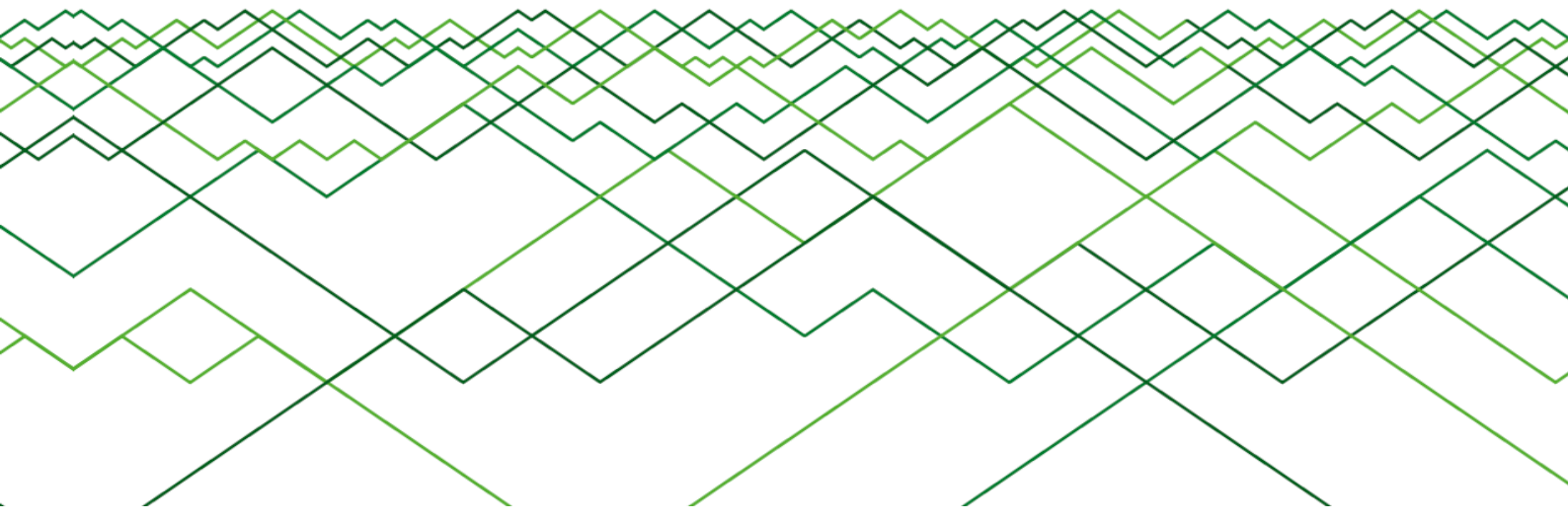
INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Analysezentrum InfoWatch
www.infowatch.com/analytics

Globale Studie von Datenpannen der vertraulichen Angaben im Jahr 2014



Inhaltsverzeichnis

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Einige Ziffern

- ✓ Im Jahr 2014 wurden auf der ganzen Welt **1395** Fällen der Datenpannen von den vertraulichen Informationen in den Medien und anderen Quellen veröffentlicht und von der analytische Zentrum InfoWatch registriert. Diese Zahl übersteigt die Anzahl der Datenpannen Jahr 2013 um 22%.
- ✓ Am meisten sind die Datenpannen mit den personenbezogenen Daten verbunden - in **92%** der Fälle wurden gerade diese Informationen gestohlen. Mehr als **767 Millionen** von personenbezogenen Daten wurden aufgrund der Fehlern oder der vorsätzlichen Handlungen von den inneren Übertreter und auch infolge der äußerlichen Angriffe kompromittiert.
- ✓ Im Jahr 2014 wurden **14** «Megadatenpannen» fixiert. Infolge jeder wurden mehr als **10 Millionen** der persönlichen Daten gestohlen. Auf der «Megadatenpannen» fallen **89%** aller kompromittierten Datensätzen.
- ✓ Die Banken zusammen mit den Internet Kundendienste, Einzelhändlern und den medizinischen Anstalt sind die Hauptquellen der personenbezogenen Datenpannen.
- ✓ In **55%** der Fälle stellte es sich heraus, dass die Mitarbeiter von Unternehmen an der Datenpanne schuld. In **1%** der Fälle - das Topmanagement eines Unternehmens.
- ✓ Russland nahm den zweiten Platz in der Zahl der bekannten Datenpannen ein. Im Laufe des untersuchten Zeitraums wurden **167** Fällen der Datenpannen von den vertraulichen Informationen aus dem Russischen Unternehmen und Staatliche Organisationen registriert. Die Anzahl der «Russischen» Datenpannen stieg im Vergleich mit dem Jahr 2013 um **73%**.

INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Inhaltsangabe

Analysezentrum der Firma InfoWatch vorlegt einen Bericht über die Studie von Datenpannen der vertraulichen Angaben im Jahr 2014. Die Autoren der Studie haben versucht, das komplette Bild von den Datenpannen in der ganzen Welt zu bauen, die Faktoren, die dieses Bild formen, zu entdecken, und die Konsequenzen der Datenpannen für kommerzielle Unternehmen, Behörden und Bürger zu zeigen.

Man kann das Jahr 2014 das Jahr von «Megapannen» personenbezogener Daten nennen. Es wurde mehr als 30 Fällen, wenn das Volumen der kompromittierten personenbezogenen Daten mehr als 1 Millionen Datensätzen ausgemacht hat. Die Hälfte dieser Datenpannen hat ein wirklich riesigen Ausmaß - 10 Millionen Datensätzen und mehr.

Die Medien haben die Angriffe auf die Infrastruktur von Einzelhändlern Home Depot, Michaels Stores, Neiman Marcus, Sally Beauty Holdings beleuchtet. Jedes Mal ging es um die Kompromittierung der persönlichen Daten einschließlich der Angaben der Plastikkarten.

Das russische Bild der Datenpannen nähert sich schnell zu dem amerikanischen. Die millionenköpfigen Datenpannen wegen der äußeren Angriffe wurden in Russland noch nicht fixiert. Aber der Betrug mit den fremden personenbezogenen Daten, die die Mitarbeitern von den Banken, den Versicherungsunternehmen, den Verkaufspunkte des Mobilfunks begehen, finden fast täglich statt. Solche Rechtsverletzungen wurden die Norm für unser Land, obwohl einige Zeit zurück als exotisch wahrgenommen wurden.

Die Autoren der Studie sind der Überzeugung, dass eine umfassende Analyse der globalen Bild von Datenpannen (wo vorherrschen die Länder, die «fortgeschritten» auf dem Gebiet der Informationssicherheit sind) sowohl für den russischen Markt, als auch für Länder mit ähnlicher Situation in der Frage des Schutzes der Informationen nützlich ist.

Methodologie

Die Studie fußt auf einer Datenbank, die von den Spezialisten des Zentrums seit 2004 ergänzt wird. In der Datenbank des Analytischen Zentrums InfoWatch werden die öffentlichen Berichte[1] über Fälle von Datenpannen[2] aus der kommerziellen und nicht kommerziellen (Staats -, Kommunal -) Organisationen, die wegen der böswilligen oder fahrlässigen Handlungen[3] der Mitarbeiter oder der externen Täter[4] passieren, zugerechnet. Datenbank des Analytischen Zentrums InfoWatch zählt mehrere tausend Vorfälle.

Während der Füllung der Datenbank wird jede Datenpanne (wenn es möglich ist, und diese Informationen in der Mitteilung über die Leckage vorhanden ist) auf einer Reihe von Kriterien klassifiziert. Das sind: die Größe der Organisation [5], der Tätigkeitsbereich (die Branche), die Schadenshöhe[6], der Typ der Datenpanne (dem Vorsatz nach), der Kanal der Datenpanne[7], die Typen der gestohlenen Daten.

Seit 2014 werden in die Datenbank auch Datenpannen, die aufgrund der äußeren Einwirkungen (Targeted Angriff, Phishing, Hacking der Web-Ressource, etc.) stattgefunden haben, hinzugefügt. Für den korrekten Vergleich der Daten von 2014 mit den Daten der früheren Perioden haben die Autoren eine Korrektur der Kennzahlen des Jahres 2013 gemacht.

Auch seit 2014 wurden die Vorfälle nach der Art der Aktionen des Täters klassifiziert. Zusammen mit den Datenpannen unterscheiden die Autoren der Studie auch die Vorfälle, wenn ein Mitarbeiter, der berechtigten Zugriff auf die Daten hat, diese Daten für Betrug benutzt (die Manipulationen mit der Zahlungsdaten oder Insiderinformationen), und wenn ein Mitarbeiter einen Zugriff auf die Daten, die er für die Erfüllung der Berufspflichten nicht braucht, erhielt (Überschreitung der Zugriffsrechte).

Die Studie umfasst nicht mehr als 1% der Vorfälle der erwarteten gesamtwirtschaftlichen Anzahl von Datenpannen. Aber die Kriterien für die Kategorisierung der Datenpannen sind so gewählt, dass die untersuchten Mengen (Kategorien) genügend oder übermäßige Anzahl der Elemente (tatsächliche Fälle von den Datenpannen) enthalten. Solche

---

[1] Die Nachrichten über Datenpannen, die von den offiziellen Behörden, Medien, Autoren der Aufzeichnung in Blogs, Online-Foren, anderen offenen Quellen veröffentlicht wurden.

[2] Die Datenpanne - die Handlung oder Unterlassung der Person, die den legitime Zugriff auf vertraulichen Informationen hat, die (Handlung) den Verlust der Kontrolle über Informationen oder die Verletzung der Vertraulichkeit dieser Informationen veranlasst, sowie der Verlust der Kontrolle über die Informationen aufgrund der externen Angriffe.

[3] Die Datenpannen werden in vorsätzliche (böswillige) und unbeabsichtigte (zufällige) in Abhängigkeit von der Anwesenheit oder Abwesenheit von Vorsatz bei der Person, die eine Datenpanne provoziert hat. Die Begriffe vorsätzliche/böswillige und unbeabsichtigte/zufällige sind paarweise gleich werden hier als Synonyme verwendet.

