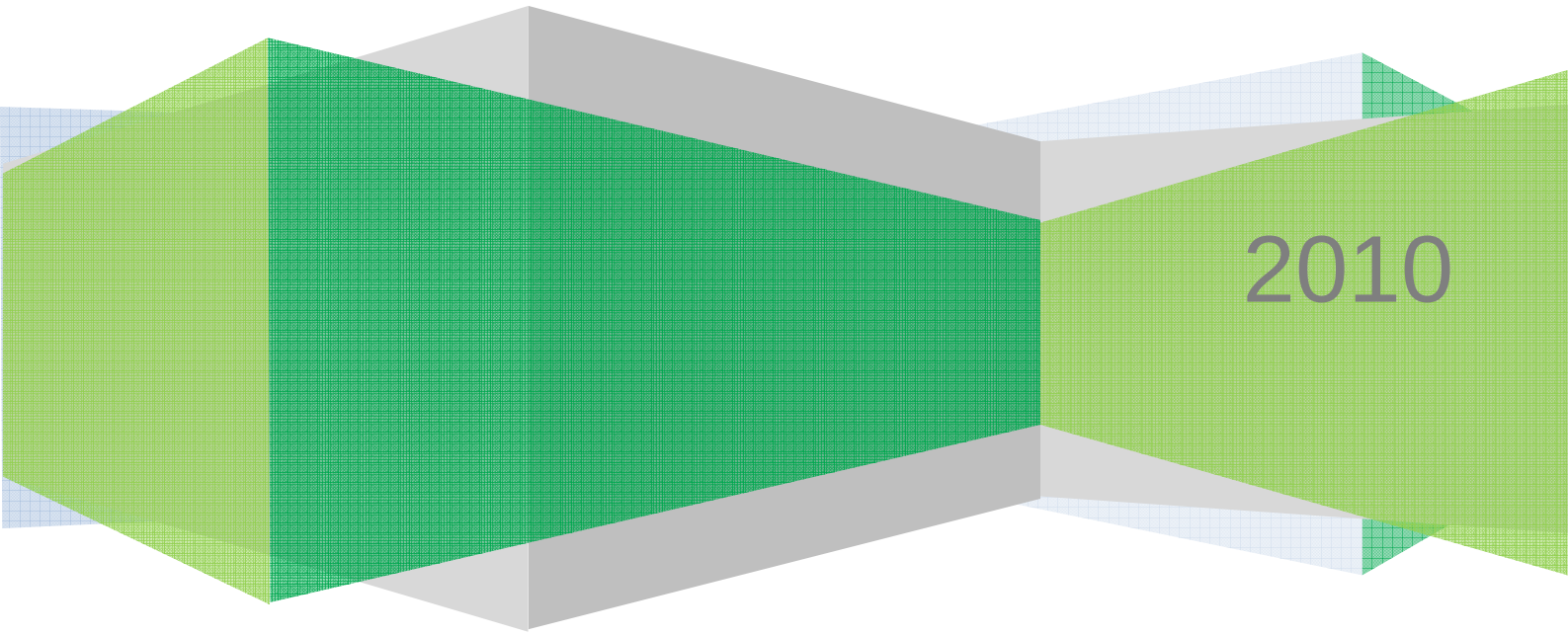
INFOWATCH

DLP-Report

Datenverluste in Unternehmen und Institutionen
Publiziert im Oktober 2010



Inhalt

Übersicht

InfoWatch stellt in diesem Dokument die neueste analytische Forschung über Zwischenfälle im Bereich vertraulicher Informationen dar. Diese Forschung dokumentiert die Zwischenfälle, die im ersten Halbjahr 2010 aufgetreten sind, und basiert auf einer täglich aktualisierten Datenbank von Datenverlusten, die von InfoWatch-Analytikern seit 2004 gepflegt wird. Die Datenbank enthält Informationen über die Gesamtzahl der Datenverluste, die bei Massenmedien, Blogs sowie Internetforen berichtet worden, oder durch andere zugängliche Informationsquellen bekannt worden sind.

Die Gesamtzahl der erfassten Datenverluste für das erste Halbjahr 2010 (181 Tage) beträgt **382 Zwischenfälle**, etwa **2.1** Zwischenfälle pro Tag. Sie sind etwas zurückgegangen, verglichen mit denen im Jahr 2009 (**2.3** Zwischenfälle pro Tag). Dieser unwesentliche Rückgang kann auf statistische Schwankungen zurückgeführt werden.

Diese Zahlen zeigen, dass Datenverluste weltweit immer noch im Brennpunkt der Aufmerksamkeit von Experten und Massenmedien steht.

Die Gesamtzahl aller Bedrohungen durch Datenverluste (gemeint sind Personaldatenverluste) beträgt **539 Millionen**, d.h. etwa 3 Millionen Datensätze pro Tag. Mit Rücksicht auf die oben genannte Statistik und ihrer heutigen Gültigkeit ziehen wir die Schlussfolgerung, dass in der Tat die Personaldaten fast jeden Bürgers in den entwickelten Ländern bei ihrer Eingabe mindestens einmal bedroht worden sind. Zum Glück ist es möglich nur ein Teil der verlorenen Daten zu finanziellen Zwecken zu missbrauchen.

Obwohl Unternehmen erklären, dass sie dem Problem des Datenmissbrauchs gewachsen sind und Vorbereitungen getroffen haben, sind die meisten Firmen nach wie vor schlecht ausgerüstet und verfolgen Datenmissbrauch nur unzureichend.

