RISIKEN KENNEN - RISIKEN MANAGEN

> News zum Thema Cyber-Risiken

Das Business ist digital: Kaum eine unternehmerische Aktion kommt heute ohne den Austausch elektronischer Daten im Cyberraum aus. Eine komplexe Geschäftswelt, die viele Sicherheitsrisiken birgt. RVM hat das Ziel, diese Risiken mit passenden Versicherungslösungen für Ihre Kunden kalkulierbar zu machen. Nachfolgend informieren wir Sie über Entwicklungen und Neuigkeiten aus dem Bereich der Cyber-Risiken und Versicherungen - u.a. mit einem Experten Interview.

NEUES AUS DER POLITIK, WIRTSCHAFT UND WISSENSCHAFT

Waren Sie schon einmal Opfer von Cyber-Kriminalität? Das wäre zumindest nicht verwunderlich, denn Internetkriminalität steht nach wie vor hoch im Negativ-Kurs: Das Jahr 2015 konnte noch einmal alle Schreckens-Statistiken toppen - 2016 geht es damit nun direkt weiter. Kein Zeitraum zuvor war dermaßen infiltriert von Datenmissbrauch und Co. Gerade die Verbreitung von Schadsoftware ist ein „dominanter Trend bei der Verbreitung von Malware und wird ein Schwerpunkt-Thema der IT-Sicherheit im Jahr 2016“, wie im Bericht BSI IT Sicherheitslage Januar - März 2016 zu lesen ist. Das Bundesamt für Sicherheit und Informationstechnik hat am 11. März 2016 ein entsprechendes Themenpapier zur Ransomware vorgestellt.

Nicht minder erschreckend sind Erkenntnisse von IBM: In ihrer Studie QUELLE 2015 verzeichnet der Konzern 64 Prozent mehr Sicherheitsvorfälle als noch im Jahr zuvor. 60 Prozent aller registrierten Attacken wurden dabei von sogenannten Insidern verübt, die Folgen wiegen damit doppelt schwer für Industrie und Wirtschaft. Als Unternehmer sollten Sie sich daher über eines im Klaren sein: unzureichender Cyberschutz ist und bleibt folgenschwer. Das IT-Sicherheitsgesetz soll Sie unterstützen und vor den kalkulierbaren Risiken schützen.

Apropos: Auch wenn Cyber-Kriminalität anhaltend steigende Kosten verursacht, wie Tim Grieveson, Chief Cyber Security Strateg ist von Hewlett Packard Enterprise erläutert, ist erst jedes zehnte Industrieunternehmen entsprechend versichert, zumindest was die Sicherheitslage deutscher Unternehmen betrifft. Dabei entstanden deutschen Unternehmen im vergangenen Jahr Schäden in Höhe von 65,2 Mrd. EUR. Es ist und bleibt also viel zu tun, um einen Kurswechsel einzuläuten.

Sicher, sicherer, am sichersten?
Cyber-Sicherheit ist kein flauschiger Kaschmirpullover, der locker über die Schulter geworfen werden kann. Dazu ist die Bedrohungslage zu ernst. Das Thema hat also Potenzial zur Chefsache: Zum 25. Juli 2015 ist das sogenannte IT-Sicherheitsgesetz in Kraft getreten (wir haben berichtet). Jetzt liegt die erste Verordnung vor. Ob und inwiefern Ihre Branche davon betroffen, lesen Sie in diesem Kurzüberblick. Weitere Informationen finden Sie natürlich auch direkt auf den Seiten des Bundesamtes für Sicherheit und Informationstechnik.

Zur Erinnerung: Was will das IT-Sicherheitsgesetz?
Sicherheit bedeutet laut Duden: „Geschützt sein vor Gefahr und Schaden“, ist aber auch Verpflichtung. In diesem Sinne müssen Betreiber kritischer Infrastrukturen (KRITIS) aus den Wirtschaftssektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen folgende Pflichten erfüllen, geht es um ihre IT-Sicherheit, andernfalls droht ein Bußgeld.

- Allem voran sind angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse zu treffen.

- Die Einhaltung dieser Vorkehrungen ist im Rahmen von IT-Sicherheits-Audits im 2-Jahres-Turnus nachzuweisen.

- Sicherheitsvorfälle mit Einfluss auf die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit informationstechnischer Systeme, Komponenten oder Prozesse, der zu einem Ausfall oder zu einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können, sind dem Bundesamt für Sicherheit in der Informationstechnik (BSI) IT-Sicherheitsvorfälle uneingeschränkt zu melden.

Welche Branche konkret als kritische Infrastruktur im Sinne des IT-Sicherheitsgesetzes gilt, sollen begleitende Rechtsverordnungen bis Ende 2016 definieren. Für die Bereiche Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation regelt die KRITIS-Verordnung nun, welche Anlagen und Unternehmen entsprechend als Kritische Infrastruktur einzuordnen sind. Bis Anfang 2017 sollen per Änderungsverordnung auch die Anlagen in den Sektoren Transport und Verkehr, Gesundheit sowie Finanz- und Versicherungswesen identifizierbar werden.

EINORDNEN, ABER WIE? DIE BSI-KRITIS-VERORDNUNG IM KURZ-DIALOG MIT DR. SVEN ERICHSEN

Woher weiß man, ob man als KRITIS eingestuft wird?
Eine Reihe von Kriterien, aufgelistet nach Prozessschritten, Anlagen und Schwellenwerten, hilft Unternehmen und Betreibern dabei, ihren Status quo zu bestimmen und zu prüfen, ob sie unter den Regelungsbereich des IT-Sicherheitsgesetzes fallen. Ist das der Fall, klärt ein dreistufiges Verfahren, ob das jeweilige Unternehmen als „kritisch“ oder „nicht kritisch“ eingestuft werden kann. Als kritisch wird ein Betreiber beispielsweise dann eingestuft, wenn er die Versorgung von 500.000 Menschen sicherstellt.

Also geht hier Sicherheit über alles?
Jein. ‚Kritisch’ anzumerken ist, dass diese Verallgemeinerung nicht per se zielführend ist. Konkret stehen beispielsweise im Sektor der dezentral erfolgenden Wasserversorgung die Schwellenwerte unter Umständen nicht in angemessenem Verhältnis zur Relevanz der Bevölkerungsvorsorge mit Wasser.

