immer noch 45 Prozent des mittleren Managements in den 1000 größten deutschen Unternehmen sich überhaupt noch nie mit der Frage befasst hatten (efr@ud.survey – Umfrage zur Wirtschaftskriminalität im eCommerce). In 40 Prozent der Unternehmen waren nicht genügend Mittel für die Informationssicherheit bereitgestellt worden, ein Viertel der Unternehmen hatte kein Sicherheitskonzept oder setzte das vorhandene nicht um. Das ist die Situation in den Vorzeige-Unternehmen, wie sieht es wohl im Mittelstand aus?



Gefährliche Computer-Kriminalität

Risiken der Datenverarbeitung

Die wichtigsten Vorteile der elektronischen Datenverarbeitung in den Unternehmen und in der weltweiten Verbindung durch das Internet sind zugleich die gängigsten Quellen von Missbrauch. Als wesentliche Aspekte sind dabei besonders zu nennen:

- Die Konzentration der Daten, also deren Speicherung in immer größeren Mengen auf kleinstem Raum.
 - Die Verfügbarkeit der Daten, die jeweils in Bruchteilen von Sekunden in der gewünschten Form bereitstehen.
 - Die Korrelation der Daten, die es ermöglicht, unterschiedlichste Inhalte miteinander zu verknüpfen und so für verschiedene – auch missbräuchliche – Nutzung zu verwerten.
 - Der Zugriff auf Daten, der von mehreren Nutzern gleichzeitig erfolgen kann, so dass die Kontrolle darüber erschwert wird, wer, wann, was aus der Datei „entwendet“ hat.
- Der Einsatz von Terminals mit Eingabemöglichkeit, der völlig neue Verwaltungs- und Organisationswege ermöglicht.
 - Die Programmentwicklung, die sich in zwei Richtungen vollzieht. Einerseits können bei kleinen, einfachen Anwendungen Routine-Aufgaben ohne EDV-Kenntnis gelöst werden. Andererseits werden komplexe Programme entworfen, die nur von Spezialisten beherrscht werden.

Bei den in Europa und Deutschland bekannt gewordenen Schäden wurden zumeist diese speziellen Eigenschaften ausgenutzt. Da viele Unternehmen zum Beispiel Schecks nicht nur vom Computer drucken, sondern auch schreiben lassen, kann eine einfache Programmmanipulation ausreichen, um Millionen zu veruntreuen.

Daten können aber auch bei der Erfassung oder Verarbeitung gefälscht

werden, um betrügerische Vorteile zu erzielen. So wurden etwa Versicherungspolice auf fiktive Personen ausgestellt und die dafür anfallende Provision von den Tätern kassiert. Oder es wurden Renten lange nach dem Tod der Empfänger weiter auf die Konten der Betrüger überwiesen. Und selbstverständlich lassen sich auch Umsatzzahlen zinken, um damit Kreditwürdigkeit bei Banken vorzutäuschen und eine längst fällig Insolvenz hinauszuschieben.



Beispiel 1

Täuschen für den Luxus

Mit der Unterschlagung von Schecks veruntreute die Angeklagte rund 1,2 Millionen Euro zur Finanzierung eines äußerst aufwendigen Lebensstils. Sie kaufte teure Autos, Schmuck und eine luxuriöse Eigentumswohnung. Die Umsätze auf ihrer American Express Karte machten bis zu 25.000 Euro monatlich aus. Die Angestellte war als Sekretärin in die Firma eingetreten und hatte sich zur Buchhalterin hochgearbeitet mit der Befugnis, selbständig Ein- und Ausgangsrechnungen sowie die gesamte Finanzbuchhaltung in der EDV zu buchen, Zahlungen an Lieferanten und Kreditoren vorzunehmen, die Bankkonten abzustimmen sowie die Kasse zu führen.

Irgendwann entschloss sie sich, auf das Firmenkonto gezogene Schecks auf ihr eigenes Konto einzureichen, zunächst mit kleinen Beträgen, später regelmäßig mit mehr als 70.000 Euro, um ihren aufwendigen Lebensstil zu finanzieren. Die Auszahlungen verschleierte sie durch ein Vielzahl von Einzelbuchungen mit manchmal mehr als 50 Zwischenbuchungen, bei denen Beträge gesplittet und neu aggregiert mit realen Vorgängen wurden, so dass sie weder der Geschäftsleitung noch der Buchprüfung auffielen. Zumal die Täterin zur Tarnung meistens Umsatzsteuerrückzahlungen des Finanzamtes nutzte, die auf fiktiven Lieferungen beruhten. Die wurden auf einem Konto „Einfuhrumsatzsteuer“ verbucht und hatten weder Einfluss auf den Gewinn noch auf die liquiden Mittel des Unternehmens.

Erst als der Schwindel aufgefliegen war, musste die Firma eine berichtigte Umsatzsteuererklärung abgeben und das Geld an das Finanzamt zurückzahlen.

Zugriff für intelligente Täter

Mit der Entwicklung der Datenverarbeitung ist auch das Wirtschaftsstrafrecht erweitert worden. Etwa um die Fälle des betrügerischen Missbrauchs der Datenverarbeitungsanlage, die „Fälschung beweisheblicher Daten“ sowie die „Löschung solcher Daten in der Absicht der Schädigung eines anderen“. Im Strafgesetzbuch gibt es die entsprechenden Paragraphen „Computerbetrug (§ 263 a) und analog zur Urkundenfälschung die „Fälschung beweisheblicher Daten“ (§ 269).

Die Täter lassen sich grob in fünf Kategorien teilen:

- politisch motivierte Personen,
- unglückliche, verärgerte Angestellte,
- allgemeine Kriminelle,
- finanziell motivierte Personen und
- intellektuell stimulierte Menschen.

Die letzte Gruppe wird von Experten als die gefährlichste angesehen. Man kann die Täter als „Intellektuelle mit

guten Umgangsformen“ beschreiben, mit einem Plattenstapel oder einer Magnetbandspule unter dem Arm. Für Unternehmen stellen sie in der Gesamtheit eine mindestens ebenso große Gefahr dar wie Viren und Hacker.