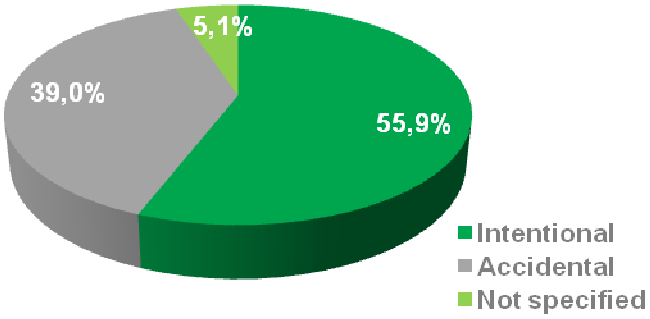
Unbeabsichtigte und absichtliche Datenverluste

Die Datenverluste können unbeabsichtigt (durch Vernachlässigung) und absichtlich entstehen. Da sich die Gegenmaßnahmen je nach Art der Datenverluste stark unterscheiden, ist die Statistik in der nachstehenden Tabelle jeweils nach Art der Datenverluste gegliedert.

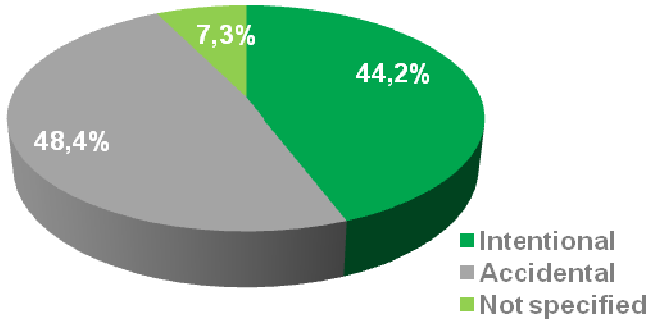
Tabelle 1: Aufteilung der Datenverluste nach Absicht

Datenverluste nach Absicht	H1 2009		H1 2010	
	Anzahl der Zwischenfälle	%	Anzahl der Zwischenfälle	%
Absichtlich (Intentional)	231	55.9%	169	44.2%
Unbeabsichtigt (Accidental)	161	39.0%	185	48.4%
Nicht spezifiziert (Unspecified)	21	5.1%	28	7.3%

H1 2009



H1 2010



Vor drei Jahren war der Anteil der unbeabsichtigten Datenverluste unvergleichbar höher (bis zu 75%), danach sank die Zahl. Dieser Rückgang ist leicht durch die Implementierung von DLP-Systemen und die Durchführung anderer Schutzmaßnahmen zu erklären, die den unbeabsichtigten Datenabfluss effektiv verhindern können. Ein gut entwickeltes DLP-System kontrolliert alle Übertragungskanäle und verhindert den unbeabsichtigten Datenabfluss fast hundertprozentig. Geht es um absichtliche Datenverluste, hängt die Effizienz der Schutzmaßnahmen zum großen Teil vom Verhältnis zwischen dem Geschick der Missetäter und den Kompetenzen der Sicherheitsfachkräfte ab. Dasselbe gilt für organisatorische Maßnahmen in Unternehmen und Institutionen, welche allerdings die unbeabsichtigten Datenverluste besser als die absichtlichen verhindern können.

2009 ging der Anteil der unbeabsichtigten Datenverluste weiter zurück. Dennoch ist die Anzahl solcher Vorfälle im ersten Halbjahr 2010 etwas gestiegen.

InfoWatch-Analytiker halten den Rückgang des unbeabsichtigten Abflusses von Daten für einen langfristigen Trend. Auf die Aufteilung der Datenverluste haben die Folgen der weltweiten Kreditbeschränkungen im ersten Halbjahr 2010 einen Einfluss ausgeübt: Knappheit an Geldmitteln hat die Implementierung von schwierigen und teureren DLP-Systemen verzögert und der Personalabbau hat die Durchführung der Schutzmaßnahmen in den Unternehmen negativ beeinflusst. Das hat den Anstieg unbeabsichtigten Datenverluste verursacht, was aber auch auf statistische Schwankungen zurückgeführt werden kann.

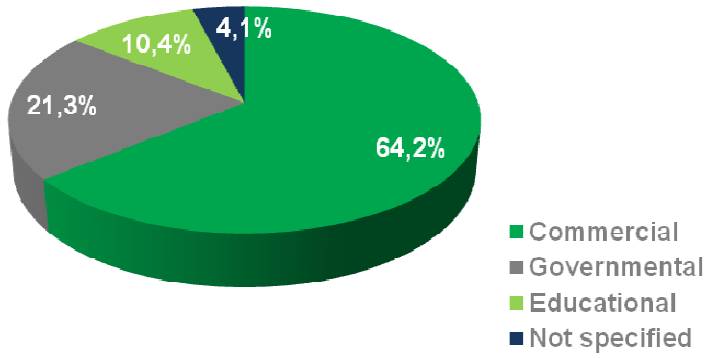
Quellen der Datenverluste

InfoWatch-Experten ordnen alle Unternehmen und Organisationen, die von Datenverlust betroffen sind, in drei Gruppen ein: Regierungsbehörden, kommerzielle Unternehmen und Bildungseinrichtungen, insofern sie öffentliche Non-Profit-Organisationen sind. Die Bildungseinrichtungen können zwar sowohl kommerziell als auch ohne Gewinnerzielungsabsicht sein, wurden aber von den Experten von InfoWatch nur in die Gruppe Bildungseinrichtungen eingeordnet, wenn es sich um Non-Profit-Bildungseinrichtungen handelt. Denn das Verfahren bei der Verarbeitung der Personaldaten in Non-Profit-Bildungseinrichtungen (wie etwa bei Studenten in den jeweiligen Bildungseinrichtungen) von dem Verfahren von kommerziellen Bildungseinrichtungen (wie bei kommerziellen Unternehmen, z.B. Banken, Polikliniken, Supermärkte usw.) unterscheidet sich wesentlich. Demgegenüber ähnelt das Verhalten in der Verarbeitung von Daten von Non-Profit-Bildungseinrichtungen eher dem von Regierungsbehörden.