[4] In dieser Studie geben die Autoren ein Bild der Datenpannen unter dem Gesichtspunkt von den verantwortlichen Personen. Zum ersten Mal treffen in dieser Einteilung zusammen mit den internen Tätern auch externe Täter.

[5] Die Analysten des Zentrums InfoWatch klassifizieren Organisation für Größe, abhängig von bekannten oder vermuteten Park von Personal Computern (PC). Kleine Unternehmen mit bis zu 50 PC, Mittelunternehmen - von 50 bis 500 PC, große Unternehmen - mehr als 500 PCs.

[6] Die Daten über die Schäden und die Anzahl der kompromittierten Datensätze stammen direkt aus den Veröffentlichungen in den Medien.

[7] Unter dem Kanal der Datenpanne versteht man ein solches Szenario (Handlungen (oder Unterlassungen) der Benutzer des Unternehmensinformationssystems, die auf Hardware oder Software Dienstleistungen gelenkt wurden), in Folge dessen die Kontrolle über die Informationen verloren wurde, oder die Vertraulichkeit dieser Informationen verletzt wurde. Klassifizierung der Kanäle der Datenpannen wird im Glossar angegeben.

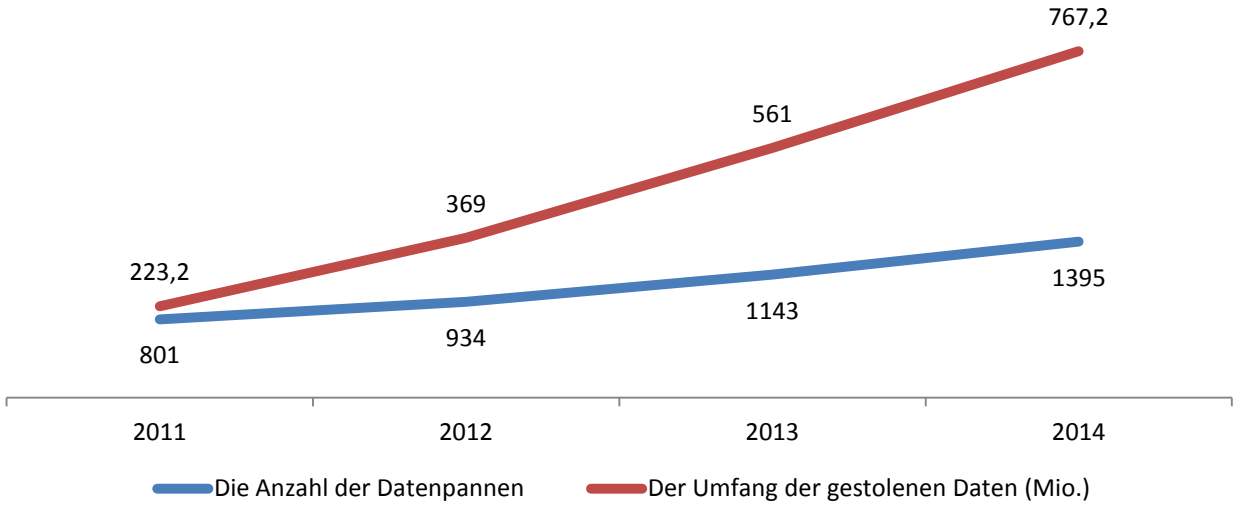
Behandlung zur Bildung des Untersuchungsfelds erlaubt die Stichprobe für theoretisch halten, sowie Schlussfolgerungen der Studie und die festgestellten für einer Stichprobe Trends für repräsentativ für die Grundgesamtheit halten.

Für die Erhaltung der Homogenität der Stichprobe bei der Zusammenstellung der Industriekarte haben wir gezielt die Datenpannen mit einem unverhältnismäßig großen (mehr als 10 Millionen) Anzahl der gestohlenen personenbezogenen Daten - «Megadatenpannen» - ausgeklammert. Bei der Zusammenstellung der Industriekarten wurden die Datenpannen mit geringen (weniger als 100) Anzahl der gestohlenen Daten aus der Stichprobe auch gelöscht.

Die Fälle von Verletzungen der Vertraulichkeit von Informationen (die erkannten Schwachstellen), andere Vorfälle (DDoS-Angriffe), die keine Datenpannen veranlasst haben, sowie Datenpannen mit obskuren Quelle der Daten (wenn es unbekannt ist, welchem Unternehmen oder welcher Organisation die kompromittierten Daten gehörten) geraten in die Stichprobe auch nicht.

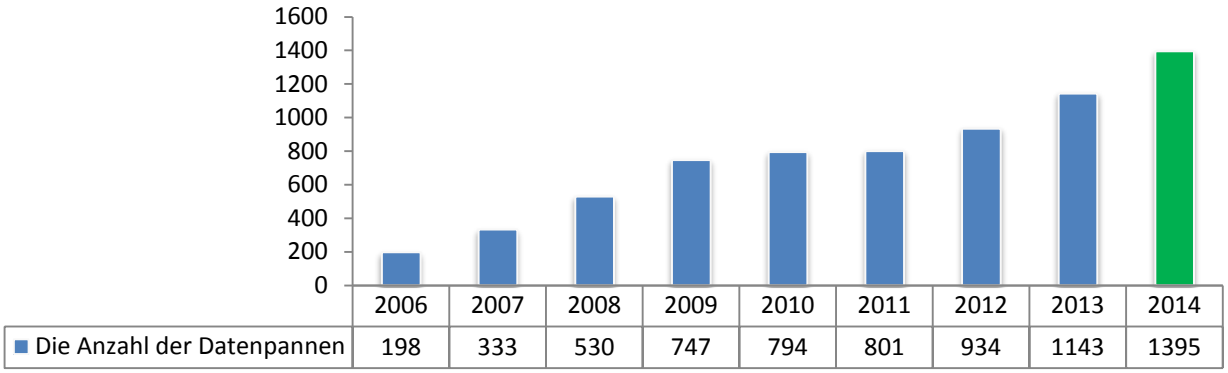
Allgemeine Statistik

Im Jahr 2014 wurden von dem Analytische Zentrum InfoWatch 1395 [8] (3,8 täglich, 116 pro Monat) Fälle von den Datenpannen registriert. Wegen der Datenpannen wurden 767 Millionen persönliche Daten (Datensätze mit den personenbezogenen Daten) darunter die Sozialversicherungsnummer, die Angaben der Plastikkarten, andere wichtige Informationen, kompromittiert (Siehe Graphik 1).



Graphik1. Die Anzahl der Datenpannen und der Umfang der gestohlenen Datensätzen mit den personenbezogenen Informationen. 2011-2014 Jahren.

Die Zahl der Datenpannen hat im Jahr 2014 fortgedauert (Siehe Graphik 2).



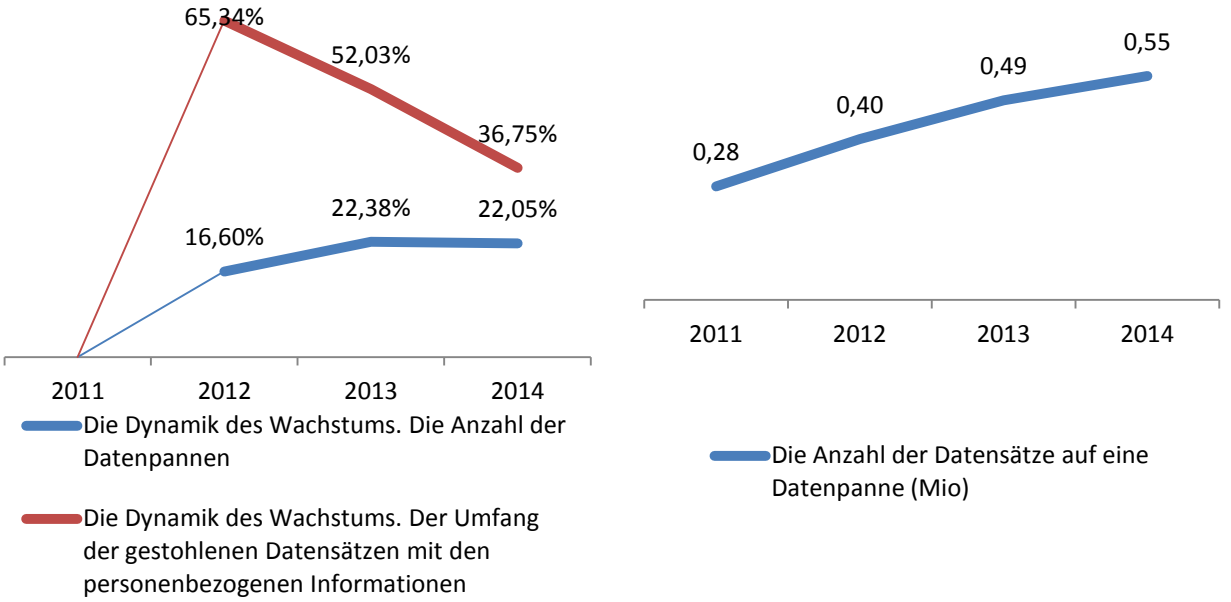
	2006	2007	2008	2009	2010	2011	2012	2013	2014
Die Anzahl der Datenpannen	198	333	530	747	794	801	934	1143	1395

Graphik 2. Die Anzahl der registrierten Datenpannen, 2006-2014 Jahren.

