



PGP[®] White Paper

August 2009

Die Novellierung des Bundesdatenschutzgesetzes und Gesetzeskonformität durch Verschlüsselung

Inhaltsverzeichnis

INHALTSVERZEICHNIS	2
EINLEITUNG	3
INHALT DER NOVELLIERUNG II DES BUNDESDATENSCHUTZGESETZES	4
STÄRKUNG DER RECHTE DES DATENSCHUTZBEAUFTRAGTEN	4
AUFTRAGSDATENVERARBEITUNG	4
ADRESSHANDEL UND WERBUNG	5
ARBEITNEHMERDATENSCHUTZ	5
MITTEILUNGSPFLICHTEN	5
ERHÖHUNG DER BUßGELDER	6
KONSEQUENZEN FÜR UNTERNEHMEN UND BEHÖRDEN.....	7
„DURCHFÜHRUNG VON REGELMÄßIGEN AUDITS ERHÖHT DEN ISMS AUFWAND.“	7
„WENN DIE INFORMATIONSPFLICHT GREIFT, KÖNNEN DIE DAMIT VERBUNDENEN KOSTEN ERHEBLICH SEIN.“	7
„BEI BEKANTWERDEN EINER DATENPANNE RISKIERT EIN UNTERNEHMEN ODER BEHÖRDE VERTRAUENSVERLUST.“	8
„ERHÖHUNG DES BUßGELDES UND STÄRKERE STELLUNG DES DATENSCHUTZBEAUFTRAGEN.“	8
LÖSUNGSANSÄTZE	9
„BEAUFTRAGUNG EXTERNER SACHVERSTÄNDIGER“	9
„ZERTIFIZIERUNG DER DIENSTLEISTER“	9
„AM BESTEN ERST GAR KEINE DATENPANNE AUFKOMMEN LASSEN.“	9
BEITRAG DER PGP CORPORATION ZUM SCHUTZ IHRER DATEN	11
PGP® ENCRYPTION PLATFORM	11
DATENSCHUTZ FÜR MOBILE ENDGERÄTE.....	12
SICHERE E-MAIL-KOMMUNIKATION	12
DATENSCHUTZ ÜBER DEN ENDPUNKT HINAUS	12
SICHERE GESCHÄFTSPROZESSE	12
FAZIT	13
ÜBER DEN AUTOR.....	13
QUELLENVERZEICHNIS.....	14
ÜBER PGP CORPORATION	15

Einleitung

Im August 2008 wurde der Verbraucherzentrale in Schleswig-Holstein eine CD mit 17.000 Kundendaten und Bankverbindungen zugespielt (1). Der Skandal um den Missbrauch von Millionen sensibler Kundendaten sorgte für großes Aufsehen in der Bevölkerung. Die Politik reagierte umgehend mit der Novellierung (2) des Bundesdatenschutzgesetzes (BDSG). Die Datenschutznovelle I (Scoring) wurde bereits am 29. Mai 2009 beschlossen und soll am 1. April 2010 in Kraft treten. Am 3. Juli 2009 verabschiedete der Deutsche Bundestag die Datenschutznovelle II (Datenhandel) und berücksichtigte dabei die Änderungsempfehlungen des Innenausschusses vom 1. Juli. Die Novelle II tritt am 1. September 2009 in Kraft. Die BDSG-Novelle III erfolgt im Zusammenhang mit der Umsetzung der EU-Richtlinien und tritt am 11. Juni 2010 in Kraft.

Dieses White Paper beschäftigt sich mit den Änderungen des BDSG durch die Novellierung II und beschreibt die wesentlichen Neuerungen, Konsequenzen für Unternehmen und Behörden sowie Lösungsansätze mittels Verschlüsselungslösungen.

