www.hsp-gruppe.de
AUSGABE 27
1. Quartal 2012

DAS QUARTAL®

DAS MANDANTENMAGAZIN DER HSP GRUPPE

1.12

MAGAZIN FÜR STEUERN, RECHT, WIRTSCHAFT UND FINANZEN

Datenschutz für Unternehmer – quo vadis?

2011 und auch schon zu Beginn des Jahres 2012 wurden in der Öffentlichkeit diverse Datenschutzthemen zum Teil kritisch und kontrovers diskutiert.

Themen im Fokus: **Seite 8**

Datenschutz für Unternehmer – quo vadis?

2011 und auch schon zu Beginn des Jahres 2012 wurden in der Öffentlichkeit diverse Datenschutzthemen zum Teil kritisch und kontrovers diskutiert.

Text: **Michael J. Schöpf**, Geschäftsführer des Beratungsunternehmens s-con Datenschutz & ITK

Unter anderem wird die Nutzung von **Facebook** vom „Düsseldorfer Kreis", der informellen Vereinigung der obersten Aufsichtsbehörden, als datenschutzrechtlich problematisch angesehen. So soll z. B. die Nutzung von **Facebook-Fanpages** gegen das Bundesdatenschutzgesetz verstoßen und auch der Einsatz von **Social-Network-Plug-ins „gefällt mir"** wird als nicht datenschutzkonform angesehen. Grundsätzlich muss jedes Unternehmen überlegen, wie zukünftig mit dem Thema **„Social Media"** umgegangen werden soll. Ein sorgloser Umgang bringt zum Teil unkalkulierbare Risiken und erleichtert z. B. Datenraubzüge der Industriespione und den unberechtigten Zugang zu Daten durch Datendiebe.

Schlagwörter wie **„Bring your own device"** begleiten uns in der aktuellen Diskussion zur Nutzung von privaten Systemen bei der Erfüllung betrieblicher Aufgaben. „Bring your own device" bedeutet, dass Mitarbeiter ihre privaten IT-Systeme zur Abarbeitung von dienstlichen Aufgaben nutzen und in das Unternehmensnetzwerk einbinden. Hier ist sorgsam zu prüfen, wie dieser Trend in Einklang mit Datenschutz und IT-Sicherheit gebracht werden kann.

Das Jahr 2012 wird weitere grundlegende Entscheidungen für den Datenschutz bringen. Die zur Verabschiedung anstehende **EU-Datenschutzverordnung** wird zum Teil nationale Datenschutzgesetze ablösen bzw. ergänzen. Die EU-Datenschutzverordnung wird bei Umsetzung gravierende verschärfende Auswirkungen auf das Thema Datenschutz in Deutschland haben. So ist zum Beispiel eine Benachrichtigungspflicht des Unternehmens im Fall eines vermuteten unberechtigten Zugriffs auf Daten binnen 24 Stunden an die zuständige Datenschutzaufsichtsbehörde geplant. Die Bußgelder sollen drastisch erhöht werden. Im Entwurf werden Zahlen zwischen 100.000 und 1.000.000 Euro oder bis zu 2 Prozent des Jahresumsatzes einer Firma genannt. Es ist davon auszugehen, dass die EU-Datenschutzverordnung sehr reale Auswirkungen auf die Geschäftsprozesse der Unternehmen haben wird.

Seit Längerem liegt in Deutschland ein Entwurf für ein **Beschäftigtendatenschutzgesetz** vor. Am 10. Februar 2012 wurde über www.zeitonline.de folgende Nachricht kommuniziert: „Die Regierungskoalition hat sich auf ein neues Gesetz geeinigt, das Arbeitnehmer besser vor heimlicher Beobachtung durch den Arbeitgeber schützen soll. Die FDP-Innenexpertin Gisela Piltz bestätigte einen entsprechenden Bericht der Financial Times Deutschland. Danach soll eine versteckte Videoüberwachung grundsätzlich verboten sein. Auf Druck der Wirtschaft können jedoch Rechte von Mitarbeitern eingeschränkt werden, wenn es entsprechende Betriebsvereinbarungen oder persönliche Einwilligungen der Arbeitnehmer gibt. Über die Initiative war zuvor monatelang debattiert worden."

