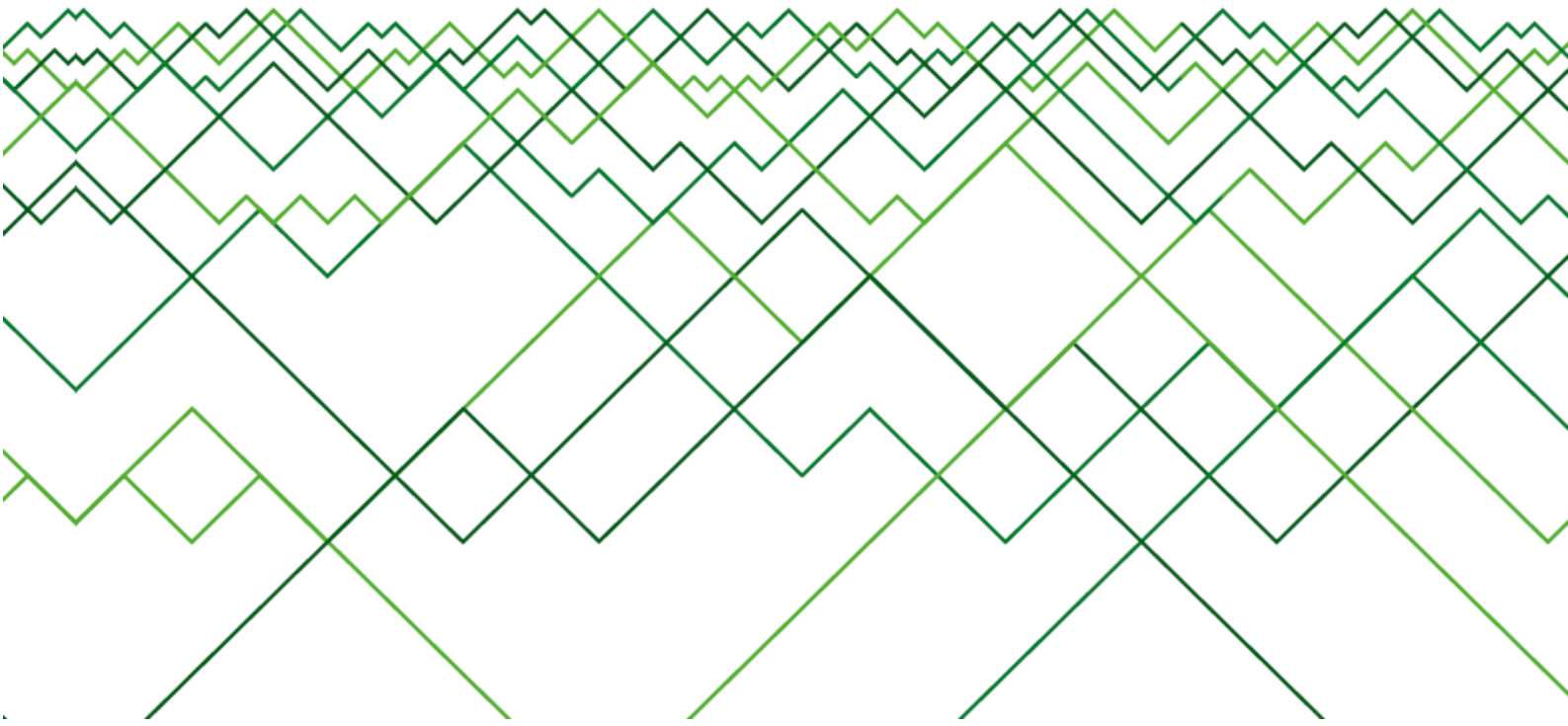
INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Analysezentrum InfoWatch

Globale Studie zu Verlusten von Unternehmens- und vertraulichen Daten 2011



INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Inhaltsverzeichnis

Übersicht

Das Analysezentrum des Unternehmens InfoWatch stellt seine jährliche Studie zu Datenverlusten, die 2011 registriert wurden, vor.

Die Studie basiert auf einer eigenen Datenbank, die von den Spezialisten des Zentrums seit 2004 gepflegt wird. Die Datenbank von InfoWatch enthält Informationen über Vorfälle in Organisationen, die auf böswilliges oder unvorsichtiges Verhalten der Mitarbeiter zurückzuführen sind und **in den Medien** oder anderen frei zugänglichen Quellen (darunter auch Internetforen und Blogs) publik gemacht wurden. Das bedeutet, dass die Studie lediglich einen geringen Teil (weniger als 1 %) aller tatsächlichen Vorfälle von Datenverlust weltweit beschreibt. Dennoch sind die Daten vollkommen repräsentativ und lassen Schlüsse auf die Gesamtsituation in diesem Bereich zu.

Ziele der Studie

Ziel der vorliegenden Studie ist die Aufzeichnung und die Analyse von Zwischenfällen mit Verlusten vertraulicher Informationen, die sich weltweit ereignet haben. Außerdem soll eine täglich aktualisierte Statistik entstehen, mit der Trendentwicklungen festgestellt und Prognosen aufgestellt werden können. Und schließlich soll man rückschließen können, wie gut verschiedene Organisationen im jeweiligen Moment vor inneren Bedrohungen geschützt sind. Die Studie erlaubt es weiterhin die häufigsten, gefährlichsten und verbreitetsten Methoden zur Verletzung der internen Informationssicherheitspolitik der Organisationen festzustellen.

Wie die InfoWatch-Datenbank entsteht

Zurzeit zählt die InfoWatch-Datenbank einige Tausend erfasste Fälle von Verlusten vertraulicher Daten, die sich infolge von Verstößen gegen die interne Informationssicherheitspolitik ereigneten.

In der Datenbank werden für jeden Vorfall das Ereignisdatum und das Veröffentlichungsdatum in den Medien festgehalten. Die Vorfälle werden gemäß des Veröffentlichungsdatums in den Medien geführt. Die Zahl der bekannt gewordenen Fälle ist bedeutend geringer als die Zahl der tatsächlichen Fälle. Als Informationsquellen dienen die Medien, Blogs und Foren.

Die Datenbank enthält Fälle von Datenverlust, die folgende Merkmale aufweisen:

- böswillige Handlungen von Insidern (vorsätzliche Verluste);
- Unaufmerksamkeit der Mitarbeiter (zufällige Verluste).

Datenabflüsse infolge von Cyberattacken und anderen Angriffen auf die Informationssicherheit (DDoS, Phishing usw.) werden in diesem Bericht nicht berücksichtigt.

Die Klassifizierung und Erfassung der Vorfälle in der Datenbank basiert auf den Ergebnissen einer Analyse, die von den InfoWatch-Analytikern durchgeführt wird. Bei dieser Analyse werden jedem Zwischenfall verschiedene Merkmale (Organisationstyp, Tätigkeitsfeld, Verlusttyp, finanzieller Schaden) und Kategorien (Verlustwege, Art der verlorenen Daten) zugeordnet, die es erlauben, eine Vorstellung über die Größenordnung des Datenverlusts zu gewinnen, die möglichen Ursachen zu analysieren und die Folgen vorherzusagen.

Die Statistik zum Umfang des Schadens wird in diesem Bericht nicht betrachtet, da die Presseberichte zu ca. 5 % der Lecks diese Information bereits enthalten.

Allgemeine Statistik

Für 2011 verzeichnete das InfoWatch-Analysezentrum 801 Fälle von Datenabfluss, bei denen vertrauliche Informationen verloren gingen. Das ist ungefähr 1 % mehr als im Vorjahr. Es handelt sich hierbei um alle Vorfälle in Organisationen, die auf böswilliges oder unvorsichtiges Verhalten der Mitarbeiter zurückzuführen sind und **in den Medien** oder anderen frei zugänglichen Quellen (darunter auch Internetforen und Blogs) publik gemacht wurden.