Gäbe es denn eine ‚sicherere’ Alternative?
Ja, qualitative Kriterien, beispielsweise die Berücksichtigung etwaiger Domino-Effekte, würden ein realistischeres Bild zeichnen. Ein Beispiel: Ein KRITIS-Betreiber überschreitet zwar die Schwelle der 500.000 zu versorgenden Menschen nicht, versorgt aber Unternehmen, die ihrerseits die Versorgung einer Vielzahl von Menschen sicherstellen und so weiter.

Übrigens: Neben KRITIS-Betreibern zählen gemäß § 8 Abs. 6 IT-SiG auch Hersteller von IT-Produkten zu den Adressaten. Von diesen kann das BSI die Mitwirkung an Störungsbeseitigungen verlangen, auch die schrittweise Ausweitung des IT-Sicherheitsgesetzes auf bislang nicht benannte Sektoren ist wahrscheinlich.

Technologie allein schützt noch niemanden
Wenn Sie in Ihrem Betrieb auf IT-Maßnahmen setzen, um sich und Ihr Business von Angriffen aus dem Netz zu schützen, haben Sie schon einmal einen wichtigen Meilenstein gesetzt, denn der Cyber-Dschungel ist ein hartes Dickicht, Gefahren lauern hinter jedem Busch. Geht es nach Tim Grieveson, Chief Cyber Security Strategist bei Hewlett Packard Enterprise (HPE), macht es längst keinen Sinn mehr, im Cyber-Diskurs von einer Bedrohungslandschaft zu sprechen.

Im Gegenteil, die aktuelle Risikosituation gleiche eher einem Minenfeld denn einer Landschaft. Harte Worte. Harte Fakten dazu liefert eine Studie, die HPE in Auftrag gegeben hat. Fazit: Trittsicherheit ist gefragt.

Das Grundproblem erläutert Grieveson im Gespräch mit der Börsen-Zeitung (Ausg. 41) wie folgt: „Das Umfeld verändert sich beständig und es ergeben sich daraus drei widerstreitende Herausforderungen für die IT-Sicherheit."

Wir klären auf:

- Der Modus Operandi verändert sich
  Das typische Script-Kiddy, das in seinem Jugendzimmer statt Matheformeln lieber Codes knackte, hat sich längst professionalisiert: Ein profitorientierter Markt mit Standardprodukten und Bedarfsartikeln ist entstanden, der das Genre Cyberkriminalität ganz neu definiert. Man kollaboriert und teilt sich ganze Arbeitsprozesse – wir hatten berichtet.

- Die Gesetzgebung wird komplexer
  Gerade im Bereich Datenschutz und Datensicherheit wird die Gesetzgebung immer komplexer, Vorschriften muten beschwerlich und unverständlich an, das gilt insbesondere auf europäischer Ebene. Deutschland für sich betrachtet hat eine relativ klare Gesetzgebung im Umgang mit Daten formuliert.

- Stetiger Wandel
  Der IT-Sektor wandelt sich permanent, Ansprüche steigen, Unternehmen wollen ‚mehr für weniger, sie wollen es schneller und sie wollen Zugang von überall her. Wer seine Daten auf mobilen Geräten nicht schützt, erschafft sich seine eigenen Katastrophen. Doch Datenschutz geht eben mit Kosten und Herausforderungen Hand in Hand.

DIE GRÖSSTEN BEDROHUNGEN UND RISIKEN

The Inner-Circle
Schwer vorstellbar, doch die größte Gefahr lauert direkt hinter der nächsten Tür, nämlich im Inneren einer Organisation selbst. Diesem „Insider Threat" ist dabei noch nicht einmal böse Absicht zu unterstellen, „es kann auch sein, dass jemand mit guter Absicht Dummes tut". Doch auch unzufriedene Mitarbeiter sind häufig genug Ursache eines Cyber-Vorfalls. Das muss nicht sein: „Mithilfe von Nutzerverhaltensanalysen lässt sich (...) herausfinden, wenn jemand abtrünnig wird. Hier werden Profile von Nutzertypen auf Basis ihrer jeweiligen Tätigkeitsbereiche und Funktionen erstellt. Beispielsweise hat ein Buchhalter normalerweise keinen Zugang zu den Personalakten. Wenn dann auf einmal ein solcher Mitarbeiter ein verändertes Verhalten an den Tag legt, zum Beispiel um drei Uhr morgens ins Büro kommt, Personalakten ausdruckt oder dem eigenen Gmail-Konto schickt oder von China aus darauf zugreift, dann wird das genauer untersucht oder unterbunden." Aber Vorsicht ist geboten, nicht alle Überwachungsmaßnahmen entsprechen hierzulande den gängigen Datenschutzrichtlinien.

Probleme bleiben Probleme
Wie ist es eigentlich um Ihre IT-Infrastruktur bestellt - kennen Sie die Lecks, die Schlupflöcher für Hacker und Konsorten? Cyberkriminelle nutzen nämlich noch immer seit Jahren gängige Schwachstellen für ihre Zwecke - mit Erfolg. Vollkommen unnötig, würde die IT-Industrie aus der Vergangenheit lernen. Doch aus Fehlern wird nicht jeder klug. Nachschlag? Bitteschön: „Von den 400 bis 500 Schwachstellen, die im vergangenen Jahr zutage getreten sind, stammt die Hälfte der Top 10 aus den Jahren 2009 oder 2010" und bereiten damit noch immer die gleichen Probleme. Man könnte sich fragen, ob diese Probleme nicht hausgemacht sind.

... UND WIE MAN SIE IN SCHACH HALTEN KANN

Die schlechte Nachricht vorab: Es gibt kein Produkt, das allumfassend schützt, keine Patentlösung. Wie so oft kommt es auch im Cyber-Sicherheitsmanagement auf die richtige Mischung an. Und eine klare Willenserklärung seitens der Unternehmen. „People, process and procedure", kombiniert mit moderner Technologie sind essentiell. Wer seine Mitarbeiter nicht in Achtsamkeit trainiert, wird fehlerhaftes Verhalten nie reduzieren können.

Auch das Durchspielen von Cyberszenarien und den Umgang damit kann ein Unternehmen im Fall der Fälle handlungsfähig halten, um den Geschäftsbetrieb zügig wieder auf Spur zu bringen. Doch erst Übung macht den Meister, die Feuerwehr wird bei der Brandbekämpfung schließlich auch nicht hektisch.

