KARIN SCHULER

Klassengesellschaft – Gefährdungsbetrachtung bei mobilen Geräten

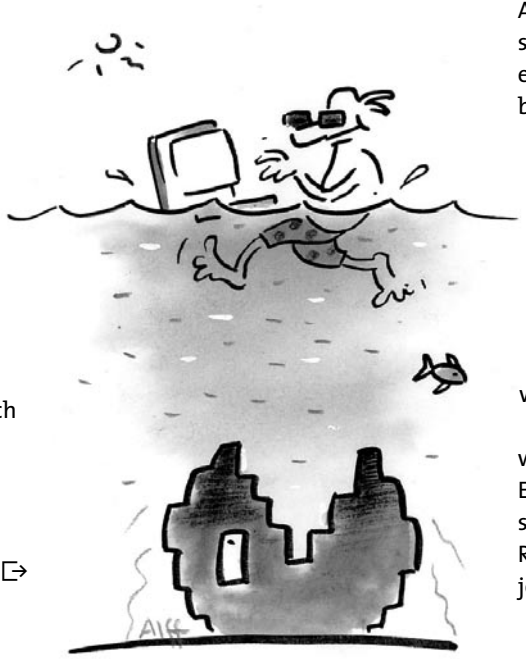
Mobile Informations- und Kommunikationstechnik bedeutet immer auch mehr Unsicherheit im Hinblick auf Datenschutz und Datensicherheit. ›Notebooks‹, aber vor allem auch ›Smartphones‹, Kleinstcomputer und ihre zahlreichen Verwandten, gehen schneller verloren und geraten eher in die Gefahr eines unbefugten Zugriffs. Es gilt deshalb, die möglichen Gefährdungen exakt zu erfassen und ein spezielles Datenschutz-/Datensicherheitskonzept zu entwickeln.

In Unternehmen werden heute neben Laptops und Notebooks zunehmend auch andere mobile Geräte der Informations- und Kommunikationstechnik (IKT) eingesetzt. Der Markt lockt mit ständig neuen Entwicklungen, die das Interesse und die Neugier auch der Beschäftigten wecken. Besonders an der Technik Interessierte fordern sogar den Einsatz immer kleinerer Geräte von ihrer IKT-Abteilung – meist bevor diese sich überhaupt mit der neuen Technologie hat beschäftigen können.

Bedarf wird jedoch nicht nur von ›Technikfreaks‹ angemeldet. Auch Fachabteilungen entdecken mehr und mehr, welche Einsparungen und welchen Komfort die mobile Technik bieten kann. Das reicht vom ...

- Vorstand des Unternehmens, der auch im Urlaub seine E-Mails mit einem ›Blackberry‹ abrufen will,
- dem Versicherungsvertreter im Außendienst, der dem Kunden gleich am mobilen PC die neue Police ausdrucken kann, über
- Schadenbegutachter, die über ›Smartphone‹ die Vor-Ort-Ergebnisse an den Unternehmens-Server übermitteln sollen, bis hin zu
- Reparaturtrupps eines Energieversorgers, die sich mit Hilfe von Kleinstcomputern (PDA) über GPS zu defekten Verteilerstellen navigieren lassen und deren Betriebsdaten dann vor Ort aus dem Unternehmensnetz abrufen können.

Aber nicht nur mobile Kleinstcomputer, sondern auch mobile Speichermedien wie USB-Sticks, USB-Festplatten oder verschiedenste Speicherkarten spielen wegen ihrer geringen Größe bei gleichzeitig hohen Speicherkapazitäten eine zunehmend wichtige Rolle (siehe Abbildung auf Seite 38).