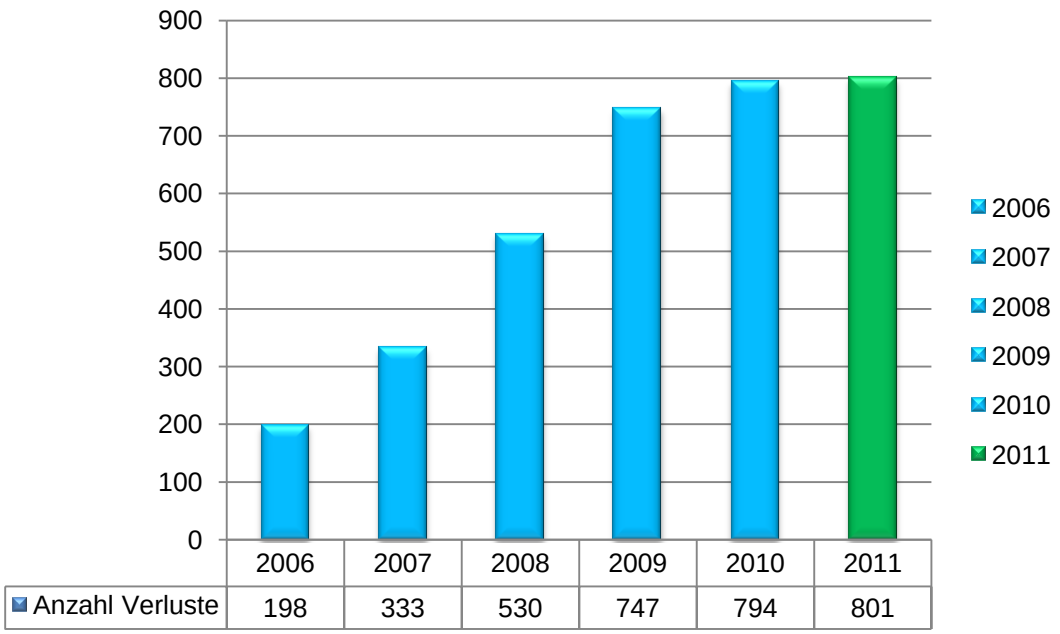


Abb. 1. Entwicklung der Anzahl Verluste, 2006-2011.

Für 2011 liegt der Monatsdurchschnitt bei 70 Vorfällen; der Tagesdurchschnitt bei 2.

Die nur geringe Veränderung der Anzahl Vorfälle zum Vorjahr hat verschiedene Gründe:

- Geheimhaltung der Datenverluste seitens der Unternehmen, da sich diese negativ auf die Unternehmensreputation auswirken;
- etwas geringeres Interesse am Thema seitens der Medien;

- Einführung von DLP-Systemen, die gut vor zufälligen Lecks schützen.

Schlussfolgerung:

In diesem Jahr beginnt möglicherweise eine neue Etappe bei den Datenverlusten und deren Bekanntmachung. Ein Merkmal dieser Etappe wird die Stabilisierung der Zahl bekannt gewordener Vorfälle sein, deren Anteil nicht bedeutend wachsen wird.

Überlegung

Das Verhältnis vorsätzlicher und zufälliger Datenverluste hat sich zum Vorjahr kaum verändert; die Prozentzahlen liegen ungefähr gleich auf.

Der von uns vor 2 Jahren prognostizierte Rückgang der Anzahl zufälliger Datenverluste zeigt sich allmählich, wenn auch noch schwach. Mit der Installierung von Sicherheitstools sollte es weniger zufällige Verluste geben, denn die auf dem Markt erhältlichen Lösungen und Produkte sind gerade bei zufälligen und weniger bei vorsätzlichen Datenverlusten sehr wirksam.

Aber selbst die einfachsten Sicherheitstools werden nicht überall und nicht sofort eingesetzt. Es bedarf seiner Zeit; man muss begreifen, dass der Einsatz solcher Tools notwendig ist. Deshalb sollte sich die prognostizierte Tendenz erst in 2-3 Jahren in vollem Umfang zeigen. Für den Moment liegt die Zahl zufälliger und vorsätzlicher Datenabflüsse jeweils bei ca. 50 %.

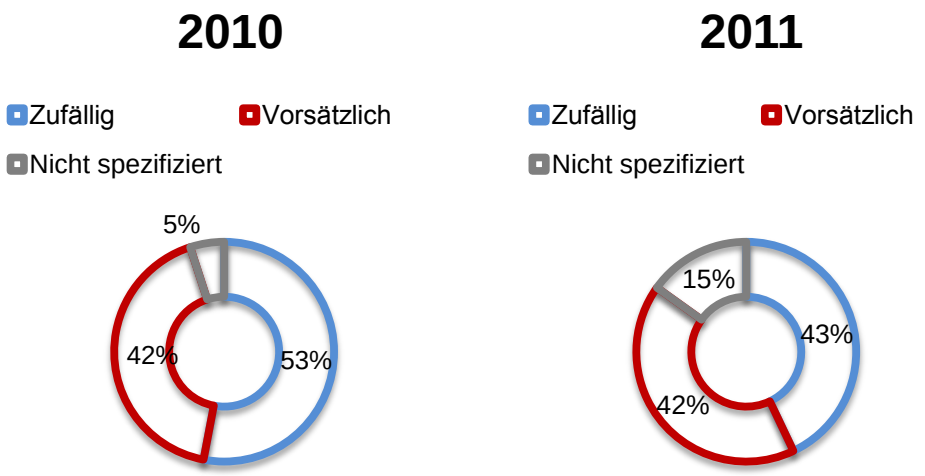
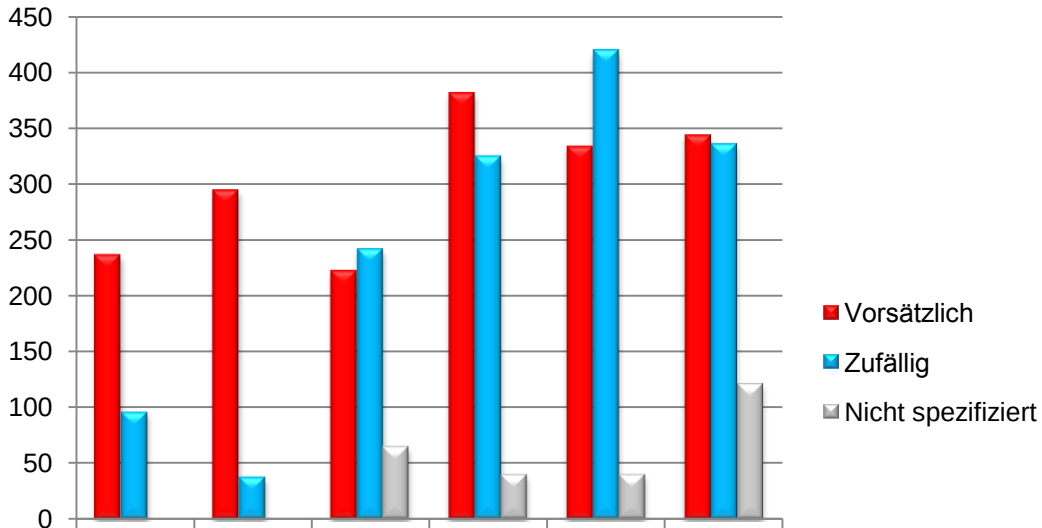


Abb. 2. Verhältnis zufälliger und vorsätzlicher Datenverluste, 2010-2011.