Natürlich hilft alle Vorbereitung nichts, wenn die eingesetzten Lösungsansätze - technische Maßnahmen inbegriffen - nicht korrespondieren. Mauern ziehen ist längst überholt, Technologien „in Position“ zu bringen, wenig zielführend. Nur wer seine Geschütze - von separaten Services über Firewalls, Antivirus oder Threat Intelligence - ganzheitlich aufstellt und auf das Zusammenspiel setzt, bleibt schlagkräftig und kann am Ende bis zu 30 Prozent an Kosten sparen.

ZU GUTER LETZT: EIN BLICK IN DIE GLASKUGEL

Die Kreditwirtschaft steht hoch im Kurs bei Cyberkriminellen. Doch auch die Medizinindustrie und der Bildungsbereich investieren zu viel in Forschung, zu wenig in Sicherheit. Und Grievesons Prognose für 2016 geht noch weiter: Attacken auf kritische nationale Infrastrukturen werden steigen, Energiedienstleister, Wasserversorger, Eisenbahnen, Transportation, Flughäfen und Flugzeuge stehen auf seiner Negativliste, Computer-Angriffe könnten darüber hinaus die neuen Waffen in politischen Auseinandersetzungen werden.

Sicherheit Made in Germany
Deutschland, die Nation der Vernunft und Bürokratie, das Land, deren Unternehmen für Qualität und Präzision stehen, verhält sich in Bezug auf Cyber-Sicherheit grob anarchistisch. Gut, es gibt das IT-Sicherheitsgesetz - nicht ohne Grund, denn schaut man in die Unternehmen selbst, tun sich wahre Abgründe auf. Deutschland steht metaphorisch gesprochen an der Klippe: Nicht einmal jedes fünfte deutsche Unternehmen hat im vergangenen Jahr seine formellen Cyber-Sicherheitsrichtlinien überprüft (Quelle: Eurostat). Schlimmer noch: Knapp 71 Prozent dieser Unternehmen haben gar keine formellen Cyber-Sicherheitsrichtlinien, die sie verfolgen. Damit ist das Land der großen Denker eines der Nicht-Mitdenker, weit abgeschlagen mit Frankreich auf die letzten Ränge der Länder, deren Unternehmen eine IKT-Sicherheitsstrategie anwenden, womit Deutschland unter dem Durchschnitt der EU-28 liegt, bei dem 32 Prozent der Unternehmen über formelle Cyber-Sicherheitsrichtlinien verfügen. Allen voran Schweden, gefolgt von Portugal, Irland und Italien.

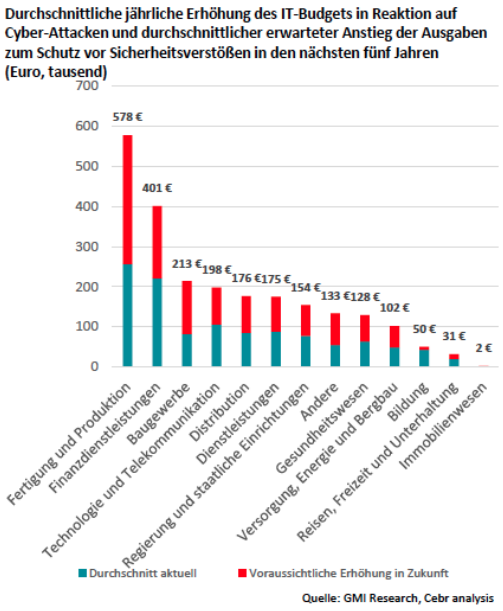
KONSEQUENZEN FÜR DIE DEUTSCHE WIRTSCHAFT

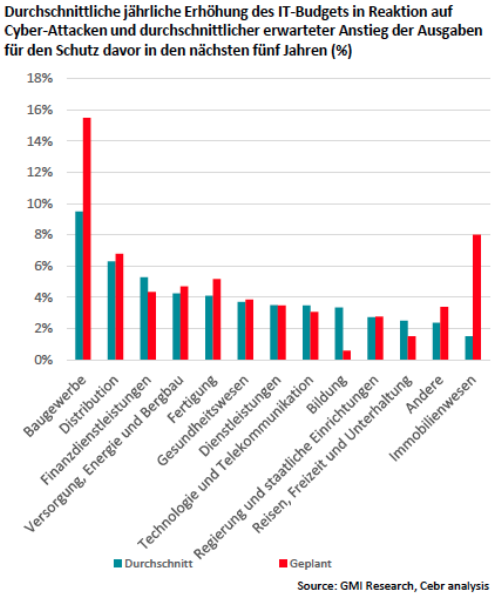
Laut Ergebnissen des © Centre for Economics and Business Research haben Cyber-Kriminelle im vergangenen Jahr 16 Millionen deutsche Verbraucher-Datensätze gestohlen. Außerdem ist das Land aufgrund der großen Masse urheberrechtlich geschützter Daten im Zusammenhang mit der 4. industriellen Revolution ein besonders attraktives Ziel für Cyber-Angriffe, die konkret die Branchen Fertigung und Produktion im Visier haben (Bundesamt für Sicherheit in der Informationstechnik (BSI), „Die Lage der IT-Sicherheit in Deutschland 2015“). Doch grundsätzlich, so warnt das BSI, steht fast jeder Aspekt der Cyber-Sicherheit in Deutschland unter hohem Risiko. In Zahlen kosten Cybersicherheits-Verstöße die deutsche Wirtschaft bis dato 65,2 Mrd. EUR, große Unternehmen mussten in den letzten fünf Jahren einen Verlust von etwa 13 Mrd. EUR in Kauf verkraften, wobei die Branchen Fertigung und Produktion mit 27 Mrd. EUR Umsatz Verlust den größten Rückgang in Kauf nehmen mussten (Quelle: GMI Research, Analysis).

Immerhin: Darauf sitzen bleiben möchte am Ende niemand, weshalb neun von 10 deutschen Unternehmen weitere Ausgaben in ihre Cyber-Abwehr planen - die jährlichen Ausgaben für Cyber-Sicherheit steigen bereits um 2,3 Mrd. EUR an:

- Erhöhung des IT-Budgets aufgrund Cyber-Sicherheitsverstöße um durchschnittlich 1,2 Mio. EUR.
- Die Branchen Fertigung und Produktion setzen das Budget auf 256.000 EUR hoch, in den nächsten fünf Jahren sind Investitionen von 322.000 EUR geplant.
- Der Finanzsektor hat sein jährliches IT-Budget um 220.000 EUR erhöht und plant weitere Investments in Höhe von 180.000 EUR in den kommenden fünf Jahren.