Im untersuchten Zeitraum blieb die Dynamik des Wachstums von den Datenpannen auf dem Niveau des Vorjahres und machte 22% zu den Datenpannen im Jahr 2013 aus. Dabei hat sich die Zunahme des Umfanges der kompromittierten personenbezogener

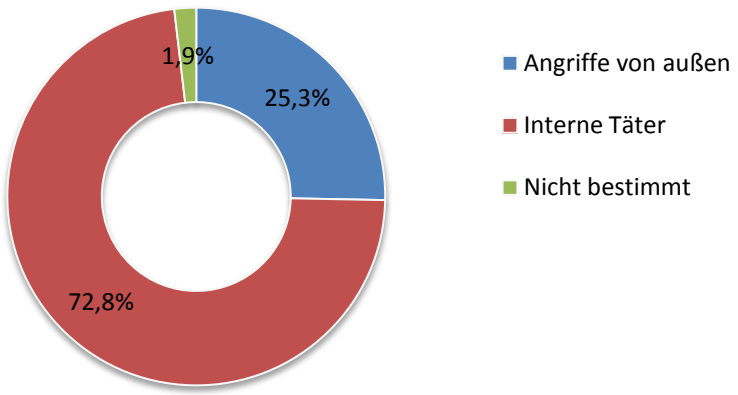
[8] Seit 2014 registriert das Analysezentrum InfoWatch zusammen mit den Datenpannen, die aufgrund der internen Täter passierten, auch die Datenpannen, die aufgrund der äußeren Einflüsse - gezielte Angriffe usw., die Kompromittierung der Daten veranlassten – passierten.

Daten verlangsamt und 37% zum Vorjahr ausgemach. Infolge einer Datenpanne wurden im Durchschnitt 0,55 Millionen Datensätzen kompromittiert – um 12% höher im Vergleich mit gleichartiger Kennziffer im Jahr 2013 (Siehe Graphik 3).



Graphik 3. Die Dynamik des Wachstums der Anzahl von den Datenpannen und des Umfangs der Datensätze. Der Umfang der personenbezogenen Daten, die im Verlauf einer Datenpanne kompromittiert wurden. 2011 -2014 Jahren.

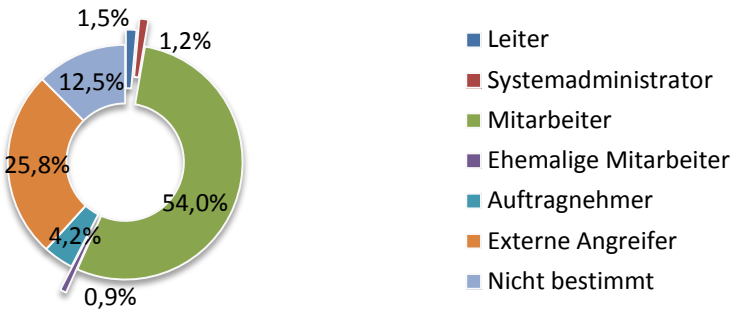
Es wurden 1016 (73%) Datenpannen, die aufgrund des internen Täters stattgefunden haben, registriert. 353 (25%) Datenpannen sind aufgrund der äußeren Einflüsse geschehen. In 2% der Vorfälle ist es unmöglich zu bestimmen, woher der Angriff durchgeführt wurde (Siehe Graphik 4).



Graphik 4. Die Verteilung der Datenpannen in den Vektor von den Auswirkungen, 2014.

Infolge der Auswirkungen der internen Täter wurden 350 Millionen persönliche Daten (0,34 Mio. auf eine Datenpanne) kompromittiert. Das Ergebnis der externen Auswirkung sind 410 Millionen kompromittierten Datensätzen (1,16 Mio. auf eine Datenpanne).

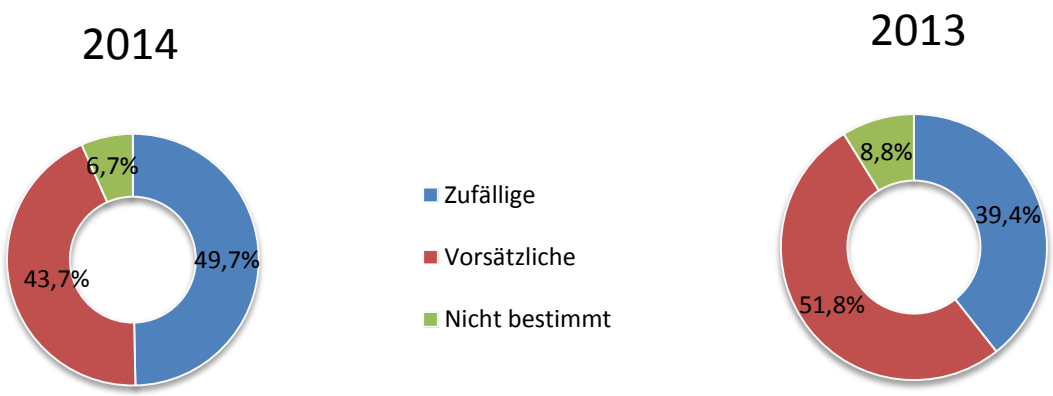
In der Verteilung auf die Täter der Datenpanne[9] machte der Anteil der Vorfälle, wenn es unmöglich ist die Täter zu bestimmen, 13% aus. In 55% der Vorfälle waren die Urheber der Datenpannen die gegenwärtige oder ehemalige Mitarbeiter, 54% und 1% dementsprechend [10](Siehe Graphik 4).



Graphik 4.Die Verteilung der Datenpannen nach der Täter, Jahr 2014.

Auch groß ist der Teil der Datenpannen, die durch Verschulden des Auftragnehmers, dessen Personal einen legitimen Zutritt auf geschützten Informationen hatte (4%), passierten. Mehr als 1% der Fälle passierten durch Verschulden der Leitung von den Organisationen (das Top-Management, die Leiter der Fachbereiche und Abteilungen) und der Benutzer mit erweiterten Zutrittsrechten auf Informationen (Systemadministratoren).

Im Jahr 2014 war weniger als die Hälfte der Datenpannen zufällig. Im Vergleich mit dem Jahr 2013 stieg der Anteil der zufälligen Datenpannen um 10%. Der Anteil von den vorsätzlichen Datenpannen verringerte sich entsprechend (Siehe Graphik 5).



Graphik 5. Die Verteilung der Datenpannen auf Vorsatz, 2013 - 2014[11]

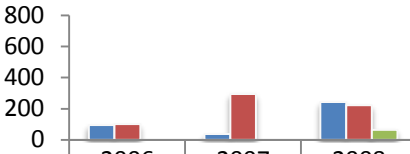
[9] Der Täter der Datenpanne – die Person, die unabsichtlich eine Datenpanne zugelassen hat, oder böswillige Handlungen, die die Kompromittierung der Informationen veranlasst hat, begangen hat.

[10] Für diese Verteilung der Stichprobe wurden die Datenpannen, wo es unmöglich ist festzugelegt, woher der Angriff verwirklicht wurde, ausgeschlossen. Auf solche Weise verteilte sich die in einem numerischen Ausdruck gleiche Anzahl der Datenpannen, die auf die Angriffe von außen fallen, als 25,3% (Graphik 4) und 25,8% (Graphik 5).

[11] Solche Datenpannen, die durch die Handlungen der externen Täter passierten, rechnen die Autoren der Studie als Voreinstellung zu den absichtlichen Datenpannen zu. Der Anteil der absichtlichen Datenpannen im Jahr 2013 wurde in einer großen Seite korrigiert, unter Berücksichtigung des Anteils der Datenpannen unter dem Einfluss der äußeren Täter, die im Jahr 2014 festgelegt wurden.

Die Umverteilung der Anteil der Datenpannen sinngemäß geschieht, weil mit der Verbreitung von Informationssicherheitsmittel (einschließlich der DLP-Lösungen) zufällige Datenpannen immer öfter fixiert werden. Die Anzahl der absichtlichen Datenpannen wächst langsamer als der zufälligen, da ihre Fixierung den Einsatz teurer Gegenmaßnahmen erfordert.

Es wurde auch eine Reduzierung des Anteils der Datenpannen, die man weder den vorsätzlichen Datenpannen, noch den zufälligen zurechnen kann, seit 9% in 2013 bis 7% im Jahr 2014. Das sind unbestimmte Datenpannen. Dieser Trend bleibt seit 2012 (Siehe Graphik 6).

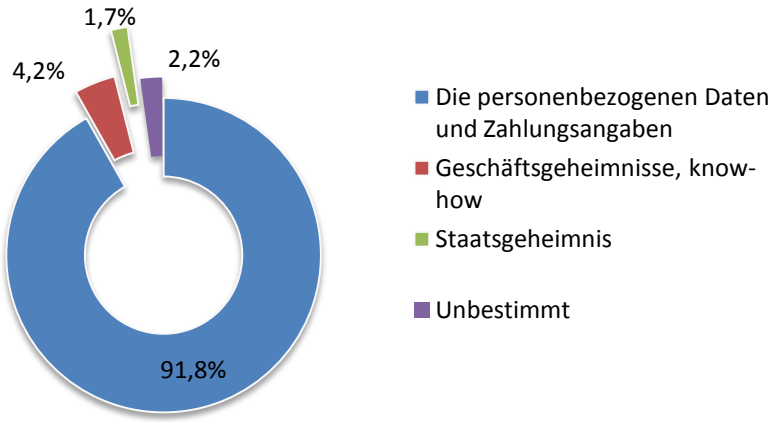


	2006	2007	2008	2009	2010	2011	2012	2013	2014
Zufällige	96	38	242	325	420	336	352	522	693
Vorsätzliche	102	295	223	382	334	344	430	687	609
Unbestimmt	0	0	65	40	40	121	152	117	93

Graphik 6. Die Dynamik der zufällige und vorsätzliche Datenpannen, 2006 -2014 Jahren

Die Forscher verbinden der Rückgang des Anteils der unbestimmten Datenpannen mit der Erhöhung der Allgemeinbildung unter den Experten für Informationssicherheit, die erfolgreich die Quelle der Datenpanne, den Täter und den Vorsatz bestimmen. Als Ergebnis bekommt man weniger Nachrichten über die Datenpannen, wenn der Kanal der Übertragung von Informationen und die Absicht des Täters unklar sind.

Der Anteil der Lecks von den personenbezogenen Daten und Zahlungsangaben in der Verteilung nach Typen der Informationen stieg um 7% im Vergleich mit den Daten des Jahres 2013 und machte 92% aus (Siehe Graphik 7).



