VON IDG
COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/selbstgefaelliger-umgang-mit-compliance,2353264

Datensicherheit

Selbstgefälliger Umgang mit Compliance

Datum: 17.09.2010
Autor(en):Thomas Pelkmann

Das Thema Datenverlust ist ein Dauerbrenner in der deutschen Wirtschaft. Zwei Drittel der Firmen sind in den letzten beiden Jahren Daten abhanden gekommen. Accenture macht in einer Studie eine fehlende "Kultur des Kümmerns" dafür verantwortlich.

Daten von Kunden und Mitarbeitern [1]sind ein sensibles Gut. Umso spektakulärer sind **Datenpannen, die den Weg in die Öffentlichkeit finden** [2]. Auf diese Weise hat etwa der **Deutsche Sparkassenverlag**[3] Ende vergangenen Jahres auf sich aufmerksam gemacht, weil fast 350.000 Kundenrechnungen im Online-Shop frei zugänglich waren.

Einen ähnlichen Weg zu mehr PR wählte auch das **Städtchen Senden im schönen Münsterland**[4]: Die Gemeinde verschickte versehentlich eine Liste mit den Daten von fast 400 Einzelpersonen und Familien, die Hilfen nach dem SGB II (SGB = Sozialgesetzbuch) erhalten haben. Die Daten enthielten neben den Vor- und Zunamen auch die Geburtsdaten sowie die Adressen der Hilfe-Empfänger aufgelistet.

Oft weniger spektakulär, für das Vertrauen von Mitarbeitern und Kunden eines Unternehmens aber durchaus ebenso erfolgskritisch, ist der Verlust vertraulicher Daten. Genau 69 Prozent der deutschen Unternehmen und Behörden haben in den vergangenen zwei Jahren den Verlust personenbezogener Daten hinnehmen müssen, wie die **Management**[5]- und Technologieberater von Accenture in der **Studie "How Global Organizations Approach the Challenge of Protecting Personal Data"**[6] herausgefunden haben. Einem knappen Drittel hiesiger Organisationen (29 Prozent) ist das nicht nur einmal, sondern gleich sechsmal oder häufiger passiert.

Zu personenbezogenen Daten von Mitarbeitern und Kunden zählen unter anderem Adresse, Familienstand, Fotos sowie Angaben über Beruf und körperliche Merkmale.

Das Ergebnis steht in auffälligem Gegensatz zum Anspruch der untersuchten Behörden und Unternehmen. Dem Schutz der Informationen räumen sie nämlich gemeinhin eine hohe Bedeutung ein: So stimmten 89 Prozent der Befragten der Aussage zu, die Sicherheit der Daten obliege ihrer Organisation. Und drei von vier Unternehmen und Behörden glauben, die ihnen vorliegenden, personenbezogenen Angaben seien adäquat geschützt.

Technische Störungen und schlampige Mitarbeiter führen zu Datenverlusten

Zu den häufigsten Auslösern für Datenverluste zählen nach Angaben der weltweit 5.500 befragten Entscheidungsträger System- oder technische Störungen (35 Prozent), gefolgt von schlampigen oder inkompetenten Mitarbeitern (24 Prozent). Fehler in den Geschäftsprozessen schlagen mit einem Anteil von 22 Prozent zu Buche, während Cyberkriminalität mit 18 Prozent dazu beiträgt. Böswillige Mitarbeiter sind genau so eher selten der Grund für die Pannen (13 Prozent) wie liederliche und unfähige Zeitarbeiter in den Unternehmen (11 Prozent).

Unterm Strich aber, so hat eine andere **Untersuchung des Datenrettungsspezialisten Kroll Ontrack**[7] ergeben, ist vordergründig der Mensch das Hauptproblem: Ihm sind - speziell bei Datenverlusten in virtuellen Umgebungen - zwei Drittel aller Datenverluste anzulasten.

Aber es wäre zu oberflächlich, den Mitarbeitern allein die Schuld in die Schuhe zu schieben. Weil auch hier der Fisch am Kopf zu stinken beginnt, nimmt Accenture vor allem die **Unternehmensverantwortlichen** [8]in die Pflicht.

So führt laut Accenture vor allem der selbstgefällige Umgang mit **Compliance**[9]-Anforderungen zum Datenverlust. Der klingt deutlich aus der geäußerten Überzeugung heraus, man habe im Unternehmen alles für den Schutz sensibler Daten getan.

Ebenfalls ein Leitungsproblem ist das häufig anzutreffende Fehlen angemessener Regelungen und Trainings für den Umgang mit sensiblen Daten. Schließlich, so Accenture, seien unfähige und **schlampige Mitarbeiter**[10] nicht nur ein persönliches Problem, sondern auch Folge des nachlässigen Umgangs mit diesem Thema in den Unternehmen.

Die wahren Ursachen für Datenverlust liegen im Management

Zu den Ursachen für Datenverluste gehören auch fehlende Kontrollen: So bemängeln die Analysten, dass Mitarbeiter in aller Regel viel zu leicht Zugriff auf sensible Daten hätten. Fast die Hälfte der befragten Unternehmen findet eine Zugangsbeschränkung zudem nicht besonders wichtig.

