

3. RETURN ON INVESTMENT IN IT-SICHERHEIT



Dr. Kai Westerwelle

Das herkömmliche Verständnis von IT-Sicherheit als Schutz vor Viren, Würmern, Trojanern und sonstigen mutmaßlichen Angriffen von außen auf die unternehmensinterne IT-Infrastruktur erfasst nur einen Teilbereich dieses für Unternehmen jeder Größe bedeutenden Themas. Folge dieses eingeschränkten Verständnisses von IT-Sicherheit im Unternehmen ist ein entsprechend fokussiertes Schutzpotenzial (nur) durch zielgerichtete Maßnahmen, wie Firewalls, Virens Scanner und ähnliches. Richtig verstanden erfordert IT-Sicherheit jedoch weit darüber hinausgehende Schutzmaßnahmen, die auch die Unternehmensorganisation selbst erfassen. Dr. Kai Westerwelle von der Rechtsanwaltssozietät Taylor Wessing gibt einen Überblick.

Die eigentlich freundliche Mitteilung „I love you“ wurde im Jahre 2000 zum Schrecken der IT-Verantwortlichen weltweit. Der unter diesem Betreff versandte Virus war die bis dahin wohl schwerste Virenattacke und verursachte nach damaligen Schätzungen der Schweizer Rück Schäden in Höhe von 2,9 Milliarden EURO. Das Virus war insbesondere deshalb so gefährlich, weil es

ringert. Ganz im Gegenteil sind die heutigen Angriffsmittel, wie beispielsweise Trojaner, die nicht erkennbar zerstören, sondern unerkannt ausspähen, deutlich gefährlicher. „I love you“ und seine Nachfolger haben aber im positiven Sinne dazu beigetragen, dass IT-Sicherheit einen anderen Stellenwert bekommen hat. Ein effektiver Schutz vor Angriffen auf die IT-Infrastruktur von außen ist für Unternehmen heute selbstverständlich. Die Erkenntnis, dass IT-Sicherheit viel mehr ist, als eine äußere Absicherung des Unternehmensnetzes, hat sich demgegenüber noch nicht vollständig durchgesetzt.

2. bei der Anwendung von informationstechnischen Systemen oder Komponenten.“

§ 2 Abs. 2 BSIG definiert insofern drei Grundpfeiler der IT-Sicherheit: Verfügbarkeit, Unversehrtheit und Vertraulichkeit. Verfügbarkeit bedeutet die Gewährleistung der ordnungsgemäßen Funktion des IT-Systems, einschließlich eines permanenten Zugriffs auf die gespeicherten Informationen. Verfügbarkeit heißt also Ausfallsicherheit. Unversehrtheit (Integrität) zielt demgegenüber auf den Schutz vor einer ungewollten oder unautorisierten Veränderung der Information. Da ein absoluter Schutz vor unbefugter Datenveränderung allerdings nur schwer oder gar nicht zu erreichen ist, soll die Integrität des IT-Systems zumindest sicherstellen, dass Daten nicht unerkannt verändert werden können. Unter Vertraulichkeit wird schließlich der Schutz der Information vor unbefugter Kenntnisnahme verstanden. Über die im Gesetz genannten Bestandteile hinaus besteht weitgehend Einigkeit darüber, dass auch Authentizität, also die Sicherstellung der Identität des Kommunizierenden, sowie die Autorisierung des Nutzers, also die Feststellung eines berechtigten Zugriffs, wesentliche Elemente der IT-Sicherheit sind.

Die Grundpfeiler der IT-Sicherheit im Unternehmen sind Verfügbarkeit, Unversehrtheit, Vertraulichkeit, Authentizität und Autorisierung.

sich gezielt unter dem Absender bekannter oder befreundeter Mailteilnehmer verschickte und dem Empfänger damit Ungefährlichkeit vorspiegelte. Die bis dahin vielfach als ausreichend empfundene ‚Schutzmaßnahme‘ in Form von Unternehmensanweisungen zur Nutzung des E-Mail-Systems wie ‚Öffnen Sie nur E-Mails von Absendern, denen Sie vertrauen‘ war damit völlig wirkungslos. Wenn gleich Angriffe ähnlichen Ausmaßes seitdem nicht mehr bekannt wurden bzw. schneller und effektiver bekämpft werden konnten, hat sich die Gefahr entsprechender Attacken keineswegs ver-

WAS IST IT-SICHERHEIT?