· Das Baugewerbe wird seine Ausgaben um in den kommenden fünf Jahren voraussichtlich um 16 Prozent auf 1 Mio. EUR erhöhen





Reicht das, um von einem Kurswechsel sprechen zu können?
Fraglich, glauben doch die meisten CISOs, dass interne IT-Sicherheitsrichtlinien Innovationen behindern, so GMI Research. Die Konsequenz daraus? Das Thema scheint zu komplex, Maßnahmen zu sperrig - erst schlankere, automatisierte Risikoprozesse könnten dazu beitragen, Risiken zu bewerten und auf sie zu reagieren.

Und wie sieht es außerhalb der Grenzen Deutschlands aus? Die Studie von IBM Security zum Jahr 2015 zeichnet ein ganz ähnliches Bild, zumindest was die allgemeine Bedrohungslage betrifft. Stan-den 2014 noch Finanzdienstleister im Fokus des kriminellen Interesses, waren 2015 vor allem Gesundheitswesen und die herstellende Industrie von Cyber-Attacken betroffen, doch mit einem Platz drei der am meisten gefährdeten Bereiche kann der Finanzsektor noch lange nicht aufatmen. Besonders erschreckend ist dabei, dass über 60 Prozent der registrierten Angriffe von ‚Insidern' begangen wurden.

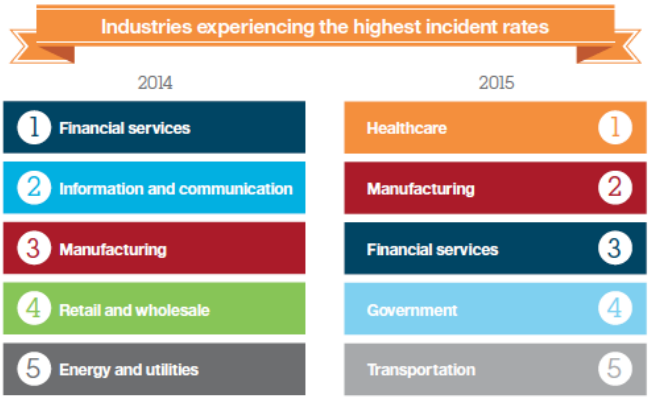


Figure 2. Healthcare moved into the top spot of the rankings as the most-attacked industry in 2015, replacing financial services, which dropped to third place. Second place went to the manufacturing industry, while government and the transportation industry took over fourth and fifth places, respectively.

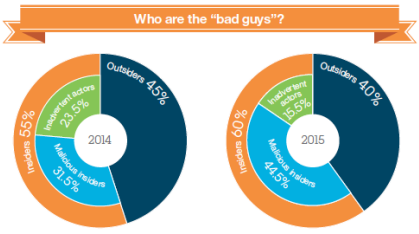


Figure 4. In 2015, outsiders were found to be responsible for 40 percent of the attacks recorded, while 60 percent of attacks were carried out by those who had insider access to organizations' systems.

Zieht Euch warm an

Die Verunsicherung seitens Bankkunden ist dieser Tage groß - fast täglich berichten die Medien über Datenklau, Kreditkartenmissbrauch und Trojaner. Vielleicht haben Sie ja selbst schon einmal einen Cyber-Vorfall ausbaden müssen. Kein Wunder, digitale Verbrechen im Bankenumfeld haben Hochkonjunktur. Die fortschreitende Digitalisierung ist ein enormes Sicherheitsleck und damit Segen und Fluch zugleich. Neue digitalisierbare Prozesse, Kanäle für mehr Internation zwischen Kunde und Vertrieb doch auch Mobile-Payment-Lösungen bieten über ihre Vernetzung eine immer größere Angriffsfläche. Und die wird ausgenutzt, so waren laut Bericht allein im Jahr 2014 fünf von sechs namhaften Unternehmen Opfer von Internetkriminalität. Die Folgekosten sind enorm, Lloyd's schätzt sie auf 400 Mrd. Dollar weltweit, wobei allein die deutsche Volkswirtschaft einen Schaden von 51 Mrd. EUR zu beklagen habe, so Bitkom.

Da Cyberkriminalität zukünftig die führenden Delikte ausmachen wird, müssen sich gerade Banken auf ganz neue Szenarien einstellen. Wie schon Tim Grieveson konstatiert, wird die Abschottungsstrategie allein nicht mehr sicher sein. Zu passiv, zu unflexibel. Aktive Mechanismen sind gefragt, um sich den immer professionelleren Angreifern und ihrer Technologiekompetenz anzugleichen. Denn dass sie mit einem Angriff Erfolg haben werden, scheint laut Börsen-Zeitung unstrittig. Die Frage ist nicht, „ob, sondern wann ein Cyber-Angriff die Bank trifft, wie schnell dieser erkannt wird und wie man den bereits entstandenen Schaden möglichst gering halten kann."

Das heißt im Klartext für Kreditinstitute:

- Cyber-Security muss zur Kernkompetenz, Risiken müssen verstanden werden
- Geschäftskritische Prozesse und Assets müssen identifiziert werden
- IT-Sicherheit ist eine strategische Frage
- Fähigkeiten zur Erkennung und aktiven Abwehr müssen etabliert werden
- Prozesse zum Umgang mit identifizierten Risiken müssen definiert werden
- Moderne, analytische und forensische Methoden sind anzuwenden
- Angreiferprofile müssen analysiert werden
- Indikatoren für Attacken wie minimal stärker ausgelastete Arbeitsspeicher oder Abweichungen im Nutzungsverhalten müssen identifiziert werden

„Statt nach dem Gießkannenprinzip gilt es dabei Schutzmaßnahmen auf geschäftskritische Assets mit dem Ziel maßzuschneidern, mögliche Angriffe zu verhindern oder zumindest frühzeitig zu erkennen." Ein Umdenken ist gefordert, schließlich ist IT-Sicherheit im Bankenbereich mehrheitlich ein reaktiver Prozess, was der Dynamik der Cyberkriminalität natürlich widerspricht. Technologien, die Analytics und Echtzeit-Überwachung einbeziehen, müssen integriert werden. Ein Reaktionsplan, der alle erforderlichen Handlungen und Abläufe festlegt, ist ebenso notwendig wie ein Krisenmanagement-Prozess, denkt man an die angemessene und zügige Information Betroffener und die Außenwirkung des Hauses. Relevante Elemente sind dabei die Validierung des Angriffes, die Aktivierung spezifischer Notfallmechanismen und die Festlegung zur Einbeziehung von Aufsichtsbehörden und Regulatoren, die Benachrichtigung externer Medienagenturen zwecks Reputationssicherung gehört ebenfalls zu einem professionellen Krisenmanagement. Für die Banken bedeutet das viel Arbeit, die alternativlos ist und bleibt, wenn die Daten- und Informationssicherheit in allen Geschäftsprozessen gesichert werden soll. Und somit am Ende auch das Vertrauen der Kunden, die wichtigste Währung der Finanzbranche, gewährleistet. Neue Strategien, Strukturen, Technologien, Prozesse und last but not least informierte, aufgeklärte Mitarbeiter sind für die wirtschaftliche Zukunft der Banken unbezahlbar. (Quelle: Börsen-Zeitung, Ausg. 41)