Leider **lässt sich in vielen Fällen nicht feststellen, ob ein Datenabfluss vorsätzlich oder zufällig war**; das können nicht einmal die Experten, welche die Untersuchung durchführen. Das gilt besonders für Fälle, bei denen mobile Datenträger, d. h. Notebooks, PDAs und USB-Sticks, verloren gehen. Nicht immer ist es klar, ob der Datenträger verloren ging oder gestohlen wurde. Und im Falle eines Diebstahls lässt sich auch nicht

immer feststellen, ob der Dieb es auf den Datenträger selbst oder auf die darauf befindlichen Daten abgesehen hatte.

Außerdem geben nicht alle Quellen, die über den Verlust informieren, einen genauen Hinweis auf den Träger. Viele Medien messen dem einfach keine Bedeutung bei. Das macht es schwieriger, die Absicht hinter dem Datenverlust zu ermitteln; deshalb fällt der Anteil der Kategorie „Nicht spezifiziert“ verglichen mit den Vorjahren größer aus (Abb. 3).



	2006	2007	2008	2009	2010	2011
Vorsätzlich	237	295	223	382	334	344
Zufällig	96	38	242	325	420	336
Nicht spezifiziert	0	0	65	40	40	121

Abb. 3. Entwicklung des Verhältnisses zufälliger und vorsätzlicher Datenverluste, 2006-2011.

Schlussfolgerung:

Seit 2008 hat sich das Verhältnis zufälliger und vorsätzlicher Verluste nicht stark verändert und liegt bei ungefähr 45 % zu 45 %. Die Absicht hinter dem Datenverlust genau festzustellen wird immer schwieriger, denn die Anzahl der Datenübertragungskanäle und die Massennutzung neuer Geräte und Kommunikationsmittel wachsen von Jahr zu Jahr in einem rasanten Tempo.

Quellen der Datenverluste

Der Datenschutzansatz muss sich am Wert der Daten für das Unternehmen orientieren. Vergleichen wir beispielsweise den Verlust von Bankkundendaten oder den Verlust eines internen Dokuments mit den Verhaltensanweisungen für die Mitarbeiter eines Handelsunternehmens.

Je wertvoller die Daten, desto strikter sollte der Ansatz zur Datensicherung sein.

Aufgrund der in verschiedenen Ländern verabschiedeten Personaldatenschutzgesetze müssen so gut wie alle Organisationen, die über Personaldaten ihrer Kunden verfügen, oder Unternehmen mit einer großen Belegschaft, entsprechende Maßnahmen für den Datenschutz ergreifen. Was sieht die Realität aus? Aus welchen Organisationen gehen Daten verloren?

In der Datenbank sind die Organisationen, die von Datenverlust betroffen sind, von uns in 3 Gruppen eingeteilt: *1) Regierungsbehörden,*

2) kommerzielle Unternehmen,

3) Non-Profit-Organisationen und Bildungseinrichtungen.

Non-Profit-Organisationen und Bildungseinrichtungen sind in einer Gruppe zusammengefasst, da sie sich nach unseren Beobachtungen in ihrer Motivation beim und den Bedingungen für Datenschutz ähnlich sind. Die Schutzmaßnahmen in diesen beiden Organisationstypen sind eher formal; neue Bedrohungen werden nicht so schnell wie in kommerziellen Organisationen abgebaut. In der Regel gibt es nur wenige Personaldaten in diesen Organisationen. Ihre geschäftliche Reputation hängt von ganz anderen Faktoren ab und das Erzielen von Gewinn ist nicht der Hauptbewertungsfaktor für ihre Arbeit.

In Non-Profit-Organisationen und Bildungseinrichtungen werden die Ergebnisse der Datenschutzmaßnahmen in erster Linie aufgrund des Umfangs der Aufwendungen bewertet. Entscheidungsgrundlage für die Verteilung der Mittel (Geld, Zeit, Mitarbeiter, Zuständigkeiten) sind die Rentabilität und/oder die dringende Notwendigkeit der Einführung eines entsprechenden Schutzes, die beispielsweise aufgrund eines Zwischenfalls aufkommen kann. Das Gleichgewicht dieser Faktoren unterscheidet sich für die drei genannten Organisationsgruppen, ähnelt sich jedoch mehr oder weniger innerhalb einer Gruppe.

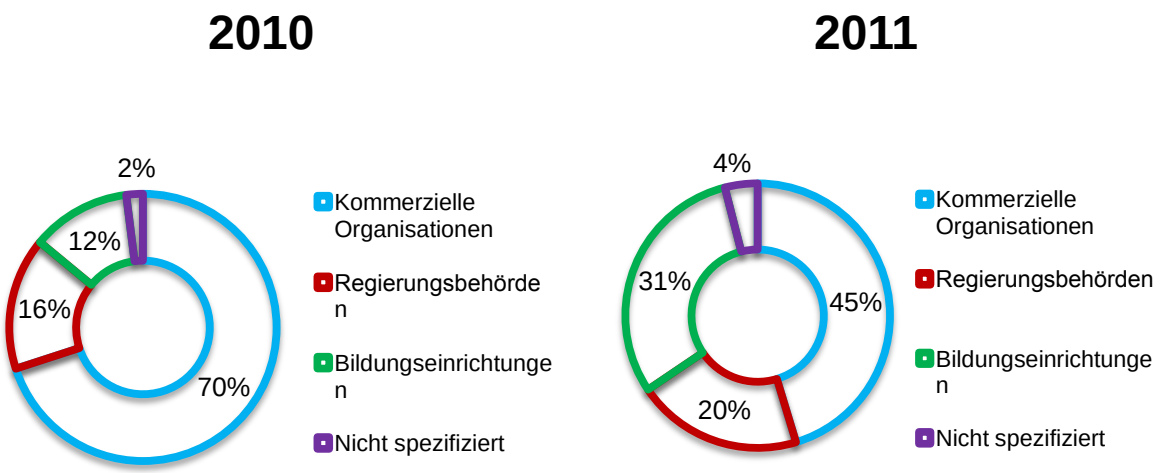


Abb. 4. Verteilung der Datenverluste nach dem Organisationstyp, 2010-2011.

Wie die statistischen Daten für 2011 zeigen, waren die Datenverluste in allen 3 Organisationstypen ungefähr in derselben Größenordnung. Dennoch dominieren die Datenverluste in kommerziellen Organisationen mit 45 % und Bildungseinrichtungen mit 31 %.

Im Vorjahr waren „kommerzielle“ Verluste mit 70 % aller Vorfälle einsame Spitze.

Die erhöhten Anteile der Non-Profit-Organisationen und Bildungseinrichtungen in der traurigen Datenverluststatistik lassen sich zweifelsohne auf die Implementierung von Schutzmaßnahmen in kommerziellen Unternehmen und Regierungsbehörden zurückführen, darunter auch Maßnahmen zur Verheimlichung der Vorfälle[1].