Die Frage „Was ist IT-Sicherheit“ lässt sich nur unscharf beantworten. Den Ansatz einer rechtlichen Definition gibt § 2 Abs. 2 des Gesetzes über das Bundesamt für die Sicherheit in der Informationstechnik (BSIG). Dort heißt es:

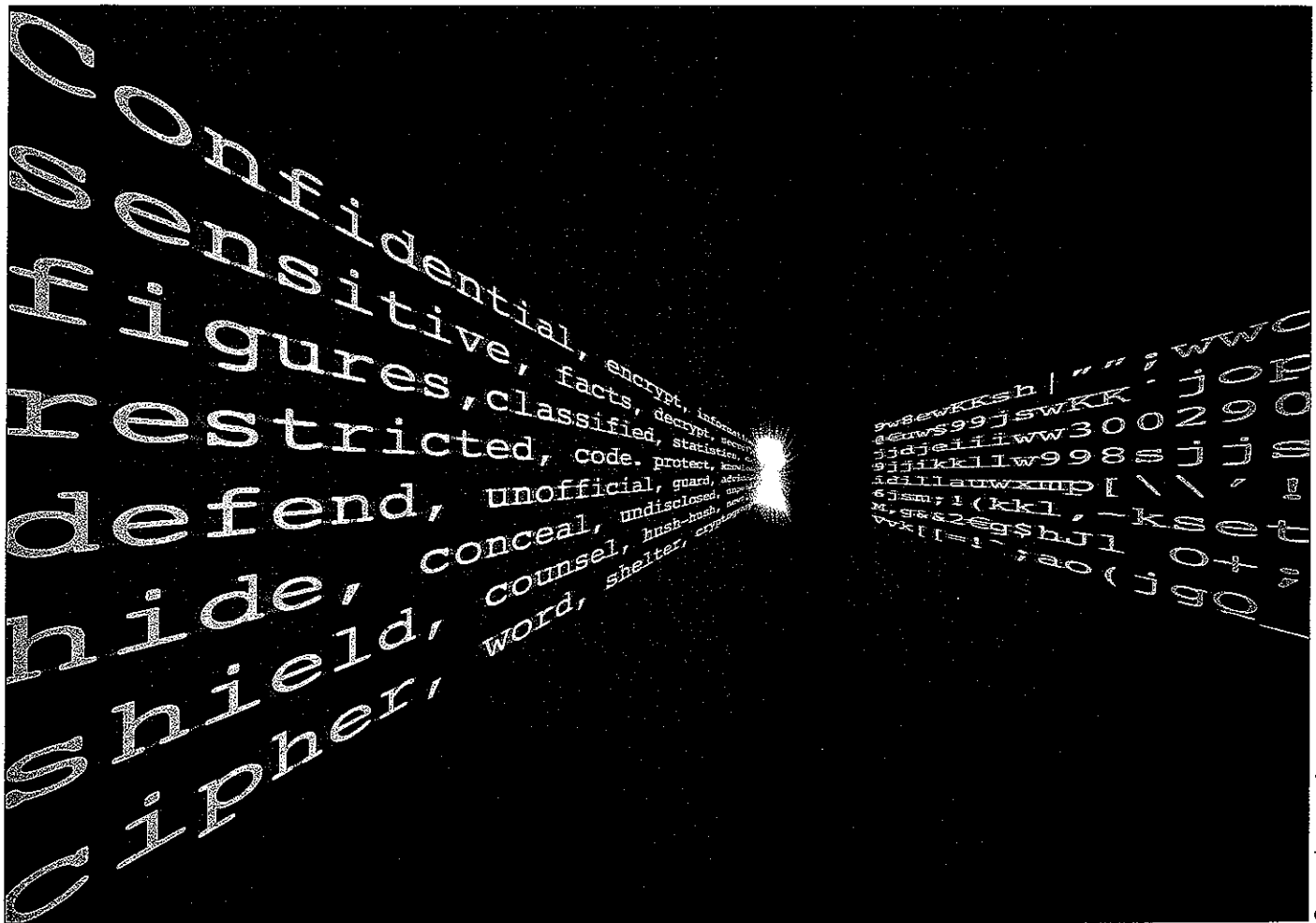
„Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