Graphik 7. Die Verteilung der Datenpannen nach Datentypen, 2014

Auf die «Megadatenpannen» mit einem Volumen von kompromittierten Daten mehr als 10 Millionen Datensätze fielen 89% aller kompromittierten Daten. Die Medien haben Angriff

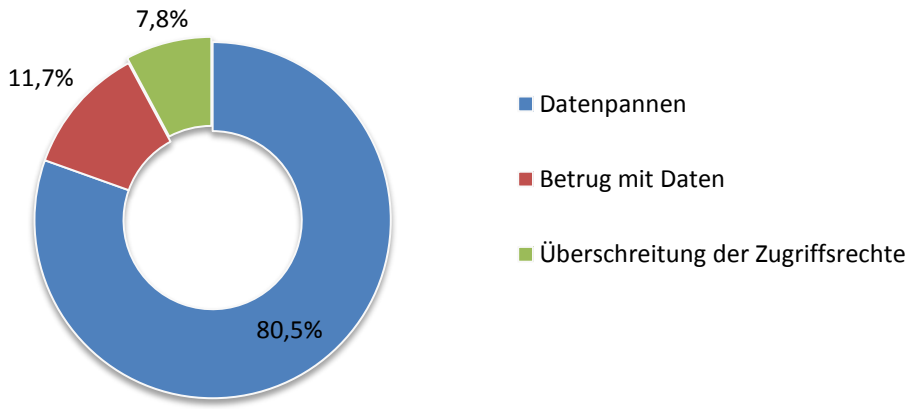
auf die Infrastruktur Target Corp aus allen Seiten beleuchtet. Auch bezeichnend war die externe Angriff auf andere Einzelhändler - Home Depot - am Ende 2014:

> securitylab.ru: *Das weltweitgrößte Unternehmen, das sich mit dem Verkauf von Baustoffen und Werkzeuge beschäftigt, Home Depot erklärte, dass 53 Millionen E-Mails von den Kunden der Handelskette kompromittiert wurde. Nach vorläufigen Schätzungen haben die Schäden von Home Depot wegen des Verlusts $56 Millionen US-Dollar. Es gelungen der Hacker, mit der Hilfe des Passwortes von außenstehenden Softwareentwicklungsingenieurn in das Netzwerk von Home Depot einzudringen. Durch die Manipulation mit den Zugriffsrechten erhielten die Verbrecher einen Zugriff auf mehrere Segmente Netzwerk des Unternehmens. Die Hacker haben das System mit der Malware infiziert, mit dessen Hilfe wurde Information - E-Mail Adressen und Bankverbindungen von Plastikkarten - gestohlen. Die Experten von Home Depot bemerken die Einzigartigkeit der Malware, die die Verbrecher für den Angriff auf Home Depot benutzt haben. Antivirensoftware von Home Depot konnten nicht die verdächtigen Aktivitäten seitens der Hackerprogramme aufdecken.*

Im Jahr 2014 wurde eine große Anzahl von den Datenpannen mit der Verwendung der personenbezogenen Daten für die Zwecke des Betrugs – die Verbrechen, die als «Identitätsdiebstahl» (identity theft) bekannt sind.

> Vedomosti: *Die Namen, Adressen, Telefonnummern und E-Mail-Adressen von rund 83 Millionen Besitzern der privaten Haushalte und der Unternehmen wurden durch das JPMorgan Chase System gestohlen. Das ist eine des größten Diebstahls von persönlichen Daten in der Geschichte. 76 Millionen von privaten Konten und 7 Millionen Konten, die kleinen Unternehmen gehören, wurden den Angriff ausgesetzt.*

In der Verteilung nach der Art der Aktionen des Täters (Siehe Graphik 8) wurden in 81% der Fälle «klassische» Datenpannen - der Verlust der Kontrolle über die Informationen fixiert.



Graphik 8. Die Verteilung der Vorfälle dem Wesen nach, 2014

8% der registrierten Vorfälle wurden als Störungen im Zusammenhang mit Erhalt eines unberechtigten Zugriffs auf Informationen klassifiziert (die Überschreitung der Zugriffsrechte, die Manipulation mit der Informationen, die die Mitarbeiter für die Erfüllung der dienstlichen Pflichten nicht brauchen).

> *databreaches.net: Ein Mitarbeiter des Büros in der spanischen Bank Santander in dem Grafschaft Leicestershire (England) wurde vom Gericht 880 Pfund Sterling Strafgeld für unnötig Interesse an dem Lohn seiner Kollegen zahlen gelassen. Der 29-jährige Dalvinder Singh arbeitete in der Abteilung gegen Geldwäsche, so hatte er einen legitimen Zugriff auf den Konten der Kunden von der Bank. Jedoch beschloss er seinen erweiterten Zugriff zu benutzen, um die Höhe des Lohnes von seiner Kollegen aufzuklären. In Ergebnis der Vorfall wurde der neugierige Mitarbeiter gefeuert. Die Vertreter der Bank haben erzählt, dass Singh kurz vor dem Vorfall das Training über die Grundsätze der Arbeit mit sensiblen Informationen besucht hatte. Aber es hat nicht geholfen.*

In 12% der Fälle wurde der Diebstahl der Informationen mit ihrer unrechtmäßigen Nutzung zum Zweck der persönlichen Bereicherung (in der Regel ist das ein finanzieller Betrug der Mitarbeiter der Kreditinstitute - Fraud) belastet.

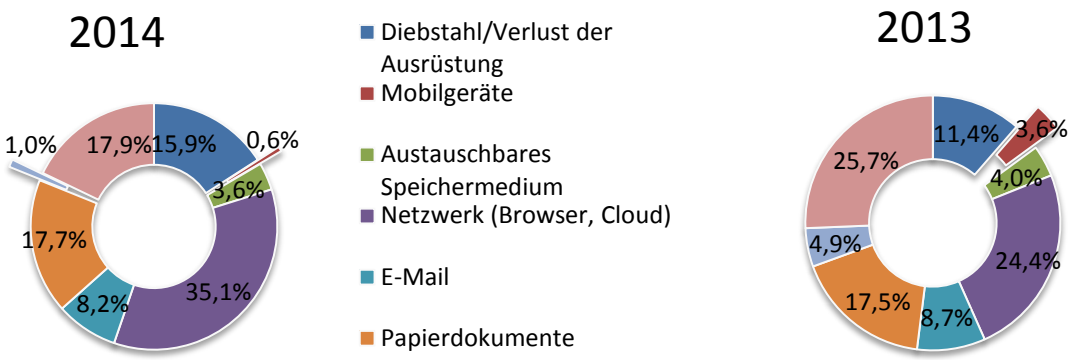
> ***Schlussfolgerung:***
>
> *Die Zunahme des Umfanges der kompromittierten personenbezogenen Daten findet durch die «Megadatenpannen» statt. Die Zunahme der Zahl von Datenpannen passiert meistens durch externe Angriffe. Die wichtigsten Indikatoren, darunter die Dynamik des Wachstums von Datenpannen, der Anteil der persönlichen Daten und Geschäftsgeheimnisse, der Anteil der Mitarbeiter in der Verteilung nach dem Täter der Datenpanne, bleiben fast unverändert von Jahr zu Jahr. Der Anteil der unbestimmten Datenpannen geht konsequent zurück.*

Kanälen der Datenpannen

Das Studium der Datenpannen unter dem Gesichtspunkt von den Kanälen, wodurch die Informationen gehen weg, hat praktische Bedeutung. In Abhängigkeit von der Häufigkeit der Datenpannen auf die eine oder andere Weise kann man die Einführung von Schutzmaßnahmen in Unternehmen oder in der Branche empfehlen und bestimmen, welchen Kanälen man erhöhte Aufmerksamkeit schenken soll.

Im Jahre 2014 verminderte sich der Anteil der Datenpannen durch austauschbaren Speichermedium (-0,4 Prozentpunkte), E-Mail (-0,5 Prozentpunkte), Stimm- und Bildkanälen, Instant Messaging (-3,9 Prozentpunkte). Der Anteil der Datenpannen der Papierdokumenten veränderte sich nur geringfügig (+0,2 Prozentpunkte). Im Vergleich mit den anderen Kategorien wuchs die Anzahl der Datenpannen, die mit dem Diebstahl oder Verlust der Ausrüstung, einschließlich Laptops und Smartphones (+4,5 Prozentpunkte) verbunden, merklich heran.

In 18% der Vorfälle gibt es in den Mitteilungen über die Datenpannen keine Informationen über den Kanal. Der Anteil solcher Fälle schrumpfte um 7,8 Prozentpunkte (Siehe Graphik 9).



Graphik 9. Die Verteilung der Datenpannen nach den Kanälen, 2013 – 2014 Jahren

Der Anteil von den Datenpannen durch das Netzwerk machte 35% (+10,7 Prozentpunkte) aus. Das ist leicht zu erklären. Gerade durch diesen Kanal finden die Datenpannen infolge der äußeren Angriffen statt.[12]

> *The Wall Street Journal: Durch einen Hackerangriff wurden die personenbezogenen Daten der Mitarbeiter, der Führung und der Kunden von dem US Postal Service (USPS) kompromittiert. Unter die Finger der Verbrecher kamen vermutlich 800 tausend Datensätze, einschließlich der Namen, der Anschriften und der Sozialversicherungsnummern von den Amerikanern. Unter den Geschädigten sind sowohl heutige Mitarbeiter, als auch ehemalige Mitarbeiter, die schon in Rente*

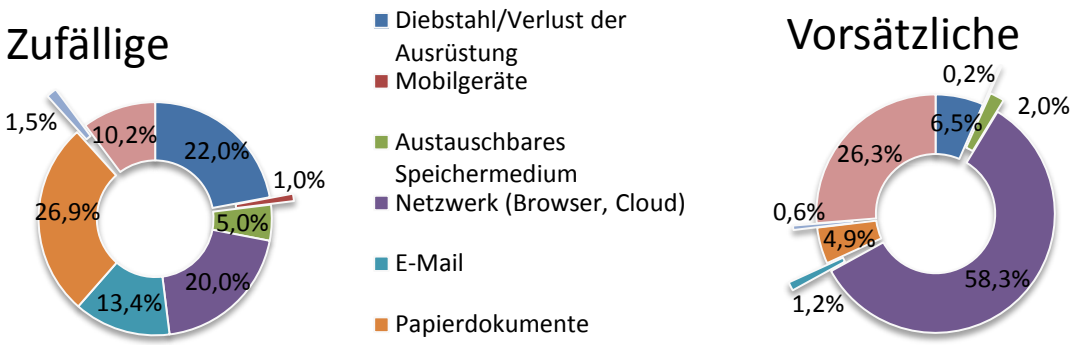
[12] Bei der Verteilung nach den Kanälen kommen in Anschlag auch die Datenpannen, die wegen der äußeren Einwirkungen passieren. Solche Datenpannen finden ausschließlich im Netzwerk statt. Deshalb haben die Autoren für die Daten des Jahres 2013 den Anteil des Netzwerkkanals in Richtung der Erhöhung im Verhältnis, das dem Anteil der Datenpannen, die wegen der äußeren Angriffen passieren, im Jahre 2014 gleich ist.

gegangen sind. Der Angriff hat die Abteilung von US Postal Service und Inspektionsdepartament betroffen.