Inhalt der Novellierung II des Bundesdatenschutzgesetzes

Die Datenschutznovelle II von 2009 führt in folgenden Bereichen zu Änderungen (4):

- Stärkung der Rechte des Datenschutzbeauftragten (§ 4f Abs. 3)
- Auftragsdatenverarbeitung (§ 11 Abs. 2)
- Adresshandel und Werbung (§ 28 Abs. 3, § 34 Abs. 1a)
- Arbeitnehmerdatenschutz (§ 32)
- Mitteilungspflichten (§ 42a)
- Erhöhung der Bußgelder (§ 43 Abs. 3)

Stärkung der Rechte des Datenschutzbeauftragten

Bisher ist der interne Datenschutzbeauftragte arbeitsrechtlich allein durch ein Benachteiligungsverbot und eine erschwerte Abberufung geschützt. Mit der Novellierung II des BDSG stellt der Gesetzgeber den Kündigungsschutz des Datenschutzbeauftragten privilegierten Funktionsträgern aus anderen Bereichen (z.B. Betriebsrat) gleich. Dieser Kündigungsschutz wird auf ein Jahr nach der Abberufung des internen Datenschutzbeauftragten erweitert.

Zur Wahrnehmung seiner Pflichten muss sich der interne Datenschutzbeauftragte permanent fortbilden. Das Unternehmen oder die Behörde muss die Teilnahme an Fortbildungen ermöglichen und die entstehenden Kosten übernehmen.

Auftragsdatenverarbeitung

Werden personenbezogene Daten nicht durch das Unternehmen oder die Behörde sondern durch Dritte verarbeitet, wird von Auftragsdatenverarbeitung gesprochen. Beispiele sind Wartungsverträge mit Systemhäusern oder die externe Datenträgervernichtung. Der Auftraggeber hatte den Auftragnehmer bisher nach seiner Eignung in Bezug auf die erforderlichen technischen und organisatorischen Maßnahmen auszuwählen. Verstöße gegen die Pflicht der ordentlichen Auswahl des Datenverarbeiters waren für den Auftraggeber bislang nicht bußgeldbewährt.

Mit der Novellierung II des BDSG wird vom Auftraggeber vor der Erteilung eines Auftrages zur Auftragsdatenverarbeitung gefordert, die Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen zu überprüfen. Bei längerfristigen Verträgen zur Auftragsdatenverarbeitung sind diese Prüfungen in regelmäßigen Intervallen zu wiederholen. Als Nachweis gegenüber den Aufsichtsbehörden sind die Prüfungen zu dokumentieren.

Die Anforderungen an den Vertrag zur Auftragsdatenverarbeitung werden in einem 10-Punkte-Katalog konkretisiert. Danach müssen diese Punkte schriftlich in dem Vertrag behandelt werden.

Verstöße gegen die Pflicht, Datenverarbeitungsaufträge ordnungsgemäß und in Übereinstimmung mit dem nun überarbeiteten § 11 BDSG zu erteilen, können fortan mit einem Bußgeld von bis zu 50.000 EUR geahndet werden.

Adresshandel und Werbung

Das bisherige sog. Listenprivileg, wonach Unternehmen Verbraucherdaten in tabellarisch zusammengefasster Form weitergeben durften, wenn nur bestimmte Kategorien von Daten enthalten waren, ist nach langer Diskussion nicht gänzlich abgeschafft, sondern lediglich eingeschränkt worden. Unternehmen müssen in Zukunft den Empfänger eines Werbeschreibens darüber informieren, woher die über ihn vorhandenen Daten ursprünglich stammen. Die Werbung zwischen Unternehmen ist davon nicht betroffen. Hierfür dürfen auch die Namen der Ansprechpartner in den Unternehmen verwendet werden, um diese direkt anschreiben zu können.

Weitere Ausnahmen gelten für den Bereich der Bewerbung von Bestandskunden, für steuerbegünstigte Spendenwerbung und Werbung nach im Gesetz genauer definierten Transparenzgeboten.

Adresshändler trifft nun die Pflicht, die Herkunft der von ihnen verwendeten Daten und die Identität des Empfängers für zwei Jahre zu speichern.