1. in informationstechnischen Systemen oder Komponenten oder

Die lediglich abstrakte Bestimmung der IT-Sicherheit in § 2 Abs. 2 BSIg wird ergänzt durch in verschiedenen Spezialgesetzen enthaltene konkretere Vorgaben an die in den betroffenen Unternehmen herzustellende IT-Sicherheit. Wichtigstes Beispiel ist hier die gesetzliche Pflicht zum technisch sicheren Umgang mit personenbezogenen Daten in § 9 des Bundesdatenschutzgesetzes (BDSG). Insbesondere die Anlage zu § 9 BDSG normiert verbindliche Kontrollpflichten

weisung des Bundesministeriums der Finanzen im Hinblick auf die Abgabe von Steuererklärungen zu beachten sind. Die behördliche Anweisung zur IT-Sicherheit DV-gestützter Buchführung wird flankiert durch die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), die ihrerseits Grundlage von Prüfungsmöglichkeiten der Finanzämter sind. Die Nichtbeachtung dieser Vorgaben an eine DV-gestützte Buchführung kann zur Nichterteilung des Testats füh-

Rechtsprechung und der juristischen Fachliteratur sind daher auch alle diejenigen Unternehmen dem TKG unterworfenen Telekommunikationsanbieter, die ihren Mitarbeitern einen Online-Zugang bereitstellen und die private Nutzung von Internet und elektronischer Post – auch nur gelegentlich – gestatten. Hierin sei bereits ein Angebot von Übertragungswegen für Dritte, mithin ein Angebot von Telekommunikationsdiensten zu sehen. Ist § 109 TKG dementsprechend aufgrund



© www.shutterstock.com

des Datenverarbeiters (Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle) sowie ein Gebot der getrennten Verarbeitung von für unterschiedliche Zwecke erhobenen personenbezogenen Daten. Für Unternehmen mit IT-gestützter Buchführung (§ 239 Abs. 4 des Handelsgesetzbuchs [HGB]) statuiert Ziffer 5 der Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS) eine Reihe von Vorgaben an die IT-Sicherheit, die nach dieser Verwaltungsan-

ren (vgl. § 321 Abs. 2 S. 3 HGB). Weitere verbindliche Vorgaben an die IT-Sicherheit im Unternehmen gibt § 109 des Telekommunikationsgesetzes (TKG), von dessen Regelungen sich die meisten Unternehmen fälschlicherweise nicht erfasst sehen, da sie meinen, keine Telekommunikationsdienste zu erbringen. Sie übersehen dabei, dass die vom TKG geforderte „geschäftsmäßige“ Erbringung von Telekommunikationsdiensten nicht mit „entgeltlicher“ Leistung für Kunden gleichzusetzen ist. Nach der

der Zulassung einer privaten Nutzung der IT-Systeme des Unternehmens anwendbar, muss das betroffene Unternehmen nicht nur besondere technische Vorgaben zum Schutze der Datenverarbeitungssysteme gegen externe Zugriffe einsetzen und „angemessene Vorkehrungen“ gegen Störungen ergreifen, sondern darüber hinaus ein Sicherheitskonzept er- sowie einen IT-Sicherheitsbeauftragten bestellen. Zur Vervollständigung sei angemerkt, dass die Qualifikation des Unternehmens als Anbieter

von Telekommunikationsdiensten äußerst gravierende Auswirkungen auf die Möglichkeiten der Kontrolle des E-Mail-Verkehrs der Mitarbeiter hat (strafbewehrte Beschränkungen der E-Mail-Kontrolle und von Filtersystemen).

Schließlich dürfte aber auch die abstrakte Bestimmung des § 2 Abs. 2 BStG selbst nicht völlig unverbindlich sein. Gerade im Hinblick auf Unternehmen, die in ihrer Geschäftstätigkeit und/oder Organisation in besonderem Maße von einer sicheren IT-Infrastruktur abhängig sind, wird man nicht umhinkönnen, die Sicherheit dieser Strukturen (auch) zum Gegenstand der Zuverlässigkeitsprüfung nach den Vorgaben der Gewerbeordnung (§ 35) zu machen.

Mit der externen Haftung des Unternehmens für Mängel der IT-Sicherheit korrespondiert die persönliche Haftung der Verantwortlichen gegenüber ihrem geschädigten Unternehmen (Rückgriffshaftung).

