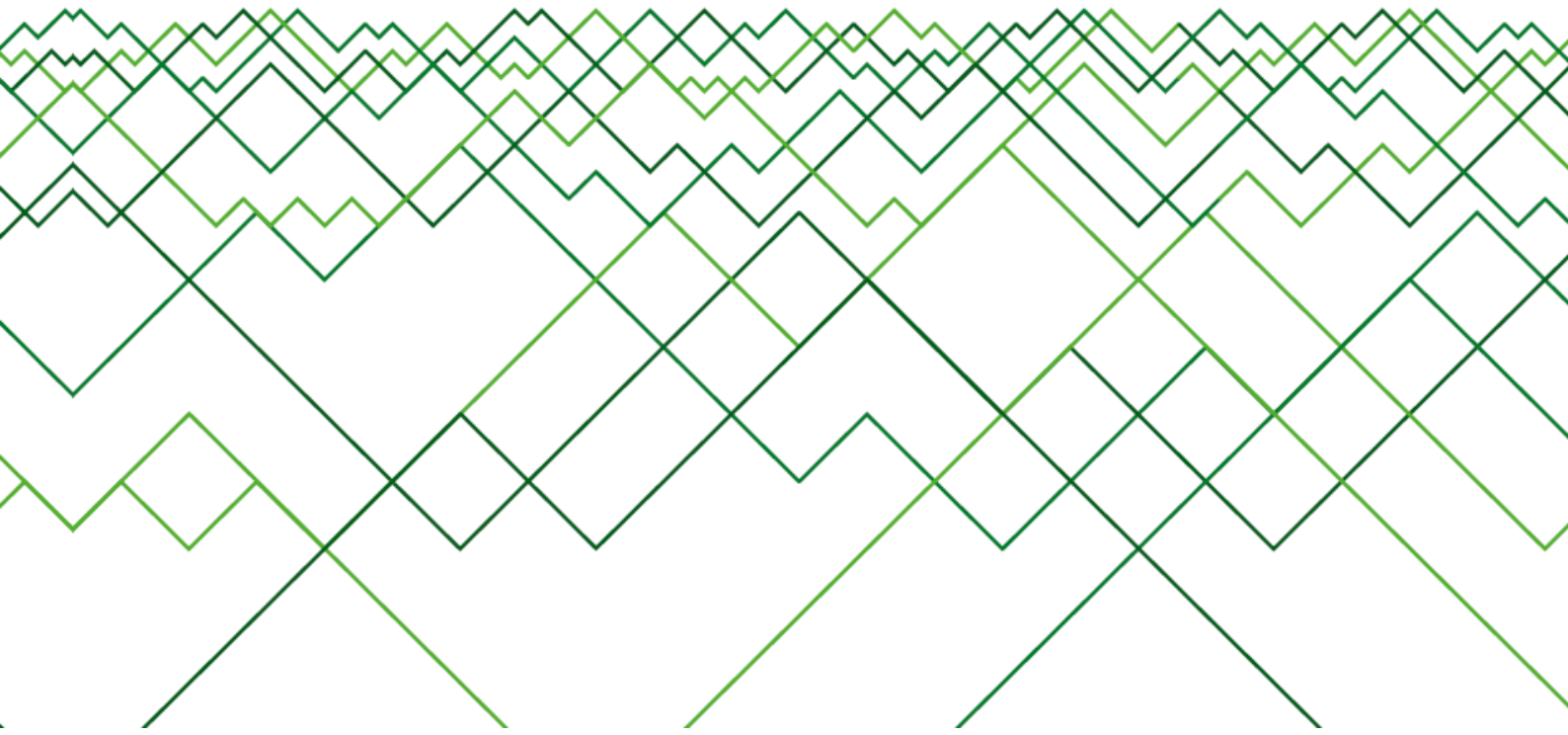
INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Analysezentrum InfoWatch

Globale Studie über Verluste von vertraulichen Daten bei Körperschaften und anderen Organisationen 2012.



Inhaltsverzeichnis

Vorwort

Das Analysezentrum von InfoWatch präsentiert die jährliche Studie über weltweite Vorfälle von Datenverlusten, die 2012 in den Medien veröffentlicht wurden.

Die Analytiker haben erstmalig festgestellt, **dass sich Datenlücken in unterschiedlichen Branchen nicht homogen darstellen.** Es lassen sich allgemein Banken, Versicherungen und Telekommunikationsunternehmen hervorheben, bei denen der Anteil der Datenlücken gesunken ist. Dieses Bild stellt mit wenigen Ausnahmen die Situation im gesamten kommerziellen Sektor dar.

Das Jahr 2012 könnte **man als das Jahr der Datenverluste im öffentlichen Sektor bezeichnen.** Der steigende Anteil der Quellen für Datenlücken in öffentlichen Strukturen, spricht für die mangelnde Aufmerksamkeit für die Datenschutzproblematik im öffentlichen Sektor. Ein Problem scheint die zunehmende Nutzung von mobilen Geräten (Smartphones, Laptops, Tablet-PC´s) zu sein, worauf die Sicherheitsbeauftragten in öffentlichen Einrichtungen eindeutig nicht vorbereitet sind.

Die vorher genannte Tendenz der Abnahme der zufälligen Datenverluste bei kommerziellen Unternehmen bestätigt sich pauschal auf der ganzen Welt. Dies ist darauf zurück zu führen, dass die Informationssicherheit immer mehr an Bedeutung gewinnt und dass die Maßnahmen gegen Datenverluste effektiver werden.

Die Verbreitung der Lösungen für die Informationssicherheit (DLP-Lösungen sind lt. Gartner bei einem Drittel der Gesellschaften vorhanden), löst nur einen Teil der Problematik, da viele Datenverluste durch Fahrlässigkeit und nicht durch Vorsatz entstehen. Eine DLP-Lösung sollte nicht als Tool gesehen werden, das Datenlücken eigenständig bekämpfen kann. Der Schutz vor fahrlässigem Datenverlust Bedarf einiger Beratung wobei auch die Arbeitsabläufe begutachtet werden sollten.

Die Meinung der Anbieter und Klienten zu DLP-Systemen wird sich in der nächsten Zeit sicherlich ändern. Die Beratung **im Bereich der Informationssicherheit soll sich weiter entwickeln und die Informationssicherheit** bei den Nutzern der DLP-Systeme als Folge kultiviert werden.

Sollte dies der Fall sein, so kann man für die nächsten 3 bis 5 Jahre sagen, dass die **typischen Datenverluste, die Vorsätzlichen sowie die Zufälligen, sinken werden.**

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Sachstand

- ✓ Im Jahr 2012 wurde weltweit in den Medien über **934** Datenlücken berichtet, was **16%** mehr als im Vorjahr bedeutet.
- ✓ Der mit dem Datenleck verbundene und in den Medien veröffentliche Direktschaden bei Finanzinstituten im ersten Halbjahr 2012 belief sich auf mehr als **37,8 Mio $**
- ✓ Es wurde mehr als **1,8 Mrd.** Finanz- und Personendatensätze öffentlich.
- ✓ Der Anteil der zufälligen Datenlücken nimmt ab und beträgt **38%**
- ✓ Der Anteil der Datenlücken in staatlichen und kommunalen Gesellschaften nimmt zu und beträgt nun **29%** (9% mehr als im Jahr 2011)
- ✓ Personendatenverluste sind führend mit einem Anteil von **89,4%**
- ✓ Der Verlust von Daten über Papierdokumente beträgt **22,3%**.

Fazit und Trends

- ✓ Den Gesamtschaden der Datenverluste können wir zunächst einmal nicht genau beziffern, die Direktschäden liegen jedoch bei rund 37,8 Mio $. Dazu kommen noch Gerichtskosten, Kosten für Veröffentlichungen, Buchprüfungen, Umstrukturierung des Informationssicherheitssystems usw. Wenn man alle diese Kosten dazu rechnet wird deutlich, dass die tatsächlichen Schäden deutlich höher sind. Den sichtbaren Schadensanteil der Datenverluste muss man sicherlich mit Faktor 30 bis 50 multiplizieren, um die tatsächliche Schadenshöhe zu ermitteln. Somit würden die tatsächlichen Kosten bei vielen Milliarden $ liegen.

  Die Problematik besteht darin, dass die tatsächlichen Schäden stark schwanken können, sodass es schwer fällt, diese genau zu beziffern. Das ist der Grund, warum das Analysezentrum InfoWatch ab 2012 Schadensschätzungen nicht mehr abgibt und nur auf die lavinenartige Erhöhung von Schäden verweist.
- ✓ Besonders zu betonen wäre auch noch die Tatsache, dass die Unternehmen über die geschehenen Vorfälle heute anderer Meinung sind. Immer öfter wird heute ein Datenleck nicht mehr von Unternehmen verheimlicht sondern den Ermittlungsmaßnahmen entsprechende Mitwirkung geleistet. Merkwürdigerweise trägt das dem Image der Unternehmen positiv bei.
- ✓ Der dritte und wichtigste Umstand ist der, dass heute nur wenige DLP-Lösungen auf zufällige Datenverluste profiliert sind. Man sollte sich heute noch über neue Technologien Gedanken machen, die die Informationen sowohl vor zufälligen als auch vor vorsätzlichen Verlusten schützen. Dazu wird es erforderlich sein, dass nicht die Daten an sich, sondern die Datenkanäle und die Infrastruktur geschützt werden. Zusätzlich vom physikalischen Lagerort der Daten, müssen die Datenwege zuverlässig ermittelt und überwacht werden. Gerade darin besteht heute die Herausforderung für die ganze DLP-Branche.

Methodik

Die Studie stützt sich auf eigene Daten, die seit 2004 von Spezialisten des Analysezentrums ermittelt und gespeichert werden. In der InfoWatch-Datenbank sind Informationen über Vorfälle enthalten, bei denen Daten aus Vorsatz oder aufgrund von Fahrlässigkeit der Mitarbeiter von Unternehmen **in den Medien** oder anderen **öffentlichen Quellen** (auch Web ond Blogs) veröffentlicht wurden.

Es sei zu vermerken, dass die Datenbank nur 1 bis 5% aller Vorfälle in der Welt umfasst. Dennoch sind die Grundkennzahlen stabil, was die Studie als repräsentativ einschätzen lässt. 1) Die Verteilung der Parameter (Arten von Datenlecks, Kanäle für Datenlecks u.ä.) ändert sich innerhalb der dargestellten Auswahl Jahr für Jahr stufenlos. 2) Die meisten Veränderungen sind vorhersehbar.

Daraus folgt, dass sich Tendenzen darstellen, die sowohl für die Auswahl als auch für die Gesamtzahl aller Vorfälle, die gemeldet oder verheimlicht wurden, stimmen.

Heute sind in der Datenbank einige Tausende Vorfälle enthalten, die gemeldet wurden. Für jedes Datenleck werden das Datum und das Datum der Veröffentlichung in den Medien erfasst.

Datenverluste, bei denen der Datenvertraulichkeitsstatus infolge von computergestützen Angriffen wie DDoS, Fishing u. ä. verletzt wurde, umfasst diese Studie nicht.

Die Registrierung und Klassifizierung der Vorfälle in der Datenbank für Datenverluste basiert auf den Analysen, die von Mitarbeitern von InfoWatch durchgeführt wurden.