Das Cyber-Barometer

Vertrauensbildende Maßnahmen: Wer sich allein auf Technologie verlässt, ist schnell verlassen. Mitarbeiterbindung und -einbindung könnten die Zufriedenheit erhöhen und das Risiko eines Angriffs aus den eigenen Reihen mildern.

Ignoranz muss man sich leisten können: Wer den Tatsachen nicht ins Gesicht sieht, kann nicht rechnen. Schäden in Milliardenhöhe wirken sich auf die Gesamtwirtschaft aus und tragen definitiv nicht zu einer stabilen Konjunktur bei.

Sicherheit auf Kredit: Banken sind besonders gefährdet und müssen dringend an der Anpassung vorhandener Sicherheitskonzepte an den technischen Status Quo arbeiten - das erfordert Investitionen - das Vertrauen der Kunden gewinnt man nicht „auf Pump".

NEUES AUS DER TECHNIK

Erpresserische Raubzüge sind im Cyber-Crime-Kosmos an der Tagesordnung. Die Frage ist also nicht: wann erobert der nächste Erpressungstrojaner die Systeme, sondern welcher Trojaner wird es diesmal sein. Nachdem TeslaCrypt - ein Trojaner, der auf Festplatten gespeicherte Bilder und Dateien verschlüsselt und nur gegen eine Lösegeldzahlung angeblich wieder entschlüsselt - und Locky, der Windows-orientierte ‚Lockstoff' haben Sicherheitsforscher nun eine neue Ransomware-Methode ausgemacht: Bart, ein Verschlüsselungs-Trojaner wie Locky und angeblich aus dem gleichen Hause, so vermuten zumindest vermuten Kryptologen von ProofPoint, schlägt ganz neue Wege ein: Bart nimmt Geiseln. Es kann also nicht oft genug über das Thema Internetsicherheit diskutiert werden.

Im ZIP-Gefängnis
Anders als der freche Nachbarschreck des Simpsons-Clans löst der Verschlüsselungs-Trojaner Bart blankes Entsetzen aus. Ganz nach dem Locky-Muster sollen potenzielle Windows-Opfer mittels gefälschter E-Mails dazu animiert werden, Datei-Anhänge zu öffnen. Soweit nichts Neues. Ebenfalls nicht neu: Nach dem Klick auf einen Anhang schleust der verwendete RockLoader die Malware via HTTPS auf den betroffenen Computer. Neu ist allerdings, dass Bart bei der Datenverschlüsselung nicht wie so oft üblich auf den Advanced Encryption Standard (AES) baut. Vielmehr nimmt der Trojaner passwortgeschützte ZIP-Archive als Geisel und drückt der betroffenen Datei seinen Stempel auf (.bart.zip). Dabei muss Bart nicht erst den Command-and-Control-Server der Kriminellen kontaktieren, der Schädling kann selbst dann zum Ziel gelangen, wenn eine Firewall entsprechende Verbindungen blockiert, erläutert ProofPoint.

Wie sein gelber Namensfetter ist der Trojaner bislang hauptsächlich in den USA zu Hause, aber offensichtlich auf einen weltweiten Einsatz vorbereitet - das wollen Kryptologen aus den zahlreichen Übersetzungen ableiten. (Quelle: Heise online)

Wenn Malware nicht nur böse, sondern extrem bösartig ist ...
Dann hat sie einen Namen: Jigsaw, ein gemeiner Trojaner, der seine Drohungen gegen Unternehmen nun noch verschärft, wie das BSI jetzt erläutert. Daten werden bei diesem Fall von Malware nämlich nicht ‚nur' verschlüsselt, bis eine erfolgreiche Lösegeldübergabe stattgefunden hat. Nein, Jigsaw droht mit der Löschung, wenn eine gesetzte Zahlungsfrist überschritten wird. Der Druck auf die Opfer der Erpressung steigt, eine angemessene Reaktion unter Zeitdruck ist kaum noch möglich.

Woran erkennt man die Verschlüsselung und wie agiert Jigsaw nach der Infektion?
Die Dateiendungen .BTC, .FUN, .KKK entlarven infizierte Computer, Jigsaw sorgt dafür, dass im Stundentakt wahllos eine Datei gelöscht wird - unwiderruflich. Falls der Benutzer in Panik den Computer neu startet, werden ‚zur Strafe 1.000 Dateien auf einen Schlag gelöscht - nach maximal 72 Stunden müssen dann alle übrigen Dateien dran glauben, sofern nicht 0,4 Bitcoin (ca. 150 US-Dollar) an die Täter überwiesen wurden. Die gute Nachricht: Es gibt wirksame Maßnahmen gegen Jigsaw! So können Betroffene Benutzer die Prozesse drpbx.exe und firefox.exe beenden, um die fortlaufende Verschlüsselung zu unterbrechen. Anschließend sollte der Autostart-Vorgang für den tatsächlich gefälschten Prozessnamen firefox.exe entfernt werden. Dieses Vorgehen ist aufgrund der geringen Komplexität in der Regel von allen IT-Mitarbeitern oder IT-kundigen Kollegen durchführbar. Ein Entschlüsselungstool mit dem Namen ‚Jigsaw Decryptor' steht als Download zur Verfügung.