Die Datenpannen wegen der mobilen Geräte haben sich vermindert (-3 Prozentpunkte). Ein kleiner Anteil von den Datenpannen ist mit niedrigem Wirkungsgrad bestehender Lösungen zum Schutz von Daten auf Smartphones, Tablet-PCs verbunden. Es bedeutet aber nicht, dass es unmöglich ist, eine Datenpanne wegen der mobilen Geräte aufzuspüren:

Triblive: Ein Top-Manager der Bank Eileen Daly fotografierte den Bildschirm des Computers mit der Hilfe des persönlichen Handys kurz bevor sie den Job wechselte. Jetzt arbeitet sie bei Morgan Stanley, ein Konkurrent der PNC Bank. Das Informationssicherheitssystem der Bank hinderte Eileen daran, einfach die Daten der Kunden in elektronischer Form zu kopieren. Deshalb fotografierte sie den Bildschirm des Computers. Nach den Schätzungen der PNC Bank, macht die Schadenssumme von den Aktionen des ehemaligen Top-Managers 250 Millionen US-Dollar aus. Die Vertreter der Bank sagten, dass mindestens 15 große Kunden an die Wettbewerber gingen.

Die Anteile der Datenpannen wegen austauschbares Speichermediums, E-Mails, Papierdokumente sind unbedeutend. Zum Vergleich: im Jahr 2013 der Anteil von vorsätzlichen Datenpannen wegen E-Mail machte 5,8% aus; im Jahr 2014 durch diesen Kanal beobachteten wir 1,2% der vorsätzlichen Datenpannen. Die Anteile der zufälligen und vorsätzlichen Datenpannen unter Ausnutzung von mobilen Geräten machten 1% и 0,2% entsprechen (Siehe Graphik 10).



Graphik 10. Die Verteilung der zufälligen und vorsätzlichen Datenpannen, 2013 – 2014

Man muss Aufmerksamkeit schenken, dass der Anteil der Datenpannen nicht immer die Größe des Risikos, das mit einer bestimmten Kanal verbunden ist, widerspiegelt. So durch den Kanal «E-Mail» werden 13% aller zufälligen Datenpannen und nur 1% aller vorsätzlichen Datenpannen registriert. Aber es ist offensichtlich, dass nur ein Fall von Datenpannen der wichtigen Informationen per E-Mail genug ist, um millionenköpfig finanzielle Verluste für die Firma zu veranlassen.

Bloomberg: Kang Gao, der ehemalige Analytiker des Fonds Two Sigma Investments LLC, wurde wegen des Diebstahls von vertraulichen Angaben angeklagt. Der Analytiker wurde noch im Januar festgenommen, nachdem er

seinen Rücktritt aus der Two-Sigma-Investments erklärt hat. Laut der Aussagen der Vertreter von Two Sigma hat Kang Gao mit der Hilfe eines Dekompilierers einen Zugriff zur Information in den verborgen Module der körperschaftlichen Software erhalten. Dann schickte er diese Information auf seine persönliche E-Mail. Die Verbreitung der gestohlenen Daten fügt Schaden der Firma zu, erkennen die Vertreter der Two Sigma an.

Man muss noch einen ziemlich exotischen Kanal nicht unerwähnt lassen. Das sind Datenpannen durch Text-und Videoservices von Instant Messaging. Dieser Kanal wird mit geringen 1,5% in dem Diagramm der zufälligen Datenpannen und mit 0,6% im Diagramm der böswilligen Datenpannen dargestellt. Aber die Entstehung solcher Datenpannen ist an und für sich ein Argument ins Gefecht der alten Wahrheit, dass es keine «Kleinigkeiten» und unwichtige «Peripheriekanäle» auf dem Gebiet der Informationssicherheit gibt.

Es ist weitbekannt, dass die DLP-Systeme in der Identifizierung und der Verhinderung von Datenlecks die effektivste sind. Die immer größere Verbreitung von Lösungen der Klasse DLP ermöglicht die Unternehmen, die zufällige Datenpannen, die bisher unentdeckt geblieben, zu registrieren und sie richtig zu klassifizieren. Damit ist die Verringerung des Anteils der zufälligen Datenpannen durch unbestimmten Kanal verbunden.

Allerdings bleibt manchmal auch für die großen Datenpannen der Datenkanal unbekannt:

delfi.lv: Der Datenverlust, der während des Verkaufs der von den lettischen Staat kontrollierten Kommerzbank Citadele passierte, hat den Staat 7 Millionen Euro gekostet, schreibt das Portal delfi.lv unter Bezugnahme auf den Minister für Wirtschaft Wjatscheslaw Dombrowski. Nach den Worten des Ministers führte der Verlust in den gegenwärtigen geopolitischen Bedingungen zu einer Abnahme der Zahl der potenziellen Investoren. Einige Investoren haben über die Interessen der Mitbewerber erfahren, erklärte Herr Dombrowski. Als Ergebnis ist der Preis des Aktivbestands bedeutend gesunken.

Kleine Anteile der Datenpannen wegen austauschbares Speichermediums, E-Mails, Papierdokumente (besonders auf dem Hintergrund des ziemlich wesentlichen Anteils dieser Kanäle in der Verteilung der zufälligen Datenpannen) sind erklärbar. Die Missetäter nutzen immer weniger diese Kanäle, um rechtswidrige Handlungen zu begehen. Der «fortgeschrittene» Täter weiß gut, dass die modernen Mittel der Kontrolle der Information es ermöglichen, erfolgreich die Übertragung von vertraulichen Informationen auf diesen Kanälen abzufangen und riskiert unüberlegt nicht.

Schlussfolgerung:

Ein bedeutender Unterschied in der Verteilung der vorsätzlichen und der zufälligen Datenpannen durch die Kanäle sagt über die wachsende Qualifikation des inneren Täters. Die Datenverluste durch die «traditionellen» Kanäle werden immer weniger fixiert, weil die Verbrecher sie nicht nutzen, weil sie gut informiert über die Funktionalität schützende Lösungen sind.

Industriekarte

Im Jahr 2014 ist der Anteil von Datenpannen aus staatlichen und kommunalen Behörden im untersuchten Zeitraum um 16 Prozentpunkte gesunken und hat 16% ausgemacht. Dabei ist der Anteil der Datenpannen aus den Unternehmen um 13 Prozentpunkte gestiegen (Siehe Graphik 11).

Graphik 11. Die Verteilung der Datenpannen nach den Typen der Organisationen ,2013 – 2014 Jahren

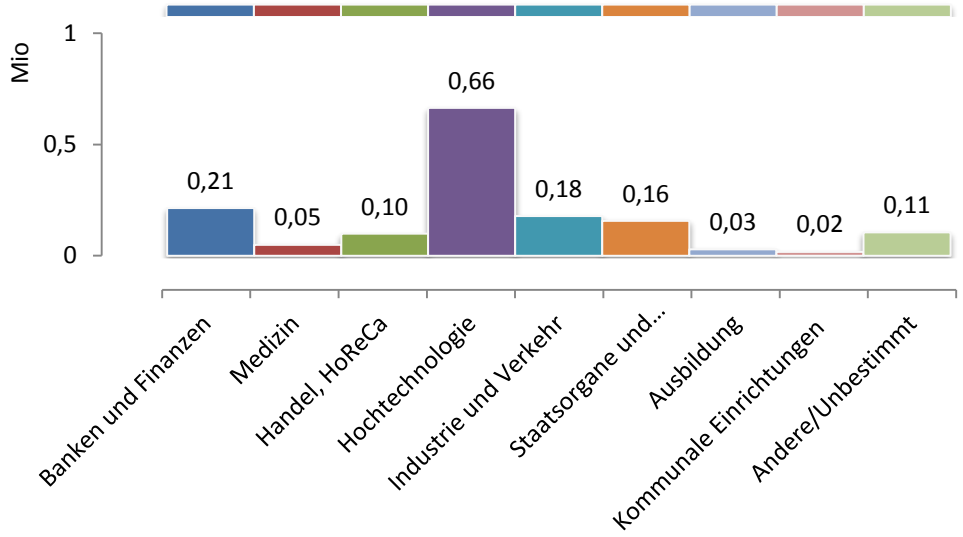
Die Datenpannen wurden meistens in der Medizin (25%) und seltener in kommunalen Einrichtungen (2%) fixiert. Dabei gehören die Siegeslorbeeren auf dem Gebiet der kompromittierten Datensätzen der Bankvertikale (41%). Halb so viel Daten wurden aus den Hochtechnologieunternahmen (17%) und den Handelsunternehmen (15%) gestohlen (Siehe Graphik 12).