Ein sorgloser Umgang bringt zum Teil unkalkulierbare Risiken und erleichtert z. B. Datenraubzüge der Industriespione und den unberechtigten Zugang zu Daten durch Datendiebe.

Daten- und IT-Sicherheit 2012/2013. Für die Zukunft prognostizieren Experten weitere Bedrohungen der IT-Sicherheit von Regierungen und Unternehmen. So wird nicht nur die Anzahl der gezielten Angriffe auf staatliche Institutionen und Unternehmen weiter steigen, es ist auch damit zu rechnen, dass die Bandbreite der Opfer merklich ausgeweitet wird. Die Sicherheitsexperten von Kaspersky Lab gehen davon aus, dass vor allem Unternehmen aus der Rohstoffgewinnung, Energie-, Verkehrs-, Lebensmittel- und Pharmaindustrie sowie Internet-Services und IT-Unternehmen die Angriffsziele der Zukunft sein werden.

Die Weiterentwicklungen innerhalb der IT-Sicherheitsbranche zur Abwehr gezielter Angriffe sowie das gewachsene Bewusstsein der Öffentlichkeit zwingt Cyberkriminelle, neue Instrumente zu entwickeln. Die herkömmliche Methode der Angriffe via E-Mail wird zunehmend weniger effektiv werden. **Attacken beim Einsatz von Browsern** werden hingegen an Popularität gewinnen.

Der Siegeszug der Tablet Computer wird sich fortsetzen. Die Anzahl der **Bedrohungen für mobile Endgeräte** wird weiterhin steigen, wobei Google Android das primäre Angriffsziel bleiben wird. Das bedeutet, dass auch bei mobilen Geräten im Hinblick auf Datenschutz und IT-Sicherheit hohe Sicherheitsanforderungen notwendig sind.

Smartphone-Anbieter müssen auf einem umkämpften Markt bestehen, der permanenten Änderungen unterworfen ist. Auf der Sicherheit der Smartphones oder der Applikationen liegt daher nicht immer die höchste Priorität. Auf der anderen Seite ermöglichen die ständig wachsenden Funktionalitäten der Smartphones den Benutzern, permanent überall erreichbar zu sein und dabei nicht nur große Datenmengen verarbeiten zu können,

10 Big Points zum Datenschutz

1. **Gesetze und Verordnungen**
2. **Technische und organisatorische Maßnahmen (TOM)**
3. **Mitarbeiter(innen)**
4. **Der/die Datenschutzbeauftragte**
5. **Dienstleister**
6. **Dokumentation**
7. **Regelungen für Systeme, Anwendungen und Dienste**
8. **Social Media**
9. **Datenschutzpannen**
10. **Verantwortung und Faustformel**

sondern auch mobil auf Unternehmens- oder Behördennetze zugreifen zu können. Smartphones sind daher höchst attraktive Angriffsziele. Es gibt eine stetig zunehmende Anzahl von Schadsoftware, die auf Smartphones spezialisiert ist. Häufig stehen dahinter ähnliche Ziele wie bei Schadsoftware für den PC. Diese Gefahren sind bei den Überlegungen zum Datenschutz und zur IT-Sicherheit unbedingt zu berücksichtigen.