Arbeitnehmerdatenschutz

Als Reaktion auf verschiedene Datenschutzvorfälle der jüngsten Vergangenheit wird eine Grundregel zum Arbeitnehmerdatenschutz eingeführt, die vor allem die eigenständige Aufklärung von Straftaten durch Unternehmen behindert. So werden beispielsweise präventive Maßnahmen zur Korruptionsbekämpfung verboten. Weiterhin darf ein Arbeitgeber um etwaigen Rechtsverstößen in seinem Unternehmen oder Behörde nachzugehen nur dann aktiv werden, wenn die im Gesetz beschriebenen Voraussetzungen gegeben sind.

Diese Vorgaben sind inhaltlich jedoch bereits ohnehin geltendes Recht und stellen somit keine wesentlichen Neuerungen dar.

Mitteilungspflichten

Besondere Risiken wird für die Wirtschaft eine weitere Neuerung mit sich bringen. Nach US-amerikanischem Vorbild werden Unternehmen und Behörden künftig, ggf. unter Einbeziehung des internen Datenschutzbeauftragten, die Datenschutzaufsichtsbehörden und die Betroffenen über Datenschutzverstöße informieren müssen.

Diese Pflicht bezieht sich auf besonders sensible, personenbezogene Daten:

- besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG),
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder
- personenbezogene Daten zu Bank- oder Kreditkartenkonten

Die Mitteilung an die zuständigen Stellen hat grundsätzlich unverzüglich zu erfolgen. Die Meldung an den Betroffenen erfolgt im Rahmen einer verantwortungsvollen Offenlegung.

Dies bedeutet, dass der Betroffene erst informiert werden darf, wenn ein etwaiger polizeilicher Ermittlungserfolg durch die Information nicht mehr gefährdet wird. Sofern die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand nach sich ziehen würde, kann diese alternativ auch durch Anzeigen in zwei bundesweit erscheinenden Tageszeitungen oder andere gleich geeignete Maßnahmen erfolgen.

Für Unternehmen, in denen der Verdacht aufkommt, dass eine Meldung über einen von der neuen Vorschrift erfassten Sachverhalt erforderlich sein könnte, stellen sich insbesondere zwei schwierig zu beurteilende Fragen:

1. Drohen tatsächlich "schwerwiegende Beeinträchtigungen der Rechte des Betroffenen", wie sie gemäß dem neu in das Gesetz eingefügten § 42a BDSG erforderlich sind, um die Mitteilungspflicht auszulösen?
2. Sollte, weil die Antwort auf Frage 1 u.U. nicht mit letzter Sicherheit zu geben ist, höchst vorsorglich die Mitteilung an die zuständige Behörde erfolgen, um ein mögliches empfindliches Bußgeld zu vermeiden?

Wer seinen Pflichten nach § 42a BDSG nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig nachkommt, kann mit einem Bußgeld von bis zu 300.000 EUR belegt werden.

Fallbeispiel:

Einem Geschäftsführer eines Industrieunternehmens wird auf einer Dienstreise ein Notebook gestohlen, auf dem Kunden- und Abrechnungsdaten gespeichert sind, (schwerwiegende Beeinträchtigung der Rechte der Betroffenen). Dieser Vorfall muss der zuständigen Aufsichtsbehörde gemeldet werden. Sobald eine Information an die Betroffenen einen polizeilichen Ermittlungserfolg nicht mehr gefährdet, sind alle betroffenen Kunden über diesen unrechtmäßigen Datenabfluss zu informieren.

Erhöhung der Bußgelder

Künftig sind bei einfachen Verstößen gegen das Bundesdatenschutzgesetz Bußgelder bis zu 50.000 und bei schwerwiegenden Verstößen Bußgelder bis zu 300.000 EUR möglich. Wenn Verstöße zu weitergehenden Gewinnen führen, kann das Bußgeld entsprechend erhöht werden.

Konsequenzen für Unternehmen und Behörden

Aus den beschriebenen Änderungen im BDSG ergeben sich einige Konsequenzen für Unternehmen und Behörden. Da in diesem Papier nicht zu allen Neuerungen Stellung genommen werden kann, soll vielmehr das Augenmerk auf die Bereiche gelegt werden, die direkten Einfluss auf die Informationsverarbeitung im engeren Sinne haben.

