UIMCommunic@tion

Stets auf dem Laufenden sein?
www.UIMC.de/Communication

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Datenschutzbeauftragter kann Schadensersatzansprüche verhindern

Der Umfang der Videoüberwachung im Rahmen der Arbeit nimmt immer stärker zu. Neben der Motivation der Verfolgung von Diebstählen und Vandalismus, der Abschreckung, der Überführung von Straftaten, der Überwachung von Gefahrenschwerpunkten oder aufgrund von behördlichen Auflagen liegen verschiedene Zweckbestimmungen vor. Doch oftmals wird hierbei der Datenschutz nicht beachtet, was neben Bußgeldern und Imageschäden zunehmend auch zu (erfolgreichen) Schmerzensgeldverfahren führt, wie ein aktuelles Urteil des Bundesarbeitsgerichts zeigt. Die gewissenhafte Betrachtung der rechtlichen Anforderungen durch den Datenschutzbeauftragten kann dies verhindern.

In der täglichen Praxis erlebt Dr. Heiko Haaz, mehrfach bestellter Datenschutzbeauftragter, dass immer mehr Unternehmen zum Mittel der Videoüberwachung greifen. Neben den durchaus üblichen Zielsetzungen der Einbruchsbekämpfung (Überführung und Abschreckung) werden aber zunehmend Tendenzen offenkundig, die Videoüberwachung auf Arbeitsbereiche der Mitarbeiter auszuweiten. Gerade bei solchen Projekten ist der Datenschutzbeauftragte frühzeitig einzubinden, um den Persönlichkeitsrechten ausreichend Rechnung zu tragen. Andernfalls drohen nicht nur Verfahren durch die Aufsichtsbehörden, sondern auch, und das zeigt die aktuelle Rechtsprechung, entsprechend Schadensersatzforderungen.

So hat das Bundesarbeitsgericht jüngst entschieden – wie auch andere Gerichte schon –, dass eine dauerhafte und verdachtsunabhängige Videoüberwachung am Arbeitsplatz unverhältnis-mäßig und damit unzulässig ist. Die Schadensersatzforderungen können hierbei durchaus nennenswerte Beträge erreichen [z. B. 25.000 Euro; ArbG Iserlohn, Urteil vom 04.06.2008 – 3 Ca 2636/07). Auch ein etwaiger Imageschaden bei Kunden, Belegschaft und Betriebsrat ist sicherlich nicht zu vernachlässigen.

Freikarten: IT-Trends Sicherheit

Wir verlosen Freikarten im Wert von EUR 60,00. Teilnahmebedingungen: siehe Folgeseite.

Zur Aufdeckung von Straftaten kann eine (verdeckte) Videoüberwachung nur dann eingesetzt werden, wenn „zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen“, dass eine Straftat begangen wurde. Dabei muss die Videoüberwachung „zur Aufdeckung erforderlich“ und verhältnismäßig sein. So sprach Dr. Haaz in einem konkreten Fall beispielsweise folgende Empfehlung aus:

- Ausführliche Dokumentation des Anfangsverdachts;
- Zeitlich beschränkte Nutzung der Videoüberwachung (ca. ein Monat);
- Unverzügliche Löschung, sobald Aufzeichnungen nicht mehr erforderlich sind (z. B. werktäglich);
- Sehr restriktive Zugriffsrechte (z. B. durch geteiltes Passwort geschützt);
- Ausschließlich zweckgebundene Zugriffe.

Ohne entsprechende Regelungen und Verfahren hätten die Videoaufzeichnungen ggf. später bei einem Gerichtsverfahren nicht verwendet werden können und der bzw. die Betroffenen hätten das Unternehmen auf Schadensersatz verklagen können. Es konnte demnach durch die Einbindung des Datenschutzbeauftragten u. U. Schaden vom Unternehmen oder gar vom Geschäftsführer persönlich abgewendet werden. Dies zeigt die Bedeutung des Datenschutzes in vielen Bereichen des Unternehmens.

Schon gewusst?

Sofern man sich der Dienstleistung eines E-Mail-Providers bedient, der sich der Initiative „**E-Mail made in Germany**“ angeschlossen hat, ist dies selbst dann nicht ausreichend für die Umsetzung der „Weitergabekontrolle“ gemäß Anlage zu § 9 BDSG, wenn sichergestellt ist, dass die E-Mails ausschließlich an Empfänger gesendet werden, die sich dieser Initiative angeschlossen haben. Vielmehr ist es für vertrauliche Daten erforderlich, eine **End-to-End-Verschlüsselung** umzusetzen. Im Hinblick auf die Umsetzung im eigenen Unternehmen:

Fragen Sie Ihren Datenschutzbeauftragten

UIMC Dr. Vossbein GmbH & Co KG, Nützenberger Straße 119, 42115 Wuppertal
Tel.: (02 02) 2 65 74 - 0, Fax: - 19, E-Mail: consultants@uimc.de, Internet: www.UIMC.de

Noch Fragen?
Treten Sie mit uns in einen Dialog ein!

ÜIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Zugriff auf Arbeitsplatzrechner mittels Online-Meeting-Tool

Mit Hilfe eines Tools zur Fernwartung bzw. für Online-Meetings können Bildschirminhalte sowie Tastatureingaben und Mausbewegungen über das Netzwerk übertragen werden. Hierdurch kann die Zusammenarbeit zwischen Projektteams standortübergreifend oder die Wartung durch die IT-Administratoren erleichtert werden.

Bei der Konfiguration sollten folgende Punkte durch die IT berücksichtigt werden:

» Es sind Verschlüsselungsverfahren zu etablieren, wenn auf Rechner zugegriffen werden soll, auf denen besonders vertrauliche Daten verarbeitet werden (z. B. im Personalbereich).

» Alle beteiligten PCs sind über restriktiv konfigurierte Firewalls zu schützen.

» Die (unverschlüsselte) Übertragung der Daten über offene Netze/Internet ist zu verhindern. So sollten bspw. auch keine „öffentlichen" Instant-Messaging-Programme hierfür ohne zusätzliche Sicherheitsmaßnahmen genutzt werden (wie z. B. Skype, ICQ o. ä.).

» Wartungsvorgänge durch IT-Administratoren sollten nachvollziehbar protokolliert werden.

» Eine Fernwartung durch Dritte/Dienstleister ist nur auf Basis expliziter Datenschutzvereinbarungen mit dem Dienstleister zulässig (Rücksprache mit Datenschutzbeauftragten empfehlenswert).

Bei der Nutzung sollte durch die User auch Nachfolgendes beachtet werden:

» Der zugreifende User hat sich bei Verbindungsaufnahme zu authentifizieren.

» Verbindungswünsche sind durch den User, auf dessen Rechner zugegriffen werden soll, explizit zu bestätigen.

» Änderungen der Tool-Einstellungen dürfen nur von IT-Administratoren ermöglicht werden.

Mehr Tipps finden Sie in der nächsten Ausgabe vom UIMCommunic@tion-Info-Brief oder erfahren Sie bei Ihrem Ansprechpartner!

Datenschutz für IT-Fachkräfte

Datenschutz und IT sind nicht nur kaum voneinander trennbar. Auch müssen IT-Mitarbeiter zunehmend datenschutzrechtliche Aspekte beachten.

Innerhalb des Seminars werden IT-Fachkräfte die notwendigen Grundlagen im Datenschutz für Ihren IT-Alltag vermittelt. Neben der reinen Wissensvermittlung zielt das Seminar auf den Erfahrungsaustausch der Teilnehmer untereinander ab.

Melden Sie sich schon jetzt an!

Saarbrücken, 12.05.2015

Mehr unter Termine.UIMC.de

IT-Trends Sicherheit

Unter allen UIMCommunication-Abonnenten, die eine Mail an communication@uimc.de mit dem Betreff „Freikarte" senden, verlosen wir eine Freikarte im Wert von EUR 60,00.

Noch kein Abonnent? Dann noch schnell anmelden!

Die „IT-Trends Sicherheit" ist ein etablierter Fachkongress; wir infomieren Sie über Datenschutz und Informationssicherheit (Vortrag und Informationsstand). Wir freuen uns auf Ihren Besuch!

Bochum, 22.04.2015

Mehr unter Termine.UIMC.de

Bitte senden Sie mir neben den angekreuzten Themen weitere Informationen zu:

☐ Datenschutzbeauftragter kann Schadensersatzansprüche verhindern

☐ Verschlüsselung im E-Mail-Verkehr bei vertraulichen Daten

☐ **Unser Tipp:** Bitte senden Sie mir zukünftig den UIMCommunic@tion-Info-Brief und regelmäßig weitere interessante Informationen per E-Mail zu!

E-Mail: _____ Unterschrift: _____

per Fax an (0202) 265 74 - 19 oder formlos per Mail an communication@uimc.de

Mehr Informationen, Hinweise und Tipps finden Sie hier: www.UIMC.de/communication

Einer künftigen Zusendung können Sie jederzeit formlos per E-Mail an communication@uimc.de widersprechen.