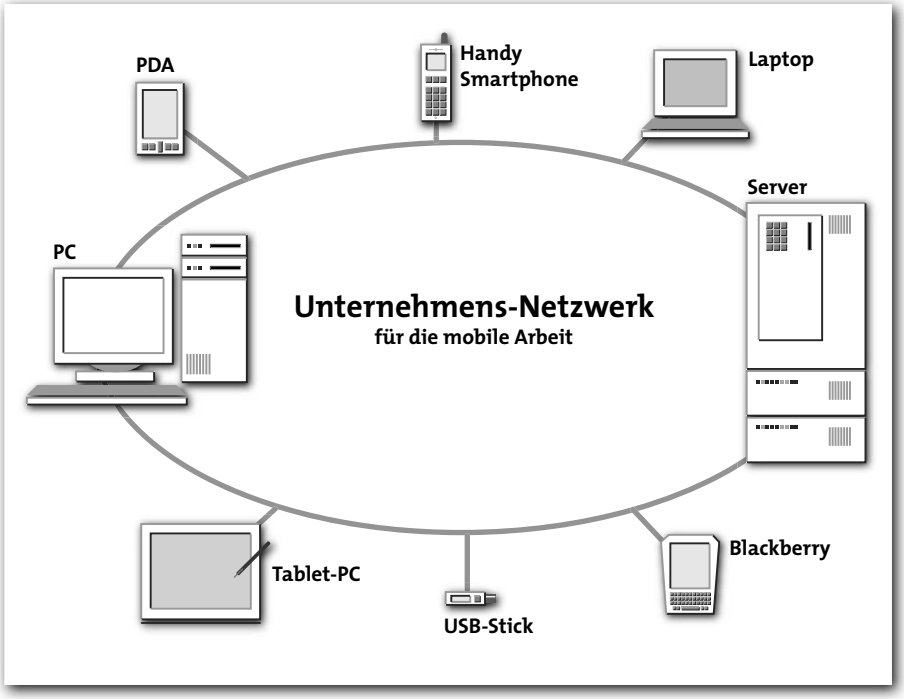


Gleichzeitig gelingt es jedoch nur wenigen Unternehmen, die Welle der Begeisterung, Innovationsfreude, Neugier und Ungeduld von vornherein in geordnete Bahnen zu lenken. Die nötigen Prüfungen durch die IKT-Abteilung (Passt das Gerät in unser Unternehmensnetz? Welche Kosten/Nutzen-Relation ist zu erwarten? Welche Gefährdungen müssen vermieden werden?) verschlingen in den Augen der Möchtegernbenutzer nicht selten viel zu viel Zeit: »Bis die sich mal entschieden haben, habe ich das Gerät bei Aldi um die Ecke schon dreimal selbst gekauft!«

Dabei macht man sich allerdings nicht bewusst, dass der Einsatz im Unternehmensnetz andere Gefährdungen mit sich bringt als im privaten Bereich. Schutzmaßnahmen sind daher unverzichtbar und müssen sinnvoll ausgewählt und umgesetzt werden – und das braucht eben Zeit.

Den häufig zu beobachtenden Wildwuchs bei der Beschaffung und beim Einsatz mobiler Geräte kann und sollte sich ein auf die Sicherheit seiner IKT-Ressourcen bedachtes Unternehmen jedenfalls nicht leisten. Sowohl der

›private‹ Einkauf nicht freigegebener Geräte als auch der eigenmächtige Netzanschluss durch einzelne Benutzer oder Fachabteilungen wäre – wenn dies denn zulässig wäre – eine ernste Gefährdung für die Sicherheit der gesamten Informations- und Kommunikationstechnik des Unternehmens. Denn der Zustand,



den man in solchen Umgebungen nach einiger Zeit des ungelenkten Einsatzes mobiler Geräte und Medien vorfindet, ist aus Sicherheitssicht nicht selten der GAU (größter anzunehmende Unfall).

Was ist anders an mobilen Geräten?

Mobile Geräte werden gerade dann eingesetzt, wenn Daten und Anwendungen auch außerhalb der Firmengrenzen verfügbar sein müssen. Alleine die vielfältigen Einsatzorte – Hotelzimmer, Flugzeug, Seminarveranstaltungen usw. – bringen vielfältige Verlustmöglichkeiten mit sich. Auch greifen die innerhalb des Unternehmens verfügbaren Schutzmaßnahmen ›draußen‹ oft nicht und für Unberechtigte ist in einer ›ungeregelten‹ Umgebung der Zugriff auf IKT-Geräte natürlich viel leichter möglich.