Ransomware ist und bleibt auf dem Vormarsch
Das bestätigen Fälle wie Jigsaw, eine BSI-Umfrage zum Thema Ransomware spiegelt die fortdauernde Bedrohung der Unternehmen deutlich wider. Demnach waren ein Drittel der befragten Unternehmen in den letzten sechs Monaten von Ransomware betroffen - KMUs wie Großunternehmen gleichermaßen. Mit 75 Prozent ist die Infektion aufgrund arglosen Umgangs mit infizierten E-Mail-Anhängen die häufigste Ursache. Mit verheerenden Folgen: Während die Mehrzahl der betroffenen Unternehmen angaben, dass einzelne Arbeitsplatzrechner betroffen waren, kam es in jedem fünften Unternehmen (22 Prozent) zu einem erheblichen Ausfall der IT-Dienste, zudem erlitten 11 Prozent einen Verlust von kritischen Dateien, so dass Daten nicht wiederhergestellt werden konnten. Und die Moral von der Geschicht'? Nicht neu, aber umso dringlicher: Neben technischen Maßnahmen ist die Schulung der Mitarbeiter zusammen mit einem übergreifenden Backup-Konzept, das auch Arbeitsplatzdaten einbezieht, unabdingbar! Wer Daten schnell und sicher wiederherstellen kann, braucht eine Ransomware nicht zu fürchten. Keinesfalls sollte man sich allein auf Antivirenprogramme verlassen, denn das kann sehr teuer werden.

Ein Betrugsfall macht Schule - und wie man sich schützen kann
Ransomware kennt viele Gesichter. Das amerikanische FBI berichtet beispielsweise über einen dramatischen Anstieg von Fällen, in denen Betrug über vorgebliche Geschäftsführungsanweisungen begangen wird (CEO Fraud). Bei dieser Betrugsmethode werden E-Mails an Mitarbeiter verschickt, die Nachrichten des Managements vortäuschen, um Geldüberweisung an die Betrüger auszulösen. Das FBI legte eine Schätzung vor, dass die Betrugsfälle mehr als 2,3 Milliarden US-Dollar Verluste für die Betroffenen in den vergangen drei Jahren betrugen.

Man kann sich wehren: Gegen diese Angriffe können zweistufige Authentisierungsverfahren (2-Faktor-Verfahren) helfen, die die Durchführung von Überweisungen allein nach Kenntnis eines Passwortes oder von TANs unterbindet. Größeren Effekt erzielt allerdings eine Umstellung von Kommunikationsprozessen: Das Management sollte grundsätzlich nur über definierte Kanäle mit Mitarbeitern kommunizieren und keine Abkürzungen bei Zahlungsprozessen vorsehen – etwa einen Vorgang ‚zur Chefsache' machen, um ihn zahlungstechnisch zu beschleunigen. Das ungewöhnliche Verhalten des scheinbaren Managements würde sofort auffallen, eine ‚rettende' Rückfrage über einen sicheren Kanal könnte zum Abbruch der Transaktion führen. Mit anderen Worten: Die Betrüger hätten keine Chance!

Das Cyber-Barometer

Wachsamkeit ist Datensicher: Bart ist ein Trojaner, der noch in den USA sein Unwesen treibt, doch es ist absehbar, dass er auch Deutschland heimsuchen wird. Wertvolles Wissen, das mit dem Aufbau der Sicherheitsstruktur genutzt werden kann.

Schlimmer geht immer: Jigsaw ist der aktive akute Beweis. Opfer derart unter Druck zu setzen, dass sie sich (scheinbar) gar nicht mehr zur Wehr setzen können um damit jede Forderung stellen zu können, ist perfide.

Zur Wehr setzen: Es hilft nicht, sich von bösartigen Trojaner in die Knie zwingen zu lassen - schlimm genug, dass man jederzeit zum Opfer werden kann. Alle zur Verfügung stehenden Maßnahmen sollten genutzt werden - das geht nicht ohne ein gesundes Interesse an der Thematik.

NEUES AUS DER SCHADENSWELT

Absurd, erschreckend, fahrlässig, gewitzt, furchteinflößend, schockierend, beeindruckend - geht es um Cyber-Schadenfälle, ist auf der Klaviatur der Beurteilung jede Note zu finden. Man kann sich einer gewissen Ehrfurcht vor der technischen Brillanz vieler Vorfälle kaum erwehren, wäre die Situation nicht so ernst. Ob politisch motivierte Manipulation, Produktspionage oder knallharte Erpressung: Cyber-Angriffe haben den Globus im Griff. Selbst im Mikrokosmos Deutschland entstehen Cyber-Schäden von rund 13 Mrd. EUR pro Jahr, jedes Unternehmen wurde seit 2011 durchschnittlich zweimal angegriffen, die herstellende Industrie hat mit schätzungsweise 27 Mrd. EUR Folgekosten die dickste Kröte zu schlucken, die Baubranche folgt mit 9,2 Mrd. EUR, Versorgung, Industrie und Bergbau kommen auf satte 6,5 Mrd. EUR. Und warum? Die zunehmende Vernetzung der Geschäfte öffnet Tür und Tor für Internetkriminalität.

„Unternehmen setzen heute eine Vielzahl von Anwendungen für verschiedene Geschäftsbereiche ein. Doch diese selbstentwickelten oder zugekauften Anwendungen weisen immer wieder Sicherheitslücken auf, die es Cyberkriminellen ermöglichen, anzugreifen und großen Schaden anzurichten“, so Julian Totzek-Hallhuber, Solution Architect bei Veracode gegenüber der Versicherungswirtschaft heute. (Quelle Center for Economics and Business Research (Cebr.))

SCHADENFÄLLE

Wenn der Haushalt wackelt
Städte und Kommunen haben heute häufig zu kämpfen, Haushaltslöcher sind zu stopfen, zumindest aber ist ‚gut haushalten' angesagt. Umso schlimmer, wenn dann auch noch mit Erpressung gedroht wird. So geschehen in Dettelbach im Kreis Kitzingen: Ein Hackerangriff – ursächlich ist ein Computertrojaner wahrscheinlich – wurden sämtliche Daten der Stadtverwaltung blockiert. Die massiven Probleme im IT-System der Stadt seien zwar beseitigt worden, die Daten angeblich wieder verfügbar, der Preis jedoch ist hoch: Die Stadt musste einer Lösegeldforderung nachkommen, die so gering nicht sein kann. Zumindest hüllt sich die Bürgermeisterin diesbezüglich in Schweigen. Und auch der Betrieb lief nur äußerst schleppend wieder an, das Einwohnermeldeamt musste über einen längeren Zeitraum geschlossen bleiben.