Auch wenn die Dunkelziffer hoch ist und die Unternehmen sich häufig schwer tun, Fälle von Computerkriminalität öffentlich zu machen, landen doch immer häufiger einschlägige Straftaten vor Gericht. So der Fall einer Buchhalterin, die wegen 42-facher Scheckfälschung zu fünf Jahren Haft verurteilt wurde (Beispiel 1), eines Angestellten, der als Verantwortlicher für die Finanzbuchhaltung einschließlich Jahresabschluss im Laufe von drei Jahren knapp zwei Millionen Euro veruntreuen konnte (Beispiel 2) oder des Schadenregulierers einer Versicherung, der sein Unternehmen durch die Manipulation von Schadensdaten in 18 Fällen im Laufe von vier Jahren um rund 2,5 Millionen Euro schädigte (Beispiel 3, Seite 10).



Beispiel 2

Alles in einer Hand

Aufgrund seiner umfassenden Verantwortung für die gesamte Finanzbuchhaltung, die ihm sogar die Veränderung von Stammdaten ermöglichte, konnte der Täter in diesem Fall unbehelligt über Jahre vorgehen. Es gab weder eine effiziente Funktionstrennung noch eine regelmäßige Kontrolle durch die Geschäftsführung, es wurde unübersichtlich gebucht, eine Abstimmung mit den Banken und Kreditoren erfolgte nur jeweils zum Jahresende. So wurden über Jahre Zahlungen an Firmen getätigt, für die es weder Lieferungs- noch Leistungsnachweise gab. Der Geschäftsführung waren die Buchungen nicht bekannt, denn die Beträge wurden über mehrere Umbuchungen auf verschiedene Debitorenkonten zerstückelt und über mehrere Jahre kürzend unter den Umsatzerlösen erfasst. Das Bankkonto wies keine Auffälligkeiten auf.

Erschreckende Sicherheitslücken

Jedes größere Unternehmen muss heute damit rechnen, im Durchschnitt alle zwei Jahre einen schwerwiegenden Vorfall in der Datensicherheit zu erleben. Die Kosten bewegen sich auch in mittleren und kleineren Firmen schnell im fünfstelligen, nicht selten auch im sechsstelligen Bereich. So hat eine weitere Studie der KPMG Deutsche Treuhand-Gesellschaft ergeben, in der 2002 weltweit 600 Unternehmen mit einem Umsatz von mehr als 50 Millionen Dollar (davon 40 aus Deutschland) befragt wurden, dass die durchschnittlichen Kosten pro Vorfall 100.000 Dollar ausmachen („Globale KPMG-Studie zum Thema IT-Sicherheit“). Und das, obwohl die Firmen im Schnitt 2,6 Millionen Dollar im Jahr für die Datensicherheit ausgeben – rund zehn Prozent ihres gesamten Budgets für Informationstechnologie.

Aber die Studie liefert auch einen Beleg für das mangelnde Sicherheitsbewusstsein in den Unternehmen. So waren etwa 58 Prozent der von KPMG befragten Manager „völlig“ davon überzeugt, dass ihre Sicherheitsmaßnahmen ausreichend seien – und dennoch sagten gleichzeitig 87 Prozent, sie seien Opfer von Sicherheitslücken geworden. Tatsächlich verfügen denn auch nur 40 Prozent über ein funktionsfähiges Überwachungssystem.



Und das obwohl die Gefahren weiter zunehmen, denn rund 43 Prozent der befragten Firmen planen, ein drahtloses Firmennetz zu installieren. Und ganz erschreckende Sicherheitslücken offenbarten sich, wenn als Ergebnis der Studie herauskommt, dass 43 Prozent der Verantwortlichen nicht sagen können, wie viel sie für die Datensicherheit ausgeben und immerhin noch 30 Prozent nicht wissen, wie viel Prozent der gesamten Ausgaben für die elektronischen Datensysteme der Sicherheit dienen. Dazu passt, dass nur 60 Prozent der Unternehmen ein funktionierendes Reporting-System für Sicherheitsvorfälle haben und gerade mal ein Drittel die Sicherheits-Performance misst.

Das Messen von Sicherheitsstandards der elektronischen Datenverarbeitung erhält aber immer größere Bedeutung. Denn es ist ein Grundsatz der modernen Management-Lehre, dass nur Dinge effektiv zu managen sind, die man auch messen kann. Hier aber besteht, das zeigen alle einschlägigen Untersuchungen über die Datensicherheit in Unternehmen, ein erheblicher Nachholbedarf. Wie sollen Unternehmen wissen, dass die Kosten für die Datensicherheit angemessen sind (und nicht möglicherweise sogar zu hoch), wie sollen sie erkennen, dass sie ihr Geld gerade in diesem existenziell wichtigen Bereich sinnvoll investieren?

Fragen zur individuellen Informationsverarbeitung	Ja	Nein
Ist sichergestellt, dass nur auf Viren geprüfte Originalsoftware durch autorisiertes Personal zentral installiert wird?	<input type="checkbox"/>	<input type="checkbox"/>
Werden Datenträger generell auf Viren geprüft?	<input type="checkbox"/>	<input type="checkbox"/>
Sind die Diskettenlaufwerke der vernetzten PC verschlossen?	<input type="checkbox"/>	<input type="checkbox"/>
Ist andernfalls sichergestellt, dass keine Kopien von Daten aus dem Unternehmen gebracht werden?	<input type="checkbox"/>	<input type="checkbox"/>
Werden ausgegebene Datenträger registriert und die Verwendung kontrolliert?	<input type="checkbox"/>	<input type="checkbox"/>
Verhindert eine Sicherheitssoftware, dass Fremdprogramme ausgeführt werden?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es pro Anwender eine ausreichende Dokumentation der Anwendungen und der verwendeten Daten und wird diese kontrolliert?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es eine Risikoabschätzung für den Verlust von mobilen Geräten und Daten?	<input type="checkbox"/>	<input type="checkbox"/>
Gelten im PC-Bereich dieselben Regeln für den Zugang wie in der zentralen Informationsverarbeitung?	<input type="checkbox"/>	<input type="checkbox"/>
Sind Daten- und Programmserver in speziell gesicherten Räumen untergebracht?	<input type="checkbox"/>	<input type="checkbox"/>
Sind PCs in den Fachabteilungen gegen Diebstahl geschützt?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es eine generelle Richtlinie für den Einsatz von PCs, die von jedem Mitarbeiter verbindlich anerkannt werden muss?	<input type="checkbox"/>	<input type="checkbox"/>