Bei Auditprüfungen der Datenbank werden jedem Eintrag Attribute zugeordnet wie Unternehmenstyp, Geschäftsbereich, Art des Datenlecks, Finanzschaden und Matriken wie Kanäle, Typen verlorener Daten etc.. Diese Zuordnung der Attribute beschreibt die Größenordnung des Lecks, lässt mögliche Gründe für die Datenlücke analysieren und dessen Folgen voraussagen.

Die Daten über den Direktschaden und die Anzahl der betroffenen Datensätze werden den Publikationen entnommen.

Wir führen keine Experteneinschätzung der Gesamtschäden aufgrund von Datenverlusten bei Unternehmen durch, um unnötige Bedenken bezüglich der indirekten Schäden auszuschliessen.

Allgemeine Statistik

Im Jahre 2012 hat das Ananysezentrum InfoWatch 934 Verluste vertraulicher Daten registriert. Das ist rund 16% mehr als in den Jahren 2011 und 2010. (jeweils 794 und 801). Im Durchschnitt gesehen sind es 2,5 Datenverluste am Tag und 75 bis 80 Datenverluste im Monat.

Ein ähnlicher Anstieg wurde zuletzt im Bericht für 2009 registriert. Damals war die Anzahl der Datenverluste um 40% zu 2008 gestiegen und war auf die Mißachtung der Informationssicherheit bei den Unternehmen aufgrund der weltweiten Rezession zurückzuführen.

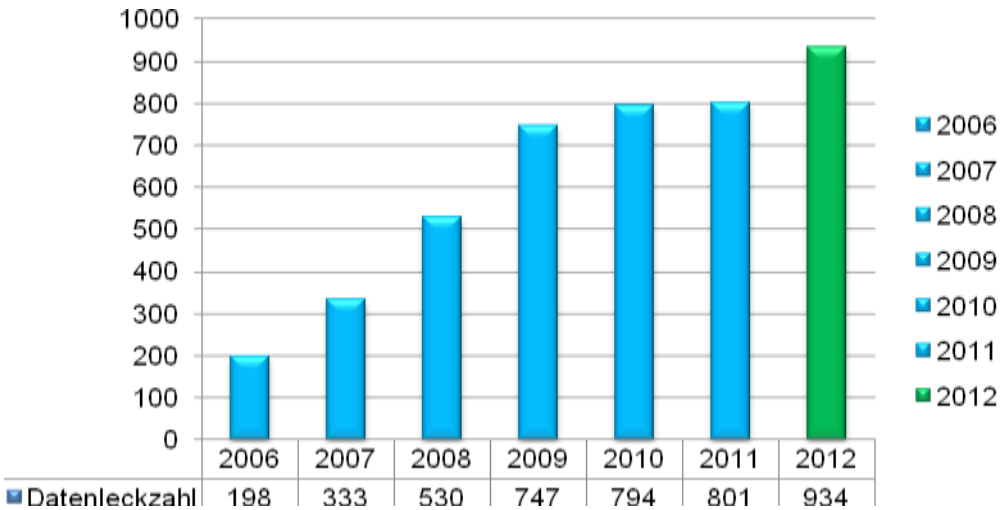


Bild.1. Anzahl der Datenlecke 2006 bis 2012 im Zeitverlauf.

Der heutige Anstieg ist im Gegensatz dazu auf die erhöhte Beachtung der Datensicherheitsaspekte durch Regelorgane, wie z. B. der Staat oder andere Interessensgemeinschaften, bedingt. Es ist bekannt, dass jeder Datenverlust bei Bürgern ein Anlass zur Rechtsverfolgung ist. Die Geschädigten und ihre Anwälte legen gern die Fälle offen, bei denen Verletzungen der Abläufe im Bereich Datenverarbeitung und -speicherung stattgefunden haben, um mögliche Schadenersatzleistungen zu erhöhen. Als Folge nimmt die Zahl der Offenlegungen in Medien zu.

Die Regelorgane verbreiten auch ihrerseits Informationen über Datenlücken aktiv. Dies ist für die USA üblich, wo Datenverluste von Bezirksstaatsanwälten als Pressemitteilungen verkündet werden.

Fazit:

Die Vorjahresprognose des Analysezentrums über die Stabilisierung der Zahl der Datenverluste hat sich nicht bestätigt. Der Grund dazu ist die erhöhte Beachtung der Datenschutzaspekte von Beteiligten, die besondere Rolle des Staates und der Regelorgane verschiedener Branchen. Leider trifft diese Aussage mehr für westliche Länder zu als für z.B. Russland.

Vorsatz

Das Verhältnis zwischen vorsätzlichen und zufälligen Datenverlusten ist grundsätzlich nicht anders als im Vorjahr. **Die von uns vor zwei Jahren vorausgesagte Tendenz zur Senkung des Anteils der zufälligen Datenverluste unter gleichzeitiger Verbreitung der DLP-Systeme wird immer deutlicher.** Insbesondere in den Branchen, die sich besonders auf den Datenschutz konzentrieren, z.B. Banken, Finanzinstitutionen, Telekommunikationsunternehmen, staatliche Strukturen etc.. Bei den Banken liegt der Anteil der zufälligen Datenverluste bei 20% - sh. Globale Studie für Datenlecks bei Banken (Finanz- und Kreditinstitutionen - 1.Halbjahr 2012).

Die Analytiker von InfoWatch prognostizierten, dass die Einführung von Schutzmaßnahmen das Verhältnis zwischen zufälligen und vorsätzlichen Datenverlusten beeinflussen wird. Die marktüblichen Schutzmaßnahmen sind mehr gegen zufällige als gegen vorsätzliche Datenverluste wirksam. Es lässt sich erkennen, dass der Anteil zufälliger Datenverluste sinkt und 2012 nur 38% ausmachten.Vor diesem Hintergrund steigt aber der Anteil vorsätzlicher Datenverluste auf 46%.(Datenverluste, deren Herkunft sich nicht einordnen lassen, blieben 2012 bei 16% konstant).

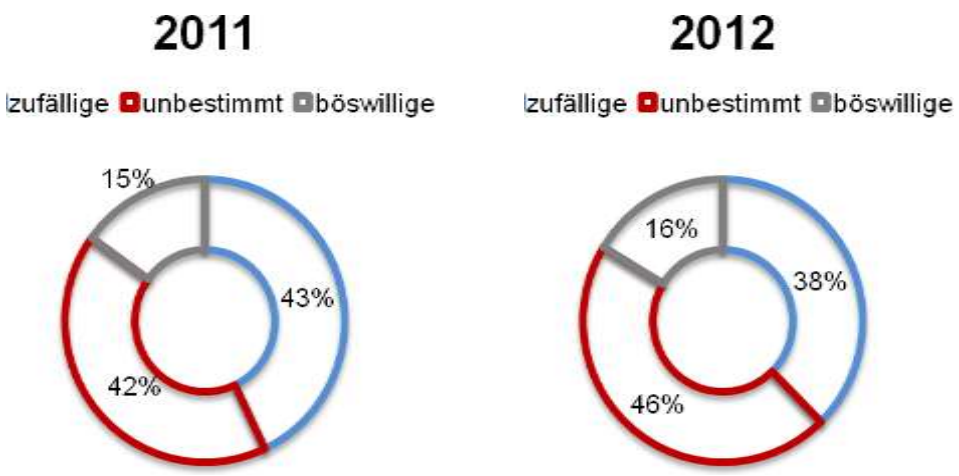
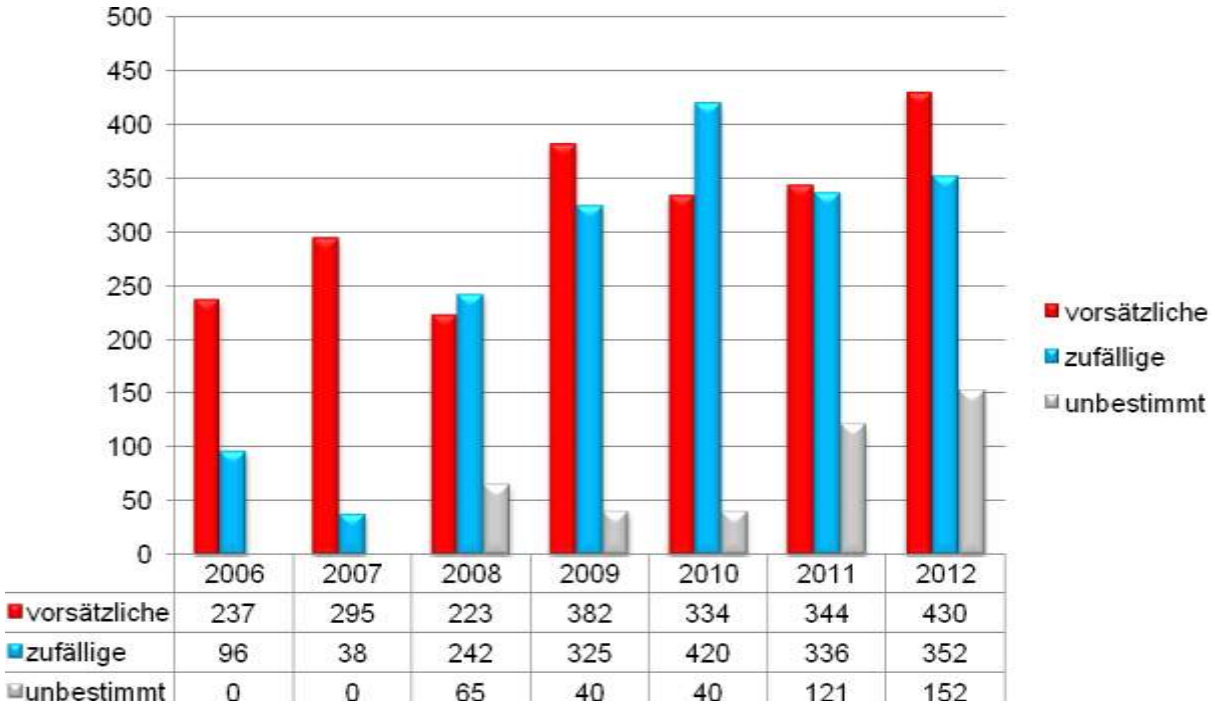


Bild 2.Verhältnis zwischen zufälligen und vorsätzlichen Datenverlusten 2011 - 2012.

Bei vielen Vorfällen lässt sich nicht feststellen, ob das Datenleck vorsätzlich oder zufällig entstand. Insbesondere beim Verlust von Datenträgern wie Laptops, Smart-Phones und USB-Datenspeichern ist die Analyse schwer. Es ist nicht immer klar, ob der Datenträger verloren ging oder gestohlen wurde. Außerdem lässt sich beim Diebstahl nicht immer feststellen, ob sich der Dieb für den Datenträger selbst oder für die gespeicherten Daten interessierte.

Nicht alle Informationsquellen über Datenlecks verweisen auf den Datenträger. Viele Medien legen darauf keinen Wert. Daher ist der Vorsatz bei Datenverlusten immer komplizierter festzustellen und diese Unbestimmtheit bleibt Jahr für Jahr konstant.