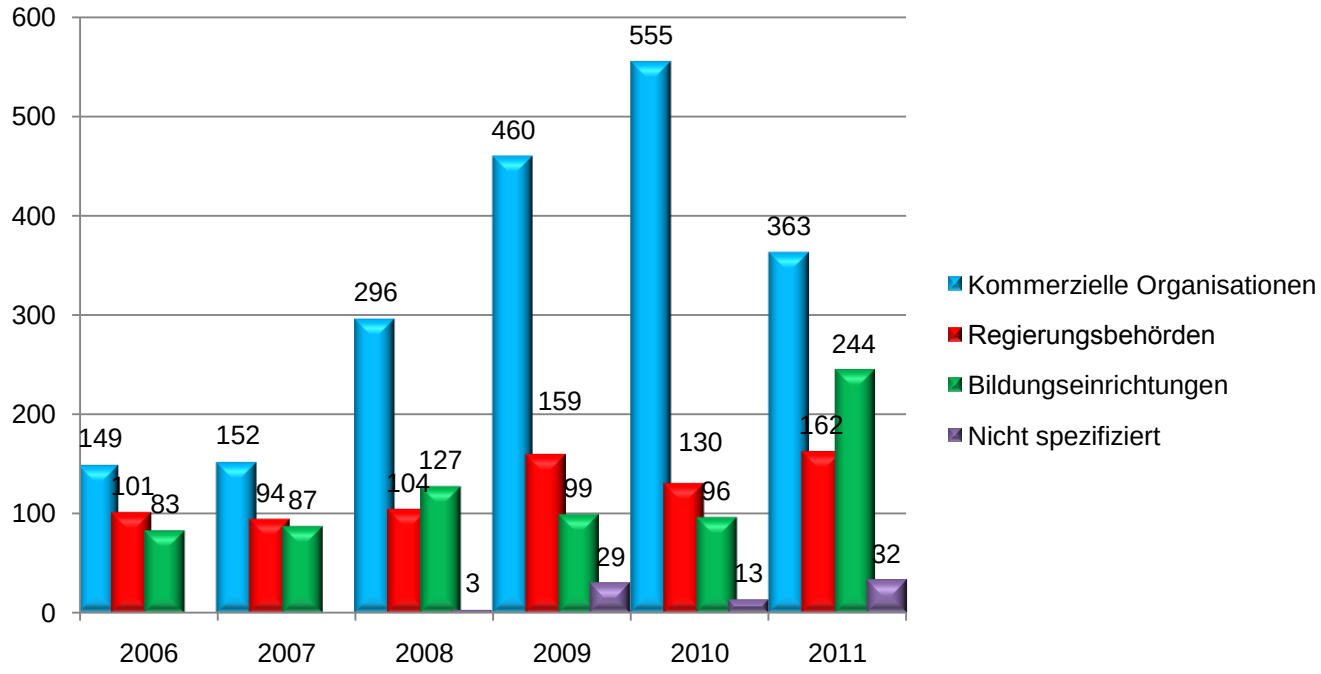


Abb. 5. Entwicklung der Datenverluste nach den Quelltypen, 2006-2011.

Für Unternehmer bedeuten Datenverluste einen Schaden. Nicht nur wegen der Datenverbreitung selbst oder wegen der Verwendung der Daten für Diebstähle, sondern auch wegen des daraus entstehenden Imageschadens. Es gibt Vorfälle, die überhaupt keinen direkten Schaden nach sich ziehen; der Schaden besteht dann einzig aus dem Verlust einiger Kunden, die sich vom Unternehmen unter dem Einfluss der Berichterstattung zum Vorfall abwenden. Hier mal ein Beispiel:

> *Im Januar 2001 wurde die Kundendatenbank des größten Telekommunikationsanbieters im Netz veröffentlicht. Das InfoWatch-Analysezentrum registrierte einen weiteren Verlust vertraulicher Daten:*

[1] Die Verheimlichung der Vorfälle vor der Öffentlichkeit oder den staatlichen Behörden widerspricht oftmals dem Gesetz oder einem Abkommen. Trotzdem gehört das aus Sicht des Datenschutzes zu den Schutzmaßnahmen, da so Schäden für ein Unternehmen minimiert werden.

Persönliche Daten von Millionen von Vodafonekunden, darunter deren Namen, Wohnanschriften, Führerscheinnummern und Kreditkarteninformationen wurden „aus Unaufmerksamkeit“ ins Internet gestellt. Dieser Datenabfluss brachte das Unternehmen vor Gericht und es verlor das Vertrauen seiner Kunden. Mehr als 9000 Kunden reichten Klage ein; Vodafone bemüht sich den Rechtsstreit so wirksam wie möglich zu schlichten.

http://www.infowatch.ru/analytics/leaks_monitoring/2254

Deswegen erwerben pragmatische Unternehmer nicht nur technische Schutztools und ergreifen organisatorische Maßnahmen zur Stärkung der Sicherheitspolitik, sondern versuchen auch die Information über die Vorfälle zu verbergen oder ihre Verbreitung einzugrenzen. Die Motivation für solche Anstrengungen ist deren direkte Wirkung auf den Gewinn. Das Ergebnis ist offensichtlich: Über Datenverlust in kommerziellen Organisationen wird weniger berichtet. Es scheint auch weniger Verluste zu geben, aber das kann nicht mit Sicherheit gesagt werden.

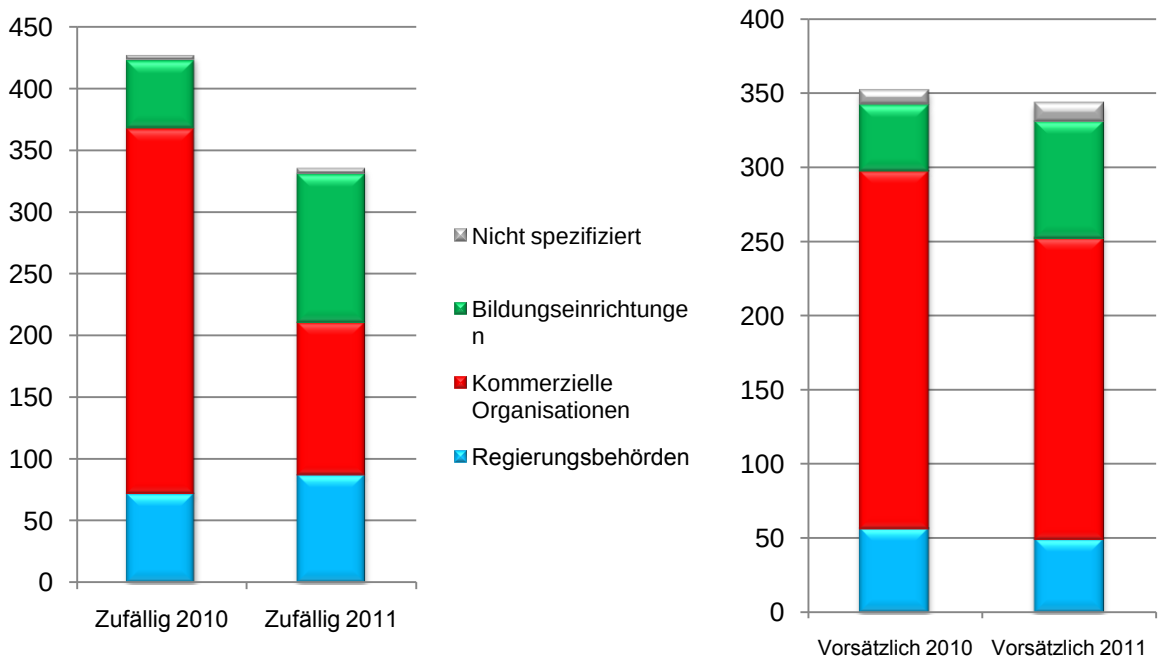


Abb. 6. Verhältnis zufälliger und vorsätzlicher Datenverluste nach Organisationstypen, 2010-2011.

Schlussfolgerung:

Die gewachsenen Anteile der Bildungseinrichtungen und Non-Profit-Organisationen sind hauptsächlich auf zufällige Datenverluste zurückzuführen; bei den vorsätzlichen Verlusten gibt es keine bedeutende Veränderung zum Vorjahr.