Fragen zu Mitarbeitern	Ja	Nein
Werden von Bewerbern alle Zeugnisse der letzten drei Jahre verlangt und Lücken aufgeklärt?	<input type="checkbox"/>	<input type="checkbox"/>
Wird bei Bewerbern mit häufigem Stellenwechsel und ungewöhnlichen Kündigungsterminen die Ursache geklärt?	<input type="checkbox"/>	<input type="checkbox"/>
Vermindert Arbeitsplatztausch die Abhängigkeit von Spezialisten?	<input type="checkbox"/>	<input type="checkbox"/>
Werden bei höheren Positionen Konkurrenzklauseln vereinbart?	<input type="checkbox"/>	<input type="checkbox"/>
Werden Mitarbeiter schriftlich zur Geheimhaltung verpflichtet?	<input type="checkbox"/>	<input type="checkbox"/>
Werden Mitarbeiter auf das Bundesdatenschutzgesetz verpflichtet und wird dies kontrolliert?	<input type="checkbox"/>	<input type="checkbox"/>
Fällt ungewöhnliches Verhalten wie Verzicht auf Urlaub oder luxuriöser Lebensstil auf?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es regelmäßige Mitarbeitergespräche über Betriebsklima und die persönliche Situation im Unternehmen?	<input type="checkbox"/>	<input type="checkbox"/>
Ist eine hinreichende Ausbildung insbesondere der Sicherheits-Verantwortlichen gewährleistet?	<input type="checkbox"/>	<input type="checkbox"/>



Beispiel 3

Schaden mit Schäden

Als Schadenregulierer nutzte der Täter die Möglichkeiten der EDV bei der Abwicklung und fügte seiner Firma damit einen erheblichen Schaden zu. Am Bildschirm eröffnete er alte Schadenfälle erneut, füllte mit Hilfe seines Passwortes einen Scheck mit einem bestimmten Betrag als Vorauszahlung aus. Zur Freigabe der Zahlung benutzte er das Passwort eines Kollegen, das er zufällig erfahren hatte, ohne dessen Wissen.

Die freigegebenen Schecks versandte er an fiktive, nicht existente Anwaltskanzleien in Deutschland. Wenn die Briefe als unzustellbar zurückkamen, entnahm er die Schecks und löste sie auf seinem eigenen Konto ein. Insgesamt 91 Schecks, die sich zu rund 2,5 Millionen Euro summieren.

Sicherheit ist Chefsache

Die wachsende Verwundbarkeit und die Gefahr massiver wirtschaftlicher Schäden durch Risiken in der Informationstechnologie erhöhen den Handlungsdruck, durch aktives Sicherheitsmanagement Schäden zu verhindern oder zumindest zu minimieren. Doch leider wird die Aufgabe noch immer in den allermeisten Fällen allein als Aufgabe der für die Datensicherheit Verantwortlichen gesehen. Und deshalb versuchen viele Unternehmen auch, sie allein technisch durch „Firewalls“ oder „Anti-Virus-Systeme“ oder Nutzungskontrollen zu lösen. Viele Manager sind der Meinung, das Problem sei allein computertechnischer Natur, und delegieren die Aufgabe an ihre Techniker.

Selbstverständlich sind technische Schutzmaßnahmen die Grundlage jedes Sicherheitssystems. Die aber erfüllen nur die Mindestanforderungen an einen funktionierenden Schutz. Häufig genug sind die Techniker überfordert und reagieren mit Aktionismus. Denn sie durchschauen zwar das Netzwerk, kennen die Unterschiede zwischen verschiedenen Betriebssystemen, wissen aber wenig über die sensiblen geschäftlichen Daten. Sicherheitsmaßnahmen werden deshalb nur punktuell umgesetzt, selten in einem betriebswirtschaftlich fundierten Zusammenhang mit dem gesamten Geschäft.



Beispiel 4

Fehlendes Backup

Ein Mittelständler betreibt ein kleines Netz mit einem zentralen Server, der ein Bandlaufwerk enthält, auf das in regelmäßigen Abständen eine Sicherungskopie gespeichert wird. Der Administrator bewahrt die Bänder in einem verschlossenen Schrank in seinem Büro auf. Als der Server durch einen Festplattendefekt ausfällt, sollen die Daten vom Sicherungsband wieder eingespielt werden.

Doch das Bandlaufwerk war seit längerer Zeit defekt, das einzige funktionierende Band ist älter als fünf Jahre. Alle Daten sind verloren und der Administrator hatte eine weitere Gefahr übersehen: Bei einem Feuer wären selbst funktionierende Bänder vernichtet worden.

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Vom Gesetz verpflichtet

Datensicherheit steht und fällt mit dem Engagement des Managements. Die Geschäftsleitung muss sich zur Sicherheit bekennen, entsprechende Grundsätze und Richtlinien aufstellen und Unterstützung anbieten. Ein ganzheitliches System, das höchstmögliche und effektive Datensicherheit im Unternehmen gewährleistet, ist genauso Chefsache wie Absatz, Produktion oder Kostenmanagement. Schon allein deshalb, weil sich auch die gesetzlichen Anforderungen an das Management in den vergangenen Jahren erheblich verschärft haben. Es wurden mehrere Rechtsvorschriften erlassen, aus denen sich unmittelbare Handlungs- und Haftungsverpflichtungen für die Geschäftsführung oder den Vorstand eines Unternehmens ergeben. Insbesondere das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) hat als so genanntes Artikelgesetz, das andere Gesetze ergänzt und erweitert, erhebliche Verschärfungen gebracht (siehe

Wirtschaft Konkret Nr. 405 „Risiken richtig managen“).

So ist im Aktiengesetz festgelegt, dass ein Vorstand persönlich haftet, wenn er Entwicklungen, die ein Risiko für das Unternehmen sein können, nicht mit einem geeigneten Risikomanagement überwacht (§ 91, Abs. 2; § 93, Abs. 2). Und im GmbH-Gesetz wird Geschäftsführern einer GmbH „die Sorgfalt eines ordentlichen Geschäftsmannes“ auferlegt (§ 43, Abs. 1). Die im Aktiengesetz genannten Pflichten eines Vorstands gelten auch im Rahmen des Handelsgesetzbuches (§ 317, Abs. 2).

Die Formulierungen klingen zwar für den juristischen Laien allgemein und unverbindlich. Tatsächlich lassen sich daraus aber konkrete Verpflichtungen für die Gewährleistung eines angemessenen Sicherheitsniveaus bei der Informationstechnik ableiten, denn wie beschrieben können Sicherheitslücken schwerwiegende Schäden verursachen und schlimmstenfalls den Bestand des Unternehmens gefährden.