Das Verhältnis zwischen vorsätzlichen und zufälligen Datenverlusten im Zeitverlauf ist in der Grafik dargestellt. Es ist bemerkenswert, dass die Anzahl vorsätzlicher Datenverluste im Vergleich zu den zufälligen 2012 bedeutsam angestiegen ist. Zuletzt konnte man einen solchen Anstieg 2009 feststellen. Die Gleichartigkeit der Kennzahlen kann auf die Sensibilität der zufälligen Datenverluste auf die Einführung der Datenschutzmaßnahmen zurückzuführen sein.
2009 waren das noch die Ausläufer des glücklichen Jahres 2008 (die erste Welle der Masseneinführung von Datenschutzmaßnahmen). Die Ergebnisse des Vorjahres deuten indirekt auf die zweite Welle der DLP-Systeme hin. Wie vorher erwähnt, diese Tendenz lässt sich am meisten in den im Sinne der Informationssicherheit "fortgeschrittenen" Branchen feststellen: Banken, Telekommunikation etc. In diesen Branchen ist der Anteil zufälliger Datenverluste noch kleiner im Vergleich zu den Vorsätzlichen.



	2006	2007	2008	2009	2010	2011	2012
vorsätzliche	237	295	223	382	334	344	430
zufällige	96	38	242	325	420	336	352
unbestimmt	0	0	65	40	40	121	152

Bild 3.Verhältnis zwischen zufälligen und vorsätzlichen Datenverlusten 2006 - 2012.

Fazit:

Ab 2008 hat sich das Verhältnis zwischen zufälligen und vorsätzlichen Datenverlusten verändert. Das Sinken des Anteils zufälliger Datenverluste in 2012 ist das Eintreten der voausgesagten Tendenz, welche auf die Masseneinführung der Datenschutzmaßnahmen zurückzuführen ist.

Quellen von Datenlücken

Die internationale Gesetzgebung schreibt vor, dass alle Organisationen, die über Kundendaten verfügen, oder eine bestimmte Anzahl an Mitarbeiter überschreiten, Maßnahmen zum Datenschutz vornehmen müssen.

Der Datenschutz wird bei Unternehmen (deren Anteil ist 41% und sank um 5% im Vergleich zum Vorjahr) und Bildungsinstitute (deren Anteil hat sich um mehr als die Hälfte reduziert und beträgt 16%) tatsächlich groß geschrieben. Daten bei staatlichen Organisationen sind dagegen schlecht geschützt (Zuwachs 9% im Vergleich zu 2011).

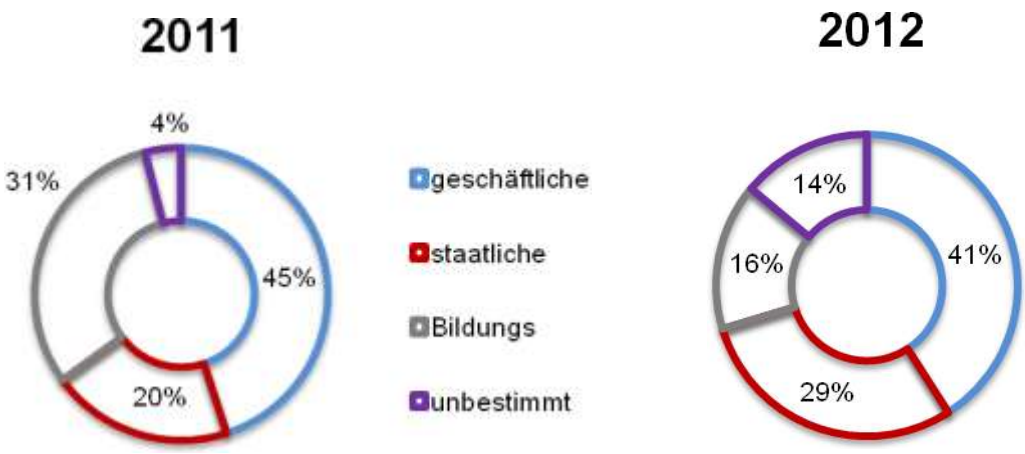


Bild 4.Verhältnis zwischen zufällige und vorsätzliche Datenverluste 2011 - 2012.

Bemerkenswert ist, dass sich der sinkende Anteil der Datenverluste in den Unternehmen und Bildungsorganisationen auch quantitativ einsschätzen lässt (sh. Bild 5).

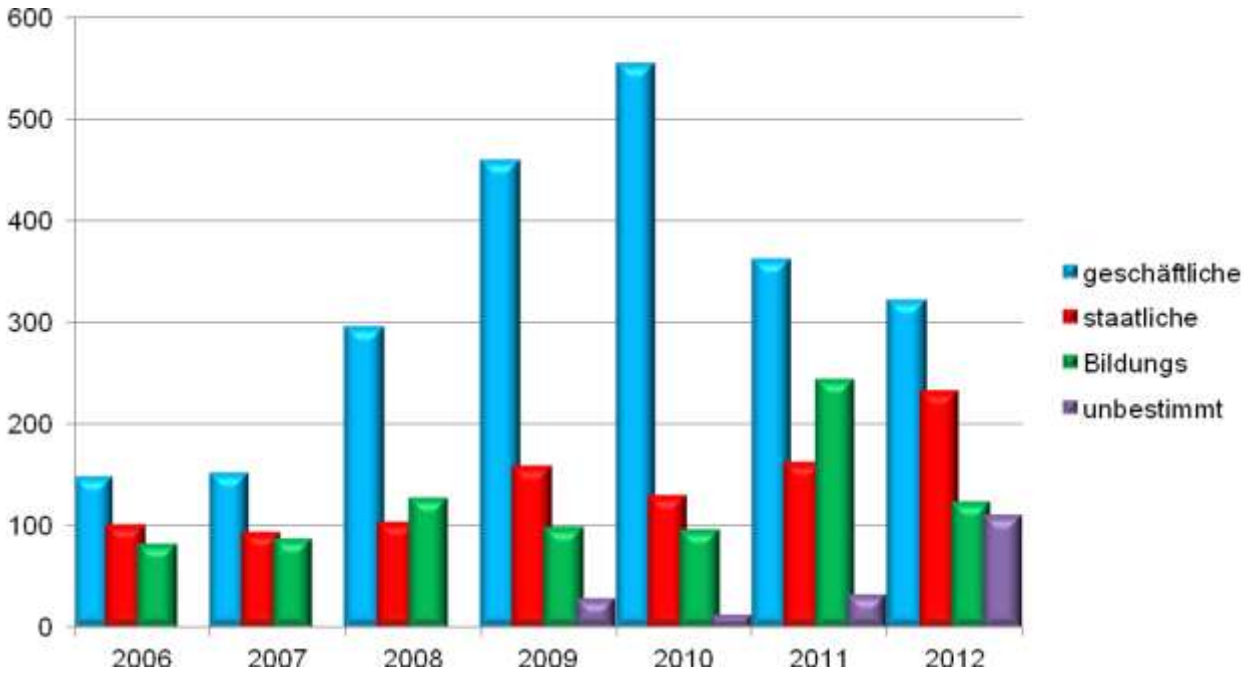


Bild 5. Anzahl der Datenverluste 2006 bis 2012 nach Quellentypen.

Schauen wir uns die Verteilung der zufälligen und vorsätzlichen Datenverluste in den Unternehmen an (Bild 6), kann man Folgendes anmerken:

- ✓ In den Banken finden zum großen Teil vorsätzliche Datenverluste statt (22% sind vorsätzliche Datenverluste). Der Anteil zufälliger Datenverluste ist mit 4% niedrig.
- ✓ Zufällige Datenverluste (61%) sind wie die Vorsätzlichen (ein Drittel von allen) für medizinische Organisationen charakteristisch.
- ✓ Der Anteil von Handelsunternehmen in beiden Fällen ist gering.

Bild 6.Verhältnis zwischen zufälligen und vorsätzlichen Datenverlusten in den Unternehmen 2011 - 2012.

Der Anteil zufälliger Datenverluste in den Unternehmen blieb konstant (ca. 37%, Bild 7). Der Anteil vorsätzlicher Datenverluste sank.

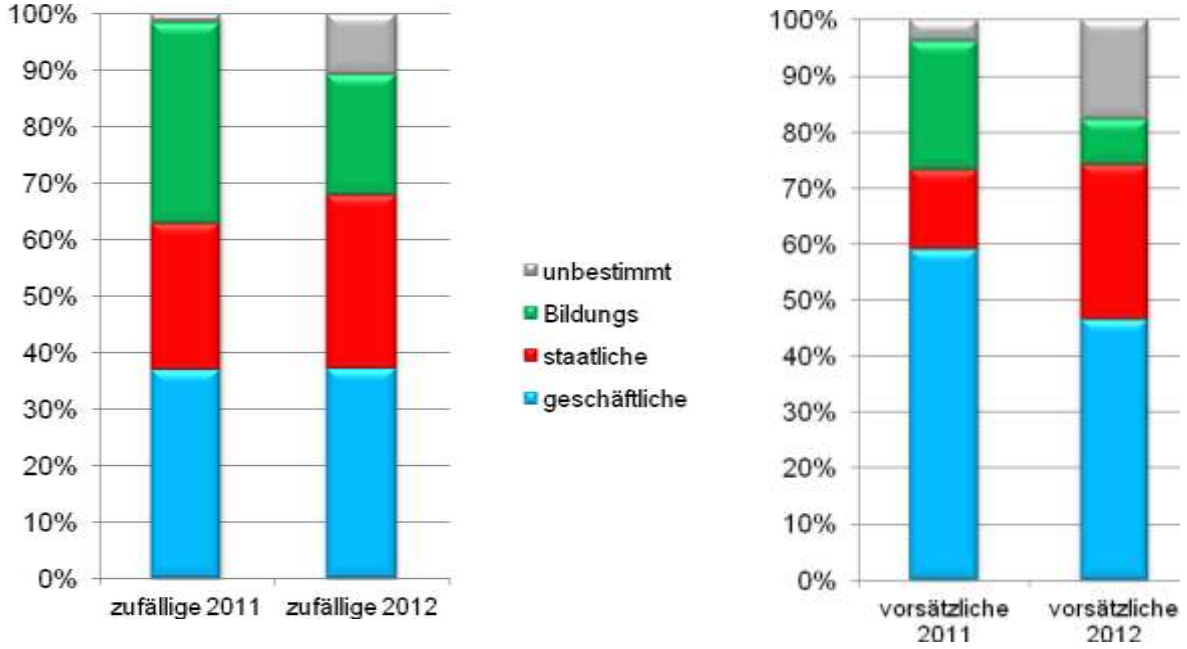


Bild 7.Verhältnis zwischen zufälligen und vorsätzlichen Datenverlusten 2011 - 2012 nach Organisationstypen.

2012 ließen sich viele Datenlücken bei staatlichen und kommunalen Organisationen feststellen.Der Anteil zufälliger und vorsätzlicher Datenverluste in staatlichen Organisationen steigt. Bedingt ist das vielleicht durch die Verzögerung bei der Einführung von Datenschutzmaßnahmen in den bürokratischen Strukturen. Ein anderer Grund ist, dass die Beamten ihre mobilen Geräte genauso gern benutzen, wie die Mitarbeiter der Unternehmen. Das BYOD-Konzept funktioniert in den staatlichen Organisationen aber nicht, da der Datenschutz selten kultiviert wird und da die internen Regelungen zur Nutzung mobiler Geräte nicht ausreichend vorbereitet sind. Dadurch steigt der Anteil sowohl zufälliger als auch vorsätzlicher Datenverluste.