Bei den kommerziellen Organisationen geht der Anteil zufälliger Verluste, dank der Anwendung von DLP-Systemen in den Unternehmen, die mit großer Wahrscheinlichkeit gerade vor solchen Verlusten schützen, deutlich zurück. Der Anteil vorsätzlicher Verluste ist immer noch genauso hoch, denn in diesen Fällen können die Übeltäter möglicherweise einen direkten Vorteil vom Diebstahl und der Verbreitung der vertraulichen Daten haben. Neben technischen Schutzmaßnahmen sind hierbei auch organisatorische, rechtliche und gesetzgebende Maßnahmen wichtig.

Personaldaten

Noch immer betrifft der Löwenanteil aller Datenlecks Personaldaten, nämlich 92,4 % (95,5 % im Vorjahr).

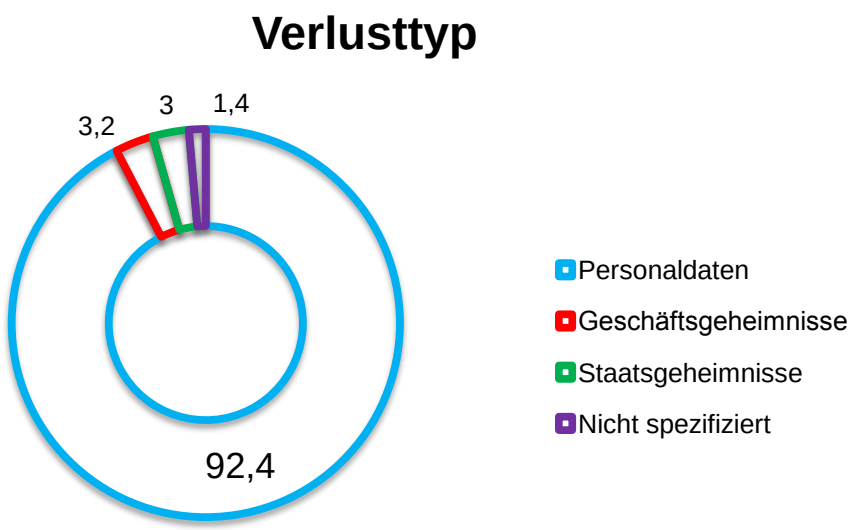


Abb. 7. Verteilung der Datenverluste nach Art der Daten, 2010-2011.

Ein derart hoher Anteil von Vorfällen mit Personaldaten ist oft auf die gesetzliche Forderung, derartige Vorfälle publik zu machen, zurückzuführen. Es ist aber genauso richtig, dass verfügbare Personaldaten für einen breiten Kreis von Übeltätern interessant sind, da sie auf dem Schwarzmarkt verkauft werden könnten. **Geschäfts- und Staatsgeheimnisse gehen gewöhnlich „auf Bestellung“ verloren und sind an sich Einzelfälle**. Die Vorfälle nehmen erst wirklich große Ausmaße an, wenn die verfügbaren Daten für Geld an einen großen Käuferkreis verkauft werden könnten.

Schlussfolgerung:

Eine Möglichkeit dem vorsätzlichen Diebstahl geheimer Daten entgegenzuwirken, besteht darin, den Verkauf der vertraulichen Daten zu erschweren, d. h. ihren Diebstahl nicht lukrativ für den Verkauf zu machen und die gesetzliche Grundlage zu stärken. Dadurch könnten die Datenangriffe drastisch zurückgehen.

Verlustwege

Der Verlustweg ist ein Merkmal, das eine direkte praktische Umsetzung nach sich zieht. Je nachdem wie häufig Daten auf dem einen oder anderen Weg verloren gehen (auf dem einen oder anderen Datenträger), kann die Einführung von Sicherheitsmaßnahmen geplant und können Prioritäten hinsichtlich der Frage, mit welchem Verlustweg man sich zuerst beschäftigen sollte, gesetzt werden. Neben den statistischen Daten ist aber auch zu berücksichtigen, wie die jeweilige Organisation arbeitet und, welche Mittel und Wege am häufigsten für die Datenübertragung benutzt werden, und gerade diese schützen und kontrollieren.

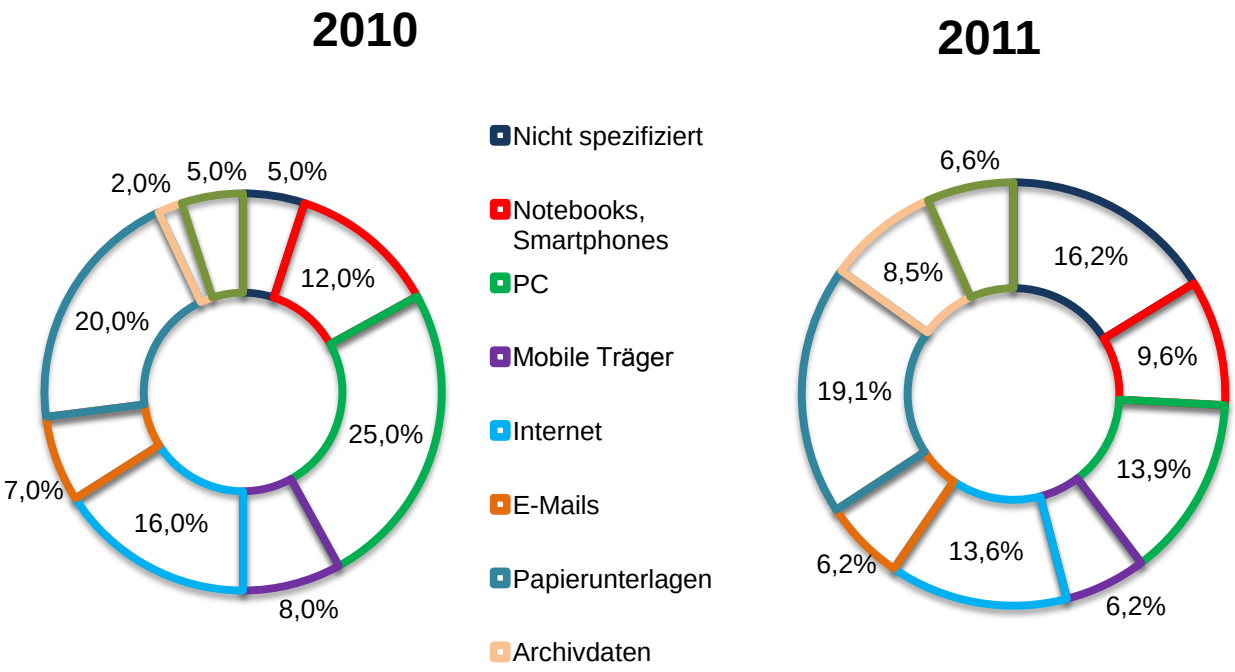


Abb. 8. Verteilung der Datenverluste nach Verlustwegen, 2010-2011.

Betrachten wir die Veränderung der Anteile der Verlustwege „Notebooks, Smartphones“ und „mobile Datenträger“. 2010 wurde für diese Wege ein geringer Anstieg der Verluste beobachtet; der Prozentsatz lag bei insgesamt 20 %. 2009 und 2011 waren der Prozentsatz jeweils etwas geringer und lag bei 19,2 % bzw. 15,8 %.

In den letzten 3 Jahren klärte InfoWatch unablässig über die Gefahren, die mit dem Verlust mobiler Datenträger zusammenhängen, auf. Mobilgeräte gehen in großer Zahl verloren bzw. werden gestohlen, aber sind aus unserem Leben nicht mehr wegzudenken. Deswegen sind derzeit technische und organisatorische Maßnahmen für die Überwachung solcher mobiler Träger und der sich darin befindlichen Informationen gefragt. Geheime Daten sollten nicht grundlos auf Mobilträgern gespeichert werden, und wenn doch, dann nur verschlüsselt. Eine Vielzahl der Vorfälle könnte durch das Einhalten dieser Regeln vermieden werden.