Worauf es wirklich ankommt

Doch Datensicherheit ist nicht allein aus juristischen Gründen Chefsache. Sie muss ein Teil der Unternehmenskultur werden, damit sie im Geschäftsalltag gelebt und von allen Mitarbeitern getragen wird. Das zu vermitteln, ist auch Chefsache. Denn es sollte immer klar sein: Sicherheit ist kein statischer Zustand, sondern ein ständiger Prozess.

Um ein funktionierendes, ganzheitliches Sicherheitskonzept zu entwickeln, muss jedes Unternehmen heute zunächst eine fundierte Risikoabschätzung vornehmen. Dabei hat der Begriff Sicherheit zumindest drei wichtige Facetten:

- Daten-Sicherheit bedeutet, dass nicht jeder die gespeicherten Daten einsehen oder verändern kann.
- Kommunikations-Sicherheit heißt, die Daten sind während ihrer Übertragung in Netzwerken gesichert.
- Sicherheit der Hardware gewährleistet ihren Schutz vor Diebstahl, Zerstörung, Manipulation.

Jeden dieser drei Bereiche kann man wiederum unter drei Aspekten betrachten, die auch für die Bewertung der materiellen wie immateriellen Schäden entscheidend sind: Vertraulichkeit, Unversehrtheit und Verfügbarkeit.

Vertraulichkeit: Dieses Kriterium bezieht sich auf den Schutz sensibler Unternehmensdaten. Vertraulichkeit wird gewährleistet durch Zugangs- und Zugriffskontrollen sowie die Verschlüs-

selung von Daten durch kryptographische Verfahren. Die Entscheidung, welche Verfahren eingesetzt werden, und damit über die Kosten, ist abhängig von der Einschätzung der Gefahr.

Unversehrtheit: Ein sicheres Computersystem muss die Integrität der gespeicherten Daten erhalten, sie also vor ungewollter Veränderung schützen, seien diese böswillig oder zufällig und unbeabsichtigt.

Verfügbarkeit: Ein in diesem Sinne sicheres Computersystem muss seine Daten jedem autorisierten Nutzer schnell und sicher zur Verfügung stellen.

Entscheidende Fragen dabei sind: Wie fehlertolerant soll das System sein? Was passiert nach einem Stromausfall? Steht bei einem Totalausfall nahtlos ein Ausweichsystem zur Verfügung?



Fragen zur individuellen Informationsverarbeitung	Ja	Nein
Wurden konkrete Ziele festgelegt, die mit Sicherheitsmaßnahmen erreicht werden sollen?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es Verantwortliche für Planung und Kontrolle der Sicherheitsmaßnahmen?	<input type="checkbox"/>	<input type="checkbox"/>
Werden in der Aufbau- und Ablauforganisation Sicherheitsmaßnahmen berücksichtigt?	<input type="checkbox"/>	<input type="checkbox"/>
Sind IT-Abteilung, Rechenzentrum und Fachabteilungen räumlich und organisatorisch getrennt?	<input type="checkbox"/>	<input type="checkbox"/>
Sind Systementwicklung und Rechenzentrum getrennt und wird dies überwacht?	<input type="checkbox"/>	<input type="checkbox"/>
Haben IT-Mitarbeiter fälschungssichere Ausweise und werden diese kontrolliert?	<input type="checkbox"/>	<input type="checkbox"/>
Wird über die Vergabe von Ausweisen, Schlüsseln, Passwörtern und Sicherheitscodes Buch geführt?	<input type="checkbox"/>	<input type="checkbox"/>
Ist sichergestellt, dass ausscheidende Mitarbeiter Schlüssel, Ausweise und vertrauliche Daten zurückgeben und betroffene Abteilungen informiert werden?	<input type="checkbox"/>	<input type="checkbox"/>
Können gekündigte Mitarbeiter das Rechenzentrum betreten?	<input type="checkbox"/>	<input type="checkbox"/>
Werden Sicherheitsverletzungen zentral gemeldet und Ursachen analysiert?	<input type="checkbox"/>	<input type="checkbox"/>

Beispiel 5

Ausfall des Administrators

Der Administrator eines mittelständischen Unternehmens, jahrelang allein für PCs und Netzwerk verantwortlich, fällt durch einen schweren Unfall aus. Nach wenigen Tagen häufen sich die Fehlermeldungen und Warnhinweise, immer mehr Rechner stehen still, bald geht nichts mehr. Das System ist praktisch nicht dokumentiert, selbst Administrations-Passwörter sind nicht hinterlegt. Eine herbeigerufene Firma für IT-Unterstützung hat große Mühe, installierte Anwendungen und branchenspezifische Lösungen zu rekonstruieren. Weitere Experten werden um Hilfe gebeten. Bis alles wieder hergestellt ist, vergehen Wochen. Das Unternehmen kann wichtige Aufträge nicht bearbeiten, die Schäden und die Kosten für die Dienstleister summieren sich zu Millionen. Das Unternehmen ist in seiner Existenz bedroht.

Quelle: Bundesamt für Sicherheit
in der Informationstechnik (BSI)

Wie ein Konzept entsteht

Aufgabe des Managements ist es, unter Berücksichtigung dieser drei Kriterien zu versuchen, die Auswirkung denkbarer Risiken auf das Unternehmen zu ermitteln und zu bewerten. Und schließlich zu entscheiden, welchen Wert die Kriterien jeweils in einem Sicherheitskonzept haben sollen. Dabei geht es um Fragen wie: Wie viele Aufträge würden wir verlieren, wenn jemand unsere Bestell- oder Vertragsdaten manipuliert (Unversehrtheit)? Wie groß wäre der Schaden, wenn ein Konkurrent unsere Daten in die Hand bekäme (Vertraulichkeit)? Funktionieren einzelne Geschäftsprozesse ohne Netzwerkanschluss überhaupt noch (Verfügbarkeit)? Wären wir im Falle einer unbefugten Veröffentlichung interner Daten gegenüber Vertragspartnern regresspflichtig (Vertraulichkeit)?

Auf diese Weise müssen alle Unternehmensbereiche auf sicherheitsrelevante Aspekte nach den drei Kriterien untersucht werden. Die Weitergabe von Kundendaten (Vertraulichkeit) kann das Image einer Firma ebenso schädigen wie die Nutzung einer fehlerhaften Adressdatei (Unversehrtheit) oder der Ausfall eines Servers mit wichtigen Informationen über Kunden oder Geschäftspartner (Verfügbarkeit). Unter die sicherheitstechnische Lupe gehören auch Themen wie Wettbewerbsfähigkeit, Kostenstruktur oder sogar Betriebsklima.