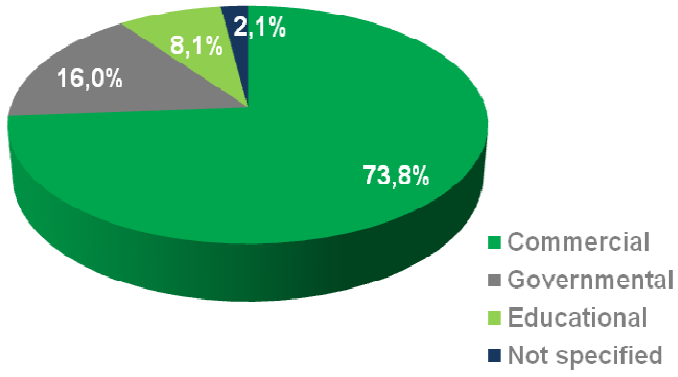
Tabelle 2a: Aufteilung der Datenverluste nach dem Organisationstyp

Organisationstyp	H1 2009		H1 2010	
	Anzahl der Zwischenfälle	%	Anzahl der Zwischenfälle	%
Kommerzielle Unternehmen (Commercial)	265	64.2%	296	73.8%
Regierungsbehörden (Governmental)	88	21.3%	61	16.0%
Bildungseinrichtungen/ Non-Profit-Organisationen (Educational / non-profit)	43	10.4%	127	8.1%
Nicht spezifizierte Organisation (Unspecified)	17	4.1%	8	2.1%

H1 2009



H1 2010



Im vergangenen Jahr konnten keine wesentlichen Änderungen in der Aufteilung der Datenverluste nach dem Organisationstyp festgestellt werden.

Die unwesentliche Vergrößerung der Datenverluste im Wirtschaftssektor ist durch die Haushaltskürzungen in Folge der Finanzkrise zu erklären. Etwas weniger relevant ist dies als Ursache bei den Regierungsbehörden und Non-Profit-Organisationen. Die Motivierung und Einstellung zu Schutzmaßnahmen unterscheiden sich zudem sehr bedeutend bei Regierungsbehörden und im Wirtschaftsbereich.

Bei der Einführung der Datenschutzmaßnahmen sind in Regierungsbehörden in erster Linie die gesetzlichen Anforderungen und Genehmigungen übergeordneter Stellen zu berücksichtigen. Die Effizienz dieser Maßnahmen ist durch die Anzahl stattgefundener und verhinderter Datenverluste einzuschätzen. Diese Situation ist mit der von Non-Profit-Organisationen vergleichbar. Im Wirtschaftsbereich ist aber die Situation etwas anders. Da jede kommerzielle Organisation die Rentabilität im Auge hat, ist die Notwendigkeit der Implementierung von Datenschutzmaßnahmen aus dieser Sicht zu betrachten. Die gesetzlichen Anforderungen beeinflussen natürlich die Entscheidung des Unternehmens, sind aber von nachrangiger Bedeutung.

Unter dem Gesichtspunkt der Rentabilität können einige Datenverluste keinen großen Schaden verursachen. Die Unternehmer sind bereit, dieses Risiko einzugehen und eine finanzielle Reserve zur Beseitigung dieser Vorfälle vorzusehen, da die Kosten für ihre Beseitigung geringer sein können als die Kosten einer Implementierung von Datenschutzmaßnahmen. Non-Profit-Organisationen können das Risiko vermeiden, indem sie externe Firmen mit der Verwaltung ihrer Personaldaten beauftragen. In der Regel können Regierungsbehörden diese Möglichkeit nicht nutzen, weil sie bei der Verarbeitung von Personaldaten die gesetzlichen Anforderungen einzuhalten haben.

Diese Unterschiede beeinflussen die Statistik der Datenverluste nach Organisationstyp. Die Implementierung von Datenschutzsystemen beeinflusst aber alle drei Organisationstypen im gleichen Maße: es ermöglicht die absichtlichen Datenverluste teilweise und die unbeabsichtigten Datenverluste vollständig zu verhindern

Nachstehend sind die unbeabsichtigten und absichtlichen Datenverluste in drei Bereichen dargestellt.

Tabelle 2b: Absichtliche und unbeabsichtigte Datenverluste nach dem Organisationstyp

Organisationstyp	unbeabsichtigt		absichtlich	
	Anzahl der Zwischenfälle	%[1]	Anzahl der Zwischenfälle	%
Kommerzielle Unternehmen (Commercial)	137	74.1%	126	74.6%
Regierungsbehörden (Governmental)	28	15.1%	27	16.0%
Bildungseinrichtungen/ Non-Profit-Organisationen (Educational / non-profit)	18	9.7%	10	5.9%
Nicht spezifizierte Organisation (Unspecified)	2	1.0%	6	3.6%

In nächster Zukunft sind keine Änderungen dieser Statistik zu erwarten. Auch eine obligatorische Implementierung der DLP-Systeme in Regierungsbehörden und in einigen Marktsegmenten ist nicht zu erwarten, obwohl InfoWatch-Experten der Meinung sind, dass die Implementierung von Datenschutzmaßnahmen weiter voranschreiten wird. Dies führt zur allmählichen Reduzierung der Gesamtzahl von Datenverlusten und des Anteils des unbeabsichtigten Datenabflusses.