Fazit:

Die aufgeführten Angaben bestätigen die Behauptung (sh. auch für Branchen), dass die Verbreitung der DLP-Systeme vor zufälligen Datenverlusten schützt. Umso wichtiger ist die Problematik vorsätzlicher Datenverluste sowie die Ansätze zum Datenschutz. Bereits heute sollten schon neue Wege im Datenschutz und in den Anforderungen an DLP-Systeme gefunden werden.

Personendaten

Nach wie vor beziehen sich die meisten Datenverluste mit 89,4% auf Personendaten (im Vorjahr waren es 92,4%).

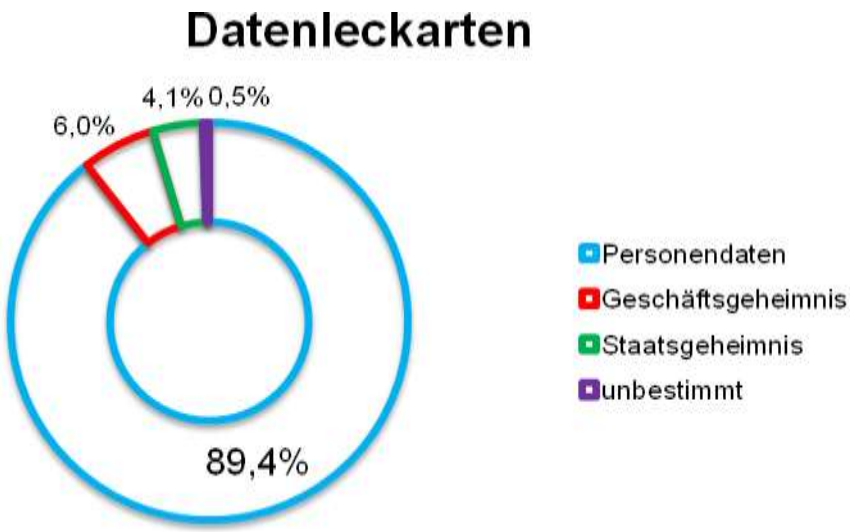


Bild 8.Verteilung der Datenverluste nach Datentypen 2011.

Uns sind die Datenverluste im Personendatenbereich bekannt, weil das Gesetz die Offenlegung der Vorfälle vorschreibt. Die Personendaten sind für böswillige Angreifer von Interesse, weil sie sich auf dem Schwarzmarkt gut verkaufen lassen. **Kommerzielle und staatliche Geheimnisse gehen meistens "auf Anfrage" verloren**. Können die Daten an viele Käufer verkauft werden, so finden Verluste von Massendaten statt.

2012 wurde eine Reihe von Vorfällen registriert, wo Geschäfts- und Staatsgeheimnis Angriffsobjekte waren. Meistens hat die Offenlegung eines Datenverlustes das Ziel, für den Geschädigten eine Rechtsverfolgung zu veranlassen. In den meisten Ländern wird man für Diebstahl von Geschäftsgeheimnissen verwaltungsmäßig oder strafmäßig haftbar gemacht. Als Folge **versuchen die Geschädigten Unternehmen die Daten verlieren (durch externe, böswillige Angreifer oder Mitarbeiter) mit aller Strenge des Gesetzes haftbar zu machen.**

Fazit:

Einer der Wege zur Eingrenzung der Entwendung von Daten ist, den Verkauf gestohlener Personaldaten zu erschweren und die Gesetzgebung zu verstärken. Dann können sich die Angriffe auf diese Daten bedeutsam reduzieren.

Kanäle für Datenverluste

Die Charakteristiken der Kanäle für Datenverluste werden praxisbezogen betrachtet. Abhängig vom Kanal des Datenverlustes (Datenträger) können Prioritäten bei der

Einführung der Datenschutzmaßnahmen gesetzt werden. In den Statistiken werden die Spezifikation des Unternehmens und dessen Informationsübertragungskanäle berücksichtigt.

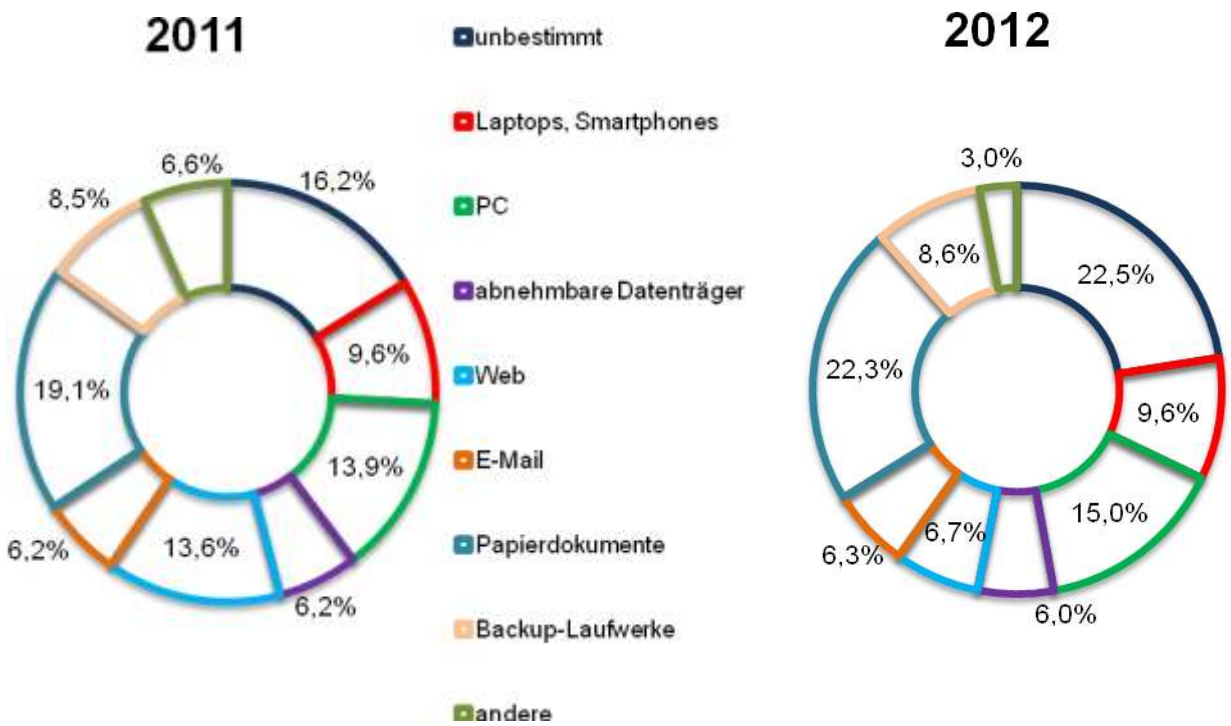


Bild 9.Verteilung der Datenlecke 2011 - 2012 nach Kanälen.

Die Datenschutzmaßnahmen verbreiten sich immer weiter, was dazu führt, dass die traditionellen Kanäle für Datenlücken, dort wo die Schutzmaßnahmen am effektivsten sind, immer weniger an Bedeutung gewinnen werden. Das trifft für die allgemeine Verteilung zu. Der Anteil der Datenverluste über das Web hat sich mit -6,7% um die Hälfte reduziert. Der Anteil der Datenverluste über den PC (+ 1%), mobile Datenträger (-0,2%) und E-Mails sind beinahe konstant geblieben.

Die geringste Veränderung gab es bei den Datenverlusten aufgund von Papierdokumenten. Merkwürdigerweise sind heute die organisatorischen Maßnahmen die schwächste Stelle der Datensicherheit. 2012 wuchs dieses Thema um 3% und betrug 22,3% von allen Datenlücken.

Die Datenverluste aus E-Mails betrugen insgesamt 6,3%. Dieser Kanal, wie auch das Web ist der beliebteste Datenübertragungskanal. Die hohe Anzahl der Datenlücken bei E-Mails von 2007 bis 2009 führte dazu, dass dieser Kanal nun ernsthaft von Unternehmen überwacht wird. Die Zahl der Datenverluste über E-Mails hat sich reduziert, obwohl sich die Gefahr noch nicht als gebannt einschätzen lässt. Nach wie vor ist der E-Mail-Kanal dank seiner Einfachheit der Beliebteste und der Anteil der bekannten Vorfälle ist sehr hoch. Vielleicht ist das der Grund warum die Zahl der Datenlücken über diesen Kanal nicht so hoch ist, als man annehmen könnte.

Im Laufe der letzten drei Jahren wies InfoWatch unablässig auf die Gefahren von Datenverlust über mobile Datenträger hin. Mobile Geräte gehen oft verloren, aber wir können heute auf die Nutzung dieser Geräte kaum verzichten. Daher wäre es wichtig organisatorisch und technisch festzulegen, was auf mobilen Geräten gespeichert werden darf. Auf mobilen Geräten sollten ohne wichtigen Grund keine vertraulichen Informationen gespeichert werden - wenn doch, dann nur in verschlüsselter Form. Alleine die Beachtung dieser Regeln würde im BYOD-Zeitalter eine Großzahl der Vorfälle ausschließen.

Schauen wir uns einmal an, wie sich die zufälligen und die vorsätzlichen Datenlücken bei verschieden Datenträgertypen unterscheiden.

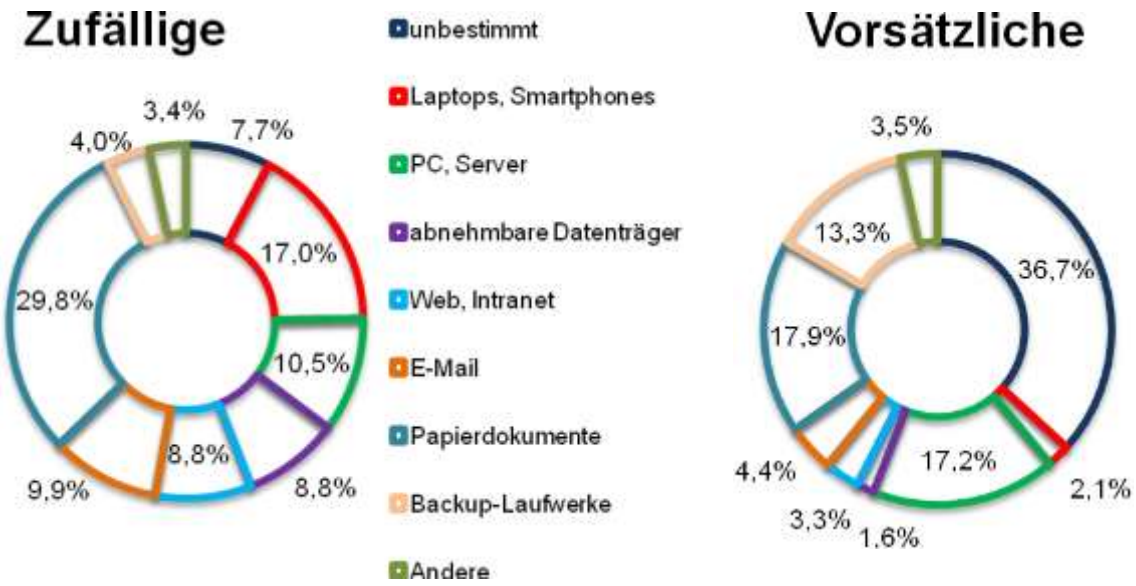


Bild 10.Verteilung der zufälligen und vorsätzlichen Datenlücken 2012 nach Kanälen.

