Maßnahmen:

1. Bei Felgen haben sich Felgenschlösser bewährt. Sie sind nicht unüberwindlich, aber sie konnten nach Aussage von Fachleuten die Diebstähle durchaus verhindern.

2. Was die Auspuffanlagen angeht, kann man auch solche Schrauben verwenden, die ohne Spezialwerkzeug nicht ohne Weiteres entfernt werden können. Da aber die Täter Profis zu sein scheinen, werden sie sich vermutlich auch die entsprechenden Werkzeuge beschaffen können. Den Versuch mit den Schrauben ist es allemal wert!

Schrauben mit Sollbruchstellen

3. Es gibt auch Schrauben, bei denen der Kopf ab einem definierten Drehmoment an einer Sollbruchstelle abreißt. Auch diese Schraube lässt sich wieder lösen, aber nur mit einem nicht sehr weit verbreiteten Werkzeug. Die Schraube wurde entwickelt, um den Diebstahl von Solarpaneelen einzudämmen. Auf der Herstellerseite findet sich ein Foto der Schraube: www.secur-screw.de/index.php?id=1.

Auspuff mit Gravur

4. Hilfreich kann es auch sein, die Auspuffanlage an einer möglichst gut sichtbaren Stelle zu gravieren. Die Auspuffanlagen sind nämlich oft von der Seite her gut sichtbar. Irgendwann kommt das Auto auch mal in eine andere Werkstatt. Dort könnte das geklaute Ersatzteil auffallen.

5. Bei gleich 36 Auspuffanlagen fragt man sich aber auch schon, warum so viele hochwertige Fahrzeuge auf einem Depotplatz der Händler nicht professioneller, z. B. durch eine Kameraanlage, überwacht werden.

Revierwachdienste

6. Auch Revierwachdienste können Diebstähle verhindern. Vor allem, wenn sie unregelmäßig auf Patrouille gehen und gelegentlich in kurzen Abständen anrollen.

7. Über Bewegungsmelder angesteuertes Licht, in Zaunnähe und auf dem Gelände strategisch platziert, könnte – je nach Lage der Standplätze und der Umfeldsituation – ebenfalls hilfreich sein.

8. Immer häufiger kommt es vor, dass die Videotechnik solcher Außenbereiche gleich auf eine Wachzentrale aufgeschaltet wird. So kann man unter Umständen noch schneller und viel gezielter reagieren. Da der zerstörungsfreie Abbau der Ersatzteile einige Zeit in Anspruch nimmt, bestehen große Chancen die Täter noch auf frischer Tat zu ertappen. (vzm)

Stichworte: Auspuff – Diebstahl – Rußfilter

Datenschutz/Recht

Zutritts- und Besuchermanagement aus datenschutz- und arbeitsrechtlicher Sicht

Gastautor Rechtsanwalt Dr. Ulrich Dieckert

Dr. Ulrich Dieckert ist Partner einer überörtlichen Anwaltskanzlei (www.wrd.de), die u. a. für die Gebäudewirtschaft beratend tätig ist. Im Bereich Sicherheitstechnik hat sich Dr. Dieckert auf die Themen Videoüberwachung, Zutrittskontrolle und Brandschutz spezialisiert. Er berät Betreiber und Errichter bei der Einführung sicherheitstechnischer Anlagen und vertritt Unternehmen gegenüber Datenschützern und Betriebsräten, auch bei der Aushandlung von Betriebsvereinbarungen. Dr. Dieckert ist Verfasser zahlreicher Fachbeiträge und tritt als Referent bei Veranstaltungen der Sicherheitsbranche auf.

Beim Einsatz von Zutrittsberechtigungs-Systemen (i.d.R. Zutrittskontrollsysteme ZKS genannt) werden regelmäßig personenbezogene Daten erhoben, verarbeitet und genutzt. Dies kann mit den Persönlichkeitsrechten der betroffenen Besucher bzw. Mitarbeiter kollidieren. Denn nach dem Grundrecht auf informationelle Selbstbestimmung (vom Bundesverfassungsgericht abgeleitet aus Artikel 1 und Artikel 2 des Grundgesetzes) soll der Einzelne grundsätzlich selbst entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. Zu den schützenwerten Daten zählt grundsätzlich auch die Kenntnis, wann sich eine Person an einem bestimmten Ort aufgehalten hat. In diese Grundrechte darf nur durch oder aufgrund eines Gesetzes eingegriffen werden. Die Erhebung und Verarbeitung personenbezogener Daten ist in Deutschland u. a. im Bundesdatenschutzgesetz (BDSG) bzw. den Datenschutzgesetzen der Länder geregelt. Hat man es mit der Erfassung von Mitarbeiterdaten zu tun, sind darüber hinaus Mitbestimmungsrechte zu beachten.