1 Prozentsatz jedes Datenverlustes (unbeabsichtigt oder absichtlich)

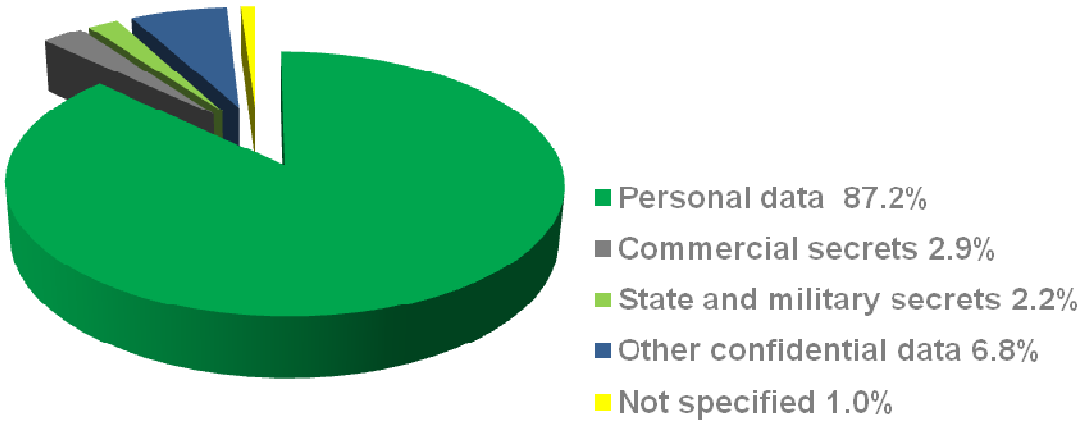
Welche Daten fließen öfter ab

Beim Starten der Datenbank über die Datenverluste haben InfoWatch-Experten alle Zwischenfälle in drei Kategorien aufgeteilt: Vorfälle mit Personaldaten, Vorfälle mit staatlichen Daten und Vorfälle mit Geschäftsgeheimnissen. Alle in der Datenbank erfassten Datenverluste waren einer der Kategorien zugeordnet. Die meisten Zwischenfälle (90-98%) für die ganze Periode der Datenbankführung sind Datenpannen in Zusammenhang mit Personaldaten.

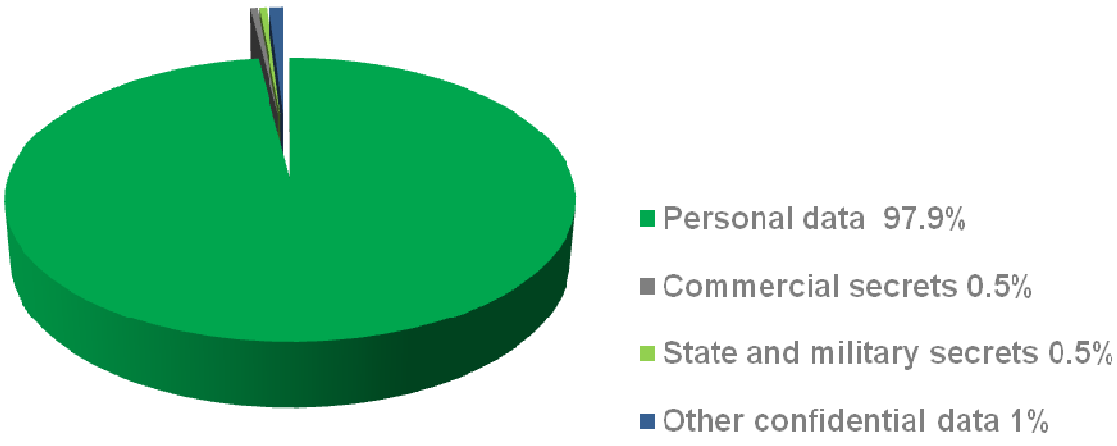
Tabelle 3: Aufteilung der Quellen der Datenverluste nach der Art vertraulicher Daten

Kategorie vertraulicher Daten	H1, 2009		H1, 2010	
	Anzahl der Zwischenfälle	%	Anzahl der Zwischenfälle	%
Personaldaten	360	87.2%	374	97.9%
Geschäftsgeheimnis, Know-how	12	2.9%	2	0.5%
Staats- und Militärgeheimnisse	9	2.2%	2	0.5%
Sonstige vertrauliche Daten	28	6.8%	4	1.0%
nicht spezifizierte Daten	4	1.0%	0	0%

H1 2009



H1 2010



Im ersten Halbjahr 2010 stehen Zwischenfälle mit Personaldaten an der Spitze. Im ersten Halbjahr 2009 ist die Anzahl der Vorfälle mit den Personaldaten etwas zurückgegangen (87,2% im ersten Halbjahr 2009 und 89,8% für das ganze Jahr), im ersten Halbjahr 2010 beträgt ihr Anteil wiederum fast 100 Prozent.

Die führende Position ist offenbar. Überall in der Welt gibt es viele Personaldaten, mit denen ständig gearbeitet wird. Tausende Organisationen verarbeiten Personaldaten, während die Weitergabe von Geschäftsgeheimnissen sehr selten und die von Staatsgeheimnissen noch seltener vorkommen.