Im Gegensatz dazu gibt es nun dreimal so viele Vorfälle mit Archivdaten (Abb. 8, Kategorie „Trägern von Sicherheitskopien“). Ihr Anteil ist nicht sehr groß, ist jedoch im Vergleich zum Vorjahr gewachsen und liegt bei 8,5 %. Leider haben nur wenige der geläufigen Systeme für Sicherheitskopien eine integrierte Verschlüsselung. Dabei kann es einfacher sein, Archivdaten als täglich verwendete Datenträger zu stehlen. Das bestätigt auch die Statistik: Vorsätzliche Verluste auf diesem Weg liegen bei 38 % und zufällige bei 27,9 %. Eine Verschlüsselung der Sicherheitskopien würde diese Art Vorfälle vollständig unterbinden.

Verluste „über das Internet“ bzw. über unsere Kategorie „Internet“ sind für Laien gewöhnlich die wichtigste, wenn nicht sogar die einzige Variante. Gerade über diese Verlustwege wird am häufigsten in der Presse berichtet; auch die Chefs sprechen von ihnen. Der Schutz dieser Wege ist die Hauptaufgabe der Datensicherheitsabteilungen vieler Unternehmen. Allerdings ist der Anteil der Verluste auf diesem Weg mit ca. 14 % im Jahr 2011 nicht besonders groß. Verglichen mit den Vorjahren ist ein Abwärtstrend zu beobachten: Im Jahr 2010 waren es 16 % und 2009 waren es 18,3 %. Das zeigt, dass dieser Weg oft verwendet wird und dass die Sicherheitsmaßnahmen zum Schutz von Verlusten über das „Internet“ bereits umgesetzt werden. Aber allein diesen Weg zu verschließen kann nicht vollständig vor Verlusten schützen.

Datenabflüsse über E-Mails, die publik gemacht werden, liegen bei nur 6 %. Dieser Verlustweg ist genauso wie „Internet“ einer der beliebtesten Kanäle zur Verbreitung und Übertragung von Daten. Die Vielzahl der Datenabflüsse über E-Mails in den vergangenen Jahren (2007-2009) führte dazu, dass die Unternehmen diesen Verlustweg nur sehr streng kontrollieren. Folglich ist ein Rückgang der Anzahl Datenverluste über E-Mails zu beobachten, wobei wir vom Ideal natürlich noch weit entfernt sind. Und wegen seiner Einfachheit bleiben E-Mails auch weiterhin der Kanal, der am meisten in Versuchung führt. Es ist möglich, dass der Anteil unveröffentlichter Datenverluste hier überwiegt, da der Prozentsatz der Verluste über diesen Kanal nicht so groß ist, wie angenommen werden könnte.

Verluste von „Papierunterlagen“ geraten im Gegenteil unverdient in Vergessenheit. Aber der Statistik zufolge gehen fast 20 % der Daten gerade als Papierunterlagen verloren; das ist der größte Anteil in unserem Diagramm (Abb. 8). Moderne DLP-Systeme können alle

Dokumente, die gedruckt werden sollen, kontrollieren und auch die Anwesenheit des jeweiligen Mitarbeiters im Büro bestätigen, der den Druckauftrag erteilt hat. Ist ein Dokument jedoch gedruckt, ist es sehr schwer, seine Verbreitung zu verfolgen. Die physische Fortbewegung von Papierunterlagen kann nur mittels organisatorisch-rechtlicher Methoden verfolgt werden; auf Technik ist hier nur wenig Verlass. Betrachtet man die Statistik der letzten 3 Jahre, ist der Anteil der Verluste auf diesem Weg praktisch unverändert und liegt nah bei 20 %. 2009 lag der Anteil der „Papierunterlagen“ bei den Verlusten bei 19,9 %; 2010 waren es 19,6 %.

Interessant ist es, ähnliche Kanäle zusammenzufassen und dann die gesammelten Daten zu vergleichen.

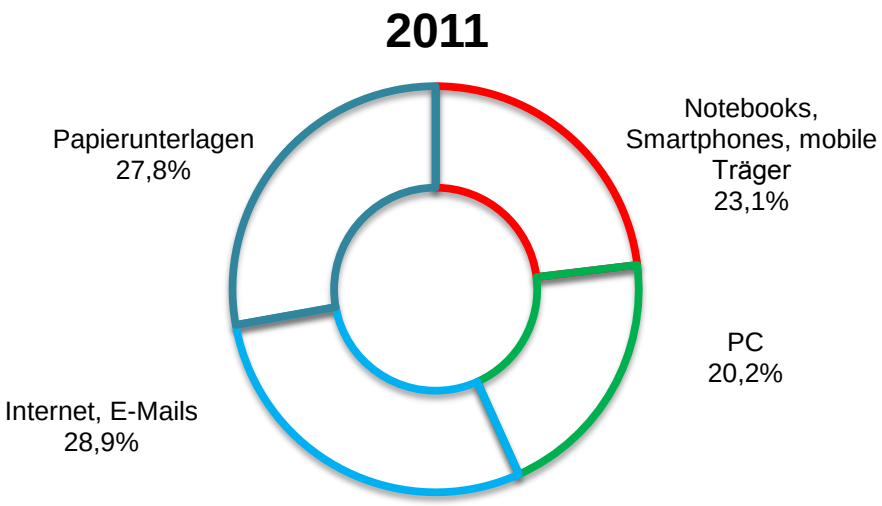


Abb. 9. Vergleich der Anteile der Hauptverlustwege, 2011.

Schlussfolgerung:

Fasst man einige vergleichbare Verlustwege in einer Kategorie zusammenfasst, verteilen sich die Anteile fast gleichmäßig (Abb. 9). Ganz oben liegt die Kategorie „Internet und E-Mail“, was prinzipiell nachvollziehbar ist, denn diese Kanäle bleiben aufgrund ihrer Einfachheit am beliebtesten; danach folgen Verluste über Papierunterlagen.

Vergleichen wir nun, inwieweit sich vorsätzliche und zufällige Verluste nach Datenträgern unterscheiden.

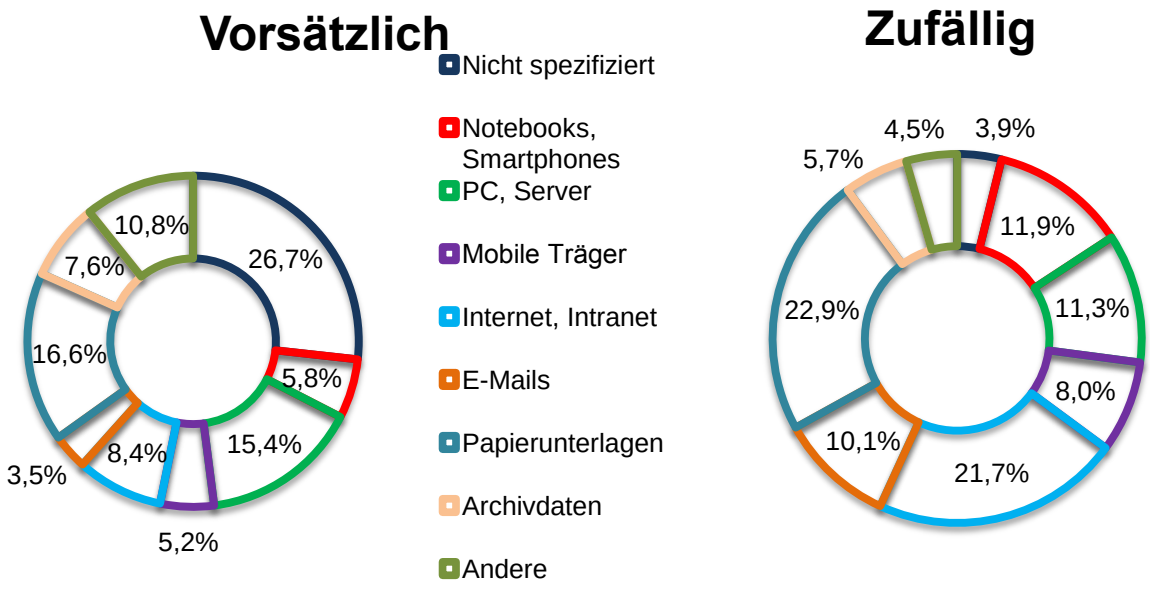


Abb. 9. Verhältnis zufälliger und vorsätzlicher Verluste nach Kanälen, 2011.

