**CHECKLISTE: Typische Schwachstellen bei der Zutrittskontrolle**

**Aspekt**

**Darauf sollten Sie achten**

**Geprüft?**

Fehlendes Gesamtkonzept

* Die Zutrittskontrolle ist ein Baustein in einem Gesamtkonzept zur Absicherung des Unternehmens. Lassen Sie sich dieses Gesamtkonzept vorlegen und schauen Sie, inwieweit dieses Hand und Fuß hat. Die Maßnahmen sollten zueinander passen und am besten miteinander verzahnt sein.
* Klären Sie, inwieweit Zuständigkeiten und Verantwortlichkeiten klar definiert sind.
* Achten Sie auch auf Regelungen. Ohne Regelungen und Vorgaben wird vieles mal so und mal so ge- handhabt.

q Ja q Nein

Lückenhafte oder fehlende Datenschutz- dokumentation

* Klären Sie, inwieweit alle datenschutzrelevanten Aspekte geprüft und dokumentiert sind. Gibt es Lücken, sollten diese geschlossen werden.
* Werfen Sie einen Blick ins Verzeichnis von Verarbeitungstätigkeiten. Die Angaben müssen vollständig und aktuell sein.

q Ja q Nein

Defizite bei der Berechtigungs- vergabe

* Hinterfragen Sie das Thema Berechtigungen und Berechtigungskonzept insgesamt. Lassen Sie sich erklären, wie dieses aufgebaut ist.
* Schauen Sie sich die Prozesse zur Vergabe von Berechtigungen an. Hier sollte es klare Standards und keine Vergabe „auf Zuruf“ geben.
* Prüfen Sie, wie Berechtigungen bei Besuchern gemanagt werden.

q Ja q Nein

Zu weitreichen- de Berechtigun- gen

* Meist ist es sinnvoll, Rollen zu definieren, die über bestimmte Zutrittsberechtigungen verfügen, etwa funktions- oder aufgabenbezogen. Diesen Rollen werden die einzelnen Mitarbeiter zugeordnet.
* Achten Sie darauf, inwieweit bei Berechtigungen das Minimalprinzip umgesetzt ist. Grundsätzlich gilt: Zutritt nur, wenn für die Aufgabe oder Funktion erforderlich.

q Ja q Nein

Fehlender zeit- naher Berechti- gungsentzug

* Idealerweise gibt es hier einen Automatismus, der etwa von der Fachabteilung oder der Personalabtei- lung gestartet wird.
* Auf jeden Fall müssen Berechtigungen unverzüglich entzogen werden, wenn ein Mitarbeiter das Unter- nehmen verlässt. Auch bei einem Aufgabenwechsel ist eine schnelle Anpassung nötig.

q Ja q Nein

Datenschutz- rechtlich unzulässige biometrische Verfahren

* Meist wird eine biometrische Zutrittskontrolle (z. B. mittels Fingerabdrucks) im datenschutzrechtli- chen Sinn nicht erforderlich sein. Es gibt mildere Mittel mit weniger sensiblen Daten, etwa Chipkarte oder Dongle.
* Oft bleibt nur die Einwilligung als Rechtsgrundlage. Die ist gerade im Beschäftigungsverhältnis prob- lematisch. Die Anforderungen sind hoch (§ 26 Abs. 2 Bundesdatenschutzgesetz).

q Ja q Nein

Mangelhafte Datensicherheit

* Einerseits handelt es sich um eine sicherheitsrelevante Einrichtung selbst, andererseits werden damit personenbezogene Daten verarbeitet. Es muss also Art. 32 Datenschutz-Grundverordnung (DSGVO) um- gesetzt sein, sprich, es muss risikoangemessene Schutzmaßnahmen geben.
* Hinterfragen Sie, inwieweit die Schutzmaßnahmen tatsächlich passen. Gerne wird hier auf ein „Hoch- glanzprospekt“ des Anbieters verwiesen. Das orientiert sich aber nicht an den konkreten Risiken Ihres Unternehmens.

q Ja q Nein

Fehlende Datenschutz- vereinbarungen

* Eventuell wird ein System genutzt, das über ein Portal des Anbieters gesteuert oder verwaltet wird. Hier liegt oft ein Fall der Auftragsverarbeitung (Art. 28 DSGVO) vor.
* Prüfen Sie, inwieweit es eine entsprechende Vereinbarung gibt und ob Schutzmaßnahmen festgelegt bzw. umgesetzt sind.

q Ja q Nein

Zweckwidrige Verwendung von Daten

* Daten, die für einen bestimmten Zweck verarbeitet werden, dürfen nicht einfach für einen anderen Zweck verwendet werden. Hier muss Art. 6 Abs. 4 DSGVO beachtet werden.
* Betriebsvereinbarungen können Verwendungsverbote enthalten. Dann kann eine Verarbeitung für einen anderen Zweck ausscheiden.

q Ja q Nein