Kein Anschluss unter dieser Nummer
Tuuuuuuut. Hallo Österreich? Tuuuuuut - Einen Hackerangriff nicht gekannter Dimension hat im Februar das Netz der Telekom Austria für mehrere Tage lahmgelegt, einer gezielten Überlastung des mobilen Datennetzes folgte auch noch die Ausschaltung des Festnetzes. Betroffen waren 2,3 Millionen Festnetz- und 5,4 Millionen Handy-Kunden, wie das Handelsblatt berichtete. Das Unternehmen hat Anzeige erstattet, schweigt sich über die Schadenhöhe jedoch aus. Wenn etwas klingelt, dann die Kasse der Cyber-Angreifer.

Die Alarmglocken klingeln bei Telekom-Kunden
Auf der einen Seite klingelt die Kasse, auf der anderen Seite klingeln die Alarmglocken: In Schwarz-markt-Foren sind Mailadressen und Passwörter von schätzungsweise 120.000 T-Online-Kunden aufgetaucht. Laut Telekom gäbe es keine Anzeichen, dass IT-Systeme gehackt worden seien, die Sicherheitsbehörden wurden informiert. Es liegt nahe, dass die Daten via ‚Phishing' an Land gezogen wurden, beispielsweise in Form gefälschter Anschreiben. Keine große Sache? Im Verhältnis zu den insgesamt sechs Millionen T-Online-Adressen gesehen mag der Schaden ‚geringen' Ausmaßes sein, doch 120.000 missbrauchte Daten sind genau 120.000 Daten zu viel. Schutzmaßnahmen gegen das Phishing gibt es kaum, einzig das regelmäßige Ändern von Passwörtern trägt zur Prävention bei. (Quelle: Reuters)

Ransomware-Infektionen schlagen hohe Wellen
Ransomware, wir haben es bereits erläutert, entwickelt sich zum „dominanten Trend bei der Verbreitung von Malware und wird ein Schwerpunkt-Thema der IT-Sicherheit im Jahr 2016“ (BSI Monatsbericht Januar - März 2016 „BSI IT Sicherheitslage“). Die Meldestelle der Allianz für Cyber-Sicherheit registriert seit Anfang des Jahres zahlreiche Ransomware-Infektionen auf Organisationen: Ob Cryptowall, Locky, Tesla Crypt oder Petya - Ransomware ist eine der massivsten Bedrohungen aus dem Netz. Umso mehr, seit Malware nicht mehr nur parasitär durch Spam oder DDos-Attacken Ressourcen von infizierten Computern entwendet - immerhin konnten die Systeme nicht nur relativ unbeeinträchtigt weiterlaufen, sondern als hoch entwickelte Technologie potenziell wichtige Daten oder Anwendungen derart schädigt, dass sie nicht mehr zur Verfügung stehen.

IT-Anwender werden vom BSI ausdrücklich gewarnt, sich mit der aktuellen Bedrohungslage auseinanderzusetzen und entsprechende Schutzmaßnahmen zu ergreifen. Wie das aussehen kann, zeigt das im März auf der CeBit präsentierte BSI-Themenpapier auf: von Angriffsvektoren über ein Schadensszenario bis hin zu konkreten Empfehlungen und Hilfestellungen für die Prävention und die Reaktion im Schadenfall deckt das Dokument alle wichtigen Fragen zu Thema ab.

Das Cyber-Barometer

Standhaft bleiben: Lösegeldforderungen, so warnen das Bundesamt für Informationssicherheit (BSI) und Polizei immer wieder eindringlich, sollte nicht nachgegeben werden. Zu unsicher ist das Ergebnis einer Erpressung.

Daten schützen: Es muss kein System gehackt werden, um an sensible und wertvolle Daten zu gelangen: Durch das Phishing werden Verbraucher clever geködert, höchste Wachsamkeit ist alternativlos.

Neue Schadenqualität: Ransomware ist für private und betriebliche Anwender zu einer extrem folgenreichen Gefahr geworden. IT-Sicherheitsverantwortlich müssen in punkto Sicherheitskonzept am Ball bleiben, das betrifft den Schutz eingesetzter Software ebenso wie die Sensibilisierung von Mitarbeitern

NEUES AUS DEM VERSICHERUNGSMARKT

Überraschend, erwartungsgemäß oder schlicht erschreckend – wie stehen Sie zu der Tatsache, dass nur 11 Prozent deutscher Unternehmen gegen die Gefahr aus dem Netz versichert sind? Hätten Sie's gedacht? Tatsächlich rast Cybercrime in Richtung Zukunft, der Abschluss einer entsprechenden Versicherung wird im Vergleich jedoch mit angezogener Handbremse vollzogen, wenngleich es einen Lichtstreif am Horizont gibt: 35 Prozent deutscher Industrieunternehmen planen oder diskutieren zumindest den Abschluss einer Versicherung, so das Ergebnis einer Studie von Bitkom Research. Gewitterwolken hingegen finden sich bei fast 50 Prozent der befragten Industrieunternehmen, für die eine Absicherung kein Thema ist. Unwetterschäden sind hier vorprogrammiert, denn nur über eine maßgeschneiderte Cyber-Police kann das Restrisiko gegen Hackerangriffe und IT-Sicherheitsvorfälle abgedeckt und auf akute Hilfe im Krisenfall gebaut werden. Im Fall des Falles übernimmt die Cyber-Versicherung schließlich diverse Kosten, zum Beispiel für die Reparatur von IT-Systemen, für Schäden aufgrund einer Betriebsunterbrechung oder für die Wiederherstellung von Daten.

Daten sind eines der attraktivsten Ziele für Angriffe und ein gutes Stichwort, spricht man über Cyber-Versicherungen: auch gegen eigene Datenschutzverstöße - oftmals schneller passiert als gedacht, etwa wenn absichtlich oder versehentlich personenbezogene Daten in die falschen Hände geraten - kann man sich mit einer professionellen Cyber-Police absichern. Womit wir beim nächsten guten Stichwort wären: Cyberkriminalität ist ein Geschäft, das auf Versicherer-Seite unzählige Produkte auf den Plan ruft. Nicht ganz unproblematisch, das Geschäftsfeld ist zu jung, um übersichtlich und klar abgegrenzt zu sein, auch werden Produkte permanent weiter entwickelt, was eine genaue Prüfung erfordert. Dr. Sven Erichsen steht im Interview zum Thema Datenschutz Rede und Antwort.

Daten schützen - Rechte wahren
Das Recht an den eigenen Daten nimmt in der öffentlichen Diskussion immer wieder breiten Raum ein. Das letzte Glied in dieser Kette ist die Verabschiedung der europäischen Datenschutz-Grundverordnung (EU-DSGVO), mit der das Datenschutzrecht in der Europäischen Union vereinheitlicht wird. Über die Hintergründe und Folgen haben wir mit Dr. Sven Erichsen gesprochen.