Ein weiterer Trend ist **Cloud Computing**. Beim Cloud Computing erfolgt die Nutzung von IT-Leistungen in Echtzeit über Datennetze (in der „Wolke") statt auf lokalen Systemen. Cloud Computing hat sich innerhalb weniger Jahre zu einem Milliarden-Markt entwickelt. Vor dem Einsatz von Cloud Computing gilt es jedoch, wichtige Sicherheits- und Datenschutzfragen zu klären. Durch Diskussionen in der jüngsten Vergangenheit waren EU-Parlamentarier sehr beunruhigt über Äußerungen eines Microsoft-Managers, demzufolge US-Sicherheitsbehörden ungehindert auf Daten von EU-Bürgern und Unternehmen zugreifen können, wenn diese Daten in der Cloud gespeichert werden. Die Grundlage dafür soll der amerikanische Patriot Act liefern.

Aufgrund der geführten Diskussionen wird z. B. Microsoft beim Datenschutz in der Cloud Maßstäbe setzen und die Vertragsbestimmungen für seinen Cloud-Dienst Office 365 in Anlehnung an die Vorstellungen deutscher Datenschützer ändern. Die neuen Regeln sollen zudem die von der EU entworfenen Standardklauseln zur Übermittlung personenbezogener Daten enthalten.

Ungesicherte USB-Anschlüsse entwickeln sich für Unternehmen zu einem immer größeren Sicherheitsrisiko. Untersuchungen haben ergeben, dass bei fast der Hälfte der Fälle die Rechner durch die Benutzer selbst infiziert werden, indem diese – in der Regel unabsichtlich – die Schadsoftware selbst starten. Besonders heikel ist, dass durch diese Art der Infizierung keinerlei Firewalls überwunden werden müssen. So werden USB-Ports zum perfekten Einfalltor für Würmer und Trojaner, um an sensible Daten zu gelangen und diese auszulesen bzw. zu verändern oder zu löschen. Das zeigt, dass durch USB-Speichermedien eine große Gefahr für den Datenschutz und die IT-Sicherheit im Unternehmen ausgeht.

Datenschutz in der Praxis. Bei allen Überlegungen und Verbreitung von Ängsten im Zusammenhang mit der Verschärfung des Datenschutzes muss jeder Unternehmer prüfen, wie er die gesetzlichen Mindestanforderungen unter Berücksichtigung der Verhältnismäßigkeit praxisorientiert umsetzen kann.

Bei allen Überlegungen und Verbreitung von Ängsten im Zusammenhang mit der Verschärfung des Datenschutzes muss jeder Unternehmen prüfen, wie er die gesetzlichen Mindestanforderungen unter Berücksichtigung der Verhältnismäßigkeit praxisorientiert umsetzen kann.

Hierzu sind 10 wichtige Punkte im Rahmen der eigenen Datenschutzorganisation zu beachten:

1. Gesetze und Verordnungen
Es ist darauf zu achten, die in 2009/2010 verschärften Datenschutzbestimmungen einzuhalten. Hierbei sind insbesondere Themen wie „Neuregelung Auftragsdatenverarbeitung (§ 11 BDSG)", „Verschärfung Auskunftsrecht (§ 34 BDSG)", „Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten (§ 42a BDSG)", neue Regelungen für die Verwendung von Daten für Werbezwecke und die Verschärfung „Technische und organisatorische Maßnahmen" (§ 9 BDSG) zu berücksichtigen und notwendige Maßnahmen zu etablieren.

2. Technische und organisatorische Maßnahmen (TOM)
Die Formulierung im BDSG (§ 9) ist auf jeden Fall zu beachten: „Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht." Das bedeutet, dass die im Gesetz vorgeschriebenen Maßnahmen unter Berücksichtigung der Angemessenheit umgesetzt werden müssen. Hier sind die Regelungen mit Dienstleistern und die Verschlüsselung ein Bestandteil der Verschärfungen aus 2009.

3. Mitarbeiter(innen)
Neben der Verpflichtung der Mitarbeiter auf das Datengeheimnis (§ 5 BDSG) ist zu prüfen, ob weitere Verpflichtungen wie z. B. auf das Fernmeldegeheimnis (§ 88 TKG) oder auf die Geheimhaltung (§ 17 UWG Verrat von Geschäfts- und Betriebsgeheimnissen) erforderlich sind.