Es liegt eine Großzahl von Datenverlusten über unbestimmte Quellen vor, was für vorsätzliche Datenverluste spricht.

Die Lage bei Sicherungskopien sieht schlecht aus. Eine hohe Prozentzahl (13,3%) der vorsätzlichen Datenverluste über diesen Kanal spricht für die mangelnde Beachtung der Archive von Sicherheitsdiensten (Backups). Leider verfügen nur wenige Backup-Geräte über eine integrierte Verschlüsselung. Es ist manchmal auch einfacher, ein Archivlaufwerk als einen ständig benutzten Datenträger zu entwenden.

Der Kanal PCs und Server ist besonders hervorzuheben. Hier kommt es oft zu vorsätzlichen Datenverlusten über Arbeitsstationen und Server. In der Regel ist das auf die Netzwerkadministratoren zurückzuführen. Buchhalter und Systemadministratoren sind meistens die Personen, die bei Offenlegung von vorsätzlichen Datenverlusten genannt werden. Die Systemadministratoren haben oft einen unbegrenzten Zugang auf die Netzwerkdaten des Unternehmens und nutzen diese Möglichkeit, um Personendaten an Dritte zu verkaufen oder Informationen an den Wettbewerb zu übergeben.

Der zufällige Datenverlust aus E-Mails beträgt ca. 10%, über Smartphones durch Geräteverlust 17,0%, und 8,8% beim Verlust von mobilen Datenträger.

Ein Drittel zufälliger Datenverluste erfolgt über Papierdokumente. Die modernen DLP-Systeme können alle Dokumente, die zum Drucker gesendet werden, prüfen und die Anwesenheit der Person im Büro bestätigen, welche den Ausdruck bekommen möchte. Jedoch nachdem gedruckt wurde, ist es sehr kompliziert, den weiteren Weg des Dokuments zu verfolgen. Die Nachverfolgung eines Papierdokuments ist eher durch ein organisatorisch-rechtliches Verfahren möglich als durch ein technisches Verfahren.

Fazit:

Die Ergebnisse zeugen dafür, dass die DLP-Entwickler heute vor neuen Herausforderungen stehen. Der geschützte Umkreis eines Unternehmens ist heute ein Begriff von gestern. Die Sicherheitssysteme müssen heute einen Datenschutz sowohl innerhalb als auch außerhalb einer Infrastruktur gewährleisten. Es ist heute notwendig, dass DLP-Systeme die unternehmenseigenen Daten auch im globalen Netz auffinden und kontrollieren können.

Regionale Besonderheiten

Die regionale Verteilung der Datenlücken war in diesem Jahr wie erwartet. Die USA stehen an erster Stelle sowohl bei der Gesamtzahl mit 576 oder 61,7% von allen Datenlücken als auch im aggregierbaren Wert (pro Kopf-Wert). An der zweiten Stelle liegt Großbritanien mit 97 Vorfällen oder 10,3%. An der dritten Stelle ist Russland mit 75 Vorfällen oder 8,3%. Wir erinnern daran, dass Russland nicht zum ersten Mal eine der führenden Positionen bekleidet. Im Vorjahr war Kanada an der dritten Stelle und im Jahr 2010 hatte Russland ebenfalls die "Bronzemedaille".

Anzahl der offengelegten Datenlecke pro eine Million Bevölkerung

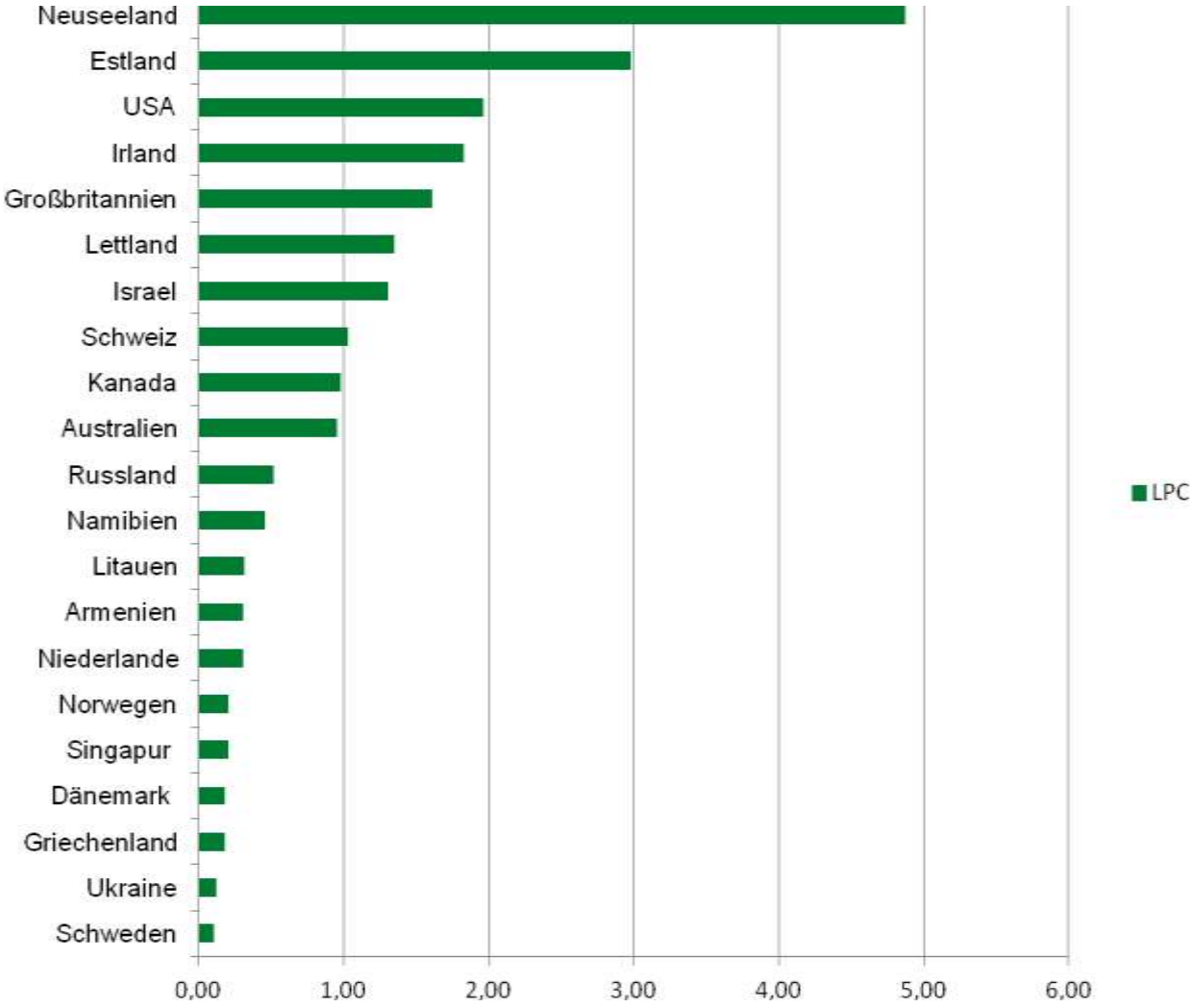


Bild 11. Verteilung der Datenlücken 2012 nach Ländern.
Länder geordnet nach Datenlückenanzahl pro eine Million Bevölkerung (LPM).

Anzahl der offengelegten Datenleche, St.

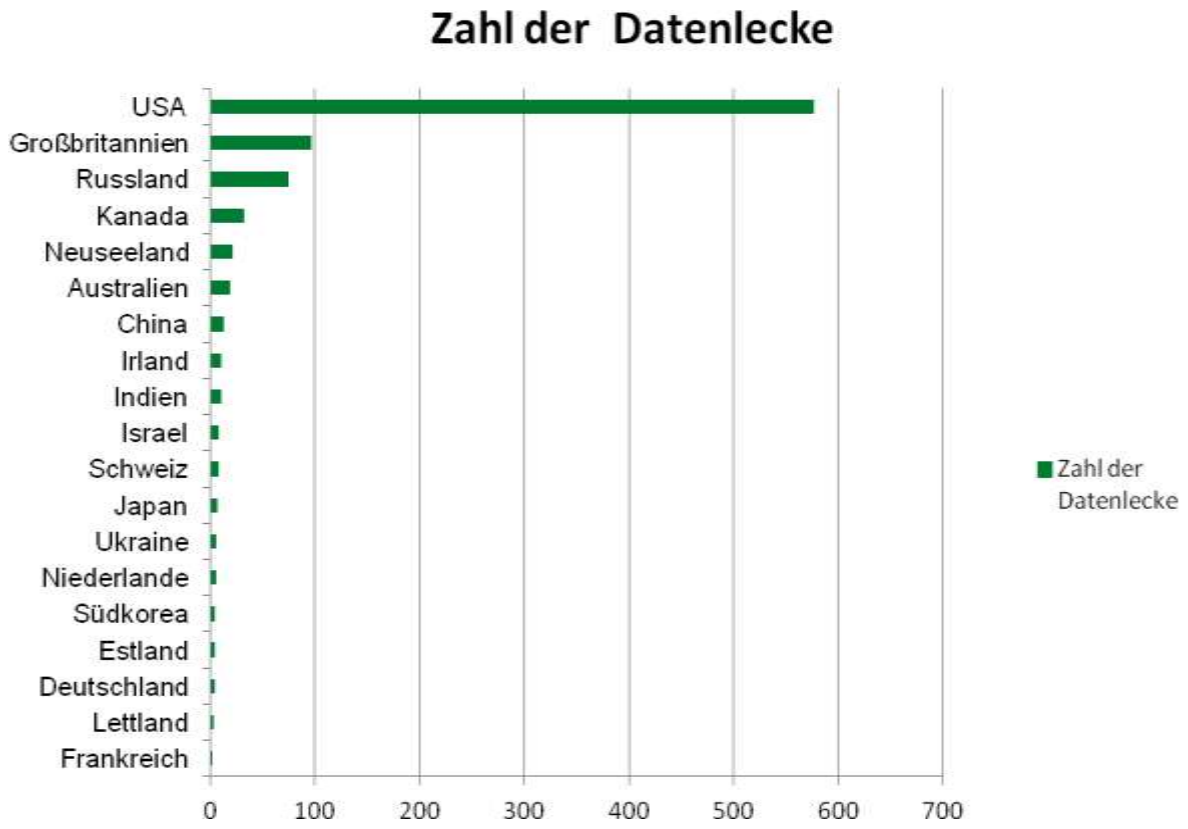


Bild 12. Datenlückenverteilung 2012 nach Ländern.