Graphik 12. Verteilung der Anzahl der Datenpannen und Umfang der kompromittierten personenbezogener Daten nach der Industrie, 2013 – 2014 Jahren

Diese Aufteilung beeinflussen stark die «Megadatenpannen», wenn die Anzahl der kompromittierten Datensätzen 10 Millionen überstiegt. Andererseits sind aus der Verteilung «leere» Datenpannen (wenn die Anzahl der kompromittierten Daten weniger als 100 oder unbekannt ist) nicht ausgeschlossen. Um den Einfluss der «leere» und «Megadatenpannen» auf das Ergebnis zu neutralisieren, haben die Autoren der Studie

die Stichprobe korrigiert und nur die Datenpannen mit dem Volumen von kompromittierten Daten mehr als 100 und weniger als 10 Millionen Datensätze benutzt. Weitere Grafiken sind aufgrund der korrigierten Daten gebaut.

Die Verteilung der kompromittierten Datensätze im Hinblick auf eine Datenpanne unter dem Gesichtspunkt von der Branche ermöglicht die Branche auszuzeichnen, die am meisten unter dem Leck von personenbezogenen Daten leiden (Siehe Graphik 13).



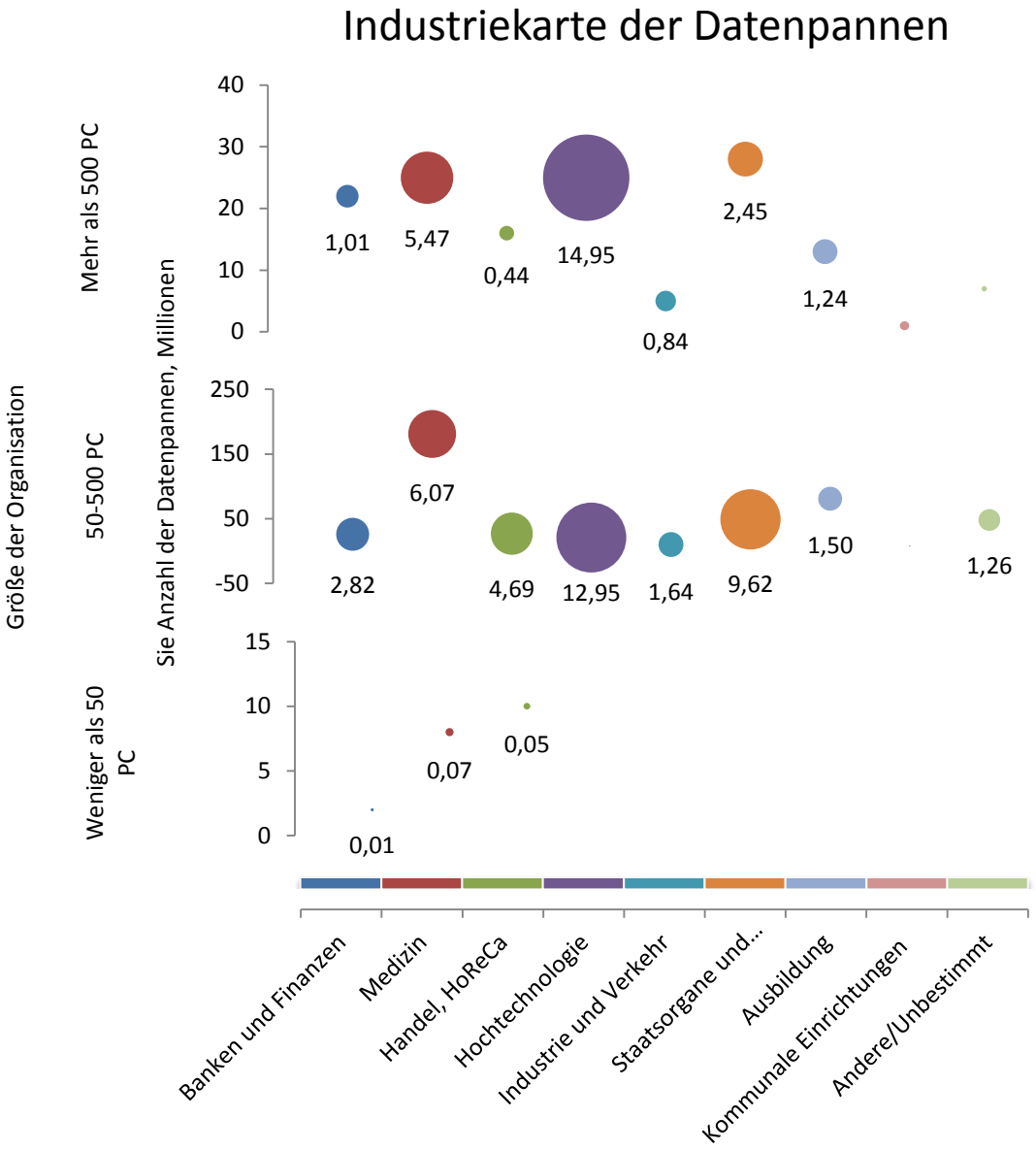
Graphik 13. Der Umfang der kompromittierten Datensätze von personenbezogenen Daten auf eine «nicht leere» Datenpanne nach Branchen. 2014, Millionen

Die führende Position bei diesem Indikator nahm die Vertikale der Hochtechnologie (wegen der Internet-Dienste), wo auf eine Datenpanne 0,66 Millionen kompromittierten personenbezogenen Daten (einschließlich Finanzdaten der Mitarbeiter und der Kunden) fallen.

> *The Irish Times: 500 tausend Euro hat der irische Hersteller der Kundenkarten Loyaltybuild auf die Aktualisierung der Informationssicherheitssystem und der Beseitigung der Folgen den größten in der Geschichte Irlands Datenpanne ausgegeben. Von dem Datenverlust wurden etwa 1,6 Millionen Menschen geschädigt. Nicht nur die Namen und die Adresse der Kunden, sondern auch die Zahlungsinformationen einschließlich der Kreditkartendaten und der Sicherheitscodes wurden gestohlen. Diese Information wurde unverschlüsselt gehalten. Während der Untersuchung wurden alle Operationen von Loyaltybuild untergebrochen. Das Unternehmen konnte die Aktivität erst 3 Monate nach dem Vorfall wieder anfangen.*

Die Banken neben den Einzelhändlern sind auch bedeutsam «Lieferer» der personenbezogenen Daten auf den Schwarzmarkt.

Die Industriekarte veranschaulicht den Geschäftsstand auf dem Gebiet der Datenpannen. In den Diagrammen sind die Gesamtgröße der kompromittierten personenbezogener Daten in der Branche (die Größe der Blasen) mit der Aufteilung nach Größe der Unternehmen und die Anzahl der aufgezeichneten Datenpannen (vertikal Position der Blasen) dargestellt (Siehe Graphik 14).



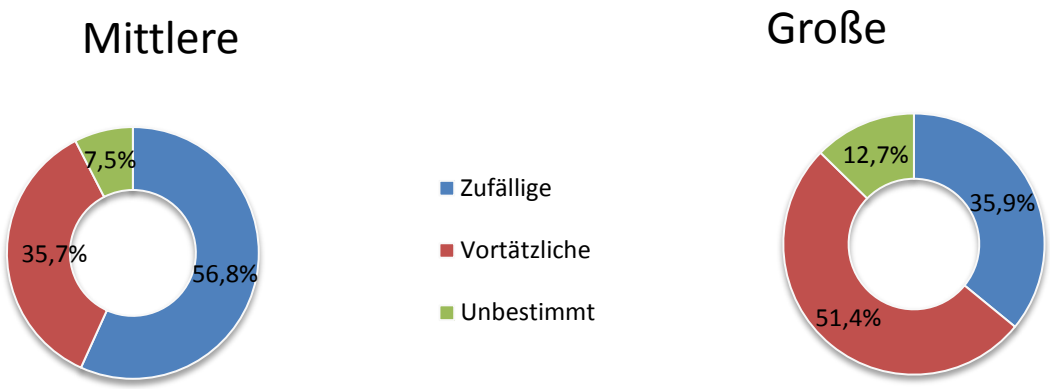
Graphik 14. Industriekarte der Lecks personenbezogener Daten, Millionen 2014

Die Industriekarte im untersuchten Zeitraum kam ungleichartig heraus. Die größte Menge von kompromittierten Daten fiel auf die Hochtechnologie Unternehmen (einschließlich Internet-Dienstleistungen). Auch bedeutend sind die Teile von den Staatsorganen, Medizin und Handel.

> *The Telegraph: Medizinische Daten von 47 Millionen Patienten der medizinischen Anstalten des Systems NHSC wurden dem Versicherungsunternehmen verkauft. Mit Hilfe dieser Informationen will das Versicherungsunternehmen sein System von Subventionen und Prämien «verbessern» und die Risiken für die Krankenversicherung durchsehen. Auf der Basis der verkauften Informationen*

stellte es sich heraus, dass die Leute vor 50 Jahren häufiger krank sind, als die Versicherer bisher gedacht haben. Es ist noch unbekannt, welche Maßnahmen die zuständigen Behörden von Britannien in Beziehung auf die Ärzten Versicherer ergreifen werden.

57% der Datenpannen aus den mittleren Unternehmen gehören zu den zufälligen Datenpannen. 36% machen vorsätzliche Datenpannen aus. In großen Unternehmen ist die Verteilung anders. Hier wurden 36% der zufälligen Datenpannen fixiert, mehr als die Hälfte (52%) bilden die vorsätzlichen Datenpannen (Siehe Graphik 15).