SICHERHEIT NACH AUSSEN, NACH INNEN UND VOR FREUNDEN

Dass die IT eines Unternehmens durch Angriffe von außen bedroht wird, ist hinlänglich bekannt. Gefahr droht dabei nicht nur durch ggf. unbewusst weitergegebene Viren, Würmer, Trojaner und ähnliches, die in regelmäßigen Abständen unter Ausnutzung von neu erkannten Sicherheitslücken der in den Unternehmen verwendeten Programme in das Netzwerk des Unternehmens gelangen, sondern auch von Hackern, die Einfallstore in die Unternehmens-IT nutzen, um an geheime Daten und Know-how des ausgespionierten Unternehmens zu gelangen. Diesen Angriffen kann das Unternehmen in den meisten Fällen durch ausreichende Sicherheitsmaßnahmen in der Abschirmung des Netzwerkes gegen externe Einflüsse begegnen (Firewall). Neben diesen äußeren Bedrohungen der IT des Unternehmens gibt es aber auch ernst zu nehmende Bedrohungen aus dem Inneren des Unternehmens. Dies betrifft in den seltensten Fällen bewusste Angriffe von Mitarbeitern in Schädigungsabsicht. Viel bedeutsamer erscheinen hier die

Fälle fehlerhafter Bedienung oder gut gemeinter Hilfe, die zu schweren Schäden, zumeist Datenverlust, führen. Es ist Aufgabe der IT-Sicherheit, auch diesen Gefahren zu begegnen. Dies kann insbesondere durch Schaffung einer mehrstufigen Berechtigungshierarchie (User / Super User / Administrator / Head of IT) geschehen, die das Zerstörungspotenzial des wohlmeinenden Users begrenzen. In die Kategorie „Gefährdung von innen“ gehört aber auch der nicht seltene Fall des versehentlichen „Einschleppens“ von Viren etc., die sich der Benutzer beispielsweise im nicht ausreichend gesicherten Home-Office auf seinen Laptop gezogen hat und die mit dem Einloggen am Arbeitsplatz, an der Firewall vorbei, unmittelbar in das Unternehmensnetzwerk gelangen. Schließlich muss die IT-Sicherheit auch „Angriffen von Freunden“ begegnen. Dies betrifft beispielsweise den direkten Anschluss von Laptops von Kunden/Externen an das Netzwerk und der damit verbundenen Gefahr der Umgehung der Firewall, dem die IT-Sicherheit z. B. mit der sog. Intrusion Detection (Erkennung nicht autorisierter Rechnersysteme innerhalb geschlossener Netzwerkkomplexe) begegnen kann. Ein ähnliches Gefährdungspotenzial ergibt sich durch externe IT-Dienstleister, die an der Firewall vorbei Remote-Support leisten (Fernwartung). Von besonderer Bedeutung ist schließlich auch die IT-Sicherheit von Outsourcing-Unternehmen. Da hier das outsourcende Unternehmen selbst als Verarbeiter der Daten gilt, ist es insbesondere auch für die Einhaltung von datenschutzrechtlichen Vorgaben verantwortlich (§ 11 BDSG). IT-Sicherheit verlangt insoweit nicht nur die vertragliche Vereinbarung entsprechender Schutzniveaus, sondern auch deren stetige Kontrolle.

HAFTUNG DES UNTERNEHMENS UND SEINER MITARBEITER FÜR SICHERHEITSLÜCKEN

Die sich aus einer mangelhaften IT-Sicherheit für das Unternehmen möglicherweise ergebenden Schäden sind vielfältig. Hier ist in erster Linie an direkte – eigene – Schäden des Unternehmens durch Ausfälle (Produktionsausfall, Abrechnungsverzögerung etc.) oder Datenverluste mit entsprechendem Wieder-