Deutschland

Im vergangenen Jahr 2012 konnte das Analysezentrum InfoWatch einige wichtige Veränderungen bei den Datenverlusten im deutschsprachigen Raum (Deutschland, Österreich, Schweiz) feststellen. Insgesamt ist eine deutlich wachsende Tendenz bei Angriffen in genannter Region zu erkennen, welche zum Verlust von Personendaten führten. Der größte Anteil der Vorfälle hat eher das Ziel, die Wirksamkeit der Datenschutzsysteme zu überprüfen und deren Schwächen herauszufinden. Solche Vorfälle sind üblicherweise nicht das Objekt einer solchen Studie, weil diese nur die Datenlücken berücksichtigt, welche in den Organisationen infolge von böswilligem oder fahrlässigem Verhalten der Mitarbeiter passierten und nicht ein Resultat eines Angriffes Externer sind . Also schaute die Situation 2012 in Deutschland wie folgt aus.

Typen von Datenlücken

2011 waren die Personendaten mit 82,6% führend und 2012 hat sich die Situation auf radikale Weise verändert. Die Verteilung der Datenlücken nach Typen der bloßgestellten Daten wurde homogener. Jede der folgenden Arten von vertraulichen Daten hat einen Anteil von 30%: Personendaten, Geschäftsgeheimnis und medizinische Daten. Vor dem Hintergrund einer stark abgenommenen Anzahl der Vorfälle mit Personendaten sind medizinische Daten (von 4,4% bis 30%) und Geschäftsgeheimnis (von 13% bis 30%) stark angewachsen. Eine deutliche Minderheit bilden mit 10 % die juristischen Daten.

Verteilung nach Kanälen für Datenlücken

Die Verteilung nach den Kanälen für Datenlücken weist eine umgekehrte Tendenz auf, und zwar von einer homogeneren zu überwiegend gedruckten Papierdokumenten, die einst in den Papierkorb geraten sind (30% der Datenlücken 2012 im Vergleich zu 8,6% 2011). Durch das Speichern auf mobilen Datenträgern entstand ein neuer Kanal für Datenlücken, welcher 2011 noch keine große Rolle spielte. Es ist vielleicht auf die fortgeschrittene Einführung von BYOD und steigende Mobilität der Unternehmen zurückzuführen. Die Bedeutung des Kanals Emails sank ein wenig (überwiegend zufällige Datenverluste) von 26,1% auf 20%. Zu 10% entwendet man Unternehmen die Daten durch den Diebstahl von Backups.

Nachstehend sind die bedeutsamsten Vorfälle bei vertraulichen Informationen in Deutschland aufgeführt.

Spionageverdacht im Gesundheitsministerium 12.2012

Spionage im Gesundheitsministerium? Ein Mitarbeiter, der jahrelang im IT-Bereich des Bundesgesundheitsministeriums gearbeitet hat, soll wichtige Unterlagen nach außen getragen haben. Ein Sprecher des Gesundheitsministeriums sagte dem *ARD-Hauptstadtstudio*, dass die Berliner Staatsanwaltschaft gegen einen externen Mitarbeiter ermittle. Offenbar wurde auch der Arbeitsplatz des Mitarbeiters im Ministerium von der Staatsanwaltschaft durchsucht.

Geld für Infos, Daten, Gesetzentwürfe

Der IT-Mitarbeiter soll E-Mails, Beschlüsse, Gesetzesentwürfe und andere Daten übermittelt und dafür Geld kassiert haben. Zahlender Empfänger soll ein Lobbyist der Apothekerschaft gewesen sein. Das berichtet die "Süddeutsche Zeitung". Die Berliner Staatsanwaltschaft habe dem Blatt entsprechende Ermittlungen bestätigt.

Ziel des Lobbyisten sei offenbar gewesen, sich über geheime Gesetzgebungsvorhaben im Pharma- und Apothekenbereich zu informieren und mit diesem Informationsvorsprung Gegenstrategien ergreifen zu können. Die Ausforschung soll 2010 begonnen und sich bis in das laufende Jahr hingezogen haben, berichtete das Blatt. Im November habe die Staatsanwaltschaft zugegriffen und Büro und Privatwohnungen durchsucht.

Lobby-Skandal?

Nach Informationen der Zeitung waren auch E-Mails aus der Leitungsebene betroffen - also Nachrichten, die von den Ministern Philipp Rösler und Daniel Bahr, ihren Staatssekretären und engsten Mitarbeitern stammten.

Bahr äußerte sich verärgert: "Ich bin stinksauer über diese kriminelle Energie", sagte der FDP-Poltiker der "Bild"-Zeitung. Die Staatsanwaltschaft müsse den Fall "schnell aufklären". Trifft der Verdacht zu, dürfte es sich nach "SZ"-Einschätzung um den größten Lobby-Skandal in der Berliner Republik handeln. Die Apotheker-Vertretung Abda äußerte sich bislang nicht zu dem Fall.

Quelle

Patientendaten geklaut 10.2012

Dieses Datenleck betrifft 300000 Datensätze

Am 19.09.2012 soll aus zwei Baden-Württembergischen Krankenhäusern in Rastatt Patientendaten gestohlen worden sein. Zu den Unterlagen gehören neben Angaben zur Person vor allem ärztliche Befunde.

Der stellvertretende Landesbeauftragte für Datenschutz, Peter Diekmann, sagt dazu: „Wir müssen von einer sechsstelligen Zahl ausgehen". Eine Anzeige gegen Unbekannt wurde eingeleitet.

Die Daten sollen während einer Raucherpause verschwunden sein. Ein Mitarbeiter der IT hatte diese auf dem Weg vom Serverraum zum Tresor eingelegt und zu diesem Zweck einen Karton mit Sicherheitskopien auf Bändern in einem Gang abgestellt. Später war der Karton nicht mehr auffindbar.

13.12.12 Update. Die Polizei konnte trotz umfangreicher Ermittlungen nicht herausfinden, wer im September die Sicherungsbänder mitgenommen hatte. Auch ein Motiv konnte nicht geklärt werden. Der Karton mit den Bändern ist bis heute ebenfalls verschwunden geblieben. Die Ermittler schließen nicht aus, dass ein Unbekannter den Karton unwissentlich als Abfall mitgenommen und entsorgt hat. Der beauftragte Mitarbeiter hatte die Box mit den Sicherungsbändern mit rund 300.000 Patientendaten des Krankenhauses kurz unbeaufsichtigt abgestellt – als er zurückkam, waren sie verschwunden.

Quelle

Ermittlungen gegen Bankkunden: Panne führte Steuerfahnder zur Credit Suisse 07.2012

Wie kamen die Steuerfahnder an die Kundendaten der Credit Suisse? Zeitungsberichten zufolge haben sie nichts für die Informationen bezahlt. Auslöser für die Ermittlungen war offenbar das peinliche Versehen eines Bankmitarbeiters.

Berlin - Die Ermittlungen gegen Tausende Credit-Suisse-Kunden sollen auf eine Datenpanne bei der Bank in Frankfurt zurückgehen. Wie die "Welt" berichtet, soll ein

Mitarbeiter entgegen den Anweisungen der Bank eine Datei überspielt haben, als er von einem Arbeitsplatz in der Schweiz nach Deutschland wechselte. Bei einer Razzia im Februar 2011 am Deutschlandsitz in Frankfurt seien die Daten dann sichergestellt worden.

Aufgrund der Hinweise haben die Ermittler bundesweit Häuser und Wohnungen von 5000 Credit-Suisse-Kunden durchsucht. Sie sollen mit Hilfe von Scheinversicherungen mehrere Milliarden Euro an Steuern hinterzogen haben. Das Geld soll über die Tochterfirma Credit Suisse Life gelaufen sein. Diese hat ihren Sitz auf den Bermudas. Ein Banksprecher sagte, es handle sich um legale Produkte, die von vielen Instituten angeboten würden. Kunden aus Deutschland seien darauf hingewiesen worden, dass die Steuerpflicht bei ihnen selbst liege.

Hintergrund der Ermittlungen war offenbar eine Datenpanne Anfang Juni. Wenige Tage danach erhielten die ersten Bankkunden laut "Handelsblatt" einen Brief vom Finanzamt. Darin heißt es, der Behörde liege "Kontrollmaterial zur weiteren Prüfung vor". Demnach komme die angeschriebene Person "als möglicher Auslandsanleger in Betracht". Man mache darauf aufmerksam, dass Steuerzahler "zur Mitwirkung bei der Ermittlung ihrer steuerlichen Verhältnisse verpflichtet seien". Im Falle einer Weigerung könne das Finanzamt "Zwangsmaßnahmen herbeiführen".

Die Credit Suisse rät ihren Kunden der Zeitung zufolge nun, sich von einem Anwalt beraten zu lassen und gegebenenfalls Selbstanzeige zu erstatten.

SPD-Finanzexperte Joachim Poß sagte der "Welt": "Der Fall Credit Suisse bekräftigt unsere Ablehnung des Steuerabkommens mit der Schweiz." Es gehe bei dem Abkommen in der Tendenz darum, die effizienten Instrumente der Steuerfahnder aus dem Verkehr zu ziehen.

Steueranwalt Karsten Randt sagte der Zeitung, falls der Bundesrat dem geplanten Steuerabkommen mit der Schweiz zustimme, wären alle jetzt eingeleiteten Ermittlungen hinfällig. Die Steuerhinterzieher müssten dann lediglich die im Abkommen vorgesehenen Abschläge auf ihr Vermögen nachzahlen.

Quelle

Personendaten auf der Straße 05.2012

Panne bei Tübinger Weiterbildungsfirma

Durch eine Panne lagen Unterlagen mit personenbezogenen Daten einer Tübinger Firma für berufliche Bildung auf der Straße herum.

Tübingen. Als ein aufmerksamer Passant am Samstag gegen 12 Uhr durch die Tübinger Ulrichstraße Richtung Innenstadt zum Einkaufen ging, traute er seinen Augen nicht. Auf dem Gehweg fanden sich, so erzählt er, vor dem dortigen Büro der Firma Team-Training zwischen Reißwolf-Schnipseln vollständige vertrauliche Schriftstücke, zumeist Original-Verträge. Sie ließen sich alle auf den ersten Blick dem Bildungsunternehmen zuordnen und waren für die Altpapiersammlung in der Südstadt an diesem Tag vorgesehen.

An der Seite standen aufgerissene Säcke, vermutlich in der Nacht zuvor mutwillig, aber wohl ohne Wissen um den Inhalt zerstört. Der Passant übergab ein paar Belege ans SCHWÄBISCHE TAGBLATT und stopfte den Rest zur Sicherheit durch den Briefkastenschlitz in den Hausflur der Firma, wie er sagt. Ob weitere Schriftstücke vorher in falsche Hände gekommen sind, ist nicht nachprüfbar.

Team-Training gibt es seit dem Jahr 1997. Die größten Geschäftsfelder sind nach eigener Darstellung die berufliche Qualifizierung und Weiterbildung sowie die Personalberatung und -vermittlung. Die GmbH mit 19 Festangestellten und 80 freien Mitarbeitern ist an 16 Standorten in neun Städten in den Landkreisen Tübingen, Reutlingen, Zollernalb und im Großraum Stuttgart tätig. Die Bundesagentur für Arbeit, Land, Bund und auch die EU stehen auf der Liste der Auftraggeber und Projektpartner.