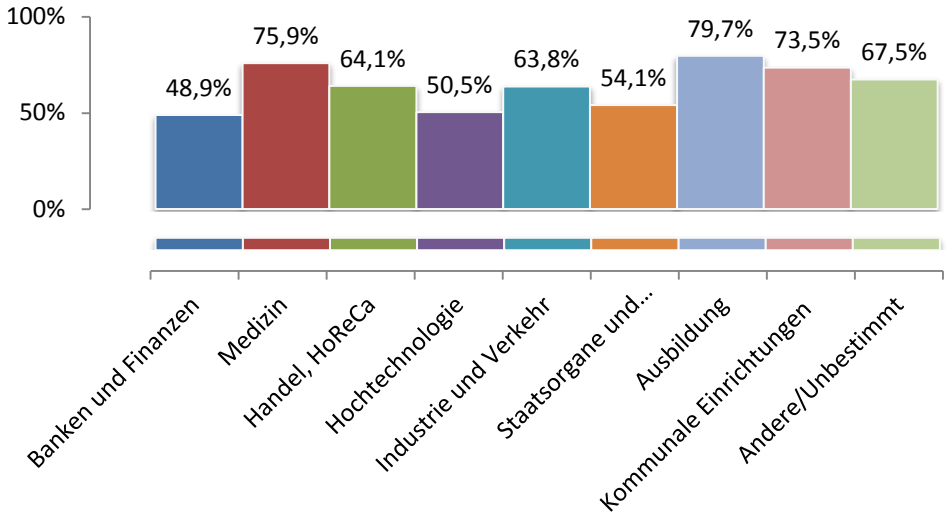
Graphik 15. Die Verteilung der Lecks der personenbezogenen Daten nach der Größe der Organisation, 2014

Die Gesamtzahl der Lecks personenbezogener Daten im Segment der mittelgroßen Unternehmen (bis 500 PC) ist deutlich höher als im Segment der großen Unternehmen. Auf mittelgroße Unternehmen fielen 71% aller Datenpannen; auf großen Unternehmen - 24%.

Die Verteilung nach Volumen der kompromittierten personenbezogener Daten kam ganz anders heraus: 45% der Datensätze wurden von den mittelgroße Unternehmen kompromittiert, 55% - von den großen (Siehe Graphik 16).

Graphik 16. Die Verteilung der Datenpannen nach der Größe der Organisation, 2014

Bei genauerer Betrachtung stellt es sich heraus, dass auf die Organisationen mittlerer Größe je nach Branche von 49% bis 80% der Datenpannen fallen.



Graphik 17. Der Anteil der Datenpannen aus mittelgroßen Unternehmen nach den Branchen. Jahre 2014

In vielen vertikalen war der Umfang personenbezogener Daten, die aus den mittelgroßen Unternehmen gestohlen wurden, nicht weniger, als den Umfang der Daten, die große Unternehmen kompromittiert haben. Im Handel und in der Medizin «gingen» aus der mittlere Unternehmen auch mehr Daten als aus den großen Unternehmen in diesen Branchen weg.

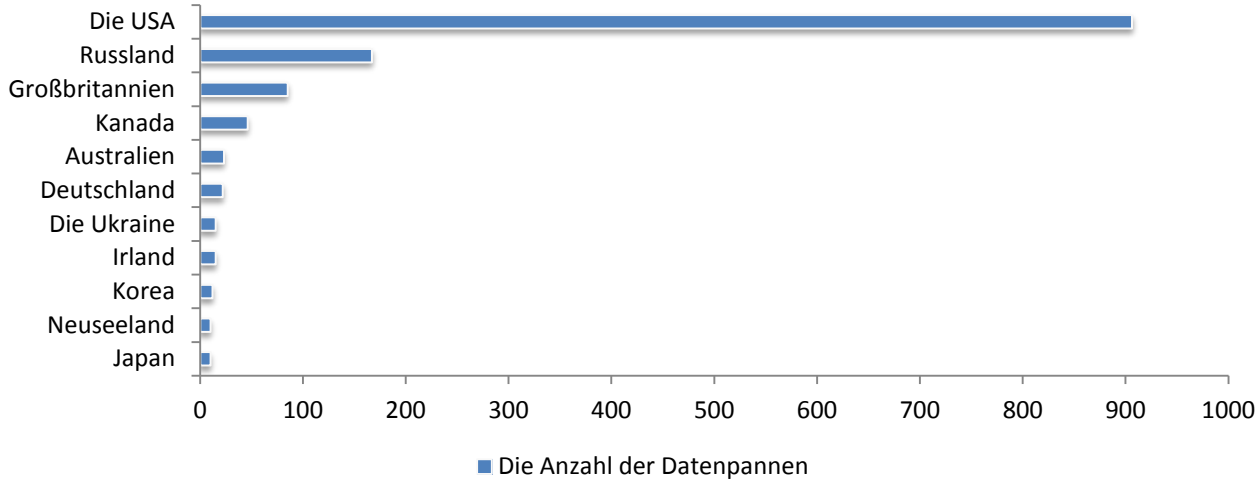
Schlussfolgerung:

Die Situation mit dem Schutz personenbezogener Daten in den Unternehmen ist weitab von dem Ideal. In höherem Grad betrifft es die mittelgroße Unternehmen, wo Datenlecks häufiger als in großen Unternehmen passierten. Dabei fiel der größte Teil der Datenpannen im mittleren Unternehmen auf die zufällige. Im Jahr 2014 nahmen die mittelgroße Unternehmen eine beherrschende Stellung in der Reihe der «Anbieter» der vertraulichen Informationen. In dieser Hinsicht sind Internet-Dienstleistungen, Bildungs-und Gesundheitseinrichtungen besonders sichtbar. Gerade diese Organisationen haben die größten Mengen von den persönlichen Daten und haben es nicht eilig, diese Daten zu schützen, da sie keine direkte finanzielle Verluste tragen.

Der Grund der so freudlosen Geschäftslage von der kleine und mittlere Unternehmen ist der Mangel an den effektiven und kostengünstigen Mitteln zum Schutz der Informationen, die auf das SMB-Segment orientiert sind.

Regionale Besonderheiten

In der Verteilung der Datenpannen nach Regionen nahmen die USA im Jahr 2014 traditionell den ersten Platz nach der Anzahl der Leckagen (906 oder 65% aller Datenpannen) ein. Russland nahm den gewohnten zweiten Platz (167 Datenpannen), wie es im Jahre 2013 war. Auf dem dritten Platz steht Großbritannien (85 Datenpannen).



Graphik 18. Die Verteilung der Datenpannen nach den Ländern, 2014

Diese Verteilung der Datenpannen hat eine Besonderheit. Die ersten Plätze nehmen die Länder, wo der Staat, die Gesellschaft und die Medien dem Thema des Datenschutzes erhöhte Aufmerksamkeit widmen. Derzeit sind das angelsächsische Länder und Russland. Für subjektive Empfinden werden in anderen Ländern nicht weniger Daten kompromittiert, aber keine Information über Datenpannen wird in den Medien veröffentlicht.

Die heutige globale Bild von Datenpannen ist mit geringfügigen Unterschieden für alle Länder, wo man mit den Informationen in elektronischer Form operiert, kennzeichnend. Hier gibt es ein Beispiel für die Nutzung personenbezogener Daten für die Zwecke des Betrugs in der amerikanischen Bank:

> *The Fresno Bee: Eine Mitarbeiterin des Finanzamtes USA (IRS) in Fresno (Kalifornien) hat sich innerhalb von zwei Jahren mit der Finanzmanipulationen unter Ausnutzung der persönlichen Daten Ihrer Kollegen beschäftigt. Virириana Hernandez arbeitete in dem Finanzamt seit 2006 und hatte aus dienstlicher Verpflichtung den Zugriff auf die Daten der Kollegen. Mit der Hilfe dieser Daten hat Virириana zusammen mit drei Komplizen von Konten der Kollegen mehr als 1,2 Millionen US-Dollar gestohlen. Jetzt droht der Betrügerin eine Haftstrafe Geldstrafe in Höhe von 250 Tausend US-Dollar. Sie kann zu dreißig Jahren Gefängnis verurteilt werden, falls ihre Schuld im Gericht beweisen wird.*

Hier gibt es eine ähnliche Situation in Russland:

> *oblvesti.ru: Die Mitarbeiterin der Geschäftsbank in Wolgograd wird vor dem Gericht wegen Betrug gestellt. Die Abteilung «K» des Innenministeriums und der lokalen FSB haben festgestellt, dass die 24-jährige Bewohnerin von Wolgograd, ihre*

Position für eigene Zwecke ausgeschlachtet hat, und die personenbezogenen Daten von den Kunden der Bank, wo sie arbeitete, ihren Komplizen übergegeben hat. Mit der Hilfe von diesen Daten stielen die Verbrecher das Geld aus den Konten der Kunden. Später haben sie dieses Geld in den Bankautomaten der Stadt Wolgograd eingelöst. Im Verlauf der Durchsuchung hat die Polizei bei der Mitarbeiterin der Bank und ihrer «Freunde» mehr als eine halbe Million Rubel in bar, 16 Karten, 10 Handys, mehr als 20 SIM-Karten verschiedener Mobilfunkbetreiber, Computertechnik, und acht Pässe der Bürger der Russischen Föderation entdeckt.

Die wesentlichen Unterschiede kann man nur in der Behandlung zum Thema der Datenpannen finden. In Russland verhalt sich man zu dem Kompromittieren der Daten sehr ruhig. Und, zum Beispiel, in den USA gibt es die Vorfälle, wenn die Mitarbeiter, deren Daten kompromittiert wurde, stellten die Ansprüche an dem Unternehmen, das eine Datenpanne zugelassen hat.

Pittsburg business times: Zwei Mitarbeiter des Krankenhauses UPMC McKeesport in Pittsburgh (USA) klagten gegen ihren Arbeitgeber wegen des unpassenden Schutz der Personenbezogenen Daten. Die Kläger behaupten, dass die unbekannten Hacker das Informationssystem des Krankenhauses gehackt haben und einen Zugriff auf die Finanzdaten der Mitarbeiter erhalten haben. Dann haben die Missetäter einige Bankkonten auf den Namen der Angestellten eröffnet und die falsche Forderung nach der Rückzahlung der Steuern (income tax returns) ausgefertigt. Die Angestellte, die durch die Handlungen der Betrüger geschädigt wurden, sind sicher, dass ihrer Klage den Kollektivstatus zuerkennt wird. Es ist bekannt über 50 ähnlichen Fällen, wenn die Daten der Angestellte des Krankenhauses bereits ausgenutzt wurden.