Als erstes fällt der große Unterschied bei den Verlusten über den Kanal „Web und Intranet“ ins Auge: Die Anteile vorsätzlicher und zufälliger Verluste liegen bei *8.4 %* bzw. *21,7 %*.

Beim Verlustweg „E-Mail“ überwiegen ebenfalls die zufälligen Verstöße gegen die Vertraulichkeit: Das Verhältnis vorsätzlicher und zufälliger Verluste liegt bei *3.5 % zu 10,1 %*. Bei den heutigen E-Mail-Diensten gibt es keine Funktion, bei der eine E-Mail vor dem Versand nochmals kontrolliert wird; auch wird die Empfängeradresse häufig verborgen bzw. durch einen Namen, der automatisch aus dem LDAP-Archiv zur Verfügung gestellt wird, ersetzt usw. Es ist nicht notwendig zu beweisen, dass Internet, Intranet und E-Mails unbedingt durch IT-Lösungen kontrolliert und geschützt werden müssen. Versehentlichem Versand vertraulicher Informationen kann durch die Einführung und Anwendung ergänzender, externer Programme, z. B. DLP-Systeme, vorgebeugt werden. Das bedeutet, dass für vorsätzlichen Datendiebstahl öfter andere Kanäle verwendet werden.

Bei Desktop Computern sind vorsätzliche Vorfälle wahrscheinlicher; im Verhältnis ist deren Anzahl praktisch 2,5 Mal so hoch, genauer 10,8 % zu 4,3 %.

Schlussfolgerung:

Wie bereits angemerkt, schützen DLP-Systeme wirksam vor zufälligen Verlusten und der Ausgang im Kampf gegen vorsätzliche Verluste hängt vom Verhältnis zwischen dem Geschick der Übeltäter und der Kompetenz der Sicherheitsfachkräfte des jeweiligen Unternehmens ab. Gab es dennoch einen Datenabfluss aus dem

Unternehmen, ermöglichen es DLP-Systeme eine Untersuchung durchzuführen und juristisch fundierte Beweise zum Vorfall zu sammeln. Jedoch reichen IT-Tools allein zur vollständigen Verhinderung von vorsätzlichem Datendiebstahl nicht aus. Organisatorische und rechtliche Maßnahmen sind ebenso wichtig.

Verteilung der Datenverluste nach Ländern

Das nachfolgende Diagramm zeigt eine Übersicht der registrierten Vorfälle verteilt nach Ländern. Der Platz in der Rangliste wird allein durch die tatsächliche Anzahl bekannt gemachter Datenverluste bestimmt; nicht publik gemachte Verluste wurden nicht berücksichtigt.

In den USA und in Großbritannien gibt es strenge gesetzliche Bestimmungen, welche die Publizierung aller Vorfälle fordern, weshalb diese Länder unsere Rangliste auch anführen.

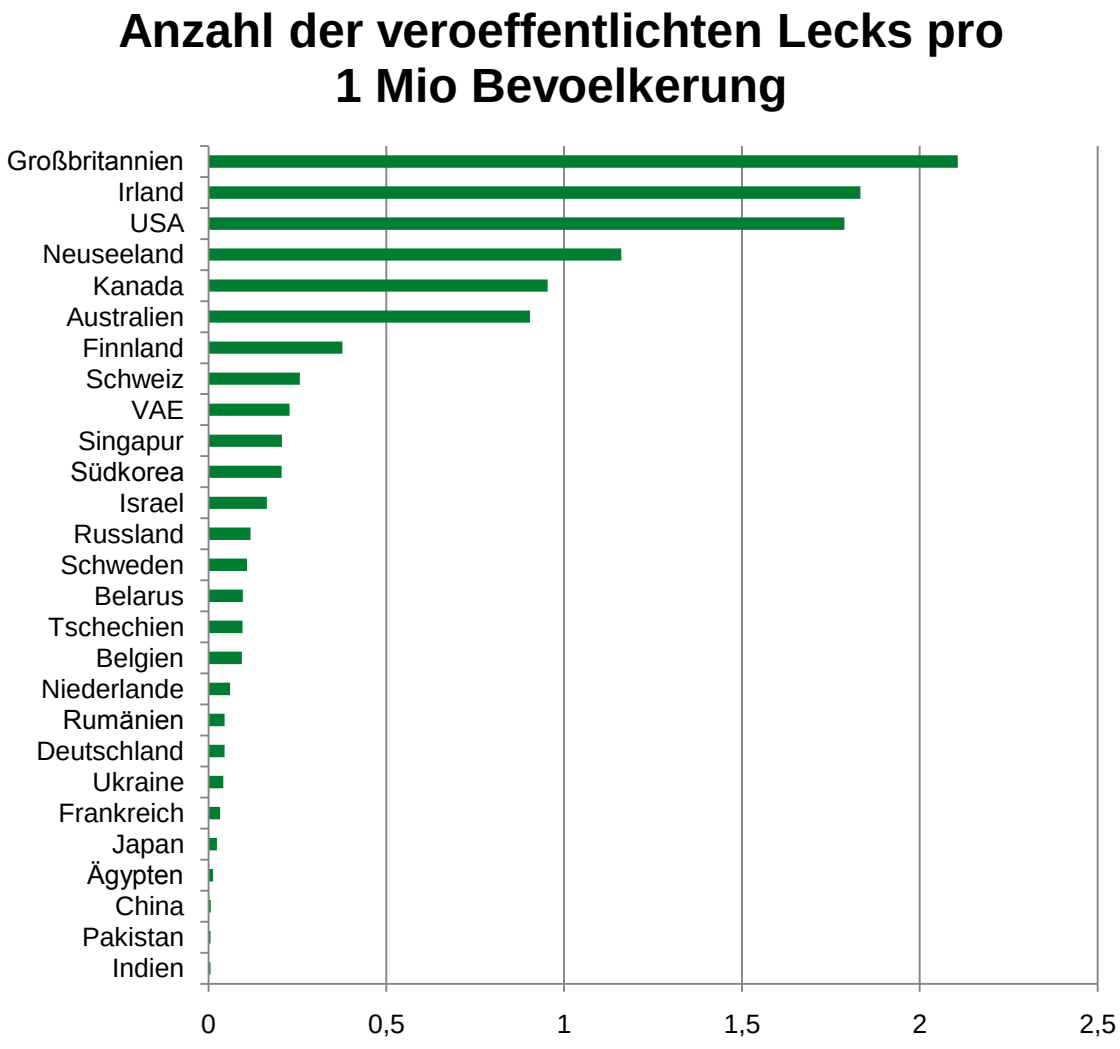


Abb. 10. Verteilung der Datenverluste nach Ländern, 2011.

Die Länder sind nach der Zahl der Verluste pro Million gelistet (LPM-Index).