Im Datenschutzgesetz wird verlangt, dass Mitarbeiter durch geeignete Maßnahmen über die besonderen Anforderungen des Datenschutzes zu unterrichten sind. Hier können neben Präsenzschulungen auch die Schulung bzw. Information mit Merkblättern oder webbasierenden Schulungstools erfolgen. Testen Sie kostenfrei das Tool von s-con Datenschutz & ITK unter http://www.s-con.de/wbt/?code=123xcv (Benutzername: name/Kennwort: passwort)

4. Der/Die Datenschutzbeauftragte
Die bestellt Person muss die zur Erfüllung der Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen. Auch eine externe Person kann die Aufgaben der Datenschutzbeauftragten/des Datenschutzbeauftragten übernehmen (externer Datenschutzbeauftragter). Bei internen Datenschutzbeauftragten gilt: besonderer Kündigungsschutz (§ 4f Abs. 3 Satz 4 BDSG) für Arbeitsverhältnisse/Fort- und Weiterbildungsanspruch (§ 4f Abs. 3 Satz 6 BDSG).

5. Dienstleister
Prüfen Sie die Zuverlässigkeit Ihrer Dienstleister, die z. B. in Ihrem Auftrag personenbezogene Daten Ihres Unternehmens bzw. Ihrer Kunden verarbeiten. Dieses ist im BDSG § 11 klar geregelt.

6. Dokumentation
Wirken Sie darauf hin, dass die/der Datenschutzbeauftragte die Datenschutzorganisation nachvollziehbar dokumentiert. Fordern Sie einen jährlichen Datenschutzbericht des Datenschutzbeauftragten.

7. Regelungen für Systeme, Anwendungen und Dienste
Regeln Sie den Umgang mit den IT-Systemen und Diensten wie z. B. die Nutzung von E-Mail und Internet. Eine Duldung ist nicht ratsam. Idealerweise verbieten Sie die private Nutzung der Unternehmens-IT. Hier ist abzuwägen, wie ein Verbot in die Unternehmenskultur passt.

8. Social Media
Soziale Netzwerke (Social Media) werden die Kommunikationssysteme der Zukunft. Dienste wie z. B. E-Mail werden voraussichtlich in naher Zukunft abgelöst durch Social Media: Regeln Sie den Umgang Ihren Mitarbeiter(innen) mit Social Media in Ihrem Unternehmen. Etablieren Sie eine Social-Media-Guideline.

9. Datenschutzpannen
Seit 2009 gibt es zum Thema „Datenschutzpannen" eine Verschärfung. § 42a BDSG formuliert die Voraussetzung für den Eintritt einer Datenschutzpanne. Überlegen Sie im Vorfeld die erforderlichen Maßnahmen bei Eintritt einer Datenschutzpanne.

10. Verantwortung und Faustformel
Legen Sie klare Verantwortlichkeiten für die Themen Datenschutz und IT-Sicherheit fest. Entwickeln Sie eine Faustformel für Ihre Mitarbeiter(innen) zum sicheren Umgang mit Daten.

Fazit. Prüfen Sie Ihre aktuelle Datenschutzsituation. Informieren Sie bei Bedarf Ihre Mitarbeiter(innen) über die neuen Anforderungen. Setzen Sie die Mindestanforderungen um. Eine zu 80 % umgesetzte Datenschutzorganisation ist besser als eine perfekt geplante und nicht realisierte Datenschutzorganisation.

An dem Thema „Datenschutz" ist kontinuierlich weiterzuarbeiten, um u. a. die möglichen zukünftigen verschärften Anforderungen der EU-Datenschutzverordnung zu erfüllen.

IHR ANSPRECHPARTNER BEI s-con Datenschutz & ITK

Michael J. Schöpf
Geschäftsführer
Tel.: (0511) 27 07 44-50
michael.schoepf@s-con.de