Außerdem ist der verwendbare Rahmen von Geschäftsgeheimnissen begrenzt: Sie können nur von den direkten Wettbewerbern und nur unter bestimmten Bedingungen verwendet werden. Der Gültigkeitsbereich einiger Personaldaten unterliegt dagegen keinem Zweifel: Es besteht ein fester Markt für verlorene/gestohlene Personaldaten. Deswegen ist dieser Diebstahl oder Missbrauch von unbeabsichtigt verlorenen Personaldaten eine weit verbreitete Erscheinung. Sogar derjenige, der eigentlich keine unlauteren Absichten hat, kann der Versuchung nicht immer widerstehen. Andere Arten vertraulicher Daten werden in der Regel nur per Auftrag gestohlen.

In den nächsten Jahren ist eine Verschlechterung der Situation zu erwarten. Statistisch gesehen könnte diese prognostizierte Verschlechterung durchaus nicht so massiv ins Gewicht fallen, weil Personendaten die bisher als vertraulich kategorisiert wurden, zukünftig als nicht vertrauliche Daten eingestuft würden, was allerdings kaum abzusehen ist. Unternehmen verwenden oft Personaldaten zur Identifizierung der Kunden bei der Fernbetreuung. In diesem Fall werden nicht vertrauliche Daten zu vertraulichen Informationen und wären zu schützen. Zu den durch die Regierung getroffenen Maßnahmen gehört der Schutz von allen Arten von Personaldaten. Diesbezüglich erwarten InfoWatch-Experten eine Erweiterung der Personaldaten-Kategorien.

Verlustwege und Technologien

Die Analyse der Datenträger, die zur Übertragung der klassifizierten Daten im geschützten Kreis oder zu ihrer Übergabe an einen unbekannten Benutzer verwendet werden, ermöglicht den etwaigen Datenabfluss durch einen Datenträger vorherzusehen und führt so zu einer Risikoverminderung dank der Implementierung von verschiedenen Datenschutzlösungen.

Die DLP-Systeme und sonstige Lösungen gegen Datenverluste umfassen bestimmte Kanäle, die zur Übertragung der Informationen im geschützten Kreise (z.B. Protokolle, mobile Datenträger, mobile Computer, Drucker usw.) verwendet werden können. Die Unternehmer verfügen nicht immer über genügend finanzielle Mittel und technisches Know-how um alle möglichen Datenverlustwege zu erfassen. In den meisten Fällen gehen unbeabsichtigte Datenverluste durch nicht kontrollierbare Kanäle aus dem Unternehmen heraus.

Die Situation bei absichtlichen Datenverlusten sieht anders aus. Ein Mitarbeiter, der über einen Zugriff auf gesicherte und geschützte Daten verfügt, wählt einen nicht geschützten Kanal mit der vorsätzlichen Absicht, Daten aus dem geschützten Kreis herauszutragen. Die Implementierung von DLP-Systemen, die nur die gewählten Datenübertragungskanäle umfassen, kann die Wahrscheinlichkeit der Datenverluste wesentlich beeinflussen. Zur Verhinderung sowohl absichtlicher als auch unbeabsichtigter Datenverluste soll eine Systemlösung im Bereich des Datenschutzes (gemeinsam mit den Organisationsmaßnahmen) eine komplexe Kontrolle über alle Kanäle und Datenträger gewährleisten.

Tabelle 4a: Hauptverlustwege

Datenverlustwege	H1 2009		H1 2010	
	Anzahl der Zwischenfälle	%	Anzahl der Zwischenfälle	%
Mobile Geräte (Laptops, PDAs)	**49**	**11.9%**	**40**	**10.5%**
Mobile Datenträger (USB-Sticks, CD, DVD, usw.)	23	5.6%	32	8.4%
Desktop-PC, Servers, HDD	**41**	**9.9%**	**90**	**23.6%**
Internet (einschließlich E-Mail)	97	23.5%	82	21.4%
Papierunterlagen	84	20.3%	78	20.4%
Archivdaten	48	11.6%	6	1.6%
Sonstiges	36	8.7%	25	6.5%
nicht spezifizierte	35	8.5%	29	7.6%

Im Vergleich zum Vorjahr ist die Anzahl der mit PCs, Servern und mobilen Datenträgern verbundenen Datenverluste erheblich gestiegen.

Der Datenabfluss durch mobile Computer und Datenträger war vor 2-3 Jahren besonders stark. Im Vorjahr ist die Anzahl der Datenverluste durch mobile Computer und Datenträger zurückgegangen. Im laufenden Jahr ist die Anzahl dieser Datenverluste etwas gestiegen, was aber auf statistische Schwankungen zurückgeführt werden kann. Dieser Rückgang ist durch die Implementierung von Verschlüsselungssystemen zu erklären. Die Verluste oder Diebstähle der Daten durch die verschlüsselten Datenträger sind in dieser Statistik nicht berücksichtigt.

Leider ist die Implementierung von Verschlüsselungen schleppend. Es ist noch nicht verpflichtend geworden firmeneigene Laptops, USB-Sticks und CDs zu verschlüsseln. Der Statistik nach benutzen nur verantwortungsvolle Mitarbeiter sowie die Abteilungen, die von diesen Mitarbeitern geleitet werden, die Datenverschlüsselung in vollem Umfang. Die meisten Mitarbeiter und Unternehmer vernachlässigen diese Schutzmaßnahme. Diese Situation ist vergleichbar mit dem Anlegen eines Sicherheitsgurtes: Jedermann weiß Bescheid, dass Sicherheitsgurte das Schadensrisiko beim Unfall senken, aber ein Unfall selbst scheint uns kaum wahrscheinlich zu sein. Sicherheitsgurte werden meistens nur durch Druck von außen, wie beispielsweise Strafen, verwendet.