Grundrecht auf informationelle Selbstbestimmung

1. Datenschutzrechtliche Zulässigkeitsvoraussetzungen

Bei der Planung bzw. Einrichtung von ZKS ist daher stets die Übereinstimmung mit datenschutzrechtlichen Regelungen zu prüfen, wenn diese Systeme zur Erhebung und Verarbeitung von Personendaten geeignet sind.

Dies ist beim Einsatz von Chipkarten bei Besucher- bzw. Mitarbeiterausweisen regelmäßig der Fall, insbesondere wenn dies durch biometrische Verfahren bzw. durch eine Videokontrolle ergänzt wird. Zwar gibt es mittlerweile Systeme, bei denen lediglich eine lokale Verifikation stattfindet, z. B. wenn biometrische Daten des Kartenträgers am Kontrollpunkt mit dem Template seiner Karte abgeglichen werden, ohne dass der Vorgang zentral verwaltet wird. Häufig allerdings werden die erhobenen Bewegungs- bzw. Bilddaten gespeichert, um diese zum Zwecke der Zeiterfassung oder Beweissicherung auswerten zu können.

Problem Personendaten bei ZKS

a) Durch Einwilligung

Eine solche Datenerhebung und Verarbeitung durch Unternehmen ist nur zulässig, wenn dies durch das BDSG oder durch eine andere Rechtsvorschrift erlaubt ist oder der Betroffene eingewilligt hat (vgl. § 4 Abs. 1 BDSG). Eine Einwilligung ist aber nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht, der zuvor auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hingewiesen wurde (vgl. § 4 a BDSG). Bei der Zustimmung durch Mitarbeiter wird die „Freiwilligkeit" von der Rechtsprechung regelmäßig in Frage gestellt, weil eine Weigerung das Arbeitsverhältnis belasten könnte. Kommt es allerdings zum Abschluss einer Betriebsvereinbarung (s. u.), dann wird diese als „andere Rechtsvorschrift" i. S. v § 4 Abs. 1 BDSG angesehen, die den Einsatz erlaubt.

Vorsicht bei „Freiwilligkeit"

b) Bei Wahrung berechtigter Interessen?

Darüber hinaus kann der Betrieb von ZKS auch nach den Generalklauseln in § 28 BDSG (Datenerhebung für Geschäftszwecke) und § 32 BDSG (Datenerhebung für Zwecke des Beschäftigungsverhältnisses) zulässig sein, wenn die Datenerhebung zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegen. Diese Voraussetzungen müssen auch bei der Erfassung von Bilddaten durch Videoüberwachungssysteme erfüllt sein, die gemäß der

Spezialvorschrift in § 6 b BDSG in öffentlich zugänglichen Räumen grundsätzlich möglich ist. So liegt es im berechtigten Interesse des Betreibers, sein Objekt vor unbefugtem Eindringen zu schützen (Hausrecht), den ungestörten Ablauf des Betriebes bzw. von Veranstaltungen sicherzustellen und Gefahren für die betrieblichen Einrichtungen und die Mitarbeiter abzuwehren. Erforderlich ist ein Zugangsregelungssystem mit Datenerfassung immer dann, wenn kein milderes, gleich gut funktionierendes Mittel möglich ist (z. B. mechanische Lösungen, Wachleute etc.). Schließlich muss die Erhebung und Verarbeitung von Personendaten verhältnismäßig sein, es darf also kein unzumutbarer Eingriff in die Privat- oder Intimsphäre vorliegen (z. B. Videoüberwachung in Waschräumen). In seiner Sozialsphäre muss sich der Betroffene hingegen Eingriffe gefallen lassen, wenn sie ihm auch nützen (z. B. Besuchermanagement).