Außerdem ist zu beobachten, dass immer mehr Funktionen auf ein und demselben mobilen Gerät vereinigt werden. So werden beispielsweise mobile Kleinstcomputer (PDA) auch für die Vor-Ort-Nutzung von Text- oder Tabellendateien (›Office‹-Dateien) verwendet und Smartphones speichern neben den Telefondaten auch Terminkalender und Adressdaten und ermöglichen das ›Surfen‹ im Internet. Solch eine Bündelung von Funktionen aber geht immer mit einer komplexeren Gefährdungslage einher.

Auch der Einsatz mobiler Speichermedien ist im Vergleich etwa zu früher üblichen Disketten oder zur CD-ROM > mit besonderen Gefährdungen verbunden. Und zwar vor allem, weil diese Medien extrem klein sind und dennoch enorme Mengen ungeschützter Daten aufnehmen können. So kommt es durchaus vor, dass PC-Benutzer ständig eine komplette Kopie ihrer PC-Festplatte auf einem USB-Stick mit sich herumtragen.

Zusätzlich lauern weitere Gefahren: So ist zum Beispiel die USB-Schnittstelle vieler Arbeitsplatzcomputer weitgehend ungeschützt und kann daher von jedem, der Zugang dazu findet, mit beliebigen, theoretisch auch unternehmensfremden USB-Geräten verwendet werden. Eine dadurch verursachte unkontrollierte Öffnung des Unternehmensnetzwerks stellt eine erhebliche Sicherheitslücke dar. Dabei ist die vollständige Sperrung der USB-Schnittstelle wegen sinnvoller und notwendiger Nutzungsmöglichkeiten häufig keine Lösung. Und eine gezielte, bestimmten Berechtigungen unterworfene Sperrung der Schnittstelle wäre technisch und administrativ ungemein aufwändig und kaum sinnvoll umzusetzen.

Nur wer die Gefahren kennt ...

Um den Gefährdungen aus dem Betrieb mobiler Geräte und Speichermedien etwas entgegenzusetzen, müssen wirksame und angemessene Schutzmaßnahmen getroffen werden. Dazu ist es unerlässlich, sich zunächst über die Art der Gefährdungen Klarheit zu verschaffen. Eine klassische Herangehensweise stellt die sogenannte Risikoanalyse dar, die allerdings einen relativ hohen Aufwand bedeutet. Stattdessen stützen sich viele Unternehmen heute auf die im ›Grundschutzhandbuch‹ des Bundesamts für die Sicherheit in der Informationstechnik (BSI) empfohlene Herangehensweise (siehe: ›Datenschutzkonzept – was hilft und was hilft nicht?‹ in cf 9/03 ab Seite 26) oder benutzen sie zumindest als Grundlage für die Entwicklung eigener Schutzmaßnahmen.

Das Grundschutzhandbuch (GSHB) lässt sich anwenden für den sogenannten mittleren Schutzbedarf, also für Unternehmensbereiche, in denen keine Hochsicherheitsanforderungen (wie z.B. in Kraftwerken oder Hochsicherheitstrakten von Banken) gestellt werden müssen und es bietet für konkrete Situationen Standard-Maßnahmen an. Es gibt aber auch andere Hilfen bei der systematischen Entwicklung von Schutzmaßnahmen (z.B. BS7799 oder ITIL).

Aber welches Vorgehen – standardisiert oder nicht – auch immer gewählt wird: Man sollte sich zunächst einen Überblick über die im Unternehmen eingesetzten mobilen Geräte verschaffen und diese systematisch erfassen. Anschließend gilt es, die Gefährdungen für jedes dieser Geräte (mobile Speicher-

medien eingeschlossen) zu beschreiben. Hierfür ist es sinnvoll, eine Klassifizierung möglicher Gefährdungen vorzunehmen, um annähernde Vollständigkeit zu erzielen.

