Zutrittskontrolle durch Schlüsselverwaltung

Das erste Gebot: Die Zutrittskontrolle

Zutrittskontrolle muss aus Sicht des Datenschutzes sicherstellen, dass nur Berechtigte die Möglichkeit haben, Betriebsmittel, mit denen personenbezogene Daten verarbeitet werden, zu nutzen. Die Zutrittskontrolle beginnt daher bereits damit, wer wann das Betriebsgelände, einzelne Gebäudeteile oder einen sensiblen Raum eines Unternehmens betreten darf. Wer hat bei Ihnen den Überblick?

Um den besonderen Anforderungen des Datenschutzes gerecht zu werden, führen § 9 BDSG und Anlagen die sogenannten acht Gebote auf. Das erste Gebot lautet:

1. Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle).

Zutrittskontrolle ist räumlich zu sehen

Die Zutrittskontrolle zielt somit auf den räumlichen Zutritt zu DV-Anlagen. Es muss verhindert werden, dass unbefugte Person in die Nähe einer Datenverarbeitung gelangen.

„DV-Anlagen" ist ein weiter Begriff

Zu den DV-Anlagen gehören neben den zentralen Rechnern auch die integrierten Laufwerke und die angeschlossenen Peripheriegeräte wie Terminals, Workstations und Drucker. Online betriebene Geräte wie einzelne PCs, Laptops und Blackberrys sind ebenfalls DV-Anlagen.

Wer gilt als befugt?

Als befugt sind sicherlich der Operator im Rechenzentrumsbetrieb, der IT-Mitarbeiter sowie der Datenerfasser oder Sachbearbeiter am PC anzusehen. Auch der DSB gehört im Rahmen seiner Kontrollpflichten dazu.

Zumindest teilweise sind auch Wartungstechniker und Mitarbeiter externer Firmen zur Programmierung sowie zur IT-Unterstützung befugt.

Was ist als „Schlüssel" zu definieren?

Als Schlüssel ist in der heutigen Zeit nicht mehr lediglich der althergebrachte Bartschlüssel oder der bessere Sicherheitsschlüssel zu definieren. Vergessen Sie keinesfalls die Keycards, Responderchips, RFID-Chips oder Zahlenschlösser, die zunehmend das mechanische Zylinderschloss ablösen.

Schlüsselchaos? Hoffentlich nicht.

Die Kombi Zeiterfassung und Zutritt

Nicht selten öffnen die Identifikationsmedien zur An- und Abwesenheitsverwaltung für die Stundenabrechnung auch gleichzeitig Tür und Tor.

Dass über das Medium „Zeiterfassung" oft ein ungehinderter und teils unkontrollierter Zugang zum Betriebsgelände oder zu Gebäudeteilen möglich ist, wird in vielen Fällen nicht erkannt.

Hightech-Systeme nicht vergessen

In sicherheitsbewussten Unternehmen dürfen keinesfalls die Fingerprintsysteme oder Iriserkennung vergessen werden. Kurzum: Alles, was Türen öffnet, fällt unter die Zutrittskontrolle.

Externe Dienstleister einbeziehen

Zudem haben oft auch externe Dienstleister Zugang zu Ihrem Unternehmen. Das dürfen Sie keineswegs außer Acht lassen. Prüfen Sie z.B., inwiefern

- Reinigungsunternehmen,
- Wachpersonal,
- externe Hausmeister,
- ggf. Feuerwehr
- oder bei gemieteten Bürobereichen das Facility Management Ihres Vermieters

ungehinderten Zutritt haben, oft noch dazu außerhalb der üblichen Arbeits- oder Bürozeiten.

Wie im Taubenschlag?

Wie Sie sehen, existieren nicht gerade wenig Möglichkeiten, um kontrolliert oder auch unkontrolliert Zugang zu schützenswerten Bereichen zu nehmen. Geht es zu wie im Taubenschlag bzw. gibt es jemanden, der wirklich den vollständigen Überblick hat?

Der DSB ist kein Pförtner!

Gleich vorweg: Es ist nicht die Aufgabe eines Datenschutzbeauftragten, sich als Pförtner zu engagieren sowie Passierscheine zum berechtigten Zugang auszustellen. Andererseits ist es aber Ihre Aufgabe, sicherzustellen, dass nur berechtigte Personen Zutritt zu Datenverarbeitungsanlagen erhalten.

Zentrale Stelle? Fehlanzeige!

Eine zentrale Stelle für die Ausgabe der verschiedenen Zutrittsmedien ist oft nicht vorhanden. Der Hausmeister verteilt die physischen Schlüssel, die Personalabteilung vergibt die Transponder-Chips für das Drehkreuz, und die IT-Abteilung verwaltet eigenständig den Zahlencode für den Zutritt zum allerheiligsten Rechenzentrum.