Computersysteme sind hochkomplexe und deshalb äußerst anfällige Systeme. Dafür zu sorgen, dass sie einwandfrei funktionieren, ist mit hohem finanziellen Aufwand verbunden. In vielen Unternehmen wird an der Wartung gespart, so dass häufig Computer ausfallen. Arbeit bleibt liegen, wird

weniger effizient ausgeführt, weil sich Mitarbeiter gegenseitig helfen, abgestürzte PCs zu reaktivieren. Fällt der Server eines Firmennetzwerkes aus, kann die Belegschaft möglicherweise tagelang nicht planmäßig arbeiten. Die Kosten tauchen in keiner Bilanz auf, sie machen sich höchstens in geringerer Produktivität bemerkbar.

Ganz zu schweigen von den Mitarbeitern, die sich falsch behandelt oder schlecht bezahlt fühlen und deshalb hin und wieder mal auf den falschen Knopf drücken. Auch die schlichte Fehlbildung von Computersystemen kostet die Wirtschaft jedes Jahr Millionen. Gerade in diesem Zusammenhang hat die Frage der Datensicherheit nichts mehr mit Computertechnik zu tun, sondern viel mit Menschenführung.



Fragen zur technischen Sicherheit des Rechenzentrums	Ja	Nein
Ist das Rechenzentrum gegen äußere Einflüsse wie Magnetfelder, Erschütterungen, Hochspannung, Radarfelder, Überschwemmungen oder Sabotage geschützt?	<input type="checkbox"/>	<input type="checkbox"/>
Werden die IT-Anlagen regelmäßig gewartet?	<input type="checkbox"/>	<input type="checkbox"/>
Ist eine Notstromversorgung gesichert?	<input type="checkbox"/>	<input type="checkbox"/>
Wird bei technischen Störungen das Management benachrichtigt?	<input type="checkbox"/>	<input type="checkbox"/>
Werden die Ursachen für Störungen und Ausfälle analysiert?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es einen detaillierten Katastrophenplan mit Verhaltensregeln und Telefonlisten?	<input type="checkbox"/>	<input type="checkbox"/>
Ist der Katastrophenplan gut zugänglich und sichtbar?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es im Katastrophenfall ein Back-up-System intern oder extern?	<input type="checkbox"/>	<input type="checkbox"/>
Wurden auf dem Ausweichsystem alle Systeme getestet?	<input type="checkbox"/>	<input type="checkbox"/>
Kann ein Notbetrieb auch ohne IT-Anlage aufrechterhalten werden?	<input type="checkbox"/>	<input type="checkbox"/>

Beispiel 6

Betriebsgeheimnisse gestohlen

Ein kleines Unternehmen stellt Lacke nach Spezialrezepturen her. Eines Tages wechselt ein Marketing-Mitarbeiter zur Konkurrenz, die ein halbes Jahr später nahezu identische Lacke auf den Markt bringt.

Die Kripo kann nachweisen, dass auf dem PC des Verdächtigen Dateien mit den fraglichen Rezepturen abgespeichert waren. Die Räume der Entwicklungsabteilung waren nachts nicht verschlossen und konnten von jedem Mitarbeiter des Unternehmens betreten werden. Nach Feierabend hatte sich der Täter mit Hilfe einer Boot-Diskette unter Umgehung des Kennwort-Schutzes Zugang zu den sensiblen Daten verschafft. Sowohl der Dieb als auch zwei Manager seines neuen Arbeitgebers wurden bestraft.

Quelle: Bundesamt für Sicherheit
in der Informationstechnik (BSI)





Risiken bei Rationalisierung

Gerade die Entwicklung und die Einführung von neuen Programmen bergen häufig unterschätzte Risiken, die durch die weltweite Verwendbarkeit in großen Unternehmen noch potenziert werden. Unkontrollierte Prozesse können zu einem regelrechten Chaos bei der Entwicklung und Anpassung von Standardsoftware führen mit nicht nur erheblichen finanziellen Risiken, sondern auch der Verzögerungen bei der Markteinführung neuer Produkte.

Eine chaotische Softwareentwicklung liefert zudem zahlreiche Möglichkeiten von Flüchtigkeitsfehlern oder Manipulationen, die mangelnde Verfügbarkeit von Produkten zur Folge haben kann, betrügerische Programmeingriffe mit erheblichen finanziellen Schäden, Rechtsrisiken bei falschen Preisangaben oder Imageschäden wegen der Zunahme von Kundenbeschwerden.

Deshalb empfiehlt es sich auch in diesen Fällen immer, ein umfassendes Risikomanagement zu installieren, das aus Risikoerkennung, Risikoanalyse, Risikoverminderung und einem Testkonzept besteht.

Ausweitung der EDV

Besondere Aufmerksamkeit bezüglich der Risiken erfordern auch Rationalisierungsprozesse mit der EDV. Zur Rationalisierung gehört ohne Zweifel auch der richtige Einsatz der EDV auf allen Stufen der Betriebsorganisation. Leider wird das Problem der Rationalisierung sehr oft nur unter dem Aspekt der Einsparung von Arbeitskraft gesehen. Die Sicherheit bleibt dabei häufig unbeachtet. Zum Glück führt das nicht immer zu so eklatanten Folgen, wie tatsächlich geschehen: Mit der Begründung, die EDV irre sich nie, wurde mit der Einführung eines neuen Systems kurzerhand die Innenrevision aufgelöst.

Die Aufrechterhaltung einer hinreichenden Sicherheit kostet natürlich Geld, was den Rationalisierungserfolg manchmal fast gänzlich wieder zunichte machen kann. Gerade kleinere Unternehmen sehen sich deshalb oft gezwungen, wichtige Sicherheitsaspekte außer Acht zu lassen. Welche kleine Firma kann es sich schon leisten, das Vier-Augen-Prinzip strikt durchzuhalten oder eine saubere Funktionstrennung zwi-

schen Programmierung und Operating zu installieren. Nicht selten werden drei Funktionen – Buchhalter, Operator, Programmierer – in einer Person vereint, das einzige Sicherheitsprinzip heißt dann „Vertrauen“.