„Durchführung von regelmäßigen Audits erhöht den ISMS Aufwand.“

Eigentlich sollten jedes Unternehmen und jede Behörde im Zuge ihres Information-Sicherheits-Management-Systems (ISMS) regelmäßig Audits bei sich und ihren Partnern, die sensitive Informationen verarbeiten, durchführen. In der Praxis wird dies jedoch oft vernachlässigt. Nun wird ein solches Audit zumindest bzgl. personenbezogener Daten gesetzlich gefordert. Ein derartiges Audit muss entsprechend geplant und umgesetzt, d.h. ein Auditplan für die Umsetzung der regelmäßigen Audits muss erstellt werden.

Die technische und organisatorische Umgebung beim Dienstleister muss durch einen Auditor geprüft und das Ergebnis dokumentiert werden. Zwar werden bei derartigen Audits nur Stichprobenprüfungen durchgeführt, aber dennoch kann der Aufwand hierfür bei Beschäftigung mehrerer Dienstleister beträchtlich sein.

„Wenn die Informationspflicht greift, können die damit verbundenen Kosten erheblich sein.“

Laut einer Studie (6) über die Kosten von Datenpannen in den USA kostete der Verlust eines Datensatzes im Jahr 2008 im Durchschnitt 202 USD (142 EUR). Die Aufwendungen für die Benachrichtigung (Benachrichtigung der betroffenen Personen über die Datenpanne) lagen im Schnitt bei 15 USD (10,60 EUR) pro gefährdeten Datensatz. Eine Veröffentlichungspflicht bei Datenpannen ist in vielen Staaten der USA schon seit Jahren gesetzlich vorgeschrieben.

Eine Vergleichsstudie (5) für das Jahr 2008 über die Kosten von Datenpannen in Deutschland ergab Kosten für den Verlust eines Datensatzes von im Durchschnitt 112 EUR. Die Aufwendungen für die Benachrichtigung lagen im Schnitt bei 4 EUR pro gefährdeten Datensatz und damit um 6,60 EUR niedriger als in den USA.

Land	Kosten pro Verlust	Kosten für Benachrichtigung
Deutschland	112	4
USA	142	10,60

Tabelle 1: Kosten von Datenpannen pro Datensatz in EUR

Die vergleichsweise geringen Kosten für die Benachrichtigung in Deutschland führen die Autoren der genannten Studie auf die unzureichend gesetzlich verankerte Veröffentlichungspflicht bei Datenpannen in Deutschland zurück. Die Veröffentlichungspflicht bei Datenpannen wird mit Inkrafttreten der Datenschutznovelle II für Unternehmen und Behörden gesetzlich gefordert.

Angenommen, für die in der Einleitung erwähnte Datenpanne (17.000 Datensätze) würden nun 6,60 EUR zusätzlich (die Kostendifferenz zwischen USA und Deutschland für die Benachrichtigung bei Datenpannen) pro gefährdeten Datensatz anfallen, bedeutete dies eine zusätzliche Belastung für das betroffene Unternehmen von 112.200,00 EUR für diesen Vorfall. Hier gilt es zu bedenken, dass 17.000 Datensätze bei einer Datenpanne noch vergleichsweise wenig sein können. Beispielsweise betraf die Panne bei der Telekom im Oktober 2008 17 Millionen Kundendaten (7).

„Bei Bekanntwerden einer Datenpanne riskiert ein Unternehmen oder eine Behörde Vertrauensverlust.“

Die Mitteilungspflichten, die sich aus der Datenschutznovelle II ergeben, zwingen jedes Unternehmen und jede Behörde bei Datenpannen, Informationen über diesen Vorfall bekanntzugeben. In jedem Fall wird der Vorfall veröffentlicht, und es kann ein erheblicher, finanziell nur schwer zu beziffernder Vertrauensverlust entstehen.