Mögliche Gefährdungsklassen

Aus der Beschreibung konkreter Gefährdungen lassen sich die wesentlichen Gefährdungsklassen für das einzelne mobile Gerät ableiten:

- Der Verlust der Hardware (durch Diebstahl oder Nachlässigkeit des Besitzers) ist um so wahrscheinlicher, je kleiner ein Gerät ist und je häufiger es außerhalb der Unternehmensgrenzen eingesetzt wird. Daher sind Handys und Kleinstcomputer (PDA) gefährdeter als Laptops, ein USB-Stick ist gefährdeter als ein PDA. Andererseits sind die stärker gefährdeten Geräte in der Regel die preiswerteren. Bei der Definition von Schutzmaßnahmen ist daher auch zu bewerten, wie schwer der finanzielle Verlust des jeweiligen Geräts wiegt.
- Geht ein Gerät verloren, so ist damit immer auch der Verlust der darauf vorhandenen Daten verbunden. Der Umfang dieser Daten kann erheblich sein: Selbst USB-Sticks und Speicherkarten verfügen heute mit bis zu einem Gigabyte ⊏→ über Kapazitäten, die lange Zeit nur Festplatten vorbehalten waren. Und inhaltlich reichen die auf mobilen Trägern festgehaltenen Daten von Telefonlisten über Adressbücher bis hin zu vollständigen Festplattensicherungen. Schutzmaßnahmen müssen in erster Linie darauf abzielen, zumindest die Wiederherstellung der verlorenen Daten vollständig zu ermöglichen (z.B. durch vorhandene Datensicherungen).
- Besonders bedrohlich ist die mit Verlust von Gerät und Daten verbundene Gefahr der Einsichtnahme durch Unberechtigte. Sind die Daten nicht (wie beispielsweise auf Laptops möglich) durch eine Verschlüsselungs-Software geschützt, so kann der Dieb oder Finder alle auf dem Gerät abgelegten Daten einsehen und missbrauchen. Je nach Art der Daten kann ein solcher Missbrauch (z.B. im Falle vertraulicher Unternehmenskorrespondenz auf dem PDA) einem Unternehmen immensen Schaden zufügen. Maßnahmen müssen sich am marktüblichen verfügbaren technischen Schutz orientieren, aber auch sinnvolle organisatorische Maßnahmen (z.B. Verschlussvorschriften für die Benutzer) einschließen.
- Durch abhanden gekommene, ungeschützte Daten entsteht im Fall personenbezogener Daten ein Verstoß gegen Datenschutzgesetze. Dies ist bereits so beim Telefonbuch, das auf einem nicht durch eine ›Persönliche Identifikations-Nummer‹ (PIN) gesicherten Handy gespeichert ist, aber auch beim Adressbuch auf einem ungeschützten PDA oder den Gehaltslisten, die sich auf der Festplattensicherung auf einem USB-Stick befinden. Auch Fotosammlungen auf einer ›Compact-Flash‹-Karte sind personenbezogene Daten. Ein eventueller Datenschutzverstoß kann sowohl durch Betroffene (Beschäftigte, Kunden usw.) wie auch durch die Aufsichtsbehörde verfolgt werden und unter Umständen – je nach Bedeutung und Schwere – Geldbußen nach sich ziehen. Viel nachteiliger für ein Unternehmen dürfte aber der ideelle Schaden sein, den die eventuelle Veröffentlichung sensibler Unternehmensdaten durch einen Dieb, Finder oder die durch sie informierten Medien bedeuten würde. Maßnahmen, die eine unberechtigte Einsichtnahme verhindern, sind auch gegen diese Gefährdung wirksam.
- Sinn und Zweck mobiler Geräte liegt eben gerade darin, dass sie an wechselnden Orten genutzt werden können und nicht statisch in der geschützten, standardisierten Umgebung des Firmennetzwerks betrieben werden. Daraus ergibt sich ein erhöhtes Risiko, sogenannte Malware (schädliche Software wie z.B. Viren) einzuschleusen oder weiterzuverbreiten. Mobile Geräte können selbst Opfer von Schadaktionen werden und sind in der Lage, schadprogrammverseuchte Dateien weiterzuverbreiten. Maßnahmen müssen sich an der technischen Verfügbarkeit von Schutzprogrammen orientieren und für reine Speichermedien müssen organisatorische Wege definiert werden, um die Übertragung von Dateien möglichst sicher zu gestalten.
- Die Nutzung mobiler Geräte kann auch eine Gefährdung der Sicherheit anderer IKT-Systeme im Unternehmen mit sich bringen. Die Schwächung der Netzsicherheit durch die offene USB-Schnittstelle etwa stellt eine solche Gefährdung dar. Schutzmaßnahmen müssen auf die jeweils möglichen Kombinationen abgestimmt werden. Ein uneinheitlicher Beschaffungsweg für mobile Geräte und Medien stellt ebenfalls eine Gefährdung dar, weil dadurch unter anderem die Durchsetzung einheitlicher Sicherheitsstandards erschwert, wenn nicht sogar teilweise unmöglich gemacht wird. Auch die damit verbundene Vielfalt von Produkten und Hardware-/Softwareausstattungen führt regelmäßig zu einem Wildwuchs, der wegen seiner Unübersichtlichkeit allen geordneten Sicherheitsmaßnahmen zuwider läuft. Maßnahmen betreffen hier besonders die Verankerung sicherer Beschaffungsprozesse.