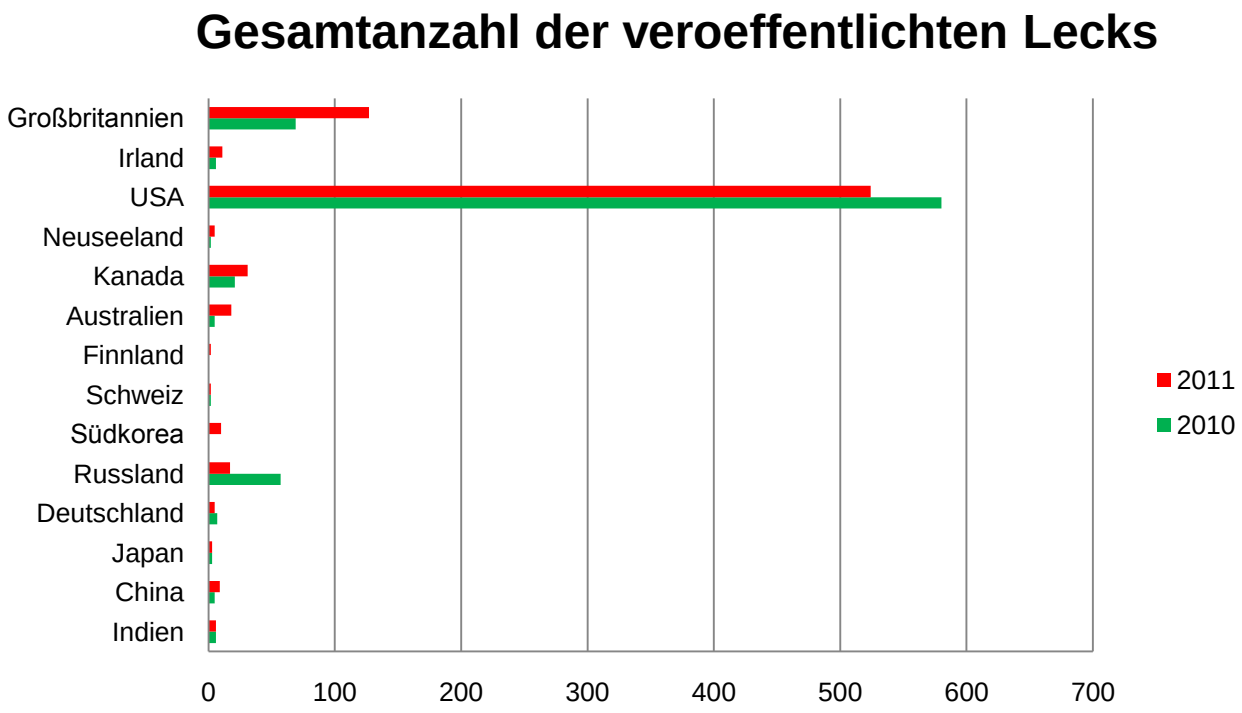


Abb. 11. Verteilung der Datenverluste nach Ländern, 2011.

Im Vorjahresvergleich ist ein sinkender Anteil der USA zu beobachten: 65 % gegenüber 73 %. Das zeugt davon, dass die gesetzlichen Bestimmungen dieses Landes befolgt und die Vorfälle immer seltener vertuscht werden.

Die Zahl der russischen Vorfälle ist im Berichtsjahr von 57 auf 17 gesunken.

> *Nikolaj Fedotov, Chefanalytiker bei InfoWatch: „Wir könnten viel mehr russische Vorfälle aufzählen, wenn alle Publizierungen der Verstöße gegen das Gesetz „Über Personaldaten" berücksichtigen würden, sowie es einige unserer Kollegen machen. Tatsächlich gibt es viele solcher Verstöße; die Aufsichtsbehörden verhängen eine Strafe gegen die Täter und veröffentlichen die Berichte hierzu in der Presse. Allerdings handelt es sich in fast allen Fällen gar nicht um Datenverluste. Und umgekehrt gilt: Tatsächliche Fälle von Datenverlust führen nicht zur Erstellung eines Protokolls und der Bestrafung der Schuldigen. Insgesamt sind die Schwächen des russischen Gesetzes „Über Personaldaten" allen Experten sehr gut bekannt".*

Deutschland

2011 wurden in den deutschsprachigen Ländern Europas, vor allem in Deutschland und Österreich, 23 mehr oder weniger große Verluste vertraulicher Informationen erfasst.

In der Jahresbilanz der Datenlecks lassen sich folgende wichtige Gesetzmäßigkeiten beobachten.

Führende Positionen in der Menge verlorener vertraulicher Informationen sind nach wie vor von persönlichen Daten der Bürger besetzt – 82,6 % aller Fälle. Mit großem Abstand folgt das Geschäftsgeheimnis – 13 %; vertrauliche medizinische Informationen (Ärztegeheimnis) sind in der Minderzahl – 4,4 %. Die Verteilung der Vorfälle nach Verlustwegen sieht folgendermaßen aus: Internet – 61 %, E-Mails – 26,1 %, Papierkörbe – 8,6 %, ungeklärte Kanäle – 4,3 %.

Zusammenfassung

Für 2011 verzeichnete das InfoWatch-Analysezentrum 801 Fälle von Datenabfluss, bei denen vertrauliche Daten verloren gingen und die in den Medien publik gemacht wurden. Das ist lediglich 1 % mehr als im Vorjahr. Eine vorläufige Analyse der Tendenzen zeigt, dass in diesem Jahr möglicherweise eine neue Etappe beginnen könnte, die durch eine Stabilisierung der Anzahl publizierter Verluste gekennzeichnet ist.

In vielen Fällen lässt sich leider nicht feststellen, ob der Verlust vorsätzlich oder zufällig war, und folglich ist es schwieriger, die Absicht hinter dem Datendiebstahl zu erkennen. Seit 2008 hat sich das Verhältnis zwischen zufälligen und vorsätzlichen Verlusten nicht stark verändert; die Zahlen liegen nah beieinander.

Der erhöhte Anteil der Verluste in Bildungseinrichtungen und Non-Profit-Organisationen ist hauptsächlich auf zufällige Datenverluste zurückzuführen. In kommerziellen Organisationen geht die Zahl zufälliger Verluste dank der Anwendung von DLP-Systemen deutlich zurück. Jedoch ist der Anteil vorsätzlicher Verluste in diesen Organisationen noch genauso hoch, denn in diesen Fällen können die Übeltäter möglicherweise einen direkten Vorteil vom Diebstahl und der Verbreitung der vertraulichen Daten haben. Neben technischen Schutzmaßnahmen sind hierbei auch organisatorische, rechtliche und gesetzgebende Maßnahmen wichtig.

Noch immer betrifft der Löwenanteil aller Datenlecks Personaldaten, nämlich 92,4 %. Eine Möglichkeit dem vorsätzlichen Diebstahl von Personaldaten entgegenzuwirken, besteht darin, der Verkauf dieser Daten zu erschweren, was nur auf Gesetzesebene möglich ist.

An der Spitze der Hauptverlustwege steht die Kategorie „Internet und E-Mail“. Diese Kanäle sind weiterhin aufgrund ihrer Einfachheit am beliebtesten; danach folgen Verluste über Papierunterlagen.

DLP-Systeme schützen wirksamer vor zufälligen Verlusten und der Ausgang im Kampf gegen vorsätzliche Verluste hängt vom Verhältnis zwischen dem Geschick der Übeltäter und der Kompetenz der Sicherheitsfachkräfte des jeweiligen Unternehmens ab.

Gab es dennoch einen Datenabfluss aus dem Unternehmen, ermöglichen es DLP-Systeme eine Untersuchung durchzuführen und juristisch fundierte Beweise zum Vorfall zu sammeln, unter Berücksichtigung der entsprechenden organisatorischen und rechtlichen Maßnahmen.