Die Bekanntgabe von Datenpannen wird sicherlich die Presse dankend übernehmen. Aber auch im Internet verfügbare Datenbanken wie die öffentlich zugängliche DATALOSSdb wird dafür sorgen, dass Datenpannen in Deutschland künftig nicht mehr unbemerkt bleiben.

„Erhöhung des Bußgeldes und stärkere Stellung des Datenschutzbeauftragten.“

Natürlich besteht die Verlockung, insbesondere auch aufgrund der oben geschilderten Unsicherheit zu beurteilen, wann es sich um "schwerwiegende Beeinträchtigungen" für die Betroffenen handelt, die Kosten für die Benachrichtigung einer Datenpanne einzusparen, indem der Vorfall nicht gemeldet wird. Der weitgehende Kündigungsschutz und damit die Unabhängigkeit des betrieblichen bzw. behördlichen Datenschutzbeauftragten könnte dies in machen Fällen erschweren. Vor allem aber dürfte die Erhöhung der Bußgelder auf bis zu 300.000 EUR – und in Einzelfällen sogar darüber hinaus – abschreckend wirken.

Lösungsansätze

Die Konsequenzen aufgrund der BDSG-Novellierungen können, wie eben beschrieben, beträchtlich sein. Daher gilt es, die organisatorischen und technischen Maßnahmen in Unternehmen und Behörden so anzupassen, dass die Anforderungen des neuen BDSG erfüllt bzw. gewisse Vorschriften wie z.B. § 42a (Mitteilungspflicht) erst gar nicht angewendet werden müssen.

„Beauftragung externer Sachverständiger“

Die Prüfung der Dienstleister durch den Auftraggeber muss nicht zwingend vor Ort durchgeführt werden. Ein Testat eines externen Sachverständigen kann ausreichend sein. Gerade für kleinere und mittelständische Unternehmen, die kein eigenes Sicherheitsmanagement betreiben, kann es wirtschaftlich sinnvoller sein, die Auditierung der Dienstleister durch einen externen Auditor durchführen zu lassen.

„Zertifizierung der Dienstleister“

Alternativ zur Prüfung des Dienstleisters im Sinne des reformierten § 11 BDSG kann eine schriftliche Auskunft des Auftragnehmers ausreichen. Aus Sicht des Auftraggebers ist dies selbstverständlich die einfachste Lösung. Es sollte jedoch sichergestellt werden, dass diese Auskunft auch belastbar ist. Sie ist es, wenn z.B. der Auftragnehmer ein Zertifikat oder Gütesiegel (ISO 27001 Zertifikat, Datenschutz Gütesiegel, etc.) vorweisen kann.

„Am besten erst gar keine Datenpanne aufkommen lassen.“

Um erst gar nicht in die missliche Lage zu geraten, der § 42a BDSG (Mitteilungspflicht bei Datenpannen) anwenden zu müssen, ist die logische Konsequenz für Unternehmen und Behörden, bereits beim Schutz der datenschutzwürdigen Informationen geeignete Maßnahmen zu ergreifen. Hierbei muss der Schutz der Daten gegen Diebstahl, fahrlässigen und vorsätzlichen Datenabfluss gewährleistet werden.

Sicherheitsmaßnahmen gliedern sich bekanntermaßen in organisatorische und technische Bereiche. Wichtig hierbei ist, dass die organisatorischen und technischen Sicherheitsmaßnahmen ineinander greifen und sich gegenseitig unterstützen. Neben einem funktionierenden Information-Sicherheits-Management-System (ISMS) mit den entsprechenden Prozessen und Sensibilisierungsmaßnahmen für die Mitarbeiter können technische Hilfsmittel den Datenschutz unterstützen.

Die technischen Werkzeuge müssen die Wege von möglichen Datenabflüssen versperren bzw. die abfließenden Daten unbrauchbar bzw. unlesbar machen. Eine wichtige Maßnahme, um dieses Ziel zu erreichen, ist die Datenverschlüsselung.