Zu den vielfältigen Angeboten gehört die Qualifizierung und Vermittlung von Langzeitarbeitslosen im Auftrag der Bundesagentur für Arbeit. Bei den auf dem Gehweg gefundenen Dokumenten handelt es sich um Verträge über Praktika und um Bestätigungen von erfolgreichen Arbeitsvermittlungen aus dem Jahr 2008. Zu erkennen sind Namen und Anschriften der jeweiligen Personen. In mindestens einem Fall ist auch eine dreiseitige Kopie einer Praktikums-Beurteilung angeheftet.

Geschäftsführer Cornelius Ambros zeigte sich, vom SCHWÄBISCHEN TAGBLATT auf die Panne hingewiesen, „schockiert“. Er wirkte hörbar betroffen und sagte: „Das tut mir

unendlich leid.“ Er sprach von einem „Riesenmissgeschick“. Die Abläufe seien eigentlich klar. Seine Firma werde regelmäßig – auch im Hinblick auf Datenschutz – überprüft und zertifiziert. Ferner gebe es eine Datenschutzerklärung, die jeder unterschreiben müsse.

Doch ein Mitarbeiter habe den Auftrag des Schredderns schlichtweg nicht vollständig ausgeführt, erklärte Ambros. Ein zweiter Mitarbeiter habe die Papiersäcke zwar kontrolliert, aber nur von oben hineingeschaut. Und dort seien bloß Schnipsel zu sehen gewesen. Team-Training hat nach eigenen Angaben alle Geschäftspartner über die Panne informiert. Der Geschäftsführer versprach, dass solch eine Datenpanne nicht wieder vorkomme. Künftig gebe es „kein Altpapier mehr an keinem Standort“. Schon bisher würden mehr als 90 Prozent aller Unterlagen bei einem professionellen Entsorger in Reutlingen vernichtet. Dort gebe es dann auch eine Bestätigung des Schredderns. Warum nicht 100 Prozent? Das sei ein Fehler gewesen, gab Ambros zerknirscht zu.

Es hätte für Team-Training noch schlimmer kommen können. Dann nämlich, wenn Paragraf 42a des Bundesdatenschutzgesetzes verletzt worden wäre (siehe Kasten). Dann hätte die Firma ein saftiges Bußgeld zu fürchten, erklärte der Landesdatenschutzbeauftragte Jörg Klingbeil auf TAGBLATT-Anfrage. Nun liege lediglich ein „Verstoß gegen die technisch-organisatorischen Maßnahmen“ vor. „Wo Menschen arbeiten, passieren Fehler“, sagte der Datenschutzexperte, will aber Pannen wie die in Tübingen nicht verharmlost wissen: „Das ist keine lässliche Sünde.“

Quelle

OÖ: Gerichtsakten von Missbrauchsfall "geleakt" 03.2012

Die Veröffentlichung vertraulicher Dokumente über die Umwege des Internets ist mittlerweile ein wichtiger Teil des Aufklärungsjournalismus. Dass das Prinzip für Unschuldige allerdings viel Ärger und Frustration bedeuten kann, mussten nun mittlerweile erwachsene Missbrauchsopfer aus dem Salzkammergut erfahren.

Mitte der 90er kam ihr Missbrauchsfall vor Gericht, doch vor knapp einem Jahr tauchten Videos der Gerichtsakten auf der Videoplattform Youtube auf. Zu den abgefilmten Inhalten

gehörten Nacktfotos der Opfer aus ihrer Jugendzeit und Zeugenaussagen neben den jeweiligen Namen. Eine Mutter, welche für die Löschung der Daten kämpfte, erklärte gegenüber orf.at, die Polizei sei in solchen Fällen „machtlos“.

Erst eine – nicht genannte – Wiener Anwaltskanzlei konnte nach rund 13 Monaten die fragwürdigen Inhalte vom Netz nehmen lassen, zur Freude der Betroffenen. Der mutmaßliche Täter ist zugleich der Hauptangeklagte in dem Missbrauchsfall: Gegenüber dem ORF soll er bereits gestanden haben, die Gerichtsakten online gestellt zu haben.

Jedoch kann die Staatsanwaltschaft trotz bereits laufender Ermittlungen keine Klage erheben, da die Höchstfreiheitsstrafe für das Veröffentlichen von Gerichtsakten bei 6 Monaten liegt, für die Auswertung der notwendigen Daten allerdings eine höhere Strafandrohung nötig wäre.

Quelle

Patientenakten im Sperrmüll 03.2012

Der Klinikkonzern Asklepios verklappt sensible Daten von Tausenden Patienten im Abfallcontainer. Der Datenschutzbeauftragte ist entsetzt - und machtlos.

HAMBURG | *taz* Deutschlands größter privater Krankenhauskonzern Asklepios, der allein in Hamburg zehn Kliniken betreibt, hat höchst sensible Patientenakten gleich kistenweise im Sperrmüllcontainer entsorgt. Notfallberichte und Abrechnungsberichte mit Tausenden von personenbezogenen Daten lagerten tagelang im offenen Container unter freiem Himmel, direkt neben einem von Spaziergängern stark genutzten Wanderweg am Rande des früheren Klinikgeländes in Hamburg-Eilbek. Hamburgs Datenschutzbeauftragter Johannes Caspar schlägt die Hände über dem Kopf zusammen: „Patientenakten im Müll sind einer der größten anzunehmenden Unfälle für eine Klinik.“

Neben ausgedienten Möbeln und Schrott befanden sich in dem von der Stadtreinigung aufgestellten Container mindestens fünf Kartons, randvoll mit alten Notfallberichten und Abrechnungsunterlagen mehrerer Krankenhäuser, darunter das AK Eilbek, das AK Harburg und das Klinikum Nord/Heidberg.

In den Ordnern befinden sich Diagnosen und Krankheitsvorgeschichten von mehreren Tausend Personen, die alle mit vollem Namen und Wohnort in den Berichten vermerkt sind. Briefwechsel mit dem Finanzdienstleister „Aktivia“ klären darüber auf, bei welchen Patienten eine Privatinsolvenz vorliegt. Hinweise auf Ehestreitigkeiten finden sich genauso in den Notfallberichten wie pikante Atteste in der Korrespondenz mit den Krankenkassen, aus der man etwa erfährt, das ein Patient aus Seevetal wohl unter einer „affektiven Psychose“ leide.

Am Dienstag hatte ein passionierter Sperrmüllsammler die taz von der brisanten Zwischenlagerung informiert. Der Mann hatte, wie nach seiner Aussage auch andere Spaziergänger, einen Blick in den Container gewagt, der zwar stattliche 2,60 Meter hoch ist, aber durch eine in dem Behälter eingelassene Stufenleiter leicht erklimmbar ist und dessen Seitenflügel zudem problemlos geöffnet werden kann.

Das Sperrmüllgefäß befindet sich direkt neben dem ehemaligen „Haus 33“ des Eilbeker Krankenhauses, in dem bis vor kurzem die Hamburger Abrechnungsstelle von Asklepios untergebracht war. Aus ihrem Bestand stammen nach taz-Recherchen die brisanten Unterlagen.

Während eine Sprecherin der Hamburger Gesundheitsbehörde sich am Freitag zu dem Vorfall nicht äußern wollte, wird Caspars Stellvertreter Hans-Joachim Menzel deutlich. „Das geht überhaupt nicht, das Patientendaten so gelagert werden“, betont Hamburgs Datenschutz-Vize. Für einen ungehinderten Zugang zu den sensiblen Daten habe es „kaum Schwellen“ gegeben. Menzel bewertet die Open-Air-Lagerung als „Verstoß gegen die ärztliche Schweigepflicht“.

Doch die wird vermutlich ungeahndet bleiben. Nachdem der Datenschutzbeauftragte die Polizei informiert hatte, stellte diese am Mittwoch die Akten sicher, sieht aber „keine Anhaltspunkte für eine Straftat“, so ihr Sprecher Andreas Schöpflin.

Auch der Datenschutzbeauftragte ist weitgehend machtlos. Er prüft derzeit „die Einleitung eines Bußgeldverfahrens“ gegen Asklepios wegen eines eklatanten „Verstoßes gegen Datenschutzrichtlinien“, muss es aber möglicherweise mit einer Rüge bewenden lassen. „Das ist für uns unbefriedigend“, sagt Johannes Caspar, der einen dringenden „legislativen Handlungsbedarf“ bei solch schwerwiegenden Verstößen gegen gültige Datenschutzrichtlinien sieht.

Denn diese sind unbestritten. Auch Asklepios-Sprecher Rudi Schmidt bestätigt, es seien „überwiegend Patientenunterlagen“ gewesen, die „ungeplant“ in dem Container gelandet seien. Schmidt: „Diese waren zur Vernichtung vorgesehen und sollten eigentlich im benachbarten Sicherheitscontainer sein“, der fest verschlossen ist. Merkwürdig daran: Mindestens einen Deckel der zur Sofortvernichtung vorgesehenen Ordner ziert ein „Vorblatt für Aktenarchivierung“ mit der Aufschrift: Aufbewahrung bis 12/2013“. Warum die Dokumente im falschen Container landeten, sei „noch nicht abschließend geklärt“, sagt Schmidt. Der Asklepios-Sprecher weiß nur: „Da ist etwas ziemlich schief gelaufen.“
Während für sein Unternehmen der Akten-GAU wohl ohne rechtliche Konsequenzen bleibt, übt sich der Konzern inzwischen in Drohgebärden gegenüber denjenigen, die den Datenskandal nun ans Licht bringen. Asklepios stellte Strafanzeige gegen den taz-Reporter, der den Datenschutzbeauftragten informierte und Einsicht in die öffentlich zugänglichen Unterlagen nahm. Der Vorwurf: „Ausspähen von Geheimnissen“.
Quelle

Datenleck am Landesgericht Wr. Neustadt 02.2012

Wiener Neustadt. Das Landesgericht Wiener Neustadt hat bei den Sammelklagen gegen den Ex-AvW-Wirtschaftsprüfer Moore Stephens Ehrenböck mit Sitz in Gloggnitz ein massives Datenschutzproblem. Unter der Internet-Adresse 5n0w.net bzw. über Google sind Daten von Hunderten AvW-Anlegern, ihre Forderungen, die Namen ihrer Anwälte und die Gerichtsbeschlüsse über Verfahrenszusammenlegungen öffentlich einzusehen. "Wir haben das entdeckt, wir sind aus dem Schaudern nicht mehr herausgekommen", sagt AvW-Anlegeranwalt Erich Holzinger, der mit seinem Kollegen Michael Bauer rund 900 Geschädigte mit etwa 32 Sammelklagen vertritt. "Eine Klientin hat uns am 6. März angerufen und gesagt, warum sie, wenn sie im Internet ihren Namen in die Google-Suchmaschine eintippt, in einer Klage am Gericht in Wiener Neustadt aufscheint." Bauer und Holzinger sind dann dem Datenleck im Web auf den Grund gegangen und haben besagte Gerichtsdokumente heruntergeladen.

"Wir kannten dadurch die Gerichtsbeschlüsse schon aus dem Internet, bevor wir sie vom Gericht zugestellt erhielten", sagt Bauer zur "Wiener Zeitung". "Ich glaube nicht, dass hier vorsätzlich gehandelt wurde, aber so etwas darf nicht passieren."