Anhand dieser Gefährdungsklassen kann nun die Einschätzung konkreter Gefährdungen für jedes eingesetzte mobile Gerät oder Speichermedium systematisch vorgenommen werden. Daran anschließend ist festzuhalten, welche Schutzmaßnahmen schon ergriffen wurden und welche der notierten Gefährdungen dadurch bereits minimiert sind. In einem dritten Schritt sollten dann Bedeutung und Eintrittswahrscheinlichkeit für die Gefährdungen abgeschätzt werden, die bisher nicht oder nur unzureichend durch Schutzmaßnahmen verringert werden.

Für alle nicht tolerierbaren Gefährdungen müssen im vierten Schritt schließlich konkrete Maßnahmen diskutiert und empfohlen werden, die technischer oder organisatorischer Natur sein können. Insoweit erstrecken sich die diversen Handlungsmöglichkeiten vom Freigeben einer Nutzung (Tolerieren eines Risikos) über die Definition von

info

Beispiele für

Gefährdungsklassen von USB-Sticks und Laptops

Die verschiedenen Gefährdungsklassen werden jeweils ›durchdekliniert‹, um dabei zunächst festzustellen, welche technischen oder organisatorischen Schutzmaßnahmen bereits ergriffen wurden oder angewandt werden (im angenommenen Fall sind bisher keine Maßnahmen ergriffen worden, so dass diese Spalte hier leer bleibt).

Gerät/ Medium	*Gefährdung*	*vorhandene Maßnahmen*	*Relevanz*	*Eintrittswahrscheinlichkeit*	*Handlungsbedarf?*	*zu ergreifende Maßnahmen*
USB-Sticks	Verlust des Mediums		gering	hoch	ja	• Empfehlungen zur sicheren Aufbewahrung (nicht am Halsband, nicht in der Manteltasche, festes Behältnis usw.) in Merkblatt aufnehmen • Richtlinien zum Umgang mit mobilen Medien erlassen
	Verlust der Daten		gering (meist keine Originaldaten)	hoch	ja	• Empfehlungen zum sicheren Speichern (nur Kopien, keine Originaldaten) • Richtlinien zum Umgang mit mobilen Medien entsprechend ergänzen
	unbefugte Einsichtnahme/ Datenschutzverstoß		hoch	hoch	ja	• nur Sticks mit Passwortschutz einsetzen • nur offiziell beschaffte Sticks einsetzen (keine privaten) • Verbot der Speicherung privater Daten auf Unternehmensgeräten und -medien • Vorgabe, dass bei Nutzung als Backup-Medium (z.B. für große Teile der Festplatte) keine Nutzung ›außer Haus‹
	Malware		mittel	hoch (externe Benutzung)	ja	• Virenscanner-Standard so einstellen, dass externe Laufwerke bei Anschluss/bei Zugriff gescannt werden.
Laptops	Verlust des Geräts		hoch	mittel	ja	• zentrale Beschaffung • zentrales Kataster • Gerätecodierung • Verschluss- und Aufsichtspflicht durch Benutzer • Merkblatt für Benutzer
	Verlust der Daten		hoch	mittel	nein	• Standard-Sicherungsverfahren für Laptops
	unbefugte Einsichnahme/ Datenschutzverstoß		hoch	mittel	nein	• Standard-Konfiguration mit Festplattenverschlüsselung • Standard-Konfiguration durch Nutzer nicht änderbar • nur zentral beschaffte Geräte zulässig • Verbot der Speicherung privater Daten auf dienstlichen Geräten
	Malware		hoch	hoch	nein	• Standardeinrichtung und -update des Virenscanners
	Gefährdung anderer Systeme		hoch	gering	ja	• Verbot, andere als Unternehmensgeräte ins Netz zu nehmen • ungenehmigten Zugang zu Netzwerkanschlüssen, auch in abgelegenen Räumen (z.B. in Besprechungsräumen) verhindern
	Beschaffungsweg		gering	gering	nein	• zentrale Beschaffungsrichtlinie für mobile Geräte und Medien