Hier gilt es insbesondere darauf zu achten, Verschlüsselung an allen exponierten und bedrohten Stellen durchgängig einzusetzen:

- Mobile Geräte (Notebooks, Smartphones, USB-Sticks, CD-ROMs, ...)
- Netzlaufwerke
- Transport über unsichere Netzwerke (E-Mail, FTP, ...)
- Datenbanken mit vertraulichem Inhalt (Kundendaten, Kreditkarten, Pläne, ...)

Werden in allen oben genannten Bereichen Verschlüsselungslösungen verwendet, stellt sich die Frage nach dem Schlüssel- und Policymanagement. Um dies bei all den komplexen Anforderungen noch sinnvoll verwalten zu können, fällt die Produktwahl zwangsläufig auf eine integrierte Lösung. Die PGP Corporation liefert mit Ihrer PGP® Encryption Platform einen derartig integrierten Ansatz.

Beitrag der PGP Corporation zum Schutz Ihrer Daten

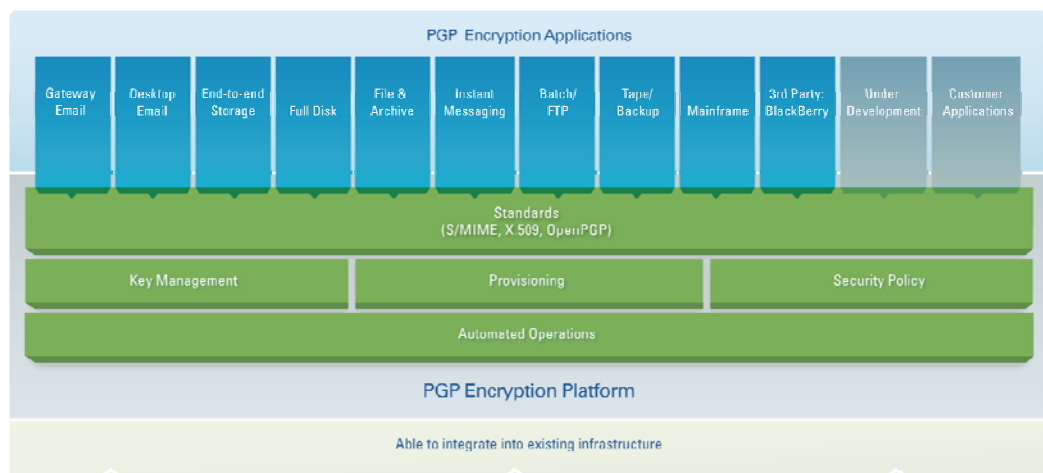
Die PGP Corporation liefert durch ihre Verschlüsselungslösungen einen wichtigen Beitrag zur Erfüllung der Anforderungen des BDSG. Insbesondere werden hierdurch Datenpannen verhindert und die damit verbundenen Kosten eingespart.

PGP® Encryption Platform

Die PGP Encryption Platform bietet eine gute Lösung beim Schutz von Unternehmensdaten, da sie es Unternehmen ermöglicht, Verschlüsselungsanwendungen kostengünstig über eine einheitliche Verwaltungskonsole bereitzustellen und zu verwalten. Da die PGP Encryption Platform bereits zusammen mit der ersten Verschlüsselungsanwendung bereitgestellt wird, braucht keine gesonderte oder zusätzliche Infrastruktur installiert werden, wenn das Unternehmen weitere Verschlüsselungsanwendungen benötigt.

Die PGP Encryption Platform bietet einen unternehmensweiten strategischen Rahmen für die gemeinsame automatisierte Verwaltung von Anwendern, Schlüsseln, Richtlinien und Provisioning über mehrere integrierte Verschlüsselungsanwendungen hinweg. Solche Verschlüsselungsanwendungen der PGP Corporation und von Drittanbietern ermöglichen es Unternehmen, automatisierte Verschlüsselungsverfahren je nach Bedarf einzusetzen, um die für die Geschäftsbedürfnisse geeignete Datensicherheit herzustellen. Diese datenzentrierte Methode schützt Daten, während sie gespeichert sind sowie bei der Übertragung, überall und jederzeit.