Imtimsphäre beachten

c) Nach dem Gesetz zur Regelung des Beschäftigungsdatenschutzes (Entwurf)

Was die Erhebung von Beschäftigtendaten im Rahmen der Zutrittskontrolle angeht, so soll diese nach den Neuregelungen im Gesetz zur Regelung des Beschäftigtendatenschutzes grundsätzlich erlaubt sein. Danach darf der Arbeitgeber z. B. biometrische Merkmale eines Beschäftigten erheben, verarbeiten und nutzen, soweit dies aus betrieblichen Gründen zur Autorisierungs- und Authentifikationszwecken erforderlich ist (vgl. § 32 h BDSG, Entwurf). Werden Videodaten erfasst, so ist der Zweck der „Zutrittskontrolle" künftig ausdrücklich im neuen § 32 f BDSG (Entwurf) als erlaubt erwähnt. Die Erhebung von Bewegungsdaten ist schließlich auch dann künftig möglich, soweit die Kenntnis der Daten für den Arbeitgeber erforderlich ist, um die gegenüber dem Beschäftigten bestehenden Rechte des Arbeitgebers einschließlich der Leistungs- und Verhaltenskontrolle wahrzunehmen (vgl. § 32 c Entwurf BDSG). Damit verbundene Eingriffe in die Persönlichkeitsrechte der Beschäftigten sind allerdings nur dann zulässig, wenn die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit gewahrt sind. Außerdem bleiben die Beteiligungsrechte der Interessenvertretungen der Beschäftigten auch durch die Neuregelungen weiterhin unberührt (§ 32 e Abs. 3 BDSG, Entwurf). Schließlich ist derzeit ungewiss, ob und wann dieser seit 2010 vorliegende Gesetzentwurf in Kraft treten wird.

Neuregelung im Auge behalten

d) Weitere Pflichten im Umgang mit den erhobenen Daten

Selbst wenn die Datenerhebung im Rahmen eines ZKS als solche zulässig ist, hat der Betreiber eine Reihe von weiteren Pflichten aus dem Bundesdatenschutzgesetz zu beachten. So sind die Betroffenen über die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verantwortlichen Stelle zu unterrichten, wenn sie hiervon nicht auf andere Weise Kenntnis haben (§ 33 BDSG). Auf Verlangen hat der Betreiber dem Betroffenen über die zu seiner Person gespeicherten Daten und den Zweck der Speicherung Auskunft zu erteilen (§ 34). Darüber hinaus sind personenbezogene Daten zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist (§ 35). Beim Einsatz von optisch-elektronischen Einrichtungen (Videoüberwachung) sind der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Hinweisschilder erkennbar zu machen (§ 6 b Abs. 2 BDSG). Beim Einsatz mobiler personenbezogener Speicher- und Verarbeitungsmedien sind die Betroffenen darüber hinaus über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten zu informieren (vgl. § 6 c BDSG). Schließ-

Missbrauch ausschließen

lich muss die datenerhebende Stelle technische und organisatorische Maßnahmen treffen, um die erhobenen Daten vor Missbrauch, Verlust und Beschädigung zu schützen (§ 9 BDSG).

e) Vorabkontrolle durch den Datenschutzbeauftragten

Sind die durch das ZKS erhobenen Daten dazu bestimmt (oder geeignet), die Persönlichkeit des Betroffenen zu bewerten, einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens, so ist vor der Einführung des Systems stets eine sogenannte „Vorabkontrolle" durch den zuständigen Datenschutzbeauftragten durchzuführen. Verfügt das Unternehmen nicht über einen eigenen (oder extern bestellten) Datenschutzbeauftragten, so ist der zuständige Landesdatenschutzbeauftragte zu beteiligen (vgl. §§ 4 d, 4 f BDSG). Unternehmen sollten jedenfalls nicht das Risiko eingehen, Zutrittskontrollanlagen mit Datenerhebungsfunktion ohne den „Segen" des zuständigen Datenschutzbeauftragten einzuführen, da ansonsten Beseitigungsanordnungen und Bußgelder ins Haus stehen können.

2. Arbeitsrechtliche Zulässigkeitsvoraussetzungen

Im Übrigen ist ein datenschutzrechtlich abgesegnetes Konzept auch aus arbeitsrechtlichen Gründen von Vorteil. Denn bei Einführung und der Anwendung technischer Einrichtungen, die dazu bestimmt (oder geeignet) sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen, sind die Interessenvertretungen der Beschäftigten gemäß § 87 Abs. 1 Nr. 6 BetrVerfG (bzw. § 75 Abs. 3 Nr. 17 BPersVetrG) zwingend zu beteiligen. Dabei haben die Interessenvertretungen darauf zu achten, dass in die Persönlichkeitsrechte der Beschäftigten nicht in unverhältnismäßiger Weise eingegriffen wird.