Und ein ganz ungewöhnlich für Russland ist, zum Beispiel, die Situation, wenn nach einer Datenlecks die Top-Manager großer Unternehmen ihre Positionen verlieren. In den russischen Medien kann man kaum eine solche Geschichte finden, und in Südkorea wurde einen ähnlichen Fall vor kurzem registriert:

Cnews: berichtet mit Bezug auf The Wall Street Journal, dass die Verantwortung für die jüngsten Datenpannen aus drei koreanischen Organisationen die Top-Manager dieser Unternehmen übergenommen haben. Mehr als 100 Millionen Kunden der größten Spieler des Finanzmarktes Korea - KB Financial Group, NongHyup Financial Group und Lotte Group wurden von der Datenpanne geschädigt. Im Zusammenhang mit dem Vorfall haben Dutzende von Top-Managern der Banken ihren Abschied eingereicht. Die Datenpanne wurde Anfang 2014 bekannt, wenn es die Behörden in Südkorea gelang, einen Mitarbeiter von Korea Credit Bureau festzunehmen. Dieser Mitarbeiter beschäftigte sich mit der Wartung der drei betroffenen Unternehmen (nach einer anderen war er ein Wirtschaftsprüfer).

Schlussfolgerungen und Prognosen

Das Jahr 2014 ist durch eine Reiche der Lecks personenbezogener Daten und Zahlungsangaben gekennzeichnet. Der Angriff auf eine Handelskette Target war am bekanntesten, aber nicht einzig. In Folge der 14 «Megadatenpannen» wurden mehr 683 Millionen Datensätzen - 89% des gesamten kompromittierten personenbezogener Daten - kompromittiert. Es wurde mehr als 30 Fällen fixiert, wenn der Umfang der kompromittierten personenbezogenen Daten mehr als 1 Millionen Datensätzen ausgemacht hat.

Fast drei Viertel der Lecks personenbezogener Daten sind mit dem «Identitätsdiebstahl» zusammengebunden. Gestohlene Information wurde in den betrügerischen Schemen benutzt. Die Verbrecher fertigten Darlehen und Steuervergünstigungen auf fremden Daten.

Unter den massiven Angriffen erlitten die Banken, wo die Informationen über die Konten der Personen, die Requisiten der Plastikkarten und so weiter, die, so genannten, «liquiden» Daten versammelt sind. Parallel war eine echte Jagd auf dasselbe Typen von Daten außerhalb der Banksysteme im Gange. Zum Beispiel haben die Verbrecher mit der Hilfe von Schadprogrammen die Zahlungsdaten aus Handelsketten gestohlen. Die große Internet-Dienstleistungen, Transportunternehmen, die staatlichen Strukturen erlitten auch unter den Angriffen.

Das Wachstum des Umfangs der kompromittierten Daten übertraf das Wachstum der Anzahl der Datenpannen. Der Umfang der kompromittierten Daten im Hinblick auf eine Datenpanne ist auch gestiegen. Der Anteil der Datenpannen, die durch Verschulden des externen Angreifers passierten, ist auch gestiegen. Anders gesagt passieren jetzt Hackerangriffe mit dem Ziel der Gewinnung von personenbezogenen Daten und andere wertvolle Informationen öfter.

Die internen Missetäter sind nicht zurückgeblieben. 12% aller Datenpannen sind mit der unberechtigten Nutzung der Informationen, auf die ein Mitarbeiter einen legitimen Zutritt hatte, zusammengebunden. In der Regel ging es in solchen Fällen um den Finanzbetrug der Bankangestellten. 8% der Datenpannen sind mit dem unberechtigten Zugriff auf Daten zusammengebunden. Interne Täter haben solche Kanäle der Übertragung von Informationen, wie Mobile Geräte, austauschbaren Speichermedien, E-Mails, Papierdokumente fast nicht benutzt. Ein «fortgeschrittener» Täter ist darüber gut informiert, dass die modernen Mittel der Kontrolle der Information es ermöglichen, erfolgreich die Übertragung von vertraulichen Informationen auf diesen Kanälen abzufangen und riskiert unüberlegt nicht.

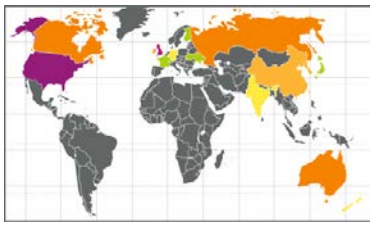
Wie haben die Unternehmen beantwortet? Die Ergebnisse der Studie zeigen, dass auch mit der Lösung des relativ einfachen Problems - die Sicherheit der personenbezogenen Daten zu gewährleisten – vielen Schwierigkeiten hatten. In höherem Grad betrifft es die mittlere Unternehmen wo Datenlecks häufiger als in großen Unternehmen passieren. Dabei fiel der größte Teil der Datenpannen im mittleren Unternehmen auf die zufällige. Im Jahr 2014 nahmen die mittelgroßen Unternehmen eine beherrschende Stellung in der Reihe der «Anbieter» der vertraulichen Informationen. In dieser Hinsicht sind Bildungs-und Gesundheitseinrichtungen besonders sichtbar.

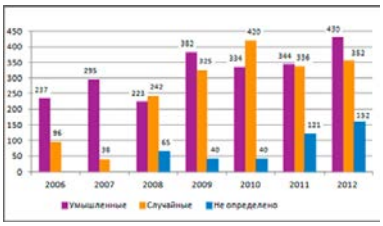
INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

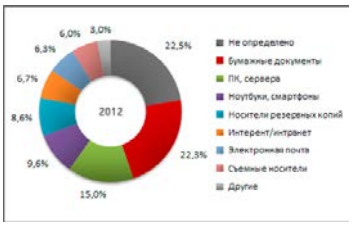
Überwachung von Datenpannen auf der Website InfoWatch

Auf der Webseite des Analysezentrums InfoWatch werden regelmäßig Berichte über die Datenpannen und die bekanntesten Vorfälle mit Kommentaren von Experten InfoWatch veröffentlicht.

Außerdem gibt es auf der Webseite auch statistische Daten über die Datenpannen in den vergangenen Jahren und dynamische Grafiken.







Verfolgen Sie die Nachrichten über die Datenpannen, die neue Berichte, analytische und populärwissenschaftliche Artikel auf unseren Kanälen:

- E-Mail
- Facebook
- Twitter
- RSS

Das Analysezentrum InfoWatch

www.infowatch.com/analytics

Glossar

Die Datenpanne – *die Handlung oder Unterlassung der Person, die den legitime Zugriff auf vertraulichen Informationen hat, die (Handlung) den Verlust der Kontrolle über Informationen oder die Verletzung der Vertraulichkeit dieser Informationen veranlasst, sowie der Verlust der Kontrolle über die Informationen aufgrund der externen Angriffe.*

Vertrauliche Informationen – *(hier) die Informationen, darauf nur ein illusterer und bekannter Kreis einen Zugriff hat, unter der Bedingung, dass diese Informationen nicht an Dritte Hände ohne Zustimmung des Besitzers der Informationen übertragen wird. In dieser Studie zählen wir zu dieser Kategorie die Informationen, die unter die Definition der personenbezogenen Daten fallen.*

Vorsätzliche (böswillige) Datenpannen – *sind die Datenpannen, wenn die Person, die mit der Information arbeitete, die möglichen negativen Konsequenzen Ihrer Handlungen vermutete, Ihr illegaler Charakter bewusste, über die Verantwortung gewarnt wurde, mit der Bereicherungsabsicht handelte und persönlicher Nutzen verfolgte. Infolge dieser Handlungen wurden die Bedingungen für den Verlust der Kontrolle über Informationen gebildet wurden und/oder die Verletzung der Vertraulichkeit von Informationen stattgefunden hat. Dabei spielt es keine Rolle, ob die Handlungen der Benutzer die negativen Folgen hatten, und ob das Unternehmen wirklich Schäden erlitten hat.*

Unbeabsichtigte (zufällige) Datenpannen – *dazu gehören die Fälle der Datenpannen, wenn die Person, die mit der Information arbeitete, die möglichen negativen Konsequenzen Ihrer Handlungen nicht vermutete und persönlicher Nutzen nicht verfolgte. Dabei spielt es keine Rolle, ob die Handlungen der Benutzer die negativen Folgen hatten, und ob das Unternehmen wirklich Schäden erlitten hat.*

Kanäle der Datenpannen – *ein solches Szenario (Handlungen (oder Unterlassungen) der Benutzer des Unternehmensinformationssystems, die auf Hardware oder Software Dienstleistungen gelenkt wurden), in Folge dessen die Kontrolle über die Informationen verloren wurde 8 , oder die Vertraulichkeit dieser Informationen verletzt wurde. Derzeit unterschied man unabhängige Kanäle der Datenpannen:*

- ✓ *Diebstahl/Verlust der Hardware (Server, Storage, Notebooks, PCs) - Kompromiss der Informationen infolge der Wartung oder der Verlust der Hardware.*
- ✓ *Mobile Geräte - die Datenpannen infolge der illegitimen Nutzung des mobilen Gerät/Diebstahl von mobilen Geräten (Smartphones, Tablets).*
  Die Verwendung solcher Geräte wird im Rahmen des Paradigmas BYOD betrachtet.
- ✓ *Austauschbaren Speichermedien – Verlust/Diebstahl von Wechselmedien (CD, USB-Karten).*
- ✓ *Netzwerk – die Datenpannen durch den Browser (die Sendung der Daten per persönlichen E-Mail, die Form der Eingabe im Browser), illegitime Nutzung der internen Ressourcen des Netzwerks, FTP, Cloud Services, illegitime Veröffentlichung der Informationen auf der Web-Seiten.*
- ✓ *E-Mail - Datenpannen durch die geschäftlichen E-Mails.*
- ✓ *Papierdokumente – Datenpanne infolge der unsachgemäßen Lagerung/Entsorgung von Papierdokumentation, infolge der Verwendung der Drucker (der Druck und Diebstahl/ Wegtragen der vertraulichen Informationen).*
- ✓ *IM - Messenger, Instant Messaging (Datenpannen bei der Übertragung den Stimme, den Text, das Video bei der Nutzung der Dienste von Instant Messaging).*
- ✓ *Unbestimmt – die Kategorie, die im Falle, wenn die Nachricht über den Vorfall in den Medien den Kanal der Datenpanne nicht bestimmen lässt, benutzt wird.*