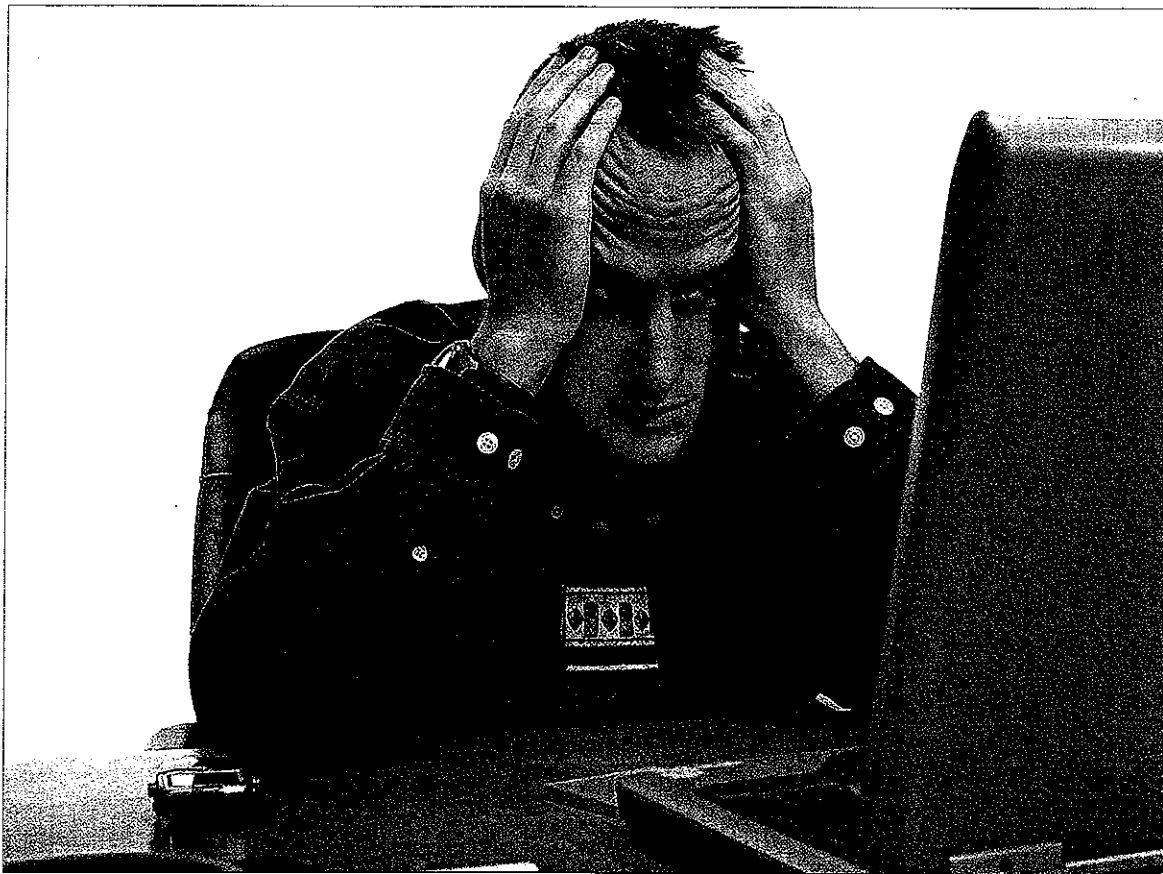
herstellungsaufwand zu denken. Die Bandbreite der möglichen Schäden geht jedoch weit über diese direkten Schäden hinaus. Führt beispielsweise ein auf Lücken in der IT-Sicherheit beruhender Ausfall der IT-Infrastruktur eines Lieferanten zu Lieferverzögerungen bei ihm und zu Produktionsverzögerungen bei seinem Abnehmer, kann sich der Lieferant aufgrund seines Organisationsverschuldens nicht exkulpieren. Er haftet also für durch seinen Verzug eingetretene Schäden des Kunden und muss im schlimmsten Fall sogar noch entsprechende, im Falle von schuldhaften Lieferverzögerungen nicht unübliche Vertragsstrafen bezahlen. Nicht besser stünde ein Unternehmen, das auf der Basis einer Vertraulichkeitsvereinbarung von seinem Vertragspartner offenbarte vertrauliche Informationen nicht ausreichend gegen unberechtigte Zugriffe Dritter schützt und diese wegen mangelhafter IT-Sicherheit ausgespäht werden. In diesem Fall haftet das Unternehmen auf der Basis der entsprechenden Vertraulichkeitsvereinbarung für sämtliche sich aus der Offenbarung der vertraulichen Information ergebenden Schäden des Vertragspartners und wird üblicherweise in Vertraulichkeitsvereinbarungen vereinbarte Vertragsstrafen zahlen müssen. Neben vertraglichen Ansprüchen kommen vielfach auch deliktische Ansprüche in Betracht, da das in § 823 Abs. 1 des Bürgerlichen Gesetzbuches (BGB) geschützte Rechtsgut ‚Eigentum‘ die Integrität von Daten erfasst. Die Beispiele lassen sich beliebig fortsetzen.