Richtig für jedes Unternehmen

Wie schwierig und teuer es auch immer ist, für Sicherheit zu sorgen, bestimmte Schritte können auch kleine Unternehmen einhalten. So lohnt es sich immer, mit dem Hersteller des Computersystems über die Probleme zu sprechen. Viele haben Checklisten für ihre Kunden entwickelt. Außerdem beraten die Landesstellen für Betriebssicherheit ihre Mitglieder. Vieles wäre auch schon erreicht, wenn nur die Empfehlungen der Normenausschüsse der Sachversicherer beachtet und umgesetzt würden und schließlich ist sicher auch ein Gespräch mit einem Versicherer ratsam. Es bleibt immer ein Restrisiko, das durch eine Versicherung abgesichert werden kann.

Fragen zu Organisation und Software-Entwicklung	Ja	Nein
Gibt es ausreichende Richtlinien für die Entwicklung und Wartung von Systemen?	<input type="checkbox"/>	<input type="checkbox"/>
Werden Entwicklung und Operating personell getrennt?	<input type="checkbox"/>	<input type="checkbox"/>
Sind Test- und Produktionssysteme strikt getrennt?	<input type="checkbox"/>	<input type="checkbox"/>
Haben alle Systeme eine umfassende Dokumentation, also System- und Programmbeschreibung, Datendefinition, Name des Programmierers, Grund, Art und Datum jeder Änderung?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es genaue schriftliche Anweisungen über die Freigabe, auch von Systemen fremder Dienstleister?	<input type="checkbox"/>	<input type="checkbox"/>
Erfolgt die Freigabe durch die Revision, nach erfolgreichem Test und Plazet der Fachabteilung?	<input type="checkbox"/>	<input type="checkbox"/>
Wird jede Programmänderung dokumentiert und der Revision mitgeteilt, bei personenbezogenen Daten auch dem Datenschutzbeauftragten?	<input type="checkbox"/>	<input type="checkbox"/>
Bestehen genaue Vorschriften für die Aufbewahrung, Verwaltung und Nutzung von Datenträgern, die auch kontrolliert werden?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es klare Anweisungen über den Zugang zu Datenträgern und Systemen?	<input type="checkbox"/>	<input type="checkbox"/>
Werden die Datenbestände von besonderen Sachbearbeitern verwaltet?	<input type="checkbox"/>	<input type="checkbox"/>
Werden regelmäßig Sicherungskopien von Daten und Programmen erstellt und gesondert aufbewahrt?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es regelmäßig Übungen zur Wiederherstellung von Systemen und Daten mit Hilfe der Sicherungskopien?	<input type="checkbox"/>	<input type="checkbox"/>
Sind die Fachabteilungen für die Richtigkeit der Eingabedaten verantwortlich?	<input type="checkbox"/>	<input type="checkbox"/>
Werden Änderungen der Daten nur auf Anweisung der Fachabteilung durchgeführt?	<input type="checkbox"/>	<input type="checkbox"/>





Was zu tun ist

W Weil es in allen Organisationen und Betrieben nahezu die gleichen Schritte sind, die zu optimaler Sicherheit führen, wurden die wesentlichen Anforderungen in Großbritannien zu einem British Standard (BS) vereinheitlicht und zusammengefasst. Daraus entwickelten die International Organization for Standardization (ISO) und die International Electrotechnical Commission (IEC) die Norm IASO/IEC 17799. Auf knapp 70 Seiten werden dort umfassende Empfehlungen zum Aufbau eines Sicherheitssystems gegeben.

Die wichtigsten Schritte

Richtiger und effektiver Datenschutz beginnt, wie beschrieben, immer mit dem Management, das sich dazu bekennt sowie entsprechende Grundsätze aufstellen und im Unternehmen kommunizieren muss.

Der zweite Schritt zur Datensicherheit besteht darin, die vorhandenen Einrichtungen und Daten zu analysieren, zu bewerten entsprechend den zentralen Kriterien Vertraulichkeit, Unversehrtheit, Verfügbarkeit und sie einer Sicherheitsstufe zuzuordnen, aus der sich die Dringlichkeit des Schutzes ergibt.

Die danach folgenden Entscheidungen beginnen beim Personal. Sicherheit beginnt bereits bei der Einstellung, also der Auswahl neuer Mitarbeiter. Aber sie hat ihren Kern natürlich in der kontinuierlichen Schulung der Beschäftigten, sowohl was die Nutzung der Daten als auch den Umgang mit Sicherheitslücken angeht. Das beste System nützt nichts, wenn Probleme nicht bekannt werden.

Selbstverständlich gehören zu einem effizienten Schutz auch die entsprechenden Gebäude, die sowohl gegen Umwelteinflüsse als auch gegen den Zutritt unbefugter Personen geschützt sind. Ganz besonderes Augenmerk ist dabei auf das Equipment zu legen, das die Geschäftsräume verlässt, zum Beispiel Notebooks oder PCs für Heimarbeitsplätze.

Und schließlich muss der Zugriff auf Informationen klar geregelt sein, was in der Regel durch Passwörter und Benutzerrechte geschieht, die sich auf Geräte, Netzwerke, Datenlaufwerke und Applikationen beziehen. Sie setzen also eine umfassende Planung, Schulung und Überwachung voraus. Denn das beste Sicherheitssystem wird nutzlos, wenn

es durch eine unzuverlässige Anwendung unterlaufen wird.

Hilfe im Notfall

Angesichts der zunehmenden Bedeutung der Computersicherheit in den Betrieben hat die Bundesregierung das Bundesamt für Sicherheit in der Informationstechnik (BSI) personell verstärkt. Die zentrale Anlaufstelle für Fragen präventiver und reaktiver Sicherheitsmaßnahmen ist dort das Computer Emergency Response Team (CERT).

Für den Mittelstand wurde Mcert als Notfallzentrum eingerichtet. Das System bietet Empfehlungen und verlässliche Informationen, um Sicherheitslücken zu schließen. Mcert will außerdem vorbeugenden Schutz bieten, indem es auf Sicherheitslücken aufmerksam macht.

Und weil IT-Sicherheit natürlich nicht auf nationaler Ebene zu erreichen ist, wurden auch die internationalen Bemühungen verstärkt. Auf Beschluss des Europarates wurde zum Jahresbeginn 2004 eine EU-Kommission für Netzwerk- und Informationssicherheit eingerichtet.