Herr Dr. Erichsen, warum soll das Datenschutzrecht vereinheitlicht werden?
Die grundlegende Zielsetzung ist die Harmonisierung der Datenschutzvorschriften innerhalb der EU. Nur so kann unionsweit ein gleichwertiger Schutz der Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten gewahrt werden (Art. 1 Abs. 2 EU-DSGVO, Anm. d. Red.).

Es geht aber doch nicht nur um sogenannte Grundrechte, Daten sind schließlich zu einem wichtigen Produktionsfaktor geworden?
Natürlich soll mit der Verordnung auch der freie Verkehr personenbezogener Daten zwischen den Mitgliedstaaten ermöglicht werden (Art. 1 Abs. 3 EU-DSGVO, Anm. d. Red.).

Wie kann das konkret aussehen?
Als räumlicher Anwendungsbereich gilt das Marktortprinzip, zum einen bei der Verarbeitung personenbezogener Daten durch einen in der EU niedergelassenen Verantwortlichen, und zwar unabhängig davon, ob die Verarbeitung in der EU stattfindet. Sofern die Datenverarbeitung dem Angebot von Waren oder Dienstleistungen dient, kommt es auch zur Geltung für außereuropäische Anbieter.

Wie bleibt der Betroffene dabei in seinen Rechten geschützt?
Es hat sich nichts daran geändert, dass auch in Zukunft jede Datenverarbeitung einer gesetzlichen Erlaubnis oder der Einwilligung des Betroffenen bedarf. Die Informationspflichten bei der Datenerfassung sind sogar deutlich umfangreicher als bislang und auch die Auskunftspflichten sind wesentlich umfangreicher.

Das müssen Sie näher erläutern, bitte.
Die Meldepflichten gelten jetzt unabhängig von der Art der Daten und der Art der Datenschutzverletzung, sprich auch der unbefugte Zugriff innerhalb der verantwortlichen Stelle ist bei der Meldepflicht gegenüber Behörden und Betroffenen inbegriffen. Nach Artikel 33 der EU-Datenschutzverordnung, der die Meldepflicht gegenüber der Aufsichtsbehörde regelt, ist der Zeitrahmen mit einer Ausnahme geregelt: Grundsätzlich muss eine Datenschutzverletzung unverzüglich, das heißt ohne schuldhaftes Zögern (§121 BGB, Anm. d. Red.) und binnen 72 Stunden angezeigt werden. Nicht so, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten führt. Die unverzügliche Meldepflicht gilt auch gegenüber dem Betroffenen, was in Artikel 34 geregelt ist. Wenn jedoch im Vorfeld geeignete technische und organisatorische Sicherheitsvorkehrungen angewandt wurden oder nachfolgende Maßnahmen, um das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen abzuwenden getroffen werden doch auch wenn ein verhältnismäßig hoher Aufwand von Nöten ist, kann auf eine öffentliche Bekanntmachung zurück gegriffen werden.

Gibt es keine Neuerungen bezüglich der Meldepflicht gegenüber Betroffenen?
Doch. Neu ist, dass eine Meldepflicht nur dann von Nöten ist, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge hat.

Ist das nicht eine erhebliche Verschärfung des bisher in Deutschland geltenden Rechts?
Ja, insbesondere die Sanktionen werden deutlich verschärft. Bisher konnte ein Bußgeld von maximal 300.000 EUR verhängt werden. Bei Verstößen gegen Dokumentationspflichten sind Sanktionen bis 10 Mio. EUR oder zwei Prozent des Vorjahresumsatzes vorgesehen. Bei anderen Verstößen Geldbußen nach Artikel 83. Die Entscheidung über die Verhängung einer Geldbuße und den genauen Betrag liegt bei der Aufsichtsbehörde, es sind Beträge von bis zu 20 Millionen EUR oder bis zu 4 % des gesamten weltweiten Jahresumsatzes eines Unternehmens möglich, ausschlaggebend ist der jeweils höchste Betrag!

Wie sieht es mit Schadenersatz aus?
Wie bisher auch nach deutschem Recht gibt es die Haftung auf Schadenersatz (§ 7 BDSG nun Art. 82 EU-DSGVO, Anm. d Red.). Anspruchsinhaber ist jede betroffene natürliche Person, Anspruchsgegner Verantwortliche beziehungsweise Auftragsverarbeiter. Die Anspruchsvoraussetzungen sind klar definiert, dazu zählen der Verstoß gegen die EU-Datenschutzverordnung, materieller oder - und das ist neu - ein immaterieller Schaden. Davon ist insbesondere das Persönlichkeitsrecht betroffen. Zu guter Letzt muss natürlich nachgewiesen sein, dass Verantwortliche beziehungsweise Auftragsverarbeiter „in keinerlei Hinsicht“ für den Umstand, durch den der Schaden eingetreten ist, verantwortlich sind (Abs. 3, Anm. d Red.). Man spricht hier auch von der Kausalität und Verschuldensvermutung.

Wird die Verordnung in beschriebener Form umgesetzt und ab wann ist sie gültig?
Die EU-Datenschutzverordnung DSGVO gilt ab dem 25. Mai 2018 und wird als unmittelbares Recht in allen Mitgliedstaaten verbindlich. Eine Umsetzung in nationales Recht ist nicht mehr erforderlich, ein deutscher Gesetzes-Entwurf übrigens für Herbst 2017 angekündigt.

Auf Länderebene ist also gar keine individuelle Handhabung mehr möglich?
Doch, mehr als 60 Öffnungsklauseln geben den nationalen Gesetzgebern die Möglichkeit, nationale Regelungen oder Konkretisierungen zu definieren.

Das Cyber-Barometer

Guter Rat ist nicht teuer: Damit Unternehmen besser einschätzen können, welche monetären Folgen IT-Sicherheitsvorfälle haben, stellt Bitkom den kostenlosen Leitfaden „Kosten eines Cyber-Schadenfalls“ als Download bereit.

Die EU-DSGVO: Der Bedarf für eine Absicherung datenschutz-rechtlicher Risiken wird deutlich steigen, höhere Anforderungen für Datenverarbeiter und Auftragsverarbeiter - insbesondere Informations-und Meldepflichten sowie organisatorische und technische Maßnahmen zur Datensicherheit