Schutzmaßnahmen bis hin zum Verbot einer Nutzung.

Die bei der vollständigen systematischen Abarbeitung der vorgeschlagenen Schritte entstehende Tabelle ist die Grundlage für die Definition und Umsetzung aller notwendigen Schutzmaßnahmen (siehe info-Kasten links).

Wichtig sind dabei vor allem die Einschätzung der Bedeutung eines möglichen Schadensfalles (»Wie schlimm ist es, wenn der Schadenfall tatsächlich eintritt?«) und die Einschätzung der Eintrittswahrscheinlichkeit (»Kommt so etwas häufig oder selten vor?«). Dabei kann es durchaus so sein, dass ein Schadenfall als sehr unwahrscheinlich eingestuft wird, bei seinem Eintreten aber das ganze Unternehmen in den Ruin stürzen würde – Beispiel: Ein Besucher dringt mit Hilfe seines Laptops ins Unternehmensnetzwerk ein und löscht alle Kundendaten. Denkbar ist aber auch, dass bestimmten Gefährdungen eine hohe Eintrittswahrscheinlichkeit zugeordnet, der entstehende Schaden aber als gering beurteilt wird – Beispiel: Ein Laptop hat keinen Spam-Filter, so dass ständig 50 Prozent der eingehenden Mails nach dem Empfang händisch zu löschen sind.

Wie auch immer: Aus der Kombination der beiden Werte Bedeutung und Eintrittswahrscheinlichkeit ergeben sich Anhaltspunkte für die Einschätzung des Handlungsbedarfs. Soll ein bestimmtes Risiko, das in einer bestimmten zu erwartenden Häufigkeit auftritt, toleriert werden oder nicht? Soll/muss das Risiko durch das Ergreifen von Maßnahmen reduziert werden? Oder muss es vollständig eliminiert werden, auch wenn dies sehr teure Maßnahmen erfordert? Dies sind Fragen, die im Rahmen der Erstellung einer Gefährdungsübersicht zu beantworten sind.

An den beiden Beispielen im info-Kasten (links) soll auch deutlich werden, dass die Gefährdungseinschätzung stark von den unternehmensspezifischen Voraussetzungen wie der IKT-Infrastruktur, der Unternehmenskultur, der Branche, dem Ausbildungsstand und vielem mehr abhängt. Ob man beispielsweise die Gefährdung durch nicht zentral beschaffte Laptops tatsächlich für gering halten sollte, hängt unter anderem davon ab, ob es technisch überhaupt möglich ist, privat beschaffte Geräte ins Unternehmensnetzwerk ›einzuklinken‹. Man muss also bei der Erstellung einer Gefährdungstabelle möglichst viele Gefährdungszusammenhänge beachten.

Wer ist für was zuständig?