Noch schlimmer scheint in diesem Zusammenhang, dass gerade einmal ein von fünf Unternehmen der Meinung ist, es sei verwerflich, Kundendaten zu verkaufen. Kein Wunder, dass bei den restlichen 80 Prozent vertrauliche Kundendaten immer wieder nach außen gelangen.

Insgesamt, stellt Accenture fest, liegen die wichtigsten Gründe für Datenverluste immer im Unternehmen selber, sind also nicht von äußeren Faktoren abhängig. Und deshalb, so schließt die Analyse, müssten solche Pannen auch intern kontrollierbar sein.

Der wirksame **Schutz vor Datenpannen**[11] beginnt damit, überhaupt erst einmal das besondere Schutzbedürfnis von Kunden- und Mitarbeiterdaten zu akzeptieren, übrigens nicht nur der Kunden und Mitarbeiter wegen. Organisationen nämlich, die eine "Kultur des Kümmerns" pflegten und die Privatheit und den Schutz von Daten respektierten, seien sehr viel weniger von Pannen bedroht, hat Accenture festgestellt.

Zudem sei ein publik gewordener Verlust vertraulicher Daten eine große Gefahr für das **Ansehen eines Unternehmens**[12]. "Verlust oder Missbrauch personenbezogener Daten können den Ruf einer Organisation enorm schädigen", heißt es dazu bei Accenture. "Gerade in Deutschland ist die öffentliche Aufmerksamkeit für solche Vorfälle besonders hoch."

In Deutschland ist Datenschutz ein besonders sensibles Thema

Noch glauben immerhin 70 Prozent der befragten Bürger in Deutschland, dass Organisationen ihre persönlichen Angaben angemessen schützen. Doch dieser Vertrauensvorschuss gilt nicht für alle Bereiche gleichermaßen. So halten die Befragten ihre persönlichen Daten am ehesten bei ihrer **Krankenkasse**[13] (49 Prozent) und ihrem Arbeitgeber (48 Prozent) für gut aufgehoben. Das wenigste Vertrauen bringen sie **Behörden und staatlichen Einrichtungen**[14] (jeweils 8 Prozent) sowie Telekommunikationsunternehmen (6 Prozent) entgegen.

Speziell in Deutschland fanden die Analysten die Einstellung, dass die Bürger die "**Hoheit** [15]über alle persönlichen Daten" haben, und das auch dann, wenn sie Unternehmen und Behörden vorlägen. Nur 26 Prozent der befragten Deutschen sind der Überzeugung, dass Informationen, die sie einer Organisation wissentlich mitteilten, ihnen nicht länger gehören. Aus dieser Vermutung leiten 77 Prozent der Befragten das Recht ab zu kontrollieren, wofür Unternehmen und Behörden ihre Daten verwenden.

"Die meisten Menschen sehen persönliche Daten als Leihgabe an", sagt Frank Fischer, bei Accenture für den Bereich Informationssicherheits- und Datenschutz-Beratung verantwortlich. "Entsprechend nachdrücklich sollten die Organisationen mit der Sicherheit dieser Informationen umgehen, um Vertrauen nicht zu verspielen."

Für einen **effektiven Umgang** [16]der Unternehmen mit **sensiblen Daten** [17]gehören nach Überzeugung von Fischer vier Säulen: "ausreichend Personal, Sensibilität der Mitarbeiter und Geschäftspartner, die richtige Technologie und die Verankerung von Schutzmaßnahmen in allen wichtigen Geschäftsprozessen". Werde eine dieser Facetten nicht berücksichtigt, wackele das gesamte Schutzkonzept, so der Accenture-Analyst.

Links im Artikel:

[1] **http://whitepaper.computerwoche.de/index.cfm?cid=38&pkdownloads=3518**
[2] **http://carta.info/20571/datenskandale-2009/**
[3] **https://www.computerwoche.de/security/1909727/**
[4] **https://www.computerwoche.de/security/1934449/**
[5] **http://whitepaper.computerwoche.de/index.cfm?cid=38&pkdownloads=3578**
[6] **https://microsite.accenture.com/dataprivacyreport/Pages/default.aspx**
[7] **https://www.cio.de/dynamicit/aktuelles/2232456/index.html**
[8] **http://whitepaper.computerwoche.de/index.cfm?cid=38&pkdownloads=3515**
[9] **http://whitepaper.computerwoche.de/index.cfm?cid=38&pkdownloads=3505**
[10] **https://www.cio.de/knowledgecenter/security/2237737/**
[11] **https://www.cio.de/schwerpunkt/d/Datenschutz.html**
[12] **http://whitepaper.computerwoche.de/index.cfm?cid=38&pkdownloads=3567**
[13] **https://www.cio.de/healthcareit/**
[14] **https://www.cio.de/public-ict/**
[15] **http://whitepaper.computerwoche.de/index.cfm?cid=38&pkdownloads=3750**
[16] **http://whitepaper.computerwoche.de/index.cfm?cid=38&pkdownloads=3573**
[17] **http://whitepaper.computerwoche.de/index.cfm?cid=38&pkdownloads=3569**

IDG Business Media GmbH
Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Business Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Business Media GmbH keine Verantwortung.