Schaubild: PGP Encryption Platform



Datenschutz für mobile Endgeräte

In der heutigen mobilen Arbeitswelt sind Daten überall: auf Laptops, Smartphones, Wechseldatenträgern wie USB-Sticks oder anderen Geräten. Einige dieser Daten sind vertraulich, einige unterliegen behördlichen Vorschriften. Die Folgen bei einem Verlust oder Diebstahl eines einzigen Geräts können, wie beschrieben, nicht nur mit einer gesetzlichen Strafe geahndet werden.

Sichere E-Mail-Kommunikation

Die vertrauliche Kommunikation mit Kunden, Geschäftspartnern, Lieferanten und Beratern schützt Ihre Privatsphäre und Ihr Unternehmen. Sie hilft Ihnen sogar dabei, behördliche Vorschriften einzuhalten. Schützen Sie Ihre vertraulichen Nachrichten mit den PGP®-Lösungen für die sichere E-Mail-Kommunikation: Sie sind standardbasiert, automatisiert und dank zentraler Richtlinien- und Schlüsselverwaltung einfach einzusetzen.

Datenschutz über den Endpunkt hinaus

In Arbeitsgruppen arbeiten häufig mehrere Mitarbeiter gemeinsam an Dateien, die auf Servern oder Endgeräten gespeichert sind. Diese Dateien müssen vor unbefugtem Zugriff geschützt werden, damit sie vertraulich bleiben und alle Vorschriften eingehalten werden. PGP-Lösungen sorgen dafür, dass ausschließlich befugte Benutzer auf autorisierte Geräte und deren geschützte Dateien zugreifen und diese nutzen können. Auf diese Weise wird ein verantwortlicher Umgang mit den Daten sichergestellt, während gleichzeitig die Datenintegrität und der Datenschutz gewährleistet sind.

Sichere Geschäftsprozesse

Gleichgültig, ob riesige Datenübertragungen, E-Mail-Anhänge, Sicherungskopien, ruhende oder mobile Daten: Verschlüsselungslösungen schützen wichtige Betriebsunterlagen und vertrauliche E-Mail-Anhänge vor unbefugtem Zugriff und anderen Gefährdungen.

Fazit

Die Novellierung II des BDSG hat weitreichende Konsequenzen für Unternehmen und Behörden. Die meisten Unternehmen und Behörden werden ihre Datenschutzrichtlinien und Maßnahmen überarbeiten müssen. Dies dient letztendlich auch der Informationssicherheit und wird hoffentlich das Informationssicherheitsniveau in Deutschland insgesamt erhöhen.

Über den Autor

Marc Heinzmann ist Geschäftsführer der plan42 GmbH, eines Beratungsunternehmens für IT-Security- und IT-Service-Management. Seine derzeitigen Arbeitsgebiete sind u.a. Beratung im Bereich der Informationssicherheit wie Aufbau von IT-Sicherheitsmanagement-Systemen, Vorbereitung und Durchführung von ISO 27001 Zertifizierungen, IT-Security Audits und Penetrationstests. Marc Heinzmann ist lizenzierter ISO 27001 Auditor auf Basis von IT-Grundschutz.

Marc Heinzmann



Bauerstr. 19
80796 München
Tel. 089 / 10765716
E-Mail: mh@plan42.com

Rechtliche Beratung

Dr. Alexander Niethammer ist Partner bei Heisse Kursawe Eversheds und berät schwerpunktmäßig nationale und internationale Unternehmen im IT-Recht und Datenschutzrecht. Zu Herrn Dr. Niethammers Mandanten zählen mehrere Fortune 100 Unternehmen, die er umfassend in datenschutzrechtlichen Compliance-Fragen und -Projekten betreut. Neben seiner Anwaltszulassung in Deutschland verfügt Herr Dr. Niethammer auch über die Zulassung als Attorney-at-Law im Staat New York, USA.