Dies führt unmittelbar zu der Frage, wer diese Arbeit eigentlich leisten soll und damit zur Frage der Sicherheitsorganisation des Unternehmens. Auch wenn die Antwort hierauf nicht zum Thema dieses Beitrags gehört, so lassen sich doch einige mögliche Akteure benennen:

Gibt es im Unternehmen einen IKT-Sicherheitsbeauftragten oder gar ein Gremium, das sich mit Gefährdungsfragen der IKT und der Festlegung zu ergreifender Schutzmaßnahmen befasst, so liegt es auch in seiner Zuständigkeit, die Sicherheit mobiler Geräte und Medien zu verbessern. Auch ist in diesem die Zusammenarbeit zwischen IKT-Abteilung, Betriebsrat und betrieblichem Datenschutzbeauftragtem vermutlich bereits organisiert. Eine eventuelle Aufgabenteilung (Gefährdungsbeurteilung, Festlegung von Maßnahmen, Genehmigung von Maßnahmen, Erlass von Richtlinien, Erstellung von Handlungshilfen, Umsetzung von Standards usw.) sollte sich in den betrieblichen Prozessen widerspiegeln.

Komplizierter wird es, wenn die Zuständigkeit für die IKT-Sicherheit nicht eindeutig vergeben ist und alle Beteiligten das Thema ohne organisierte Zusammenarbeit jeweils nur aus ihrer Sicht bearbeiten. Dies führt erfahrungsgemäß früher oder später zu einander widersprechenden Richtlinien aus verschiedenen Fachabteilungen, zu ineffizienten Schutzmaßnahmen, zu nicht mitbestimmten aber mitbestimmungspflichtigen IKT-Anwendungen, zu nicht abgewogenen Konflikten von Datenschutz- und IKT-Sicherheitsanforderungen und nicht zuletzt zu frustrierten IKT-Benutzern.

Es empfiehlt sich daher immer, vor der Durchführung von Gefährdungsanalysen und der Durchsetzung von Schutzmaßnahmen die innerbetriebliche Richtlinienkompetenz für Sicherheitsfragen eindeutig festzulegen und eine tragfähige Sicherheitsorganisation zu etablieren.

Karin Schuler ist freiberufliche Beraterin für Datenschutz und IKT-Sicherheit, stellvertretende Vorsitzende der Deutschen Vereinigung für Datenschutz e.V. und vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannte Sachverständige für IKT-Produkte (rechtlich/technisch); sie berät Betriebs- und Personalräte, betriebliche Datenschutzbeauftragte und IKT-Sicherheitsbeauftragte; Kontakt: fon 0228-2420733, **service@schuler-ds.de**, **www.schuler-ds.de**

[→ Blackberry [→ Seite 6]

[→ Gigabyte = Maßeinheit für Speicherkapazität (1 Buchstabe/Ziffer = 1 Byte = 8 Bit [→ Seite 17]); Kilobyte = ca. 1000 Byte, Megabyte = ca. 1 000 000 Byte, Gigabyte = 1 000 000 000 Byte

[→ GPS (Global Positioning System) = satellitengestütztes Ortungs/Navigationssystem

[→ Laptop [→ Seite 17]

[→ Notebook [→ Seite 17]

[→ PDA [→ Seite 17]

[→ Server (Zusteller) = spezielle Computer zur Verwaltung von Netzwerken mit verschiedenen Aufgaben (Netzsteuerung, zentrale Datenspeicherung, Softwarebereitstellung)

[→ Smartphone [→ Seite 17]

[→ Speicherkarte (auch: Flash-Card, Memory-Card) = mobile Datenspeicher in kleinen flachen Gehäusen, die vorwiegend in mobile IKT-Geräte zur Erweiterung der Speicherkapazität eingeschoben werden; in sehr vielen verschiedenen Größen und Techniken zu erhalten

[→ USB (Universal Serial Bus) = USB ist eine Technik zur schnellen Übertragung von Daten zwischen IKT-Geräten (PC, Maus, Festplatte, Tastatur usw.); USB hat sich aufgrund seiner Schnelligkeit und Einfachheit als Standard vor für die Verbindung zwischen mobilen Geräten etabliert (typisch: flacher, eckiger Stecker)

[→ USB-Festplatte = mobile, räumlich kleine Festplatte für USB-Anschlüsse z.B. an Notebooks

[→ USB-Stick = etwa daumengroßes Speichermedium mit USB-Anschluss, das sich besonders leicht transportieren lässt; mit Ohrhöreranschluss und entsprechender Technik auch für die Musikspeicherung und Wiedergabe geeignet (MP3-Stick)