Kontrolle von Fenstern bei Ortsbegehungen

Zusammenfassung: Fenster müssen besonders gesichert sein. Die Wirksamkeit der entsprechenden Maßnahmen muss regelmäßig auditiert werden.

Zu den Aufgaben von Datenschutzbeauftragten gehört auch Ortsbegehungen vorzunehmen. Dabei ist im Rahmen der Zutrittskontrolle auch zu prüfen, ob die Fenster so geschützt sind, dass ein unbefugtes Eindringen mit anschließendem Diebstahl von IT-Geräten und Daten so weit erschwert wird, dass ein Einbruch über die Fenster unwahrscheinlich wird.

.

Der Praxisfall: Bei einem Einbruch in ein Unternehmen wurden Server, Computer und Beamer gestohlen. Auf den Geräten waren personenbezogene Daten in erheblichem Umfang gespeichert. Die Täter waren über ein mangelhaft gesichertes Fenster im Serverraum eingestiegen. Eine Alarmanlage war nicht vorhanden.

Warum Ortsbegehungen? Hauptzweck des Datenschutzes ist, Menschen (so gennannte Betroffene) vor der Verletzung ihrer Datenschutzrechte zu schützen. Zu diesen Betroffenen gehören Beschäftigte, Kunden, Lieferanten, gegebenenfalls Patienten – kurz alle Menschen, mit denen das Unternehmen Kontakt hat. Bei einem Einbruch können Daten dieser Menschen in erheblichem Umfang in die Hände Unbefugter gelangen.

Datenschutzbeauftragte haben die Aufgabe, diese Datenverluste verhindern zu helfen. Im Bundesdatenschutzgesetz ist bei den technischen und organisatorischen Maßnahmen auch die Zutrittskontrolle gefordert. Der unbefugte Zutritt zu IT-Systemen ist zu unterbinden. Bei einem Einbruch geschieht aber genau das – und so müssen Maßnahmen zur Verhinderung eines solchen Einbruchs getroffen werden.

Dazu sind Ortsbegehungen unabdingbar. Datenschutzbeauftragte sollten vor allem in Serverräumen prüfen, ob eventuell vorhandene Fenster so gesichert sind, dass ein Eindringen zumindest erschwert wird. Hundertprozentige Sicherheit wird es auch bei Fenstern nicht geben, sie können jedoch so gesichert werden, dass ein möglicher Einbrecher das Risiko als zu hoch einstuft und den Einbruch mit großer Wahrscheinlichkeit unterlassen wird.

Schutz von Fenstern in Büros

Die Vorgaben der Zutrittskontrolle verlangen, dass der Zutritt von Unbefugten in Räume mit IT-Systemen zu verhindern ist. Dazu müssen auch die Fenster in Büros auf Sicherheit und Mängel überprüft werden. Viele unterschiedliche Gefährdungen bei unterschiedlicher Lage der Büros sind hierbei zu unterscheiden.

Fenster in Erdgeschoss-Räumen, die von öffentlichen Bereichen aus zugänglich sind

Hierzu gehören Büros, die im Erdgeschoss liegen. Vor den Fenstern befinden sich öffentliche Bereiche wie Straßen, Fußgängerzonen oder Einfahrten. Hier sind folgende Gefährdungen real vorhanden:

- Vorübergehende können Einsicht auf Bildschirme nehmen
- Geöffnete Fenster könnten zum Einsteigen genutzt werden
- Gekippte Fenster könnten zum Einsteigen genutzt werden

Zutrittskontrolle

Fenster im Erdgeschoss

Fenster im Erdgeschoss, die zum öffentlichen Raum führen

Aus Datenschutzsicht eine Herausforderung in mehrfacher Hinsicht sind Erdgeschoss-Fenster in Büros, die zur Straße oder sonst in den öffentlichen Raum führen. Eine Gefährdung kann hier sein, dass Bildschirminhalte eventuell von der Straße bzw. vom öffentlichen Raum aus einsehbar sein können, vor allem in der dunklen Jahreszeit.

Besonders kritisch kann dies sein, wenn an diesen Arbeitsplätzen besondere Arten von Daten nach § 3 Abs. 9 BDSG oder Daten, bei denen automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, verarbeitet werden. Letztere können beispielsweise Bank- und Kontendaten, Kreditkartendaten, Beurteilungsdaten usw. sein.

Beispiel: Ein Reisebüro verfügt über Büros, deren Fenster zum öffentlichen Raum hin zeigen. Einzelne Arbeitsplätze sind so angeordnet, dass die Beschäftigten schräg oder mit dem Rücken zum Fenster sitzen, so dass bei entsprechenden Lichtverhältnissen die Bildschirminhalte von der Straße aus eingesehen werden können. Werden an diesen Arbeitsplätzen Buchungen unter Anwendung von Kreditkartendaten vorgenommen, so ist diese Tatsache als besonders kritisch einzustufen. Hier müssen geeignete Maßnahmen zum Schutz dieser Da-

ten vor unbefugter Einsichtnahme ergriffen werden.