a) Abschluss von Betriebsvereinbarungen

Dies wird durch den Abschluss von Betriebsvereinbarungen sichergestellt, in denen Art und Weise sowie Zweck der Zugangsregelungssysteme näher festgelegt und Bestimmungen über Zugangs- und Zugriffsberechtigungen, Auswertung der Daten, Speicherung und Löschung sowie Nutzung und Weitergabe der Daten getroffen werden. Derartige Betriebsvereinbarungen stellen wie oben bereits erwähnt eine „andere Rechtsvorschrift" i. S. v. § 4 Abs. 1

BDSG dar, mit der die Erhebung der Zutritts- und Bewegungsdaten datenschutzrechtlich legitimiert wird. Der einzelne Arbeitnehmer ist an eine solche Vereinbarung allerdings nicht gebunden, sodass er die gesetzliche Zulässigkeit der Maßnahme gerichtlich überprüfen lassen kann, wenn er sich subjektiv in seinen Rechten verletzt sieht.

b) Arbeitsgerichtliche Klärung

erst Einigungsstelle, dann Arbeitsgericht

Kommt eine Einigung nicht zustande, so können die Parteien die Einigungsstelle anrufen (§ 87 Abs. 2 i. V. m. § 76 BetrVerfG), welche auf Antrag des Arbeitgebers die Zustimmung des Betriebs-/Personalrats durch einen eigenen Spruch ersetzen kann. Sind die Parteien mit dem Spruch der Einigungsstelle nicht einverstanden, so können sie diesen arbeitsgerichtlich überprüfen lassen. Auf diese Weise sind bereits einige Grundsatzentscheidungen des Bundesarbeitsgerichts zum Beschäftigtendatenschutz zustande gekommen.

3. Zusammenfassung

datenschutzrechtliche Vorabkontrolle sinnvoll

Soweit also bei der Einführung von Zugangsregelungssystemen personenbezogene Daten erhoben und verarbeitet werden, sollte stets eine datenschutzrechtliche Vorabkontrolle auf Grundlage eines entsprechenden Konzeptes durchgeführt werden. Auf dieser Grundlage sollte man dann in Verhandlungen mit den Interessenvertretern der Beschäftigten über den Abschluss einer Betriebsvereinbarung eintreten. Unternehmen sollten sich sinnvolle sicherheitstechnische Lösungen dabei von „Bedenkenträgern" nicht kleinreden lassen. Die einschlägigen Gesetze erlauben bei kreativer Auslegung mehr, als Datenschützer und Betriebsräte glauben. Hier kommt es auf sichere Rechtskenntnisse, gute Argumente und selbstbewusste Verhandlungsführung an.

Stichworte: Arbeitsrecht – Besuchermanagement – Zutrittsmanagement

IT-Sicherheit

Angriffe auf IT-Systeme nehmen deutlich zu

Laut Studien von HP (HP Cyber Security Risk Report 2011) und IBM (IBM X-Force 2011 Mid-year Trend & Risk Reports) hat sich die Anzahl der Angriffe auf IT-Systeme im zweiten Halbjahr 2011 stark erhöht. Demnach zielten ca. 36 Prozent aller Angriffe auf gewerbliche Internet-Anwendungen.

Angriffe immer raffinierter

Grundsätzlich wurde ein Wandel in der aktuellen Bedrohungslage festgestellt. Die organisierten IT-Angriffe durch politisch motivierte Hacker (z.B. Anonymous, LulzSec) treten in den Vordergrund. Die Angriffsmethoden werden schnell und stark verändert, damit die Attacken eine höhere Erfolgsquote versprechen. Deshalb mussten die angegriffenen Unternehmen auf die schnell wechselnden Bedrohungen zeitnah reagieren, um einen wirtschaftlichen Schaden oder einen Image-Schaden möglichst noch abwenden zu können.

Trotz der gestiegenen Zunahme von Angriffen auf IT-Systeme wurde ein Rückgang der gemeldeten Sicherheitsverletzungen in den Unternehmen festgestellt. Dies führen die Forscher darauf zurück, dass erfolgreiche Angriffe von vielen Firmen nicht gemeldet wurden und somit nicht erfasst werden konnten. Der Grund dafür liegt auf der Hand: Viel Aufwand für keinen Erfolg, das kann ein Unternehmen nicht motivieren. I.d.R. gibt es eine Anzeige gegen Unbekannt. LKA und BKA sind die Einzigen, die von dieser Anzeige profitieren, weil sie dann in die Statistik eingeht. Die aufnehmende Polizeidienststelle