Heute sind die Folgen des Verlusts oder Diebstahls eines firmeneigenen Laptops jedem bekannt. Die Datenverschlüsselung könnte dieses Risiko erheblich senken, aber da die Wahrscheinlichkeit dieses Vorfalls niedrig ist, unterschätzt man die Wichtigkeit der Verschlüsselung. Wir meinen, dass die Massenimplementierung von Verschlüsselungssystemen nur aufgrund von gesetzlichen Bestimmungen möglich ist, z.B. durch Strafen bei Verzicht auf die Verschlüsselung aller mobilen Datenträger. Der Anteil der Unternehmer, die diesen Ansatz verfolgen, ist sehr niedrig. Es ist erstaunlich, dass sogar Regierungsbehörden keinen großen Wert auf Verschlüsselung legen, obwohl ihre Laptops Staats- oder Militärgeheimnisse enthalten können.

InfoWatch-Experten sind der Meinung, dass Verschlüsselung von Datenträgern sich langsam verbreiten wird. Freiwillige Maßnahmen sind bereits getroffen und eine weitere Implementierung ist nur bei der administrativen Unterstützung auf Unternehmens-, Industrie- und Regierungsniveau möglich.

Andererseits erhöht sich die Anzahl mobiler Datenträger, was eine Erhöhung von Datenverlusten über Laptops, USB-Sticks usw. ergeben kann.

Der Anteil von Datenverlusten über Papierunterlagen bleibt immer noch hoch. Wie in den vorhergehenden Ergebnissen gezeigt wurde, ist die Ursache dieser Erscheinung offensichtlich. Effektive, technische Lösungen können unbeabsichtigte Datenverluste durch geschützte Kanäle verhindern, aber nicht alle DLP-Systeme können die Kontrolle über das Unterlagenausdrucken sichern. Sobald das Dokument ausgedruckt ist, kann es nur durch Personen-Kontrollen des Sicherheitspersonals überprüft werden, was schwierig und nicht sehr effektiv ist.

Ein typischer Papier-basierter Datenverlust passiert als Systemfehler beim Ausdrucken von Kundenbriefen. Die Adressen auf den Briefumschlägen werden ebenfalls automatisch gedruckt, manchmal werden auch Briefe automatisch zugeklebt. Lediglich durch einen unwesentlichen Systemfehler, können Kunden dadurch Briefe mit den Personaldaten anderer Kunden empfangen.

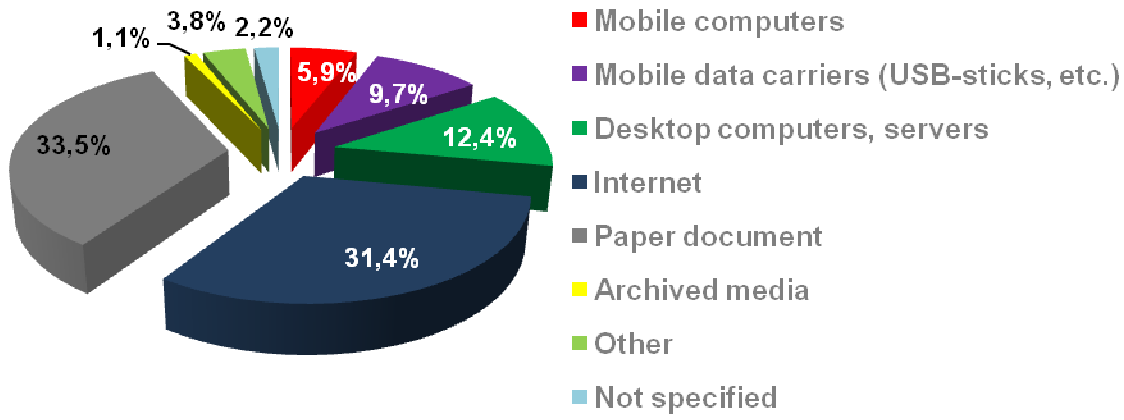
Um die Anzahl der Datenverluste über Papier-Ausdrucke zu reduzieren sind einige organisatorische und technische Maßnahmen zu treffen: Unter der technischen Maßnahme wird die Implementierung eines DLP-Systems verstanden, das die laufende Kontrolle über das Ausdrucken von Unterlagen (einschließlich einer Sperre) sichert und über ein Utility zur Prüfung der Adressen auf die Übereinstimmung mit den Adressaten verfügt. Diese Maßnahmen sind ziemlich teuer insbesondere im Vergleich zu den Druckkosten, deswegen wird die Anzahl der Papierdatenverluste langsam zurückgehen, im Wesentlichen durch die Reduzierung der Verwendung von Ausdrucken auf Papier.

Die nachstehende Tabelle zeigt die Wege unbeabsichtigter und absichtlicher Datenverluste auf.