Datenschutz-Desaster

Wer über die Suchmaschine Google zum Beispiel den Namen "Holzinger" und "MSE" für die gerichtliche Aktenverwaltung eintippt, konnte am Dienstag die Daten eines Anleger-Ehepaars aus Stein an der Enns abrufen, die per Klage vom Ex-AvW-Wirtschaftsprüfer 30.782,50 Euro einfordern. Auch Josef U. (Streitwert: 102.480 Euro), Marina M-D. (Streitwert: 8119 Euro), Erich N., Josef D., Helga P. und Hunderte weitere Anleger finden sich in den Suchergebnissen zu 5n0w.net/beschluss/.

Die "Wiener Zeitung" konfrontierte die Wiener Neustädter Landesgerichtspräsidentin Ingeborg Kristen mit dem Datenleck, die davon nichts wusste. Sie kontaktierte Richter Peter Wöhrer, der besagte interne Homepage konzipierte: "Willkommen beim Aktenverwaltungssystem für die Massenverfahren AvW vs. Wirtschaftsprüfer", hieß es auf der Seite "MSE Akten Verwaltung", die infolge der Recherchen der "Wiener Zeitung" abgeschaltet wurde.

Richter Wöhrer suchte am Dienstag eine Erklärung für die desaströse Datenschutzpanne. "Eine meiner Vermutungen ist, dass es diese Adresse 5n0w.net gegeben hat, für die es eine alte Registernummer gibt. Sie ist aus welchen Gründen auch immer nicht gelöscht worden", sagt Richter Peter Wöhrer zur "Wiener Zeitung". Er nimmt daher an, dass die neue interne IP-Adresse für die "MSE Aktenverwaltung" am Server direkt zu der alten Adresse 5n0w.net führt. Trotz Blockierung der Homepage können die Daten weiterhin über Google abgerufen werden. Wöhrer: "Wenn es eine alte Verlinkung mit Google gibt, dann hat Google eben auf dieser Adresse wieder vorbeigeschaut."

Indes hat AvW-Anlegeranwalt Bauer am Dienstag die Datenschutzverletzung beim Landesgericht Wiener Neustadt angezeigt, Auskunft über das datenschutzwidrige Vorgehen eines Organs der Gerichtsbarkeit und die Löschung der unzulässigerweise verarbeitenden Daten verlangt.

Quelle

Datenleck: "Wie in der Steinzeit der EDV" 02.2012

Wien/Hamburg. Ein bedauerlicher Einzelfall einer Mitarbeiterin sei es gewesen - so argumentierte die Verwaltung des Hamburger Fondsgiganten MPC-Capital. Wie die "Wiener Zeitung" berichtete, wurden in einem Excel-Dokument mehr als 1600 vertrauliche Anleger-Daten - inklusive Investitionssumme und Steuernummer - an einen Kunden in Wien verschickt. Eine Panne, die a priori verhindert hätte werden können, meint hingegen der Datenschutzexperte Hans G. Zeger (Arge Daten). Das betroffene Unternehmen, das ein beachtliches Investitionsvolumen von 18,7 Milliarden Euro repräsentiert, hätte nur etwas Geld in EDV-Sicherheit investieren müssen.
Zeger findet es ein schweres Versäumnis, immer noch vertrauliche Daten als Attachement zu verschicken: "Das ist überhaupt nicht mehr Stand der Technik - und zwar schon seit zehn Jahren", so Zeger. Schuld seien dabei die Firmen, die "Leute anstellen, die EDV-mäßig immer noch in der Steinzeit sind und dauernd Daten per Mail hin- und herschicken". Zugleich gebe es mehrere Möglichkeiten, solche Irrläufer wie bei MPC-Capital auszuschließen: "Man kann das ganz leicht verhindern, indem man etwa überhaupt Datei-Anhänge verbietet. In einer sensitiven Umgebung muss man eben Bequemlichkeit zugunsten der Sicherheit zurückschrauben", sagt Zeger. Eine andere Möglichkeit ist eine Art Virenscanner, der abgehende Mails auf bestimmte Muster untersucht und gegebenenfalls blockiert. "Viele Unternehmen verwenden solche Filterprogramme zum Schutz vor Betriebsspionage."
Warum das selbst bei großen Firmen nicht passiert? "Schlicht aus Bequemlichkeit!"
Beschwerde wird überlegt
Der unfreiwillige Empfänger des Datensatzes will nun übrigens die heimische sowie die deutsche Datenschutzbehörde einschalten: "Dass es ein Einzelfehler war, klingt sehr nach Ausrede. Bei guten Sicherheitssystemen kann so etwas nicht passieren", argumentiert der Wiener. Laut Eva Souhrada-Kirchmayer von der Österreichischen Datenschutzkommission ist die Chance gering: "Wenn das wirklich nur, passiert ist, wäre das nach dem Datenschutzgesetz nicht strafbar." Es fehle nämlich der Vorsatz.

Quelle

Schludriger Umgang mit Passwörtern 01.2012

Peinliche Panne: Rund 49.000 Gesundheitsakten der "Médico-sportif" wurden gestohlen. Jemand hatte sein Passwort liegen lassen. Das Sportsministerium hat das Centre informatique de l' Etat angewiesen Anzeige zu erstatten.

Knapp 49.000 Datensätze der "Médico-sportif"-Datenbank sind durch Nachlässigkeit gestohlen worden. Es handelte sich dabei um persönliche Informationen, die eigentlich nicht an die Öffentlichkeit hätten gelangen dürfen. Dies bestätigte am Donnerstagnachmittag Justizminister François Biltgen in einer eilig herbeigerufenen Pressekonferenz. Es wurde Anzeige gegen Unbekannt erstattet. Die Ermittlungen laufen, heißt es, ohne Details zu nennen.

Es handle sich hierbei nicht um einen Hacker-Angriff, sondern um einen menschlichen Fehler, versuchte der Minister zu beschwichtigen. Ein Angestellter habe im Büro ein Passwort vergessen. Damit verschaffte sich wenig später eine unbekannte Person Zugriff auf die ärztlichen Gutachten der vergangenen sieben Jahre.

Kein besonderer Schutz

Das staatliche Informatik-System sei offen. Beamte könnten von Zuhause auf das interne System zugreifen. Allerdings braucht man dafür ein USB-Stift, Passwort und eine Kenn-Nummer. Dies wird von der Piratenpartei heftig kritisiert. Der Personenkreis, der Einblick zu den Daten erhält, muss strengsten Kriterien unterliegen, heißt es.

Bristant ist, dass die sensiblen Datensätze keinem besonderen Schutz unterlagen. "Die gestohlenen Daten waren nicht durch Luxtrust geschützt," so Biltgen. In diesem Zusammenhang sei jetzt die Sicherheit erhöht worden. Zudem seien die Mitarbeiter aufgefordert worden ihre Passwörter auszutauschen.

Weitere Untersuchungen laufen

Ob weitere Datensätze aus anderen staatlichen Instanzen abgezogen wurden ist unklar. Hier laufen derzeit die Untersuchungen. Wann der Datendieb zugeschlagen hat ist ebenfalls unklar. Alle Staatsbeamten sollen in Zukunft in Kursen auf die Gefahren durch Datendiebstahl "sensibilisiert" werden.

Heftige Kritik gab es Stunden zuvor von der Piratenpartei. Die Piraten sprechen von einem fahrlässigen Umgang mit den sensiblen Daten. Sie kritisieren die unprofessionellen und unseriösen Sicherheitsstandards beim Speichern solcher Daten.

Die Philosophie der Regierung in Sachen Datenschutz müsse sich nach Ansicht der Piraten grundlegend ändern. Sie verweisen dabei auf zukünftige Großprojekte wie Schülerdatenbank, e-Perso oder e-Santé.

Quelle

Golem.de **01.2012**

Ich versuche derzeit mit dem Rauchen aufzuhören. Deswegen bestellte ich schon zweimal Nikotinpflaster bei einer deutschen Online-Apotheke. Die Bestellungen liefen zweimal unproblematisch und kamen schnell. Bei der dritten Bestellung überraschte mich allerdings das Polstermaterial - und weckte meine Aufmerksamkeit, das sah nicht nur nach geschredderter Werbung aus. Eine Stunde später hatte ich den Nachnamen eines anderen Kunden plus dessen Bestellung und Rudimente einer Adresse eines anderen Kunden zusammengepuzzelt.

Quelle

Schlussfolgerung

Im Jahre 2012 hat das Ananysezentrum InfoWatch **934** Verluste vertraulicher Daten registriert. Das sind 16% mehr als im Vorjahr.

Bei vielen Vorfällen lässt sich nicht feststellen, ob das Datenleck vorsätzlich oder zufällig geschah. Die Datenlücken aus unbestimmten Quellen liegt das Verhältnis von zufälligen und vorsätzlichen Datenlücken bei 16%.

Der Anteil der Datenverluste aus bildenden und geschäftlichen Organisationen haben sich, wie vorausgesagt, als eher zufällige Datenlücken heraus gestellt. In den Unternehmen sinkt der Anteil zufälliger Datenverluste, was die Annahme zulässt, dass der Anteil zufälliger Datenlücken bei den Unternehmen mit dem Tempo der DLP-Einführung zusammenhängt. Der Anteil vorsätzlicher Datenverluste ist dabei immer noch hoch, weil dieser direkt mit dem Gewinn vom Verkauf vertraulicher Daten zusammenhängt. Neben den technischen Schutzmaßnahmen sind hier auch noch organisatorische und rechtliche Maßnahmen von Bedeutung.

Der Anteil an Vorfällen mit Personendaten ist mit 89,4% nach wie vor hoch. Wird der Verkauf gestohlener Daten erschwert, so trägt dies zur Bekämpfung des Diebstahls von Personendaten bei. Dazu sind rechtliche Maßnahmen erfolderlich. Es müssen auch zusätzliche Sanktionen für nicht bestimmungsgemäße Datenverarbeitung erarbeitet und staatlich politischen Schritte vorgenommen werden.

Die meisten Datenverluste finden über Papierdokumente statt. Als Angriffsobjekt der böswilligen Angreifer gilt auch noch die Sicherungskopie, die Arbeitsstaionen selbst und die Netzwerklaufwerke. Der Anteil der mobilen Geräte als Kanal der Datenlücke sank. Vielleicht aus dem Grund, weil man nicht in jedem Fall sagen kann, ob es ein Datenleck oder ein Hardware-Diebstahl war. Bemerkenswert ist auch, dass böswillige Angreifer E-Mails nicht als Angriffspunkt nutzen. Vielleicht aus dem Grund, dass man der Meinung ist, E-Mails seien gut überwacht.

Es kann nicht bei jedem Vorfall mit Sicherheit bestimmt werden, ob die Datenlücke beabsichtigt oder nicht beabsichtigt war. Beide Arten der Datenlücken überlappen sich.Schon heute müssen wir zu universellen Technologien zur Feststellung der Datenlücken sowie zur Kontrolle der Informationsflüsse übergehen. SIcherlich müssen die contentorientierte Systeme zum Datenschutz die Daten sowohl innerhalb der Organisation (Datenspeicherung, Datentransport) als auch außerhalb der Organisation im globalen Netz gleich effektiv funktionieren.