Risiko: Daten, bei deren unbefugter Einsichtnahme besondere Risiken für die Freiheits- und Persönlichkeitsrechte der Betroffenen vorliegen, können von Unbefugten eingesehen oder mit optisch-elektronischen Maßnahmen unbefugt aufgezeichnet werden. Dies ist vor allem in der dunklen Jahreszeit als sehr kritisch anzusehen.

Mögliche Maßnahmen:

Umstellen der Arbeitsplätze: Wenn möglich, sollten die Arbeitsplätze so umgestellt werden, dass eine Einsichtnahme in die Bildschirminhalte ausgeschlossen werden kann. Dies ist auch aus Sicht des Arbeitsschutzes wünschenswert, denn Arbeitsplätze, bei denen von hinten ein starker Lichteinfall vorliegt, können durch Bildschirmreflexionen zu Unwohlsein oder Kopfschmerzen führen. Sind die Bildschirme schräg zum Fenster angeordnet, hilft unter Umständen schon eine Sichtschutzfolie, die dafür sorgt, dass die Daten nur noch ein einem bestimmten Betrachtungswinkel am Bildschirm beobachtet werden können.

Sichtschutzfolie: Können die Arbeitsplätze nicht anders angeordnet werden, ist für einen verlässlichen Sichtschutz zu sorgen. Eine Möglichkeit ist das Anbringen einer Sichtschutzfolie auf den Fenstern, so dass der Lichteinfall zwar getrübt wird, aber dennoch bei Tageslicht auf eine künstliche Beleuchtung verzichtet werden kann. Von außen können dann höchstens noch Schemen erkannt werden, Einzelheiten auf Bildschirmen jedoch in keinem Fall. Die Sichtschutzfolie kann unter Umständen auch so gestaltet werden, dass sie von innen weitgehen transparent, von außen jedoch als gestaltende Folie, beispielsweise mit werblichem Charakter, ausgeführt sein kann.

Jalousie: Wenn eine Folie aus welchen Gründen auch immer nicht aufgebracht werden kann, ist zu prüfen, ob eine Innenjalousie so angebracht werden kann, dass eine Einsichtnahme der Bildschirme von außen ausgeschlossen werden kann.

Sichtschutz durch Pflanzen, Paravents oder ähnliche Accessoires: Eine weitere Möglichkeit des Sichtschutzes können Pflanzen, Raumteiler wie Paravents oder ähnliche Einrichtungsgegenstände sein, die bei richtiger Anordnung ebenfalls den Sichtschutz gewährleisten können.

Regelmäßige Prüfungen vor Ort: Datenschutzbeauftragte sollten in den hier geschilderten Fällen bei der ersten Ortsbegehung ein Protokoll anfertigen, aus dem die Gefährdungen des Datenschutzes eindeutig hervorgehen. In der Folge sollte geklärt werden, wer die erforderlichen Gegenmaßnahmen ausarbeitet und umsetzt. Hier können Datenschutzbeauftragte gute Unterstützung leisten. Die Maßnahmen sollten vor der Umsetzung mit den Beschäftigten besprochen werden, das erhöht die Akzeptanz der jeweiligen Maßnahmen. In der Folge sollten Datenschutzbeauftragte regelmäßig und unregelmäßig erneute Prüfungen vornehmen, um sicherzustellen, dass die erforderlichen Maßnahmen so umgesetzt werden, dass die Gefährdungen des Datenschutzes nicht mehr bestehen.

Fenster im Erdgeschoss, die auf Firmengelände oder in Innenhöfe führen

Fall 1: Gelände ist geschützt

Fall 2: Gelände ist grundsätzlich geschützt, aber Unbefugte, die berechtigt sind, könnten Zutritt haben

Kellerfenster

Eberhard Häcker, Ensdorf

Der Autor Eberhard Häcker ist Geschäftsführer der TDSSG GmbH – Team Datenschutz Services – und seit vielen Jahren als Externer Datenschutzbeauftragter und Datenschutzberater tätig. Seine Fachaufsätze erscheinen regelmäßig in unterschiedlichen Publikationen. Außerdem ist er Geschäftsführer der HäckerSoft GmbH, die unter anderem mit der Datenschutzsoftware DATSIS und der Lernplattform Optilearn (Pflichtschulungen für Datenschutzbeauftragte) am Markt aktiv ist. Sein Lieblingsprojekt ist datenschutzkabarett.de