Fragen zur zentralen Informationsverarbeitung	Ja	Nein
Wurden für die IT-Abteilung und das Rechenzentrum Sicherheitszonen festgelegt und der Zugang definiert?	<input type="checkbox"/>	<input type="checkbox"/>
Werden die Sicherheitszonen regelmäßig überprüft?	<input type="checkbox"/>	<input type="checkbox"/>
Werden die Zugänge zu Maschinen und Archivräumen permanent kontrolliert?	<input type="checkbox"/>	<input type="checkbox"/>
Wird darauf geachtet, dass ein Mitarbeiter nie allein im Maschinenraum arbeitet?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es Regeln für den Zutritt von nicht autorisiertem Personal zum Maschinenraum (Reinigung)?	<input type="checkbox"/>	<input type="checkbox"/>
Werden Terminals gegen Missbrauch geschützt?	<input type="checkbox"/>	<input type="checkbox"/>
Ist gesichert, dass Passwörter regelmäßig geändert werden?	<input type="checkbox"/>	<input type="checkbox"/>
Wird der IT-Betrieb ausreichend protokolliert und werden die Protokolle ausgewertet?	<input type="checkbox"/>	<input type="checkbox"/>
Erhält das Management unaufgefordert Kenntnis von Abweichungen und unberechtigten Zugriffen?	<input type="checkbox"/>	<input type="checkbox"/>



Die häufigsten Fehler

Typische Versäumnisse variieren nur geringfügig nach Unternehmensgröße und Branche.

Die häufigsten sind:

- Sicherheit hat einen zu geringen Stellenwert und wird nur als Kostentreiber gesehen. Besonders bei Neuananschaffungen werden die Sicherheitseigenschaften eines Systems vernachlässigt.
- Dauerhafte Prozesse zur Gewährleistung der Sicherheit fehlen, häufig werden nur Einzelprojekte verfolgt. So werden zwar Schwachstellenanalysen durchgeführt, deren Umsetzung jedoch nicht konsequent verfolgt.
- Sicherheitsvorgaben werden nicht dokumentiert. Insbesondere in mittelständischen Unternehmen ist das der Fall. Viele Richtlinien lassen zudem zuviel Interpretationsspielraum oder haben keinen vertraglich verbindlichen Charakter für die Mitarbeiter.
- Kontrolle und Aufklärung fehlen bei Verstößen. Sicherheitsrichtlinien sind nur wirksam, wenn ihre Einhaltung kontrolliert und ein Verstoß geahndet wird. Fehlt beides, werden Vorgaben zunehmend missachtet.
- Nutzungsrechte werden zu großzügig vergeben. Jeder Benutzer sollte nur auf die Datenbestände zugreifen können, die er auch wirklich für seine Arbeit braucht (Need-to-know-Prinzip).
- Die IT-Systeme sind schlecht konfiguriert. Würden die in Standardsoftware vorhandenen Sicherheitsfunktionen richtig und vollständig genutzt, wäre das Sicherheitsniveau in Unternehmen höher.
- Sensitive Systeme sind gegen offene Netze unzureichend abgeschottet. Die sichere Anbindung bestehender Applikationen an das Internet erfordert von den Administratoren spezielle Kenntnisse.
- Mangelhafte Schulung der Nutzer. Schulungen decken oft nicht die spezifischen Bedürfnisse der Nutzer ab, zudem sind Seminare teuer, teilnehmende Mitarbeiter fallen als Arbeitskräfte aus.
- Sorgloser Umgang mit Passwörtern. Das Aufbewahren des Passwortes unter der Tastatur oder in der obersten Schreibtischschublade macht es Tätern leicht. So finden täglich Einbrüche in IT-Systeme statt.
- Räume und Systeme werden nur unzureichend geschützt. Gekippte Fenster über Nacht, unverschlossene IT-Räume, unbeaufsichtigte Besucher oder im Auto gelassene Notebooks bieten ungebetenen Gästen reichlich Möglichkeiten.

Quelle: Leitfaden IT-Sicherheit, Bundesamt für Sicherheit in der Informationstechnik (BIS)

Glossar der IT-Sicherheit

Authentisierung:

Bei der Anmeldung in einem System wird die Identität der Person geprüft und verifiziert. Der Begriff wird auch verwendet, wenn die Identität von IT-Komponenten oder Anwendungen geprüft wird.

Autorisierung:

Bei einer Autorisierung wird geprüft, ob eine Person, IT-Komponente oder Anwendung berechtigt ist.

Datenschutz:

Darunter versteht man den Schutz personenbezogener Daten vor dem Missbrauch durch Dritte.

Datensicherheit:

Der Begriff bezeichnet den Schutz von Daten bezüglich Vertraulichkeit, Verfügbarkeit und Unversehrtheit. Ein synonyme Begriff ist IT-Sicherheit.

Datensicherung (Backup):

Bei einer Datensicherung werden Kopien zum Schutz vor Verlust hergestellt.

Penetrationstest:

Ein gezielter, simulierter Angriffsversuch auf ein IT-System zur Prüfung der Sicherheit.

Risikoanalyse (Risk Assessment):

Dabei wird untersucht, wie wahrscheinlich das Eintreten eines bestimmten Schadens ist und welche Folgen er hätte.

Sicherheitsrichtlinie (Security Policy):

Darin werden die zentralen Schutzziele und Maßnahmen formuliert. Detaillierte Maßnahmen sind in einem Sicherheitskonzept enthalten.



Bei weiteren Fragen hilft Ihnen gern der Autor:

Dr. Jan-Lubomir Heidinger
Euler Hermes Kreditversicherungs-AG
Tel.: +49 (0) 40/88 34-50 32
Fax: +49 (0) 40/88 34-50 50
E-Mail: jan-lubomir.heidinger
@eulerhermes.com



Weiterführende Links*

www.bsi.bund.de

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

www.sicherheit-im-internet.de

Informationen der Bundesregierung
zu Fragen der IT-Sicherheit

www.cert.org

Informationen bei Sicherheits-
problemen von Soft- und Hardware

www.mcert.de

Spezielle Hilfe für den Mittelstand

www.bsi-global.com

www.iso.org

www.isaca.org

www.isfsecuritystandard.com

Informationen über den British
Standard und internationale Normen

www.bfd.bund.de

www.datenschutz.de

Datenschutz

* Für den Inhalt der Seiten ist die
Euler Hermes Kreditversicherungs-AG
nicht verantwortlich.