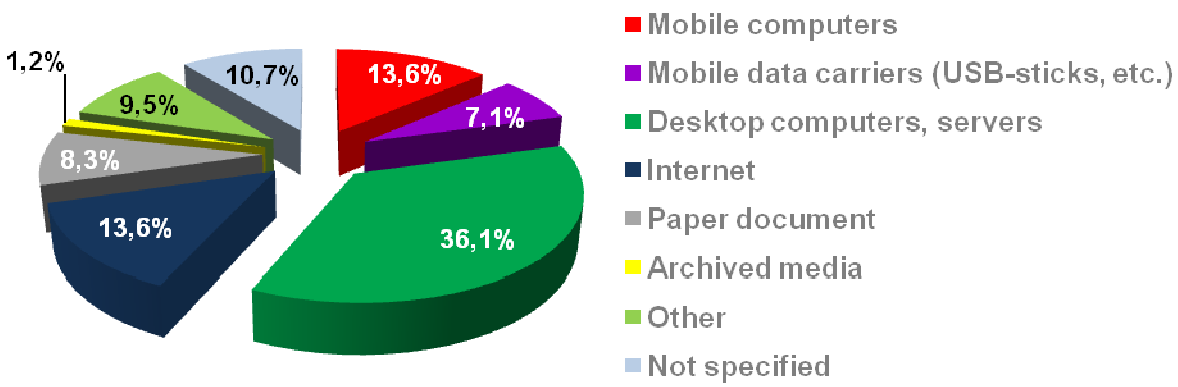
Tabelle 4b: Hauptwege der absichtlichen und unbeabsichtigten Datenverluste

Datenverlustwege	unbeabsichtigt		absichtlich	
	Anzahl der Zwischenfälle	%	Anzahl der Zwischenfälle	%
Mobile Geräte (Laptops, PDAs)	11	5.9%	23	13.6%
Mobile Datenträger (USB-Sticks, CDs, DVDs, usw.)	18	9.7%	12	7.1%
Desktop Computer, Server, HDDs	23	12.4%	61	36.1%
Internet (einschließlich E-Mail)	**58**	**31.4%**	**23**	**13.6%**
Papierunterlagen	**62**	**33.5%**	**14**	**8.3%**
Archivdaten	2	1.1%	2	1.2%
Sonstiges	7	3.8%	16	9.5%
nicht spezifiziert	4	2.2%	18	10.7

Unbeabsichtigter Datenverlust



Absichtlicher Datenverlust



Die wesentlichen Unterschiede zwischen den unbeabsichtigten und absichtlichen Datenverlusten kann man deutlich in den Kategorien „Internet“ und „Papier-Ausdruck“ beobachten.

Der weit verbreiteten Meinung entgegen dringen die Missetäter in die Unternehmensnetze von außen nicht so oft ein. In den meisten Fällen verletzen verantwortungslose Mitarbeiter die Vertraulichkeit von Daten im Unternehmensnetz (Siehe Verizon 2010 Data Breach Investigations Report: Der Anteil der Verstöße, der auf äußere Einflüsse zurückzuführen ist beträgt 9%, während die Anzahl der Verstöße durch die Mitarbeiter mehr als um ein zweifaches gestiegen ist). Ein typisches Beispiel von Datenschutz-Verletzungen durch Mitarbeiter ist ein zufälliges Kopieren von vertraulichen Informationen in eine Datenbank, die von einem Webserver als Datenquelle benutzt wird. So können vertrauliche Informationen ins Netz geraten.

Die Papier-Dokumente werden öfter von Mitarbeitern als von durch Einbrüche von extern gestohlen. Außerdem verursacht ein gestiegenes Interesse der Öffentlichkeit an Datenverlusten den Anreiz zum Missbrauch vertraulicher Unterlagen. Oft werden Unterlagen mit vertraulichen Informationen in Mülltonnen gefunden und an Massenmedien weitergeleitet. Suche nach den vertraulichen Informationen in Mülltonnen erfordert weniger Fertigkeiten als die Suche nach Schwachstellen im Netz. Eine generelle Haltung von Menschen zu personenbezogenen Daten trägt sicherlich auch zu einer gewissen Popularität des Themas 'Datenlecks über Papier-Ausdrucke bei, dass ein Kunde, wenn er fälschlicherweise einen Brief mit den Personaldaten anderer Kunden bekommt, in vielen Fällen die Aufmerksamkeit der Massenmedien auf sich zieht.

Die Diagramme oben zeigen, dass das DLP-System in erster Linie als Schutzfilter zwischen dem geschützten Firmennetzwerk und dem öffentlichen Netz an Druckern (Print-Server), sowie bei der Datenspeicherung auf mobile Datenträger (wie USB-Sticks) implementiert werden muss. Diese Kanäle verursachen die meisten Datenverluste. Da aber mobile Datenträger die Produktivität eines Unternehmens steigern können, ist nicht zu erwarten, dass sich ihr Einsatz reduzieren wird. Zum Schutz dieser Kanäle und zur Kontrolle über die Daten außerhalb des Unternehmensgebäudes sollte Datenverschlüsselung verwendet werden.

Im Gegensatz zu DLP-Systemen sind Verschlüsselungs-Tools in den meisten Fällen preisgünstig. Die Stärke der Verschlüsselungsalgorithmen ist nicht von so eklatanter Bedeutung, da der etwaige Datendieb meinst keine nötigen mathematischen und analytischen Kenntnisse zum Entschlüsseln besitzt. Obwohl Verschlüsselung als unzureichend für den Schutz von Staatsgeheimnissen gehalten wird, ist sie perfekt geeignet, um Daten auf einem verlorenen Laptop oder USB-Stick vor unbefugtem Zugriff und deren Nutzung zu schützen.

