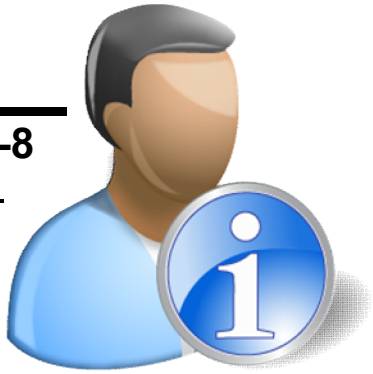

Fälle aus der Datenschutz-Praxis – Ausgabe 2011-8

An die Geschäftsführung: Es gibt gute Gründe für Datenschutz- und IT-Sicherheitsberatung!

Befragungen namhafter Institute und der Global Player in IT Infrastructure und Security belegen:

- Fortinet Studie zur IT-Sicherheit 2011: Rund 16 Prozent aller befragten Unternehmen hätten überhaupt keine Sicherheitsstrategie oder diese länger als drei Jahre nicht überprüft; nur 60 Prozent hätten ihre Strategie in den vergangenen 12 Monaten ganzheitlich neu bewertet.
- Sophos: Mehr als 80 Prozent aller Computer in Unternehmen arbeiten ohne aktuelle Anti-Viren-Software, Firewalls oder Security-Patches

- TNS Emnid Sicherheitsstudie 2010 für PricewaterhouseCoopers: Die häufigsten Ursachen für Datenschutzverletzungen sind unachtsame und unwissende Mitarbeiter (73 bzw. 63 Prozent) und eine schlechte Kommunikation (39 Prozent). Jeweils nur vier Prozent der Vorfälle sind auf Datendiebstahl durch Mitarbeiter oder durch Dritte zurückzuführen.
- Umfrageergbenisse der Zeitschrift <KES> und Microsoft in 2010: Die IT-Sicherheit scheitert am Sicherheitsbewusstsein der Mitarbeiter (59 %) oder des TOP-Managements (47 %), 41 % sind der Meinung, dass es an verfügbaren und kompetenten Mitarbeitern fehlt, regelmäßige Schulungen der Datenschutzbeauftragten finden nur bei 45 % der befragten Unternehmen statt.
- BITKOM-Studie 2011 „Datenschutz im Internet“: Jeder zehnte Internetnutzer (elf Prozent) bringt Online-Händlern gar kein Vertrauen entgegen. Der Wirtschaft allgemein vertrauen nur 41 Prozent der Internetnutzer stark bis sehr stark, wenn es um den Umgang mit ihren persönlichen Daten geht. Bei 38 Prozent aller Internetnutzer wurde der Computer bereits mit Schadprogrammen, z.B. Viren, infiziert. Datendiebstahl oder Schadprogramme können zu finanziellen Schäden führen. Bei sechs Prozent der Internetnutzer ist es bereits dazu gekommen.
- DeloitteSicherheitsstudie 2011: Insider-Betrug (28 %), d. h. Betrug durch Mitarbeiter, und der unberechtigte Zugriff auf Kundendaten (18 %) zählen zu den drei häufigsten internen Sicherheitsverletzungen.
- Ergebnis des Sicherheitschecks von „Deutschland sicher im Netz“ - DsiN: Rund 75 Prozent aller kleinen und mittleren Unternehmen in Deutschland verzichten auf regelmäßige Schulung und Information ihrer Mitarbeiter, wenn es um IT-Sicherheit und Datenschutz geht.
- NIFIS Nationale Initiative für Informations- und Internet-Sicherheit e.V. - Studie "IT-Sicherheit und Datenschutz 2011": Es wird zu wenig gegen Gefahren von außen gemacht: Keine Beschränkung hinsichtlich externer Datenträger und keine Beschränkung beim Surfen im Netz (bei 38 Prozent der befragten Unternehmen). Hauptproblem sind die Mitarbeiter. Diese gehen zu sorglos mit dem Thema Sicherheit um (bei 24 Prozent der Unternehmen)
- Ponemon Institut: Über die Hälfte der IT-Sicherheitsverantwortlichen glaubt, dass die Mitarbeiter kein ausreichendes Bewusstsein für Datenschutz und Datensicherheit haben. 53 Prozent der IT-Administratoren halten Maßnahmen zur Stärkung des Datenschutzbewusstseins für das zentrale Element einer richtigen Sicherheitsstrategie.
- Verizon „Data Breach Investigations Report“ 2011: 92 Prozent aller Datenangriffe erfolgen von außen (Zuwachs um 22 Prozent), 50 Prozent der Angriffe gehen auf die Konten von Hackern (plus zehn Prozent), bei 49 Prozent kam Schadsoftware zum Einsatz (plus elf Prozent), 97 Prozent aller Angriffe hätten durch einfache Kontrollen vermieden werden können.