Mit der externen Haftung des Unternehmens für Mängel der IT-Sicherheit korrespondiert die persönliche Haftung der Verantwortlichen gegenüber ihrem geschädigten Unternehmen (Rückgriffshaftung). Bei Aktiengesellschaften trifft diese zunächst den Aufsichtsrat aufgrund seiner Verpflichtung zur Überwachung einer ordnungsgemäßen Geschäftsführung des Vorstands (§ 111 Abs. 1 des Aktiengesetzes [AktG]). Der Vorstand wiederum dürfte zur Gewährleistung adäquater IT-Sicherheit aufgrund seiner Verpflichtung zur Anwendung der Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters und seiner aus § 91 Abs. 2 AktG resultierenden Pflicht zur Einrichtung von Risikoüberwachungssystemen

verpflichtet sein. Ein ähnliches Bild ergibt sich für Geschäftsführer einer GmbH. Für diese kommt eine persönliche Haftung für aus der Nichtgewährung der IT-Sicherheit entstehende Schäden aus der allgemeinen Geschäftsführerhaftung in Betracht (§ 43 Abs. 2 GmbH-Gesetz). Die persönliche Verantwortlichkeit der leitenden Angestellten und Mitarbeiter folgt demgegenüber normalen arbeitsrechtlichen Grundsätzen. Im Falle der persönlichen Verantwortlichkeit eines Mitarbeiters gegenüber seinem Unternehmen ist jedoch das differenzierte System der Haftungsprivilegierungen

des Unternehmens gegen Dritte hinzuweisen, welches bei unterlassender oder mangelhafter IT-Sicherheit sogar zum vollständigen Verlust eines an sich gegebenen Schadensersatzanspruches führen kann. So hat das OLG Hamm unter Berufung auf einen Sachverständigen, der die Unterlassung einer zuverlässigen, zeitnahen und umfassenden Datenroutine (Datensicherung) als „blauäugig“ und grob fahrlässig bezeichnete, den geltend gemachten Ersatzanspruch des geschädigten Unternehmens wegen „überwiegenden Mitverschuldens“ abgeprochen.

cherung der jeweiligen Verantwortlichen gegenüber persönlicher Inanspruchnahme. Nicht übersehen werden sollte auch ein heutzutage keineswegs unbedeutender Ertrag eines Investments in IT-Sicherheit in Form eines durch eine Verringerung der operationellen Risiken des Unternehmens ggf. zu erzielendes besseres Rating des Unternehmens im Bereich „Basel II“. Wichtigstes Return on Investment in IT-Sicherheit ist jedoch, dass die Einhaltung von entsprechenden Sicherheitsstandards nicht nur Vertrauensverlusten der Kunden/Vertragspartner vorbeugt, sondern ggf. das Vertrauen der



© www.shutterstock.com

nach Verschuldensformen zu berücksichtigen (keine Haftung bei leichter Fahrlässigkeit, geteilte Haftung bei mittlerer Fahrlässigkeit und volle Haftung bei grober Fahrlässigkeit), welches auch für IT- und/oder datenschutzverantwortliche Mitarbeiter gilt. Bei diesen Mitarbeitern dürften etwaige Zumutbarkeitserwägungen allerdings strenger zu Ungunsten der Verantwortlichen ausfallen.

In diesem Zusammenhang ist auf die Berücksichtigung eines Mitverschuldens (§ 254 BGB) bei Schadensersatzansprüchen

UNSICHTBARES RETURN ON INVESTMENT? Das oft unsichtbare Return on Investment in IT-Sicherheit wird bereits durch das Vorstehende deutlich sichtbar. Die Vermeidung von eigenen Schäden des Unternehmens, die Vorsorge gegen Haftungsansprüche Dritter für deren Schäden, der Erhalt von Ansprüchen des Unternehmens gegen Dritte und schließlich die Wahrung des Versicherungsschutzes sind ein respektables Ergebnis von Investitionen in IT-Sicherheit. Hinzu kommt die durchaus bedeutsame Absi-

Kunden/Vertragspartner in die Leistung des Unternehmens verstärkt, insbesondere wenn sich die Investitionen in die IT-Sicherheit durch entsprechende Zertifizierungen belegen lassen (Beispiel: ISO 17799 – Code of Practice for Information Security Management). Wird dies erreicht, zeigt sich das Return on Investment in IT-Sicherheit nicht nur in Rechtssicherheit, sondern in (sicht)barer Münze.

*Dr. Kai Westerwelle /
Kanzlei Taylor Wessing,
Frankfurt am Main ■*