Dr. Alexander Niethammer, LL.M. (UConn), Rechtsanwalt



HEISSE KURSAWE EVERSHEADS

Maximiliansplatz 5
80333 München
Tel. 089 / 54 56 5-0
E-Mail: alexander.niethammer@eversheds.de

Quellenverzeichnis

- (1) Süddeutsche Zeitung, „17.000 Datensätze von Bankkunden missbraucht“ , 12.08.2008, <http://www.sueddeutsche.de/computer/976/305941/text/>
- (2) Der Sächsische Datenschutzbeauftragte, „Änderungen des Bundesdatenschutzgesetzes“, <http://www.saechsdsb.de/aenderungen-des-bdsg>
- (3) Deutscher Bundestag, „Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften“, 18.02.2009, <http://dip21.bundestag.de/dip21/btd/16/120/1612011.pdf>
- (4) Dr. Michael Rath, „Wesentliche Inhalte der Datenschutz-Reform“, 21.07.2009, <http://www.compliancemagazin.de/compliancefachbeitraege/recht/luther210709.html>
- (5) Ponemon Institute, „Jahresstudie 2008: Kosten von Datenpannen in Deutschland“, Februar 2009, <http://www.encryptionreports.com/costofdatabreach.html>
- (6) Ponemon Institute, „2008 Annual Study: Cost of a Data Breach“, Februar 2009, <http://www.encryptionreports.com/costofdatabreach.html>
- (7) PRESSEBOX, „Datenverlust der Telekom nur Spitze des Eisbergs“, 07.10.2008, <http://www.pressebox.de/pressemeldungen/workshare-inc/boxid-208571.html>

Über PGP Corporation

PGP Corporation ist ein weltweiter Anbieter von Sicherheitssoftware und Marktführer in der Verschlüsselung von E-Mails und Daten. Auf der Basis einer einheitlichen Infrastruktur zur Schlüssel- und Richtlinienverwaltung bietet die PGP Encryption Platform eine umfassende Palette integrierter Sicherheitsanwendungen für Unternehmen. Mit der PGP Encryption Platform und den entsprechenden Anwendungen können Unternehmen aktuelle Anforderungen zur Datensicherheit erfüllen und bei wachsendem Bedarf auf einfache Weise weitere PGP-Anwendungen hinzufügen, zum Beispiel zur Verschlüsselung von E-Mails, Laptops, Desktop-Computern, Instant Messages, Smartphones, Dateiservern, FTP, großen Datenübertragungen und Backups.

PGP®-Lösungen werden weltweit von mehr als 100.000 Unternehmen und Behörden genutzt, darunter 87 Prozent der deutschen DAX-Unternehmen, 95 Prozent der Fortune® 100 Unternehmen und 75 Prozent der Fortune® Global 100 Unternehmen. Die PGP Corporation hat eine weltweite Reputation für innovative, standardbasierte und vertrauenswürdige Sicherheitsprodukte erworben. PGP-Produkte helfen vertrauliche Informationen und Kundendaten zu sichern, Sicherheitsrichtlinien einzuhalten sowie den Markenwert und Ruf von Unternehmen zu schützen.

Weitere Informationen zur PGP Corporation und der PGP Deutschland AG unter www.pgp.de oder +49 (69) 83 83 10-0.

PGP Deutschland AG

Strahlenberger Str. 110
63067 Offenbach
Tel: +49 69 8383 10-0
Fax: +49 69 8383 10-66
Sales: +49 69 8383 10-44
Support: support.pgp.com
Website: www.pgp.de

© 2009 PGP Corporation

All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form by any means without the prior written approval of PGP Corporation.

The information described in this document may be protected by one or more U.S. patents, foreign patents, or pending applications.

PGP and the PGP logo are registered trademarks of PGP Corporation. Product and brand names used in the document may be trademarks or registered trademarks of their respective owners. Any such trademarks or registered trademarks are the sole property of their respective owners.

The information in this document is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors.

All strategic and product statements in this document are subject to change at PGP Corporation's sole discretion, including the right to alter or cancel features, functionality, or release dates.

Changes to this document may be made at any time without notice.