Feststellung: Datenschutz und das Streben nach IT-Sicherheit harmonieren! Obwohl die beiden Aufgaben zunächst unterschiedliche Ziele haben, weisen sie in der Umsetzung eine große Schnittmenge auf und sind aufeinander angewiesen. Der Datenschutz betrachtet die Maßnahmen der IT-Sicherheit als wesentliches Werkzeug, um Datenschutzziele zu erreichen. Umgekehrt betrachtet die IT-Sicherheit den Datenschutz bei Verfahren, in denen personenbezogene Daten verarbeitet werden, als eine wesentliche Quelle für Anforderungen, die sie umzusetzen hat. Datenschutz und IT-Sicherheit weisen also eine bedeutende Schnittmenge auf.

Link: Weiterführende Informationen unter www.dbsc.de > Datenschutz > Quick Intro > Datenschutz und IT-Sicherheit - ein Abschnitt aus „Schnelleinführung in den Datenschutz“.

(In-) Diskretion in Arztpraxen

Patientin hatte sich über mangelnde Diskretion in einer Arztpraxis beklagt. Die Anmeldung der Patienten in der Praxis erfolgte an einem Tresen bei den Mitarbeiterinnen der Praxis. Die Petentin monierte, dass dieser Tresen sich unmittelbar im Wartezimmer befindet. Weder eine akustische noch eine visuelle Abschirmung ist dort vorhanden. Jeder Patient, der sich im Wartezimmer befindet, kann die bei der Anmeldung geführten Gespräche mithören. Es können sogar Gespräche über Patientendaten, die zwischen den Helferinnen bei der Anmeldung und den Ärzten geführt werden von den wartenden Patienten mitgehört werden.

Feststellung: Der Anmelde- bzw. Empfangsbereich einer Arztpraxis ist sehr häufig anfällig für Indiskretionen. Deshalb ist der beste Schutz vor Indiskretionen eine bauliche/räumliche Trennung von Warte- und Anmeldebereich.

Dies ist jedoch aufgrund der Verhältnisse vor Ort bzw. wegen zu hoher Kosten nicht immer möglich. Um dennoch den Patientenschutz zu gewährleisten sind folgende Maßnahmen geeignet:

- Der Arzt hat darauf zu achten und dies gegebenenfalls in einer Dienstanweisung, die dem gesamten Personal zur Kenntnis gegeben werden muss, festzulegen, dass keine mündlichen Therapie- oder sonstige Anweisungen gegeben werden, wenn Umstehende daraus auf Patienten schließen können.
- Die Verpflichtung der Mitarbeiter auf das Datengeheimnis ist vorzunehmen und gegebenenfalls sind die Mitarbeiter öfter daran erinnern.
- Notwendige Behandlungsanweisungen durch den Arzt an die Helferinnen sollten nur im Behandlungszimmer oder schriftlich gegeben werden.
- Auch wenn keine gesetzliche Verpflichtung dazu besteht, kann ein Datenschutzbeauftragter bestellt werden, der auf die Einhaltung der Datenschutzbestimmungen achtet.
- Auf dem Tresen sollen keine Patientenakten oder sonstige Unterlagen mit Patientendaten abgelegt werden. Es kommt nicht darauf an, dass Umstehende tatsächlich die Angaben lesen, sondern nur ob die Möglichkeit dazu besteht.
- Die Computerbildschirme sind so aufzustellen, dass Umstehende keinen Einblick in Patientendaten nehmen können.

Im vorliegenden Fall hat der betroffene Arzt solche Maßnahmen umgesetzt, und gegenüber der Aufsichtsbehörde zugesichert, darauf zu achten, dass das Recht der Patienten auf Diskretion künftig beachtet wird.

Quelle: Tätigkeitsbericht 2009/2010 der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich des Saarlandes.

Anzeige von Krankheitstagen im Intranet

Ein Unternehmen zeigte die Krankheitstage seiner Beschäftigten personenbezogen im Intranet an.

Die Zulässigkeit dieser Datenverwendung richtet sich nach § 32 Abs. 1 Satz 1 BDSG. Sie ist für die Durchführung des Beschäftigungsverhältnisses nicht erforderlich, da unverhältnismäßig, und somit unzulässig. Es darf außerhalb der personalverantwortlichen Stelle nicht als allgemeine Information zugänglich sein, wenn ein Beschäftigter aufgrund von Krankheit fehlt.

Wenn die An- oder Abwesenheit aufgrund von Arbeitseinteilung und Organisation im Unternehmen bekannt sein muss, kann dies im Intranet neutral vermerkt werden.

Feststellung: Die offene Anzeige von Krankheitstagen im Intranet ist unzulässig.

Quelle: Tätigkeitsbericht 2009/2010 Bayerisches Landesamt für Datenschutzaufsicht.

Links

- http://www.bfdi.bund.de: Bundesbeauftragter für den Datenschutz und die Informationsfreiheit.
- http://www.dbsc.de: IT-Consulting und Datentschutz-Büro.

 zusammengetragen u. editiert von G.Ruban