Anhang

In der Reihe „Wirtschaft Konkret“ sind außerdem erschienen:

Schutz vor Forderungsausfall

Nr. 100	Liefern unter Vorbehalt – Wie Unternehmen ihre Eigentumsrechte durchsetzen können
Nr. 103*	Vertrauen durch Transparenz – Internationale Standards der Rechnungslegung
Nr. 104*	Im sicheren Hafen – Die richtige Finanzierung für hohe Risiken im Auslandsgeschäft
Nr. 105	Auf der sicheren Seite – Der richtige Schutz vor Forderungsausfall und seinen Folgen

Avale

Nr. 201	Sicherheiten im Baugeschäft – Wie sich Auftraggeber gegen Ausfälle und Mängel schützen
----------------	--

Schutz vor Veruntreuung

Nr. 302	Gewappnet für den Ernstfall – Rechtzeitige Vorsorge ist ein guter Schutz gegen Vertrauensschäden
----------------	--

Allgemeine Themen

Nr. 401	Zensuren für die Firma – Rating setzt sich auch in Deutschland durch
Nr. 404*	Erfolgreich neue Märkte erobern – Worauf es bei der Expansion ins Ausland wirklich ankommt
Nr. 412*	Wissen richtig managen – Das Know-how der Mitarbeiter ist das Kapital für künftigen Erfolg
Nr. 414	Ursachen von Insolvenzen – Gründe für Unternehmensinsolvenzen aus der Sicht von Insolvenzverwaltern
Nr. 416	Fair Trade und Umwelt – Handel(n) ohne Grenzen
Nr. 417	Die Zukunft Deutschlands – Bildung und Demografie im Wandel
Nr. 418	Rettung aus der Insolvenz – Chancen, Barrieren und die besondere Rolle von Private Equity

* Nur im Internet abrufbar.

Diese Broschüren liegen als Druckstücke nur unter Vorbehalt vor. Zu beziehen über Euler Hermes Kreditversicherungs-AG, Hamburg. Alle Ausgaben sind auch im Internet verfügbar unter www.wirtschaft-konkret.de

Euler Hermes
Kreditversicherungs-AG
Friedensallee 254
22746 Hamburg
Tel. + 49 (0) 40/88 34-0
Fax + 49 (0) 40/88 34-77 44
info.de@eulerhermes.com
www.eulerhermes.de

Sie finden uns ganz in Ihrer Nähe

Hauptverwaltung

22763 Hamburg
Friedensallee 254
Postanschrift
22746 Hamburg
Tel. +49 (0) 40/88 34-0
Fax +49 (0) 40/88 34-77 44
info.de@eulerhermes.com

Niederlassungen und Geschäftsstellen

12435 Berlin
An den Treptowers 1
Tel. +49 (0) 30/20 28 43-00
Fax +49 (0) 30/20 28 43-01
nl.berlin@eulerhermes.com

33602 Bielefeld
Zimmerstraße 8
Tel. +49 (0) 5 21/9 64 56-0
Fax +49 (0) 5 21/9 64 56-50
gs.bielefeld@eulerhermes.com

28195 Bremen
Martinistraße 34
Tel. +49 (0) 4 21/1 65 97-0
Fax +49 (0) 4 21/1 65 97-49
gs.bremen@eulerhermes.com

44137 Dortmund
Westfalen-Center
Lindemannstraße 79
Tel. +49 (0) 2 31/1 82 99-0
Fax +49 (0) 2 31/1 82 99-99
gs.dortmund@eulerhermes.com

01129 Dresden
Rieser Straße 5
Tel. +49 (0) 3 51/8 53 77-0
Fax +49 (0) 3 51/8 53 77-10
gs.dresden@eulerhermes.com

40472 Düsseldorf
Kanzlerstraße 4
Tel. +49 (0) 2 11/9 65 76-0
Fax +49 (0) 2 11/9 65 76-99
gs.duesseldorf@eulerhermes.com

60311 Frankfurt
Große Gallusstraße 1–7
Tel. +49 (0) 69/13 48-0
Fax +49 (0) 69/13 48-1 70
nl.frankfurt@eulerhermes.com

79100 Freiburg
Rehlingstraße 6e
Tel. +49 (0) 7 61/4 00 79-0
Fax +49 (0) 7 61/4 00 79-50
gs.freiburg@eulerhermes.com

20251 Hamburg
Straßenbahnring 11
Tel. +49 (0) 40/2 36 36-0
Fax +49 (0) 40/2 36 36-1 66
nl.hamburg@eulerhermes.com

30159 Hannover
Georgstraße 36
Tel. +49 (0) 5 11/3 64 01-0
Fax +49 (0) 5 11/3 64 01-70
nl.hannover@eulerhermes.com

50672 Köln
Hohenzollernring 31–35
Tel. +49 (0) 2 21/9 20 60-0
Fax +49 (0) 2 21/9 20 60-1 59
nl.koeln@eulerhermes.com

04157 Leipzig
Landsberger Straße 23
Tel. +49 (0) 3 41/9 08 23-0
Fax +49 (0) 3 41/9 08 23-10
gs.leipzig@eulerhermes.com

68259 Mannheim
Hauptstraße 161
Tel. +49 (0) 6 21/1 29 05-0
Fax +49 (0) 6 21/1 29 05-99
gs.mannheim@eulerhermes.com

80339 München
Ridlerstraße 35
Tel. +49 (0) 89/5 43 09-0
Fax +49 (0) 89/5 43 09-1 66
nl.muenchen@eulerhermes.com

90429 Nürnberg
Spittlertorgaben 3
Tel. +49 (0) 9 11/2 44 05-0
Fax +49 (0) 9 11/2 44 05-30
gs.nuernberg@eulerhermes.com

66111 Saarbrücken
Bahnhofstraße 80
Tel. +49 (0) 6 81/3 89 96-0
Fax +49 (0) 6 81/3 89 96-99
gs.mannheim@eulerhermes.com

70597 Stuttgart
Löffelstraße 44
Tel. +49 (0) 7 11/9 00 49-0
Fax +49 (0) 7 11/9 00 49-70
nl.stuttgart@eulerhermes.com

Exportkreditgarantien des Bundes Büro Berlin

10117 Berlin
Friedrichstadt-Passagen
Quartier 205
Friedrichstraße 69
Tel. +49 (0) 30/20 94-53 10
Fax +49 (0) 30/20 94-53 30
aga-berlin@eulerhermes.com