Ihre Aufgabe als DSB

Damit Sie Ihrer Aufgabe gerecht werden, sollten Sie zumindest eine Bestandsaufnahme über alle Schließsysteme machen. Des Weiteren gehört dazu, die Ausgabe der Zutrittsmedien protokollieren zu lassen und den Schlüsselnehmer über seine Pflichten zu informieren.

Ideal: die elektronische Unterstützung

In größeren Unternehmen kann bereits eine elektronische Verwaltung der physischen Schlüssel implementiert sein. Das ist die ideale Voraussetzung für eine eine wirksame Kontrolle – insbesondere bei mechanischen Schließanlagen. Fragen wie „Wer besitzt Schlüssel-Nr. xx?“ oder „Welche Türen schließt Schlüssel-Nr. xx?“ sind in Sekundenschnelle beantwortet.

Die Ausgabe dokumentieren

Grundsätzlich sollte die Ausgabe jedes Zutrittsmediums möglichst schriftlich dokumentiert werden.

Merkblatt für Schlüsselnehmer

Der Schlüsselnehmer sollte zudem über ein Merkblatt bzw. Übergabeprotokoll zu bestimmten Verhaltensregeln verpflichtet werden, wie den Schlüssel oder Zutrittsmedium keinesfalls Dritten zu überlassen oder den Verlust sofort dem Schlüsselgeber zu melden.

Regelung bei Verlustmeldung

Die Stelle, die die Schüssel ausgibt, muss eine interne Regelung ausarbeiten, was bei einem Schlüsselverlust zu tun ist. Wichtige Punkte neben einem definierten Ansprechpartner sind u.a.:

1. Lässt sich die Zugangskontrolle vorübergehend mit anderen Mitteln sicherstellen (z.B. Türkette, elektronische Deaktivierung des Mediums)?
2. Sind weitere Zugänge betroffen (Schließanlage, Generalschlüssel)?
3. Muss das Schloss/die Schließanlage ausgetauscht und müssen neue Schlüssel ausgegeben werden?
4. Ist die Geschäftsleitung zu informieren?

Diese Liste ist keine abschließende Variante. Die Anforderungen variieren je nach Sensibilität und Schutzinteresse des abhandengekommenen Zutrittsmediums. Grundsätzlich sind mechanische Systeme jedoch schwerer zu verwalten als elektronische Schließsysteme.

Mitarbeiterbestätigung zur Firmenschlüsselübergabe

Der Schlüsselnehmer verpflichtet sich, die ihm anvertrauten Schlüssel sorgsam zu verwahren und in keinem Fall Dritten zu überlassen.

Des Weiteren ist dem Schlüsselnehmer bekannt, dass der/die überlassene/n Schlüssel bei Beendigung des Beschäftigungsverhältnisses unaufgefordert zurückgeben werden muss/müssen.

Bei Verlust der Schlüssel ist umgehend die Assistenz der Geschäftsleitung zu informieren. Bei Neuausgabe oder Nichtabgabe im Falle des Austritts behält sich das Unternehmen vor, eine Gebühr je Schlüssel in Rechnung zu stellen.

Schlüssel-Nr.: _____

Schlüsselausgabedatum: _____

Übergeben durch: _____

Übernommen durch: _____

Schlüsselrückgabedatum: _____

Übergeben durch: _____

Entgegengenommen durch: _____

Protokoll zur Schlüsselübergabe. Das Muster finden Sie als Word-Dokument unter http://www.datenschutz-praxis.de/fachwissen/vorlagen/muster

Auch die Rücknahme dokumentieren

Neben der Ausgabe von Zugangsberechtigungen ist auch eine dokumentierte Rücknahme z.B. beim Ausscheiden eines Schlüsselträgers eine der Kernaufgaben zur wirksamen Zutrittskontrolle.

Idealerweise wird die Entgegennahme auf dem gleichen Protokoll vermerkt (siehe Muster) und der bisherige Inhaber dadurch schriftlich entlastet.

Weitere Maßnahmen

Dieser Betrag konnte nur einen Teilaspekt der Zutrittskontrolle beleuchten. Als weitere Schritte wären Maßnahmen zu definieren, um das gewaltsame Eindringen in Gebäude/Räume mit IT-Anlagen zu verhindern.

Über das Thema Einbruchsicherheit sollten Sie sich allerdings erst nach erfolgreicher Umsetzung der Schlüsselkontrolle Gedanken machen.

Hermann Keck

Hermann Keck ist externer Datenschutzbeauftragter *(http://www.keck-dsb.de)*.