Aufteilung der Datenverluste nach Ländern

In der untenstehenden Tabelle sind aktuelle Datenverluste nach den Ländern aufgeteilt. Bedingt durch Latenz spiegelt diese Tabelle die Geografie der Datenverluste nicht sehr exakt wider, sie zeigt aber, wie oft die Zwischenfälle in den Ländern verborgen bleiben. Der LPC-Index ist das Verhältnis zwischen der Anzahl der Datenverluste in dem jeweiligen Land und der Bevölkerung dieses Landes (in Millionen). Die Länder mit einer niedrigen Latenz, wie die USA und Großbritannien, gelten als Bezugspunkte. Laut Gesetzgebung in den USA und Großbritannien sind alle Unternehmen verpflichtet die Regierung über Datenverluste zu benachrichtigen. Vergleicht man die Kennwerte der USA und Großbritannien mit denen anderer Länder, können wir bestimmen, wie viele Datenverluste öffentlich unbekannt bleiben.

Tabelle 5: Aufteilung der Datenverluste nach Ländern

(CC) Land	Anzahl der Zwischenfälle	%	LPC
AU Australien	2	0.56%	0.100
CA Kanada	11	2.88%	0,338
CH die Schweiz	2	0.56%	0.257
CN China	1	0.26%	0.001
DE Deutschland	5	1.31%	0.061
ES Spanien	1	0.26%	0.025
GB Großbritannien	36	9.42%	0.597
GR Griechenland	1	0.26%	0.090
IE Irland	3	0.56%	0.333
IL Israel	1	0.26%	0.164
IN Indien	3	0.84%	0.003
IT И Italien	1	0.26%	0.017
JP Japan	1	0.26%	0.008
MX Mexiko	1	0.26%	0.010
NL die Niederlande	5	1.31%	0.304
NO Norwegen	1	0.26%	0.208
NZ Neuseeland	1	0.26%	0.232
PK Pakistan	1	0.26%	0.006
RU Russland	15	3.93%	0.104
UA die Ukraine	1	0.26%	0.021
US die USA	284	74.4%	0.969
einige Länder	1	0.26%	
nicht spezifiziert	5	1.31%	

Im Vorjahr waren die USA und Großbritannien an der Spitze der Liste der LPC-Indizes. 2008 gab es in Großbritannien noch kein Gesetz über die obligatorische Meldung von Datenverlusten, daher war der LPC-Index in diesem Zeitraum erheblich niedriger.

Kanada ist dem Beispiel seines südlichen Nachbarn gefolgt und hat den Datenschutz im laufenden Jahr verbessert. Sein LPC-Index ist erheblich gestiegen, und das Land nimmt den dritten Patz in der Liste der LPC-Indices im ersten Halbjahr 2010 ein.

InfoWatch-Experten gehen davon aus, dass die Gesamtzahl der Datenverluste in den entwickelten Ländern etwa gleich ist und etwa 2 Zwischenfälle pro Jahr je Million Einwohner beträgt. Die Differenzen in der Statistik sind durch die Unterschiede in den gesetzlichen Benachrichtigungsregelungen zu erklären. Die niedrigste Latenz ist in den USA zu beobachten.

Zwischenfälle der größten Datenverluste

In der folfenden Tabelle sind Zwischenfälle der größten Datenverluste für das erste Halbjahr 2010 aufgelistet.

Tabelle 6: Zwischenfälle der größten Datenverluste

Datum	Beschreibung	Links
18.01.10	Sicherheitslücke die in einer britischen Datenbank entdeckt wurde, die Personaldaten von **11 Millionen** Kindern enthält.	http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/6836911/ContactPoint-database-of-11-million-children-suffers-security-breaches-in-trials.html
16.02.10	Sicherheitslücke in einem Microsoft Authentifizierungssystem kann über **460 Millionen** Benutzer betreffen	http://www.bloomberg.com/apps/news?pid=20601087&sid=affIdPDIbclA&pos=7
27.03.10	In den USA haben wurden Daten von über **3.3 Millionen** Studenten aus einem Unternehmen gestohlen, das im Bereich von Bildungskrediten tätig ist.	http://updatednews.ca/?p=10521
01.05.10	Verdacht auf Diebstahl einer Datenbank von **25 Millionen** Steuerzahlern und ihres Verkaufs an Spammer in Großbritannien	http://www.telegraph.co.uk/news/uknews/7665782/Tax-records-sold-to-junk-mail-firms.html

Zusammenfassung

- Die Gesamtanzahl der bestätigten Datenverluste bleibt unverändert und beträgt etwa 2 Zwischenfälle pro Tag, was etwa um 10% niedriger ist als im gleichen Zeitraum 2009.
- Das Thema der Datenverluste (insbesondere Personaldatenverluste) bleibt auf der ganzen Welt sehr populär.
- Der Prozentsatz unbeabsichtigter Datenverluste, der in den Vorjahren einen tendenziellen Rückgang zeigte, ist gestoppt und inzwischen wieder etwas gestiegen.
- Regierungsbehörden, Bildungseinrichtungen und Non-Profit-Organisationen sollten die gleichen Mittel und Verfahren verwenden um Datenverluste zu verhindern.
- Die Anzahl der Datenverluste durch Diebstahl oder Verlust unverschlüsselter mobiler Computer oder mobilen Datenträger bleibt unverändert hoch.
- Die Anzahl der Datenverluste über Netzwerke ist etwas zurückgegangen.
- Ein Großteil der Vorfälle liegt beim Ausdruck da Drucker und gedruckte Dokumente nicht genügend kontrolliert werden.
- Die Gefahr der Datenverluste ist in allen Ländern außer den USA und Großbritannien hoch, wo eine obligatorische Benachrichtigung über die Datenverluste eingeführt wurde. Die Gesamtanzahl der Datenverluste in den entwickelten Ländern ist fast gleich und beträgt etwa 2 Zwischenfälle pro Jahr auf eine Million Einwohner.