Kategorie geöffnete Fenster

Konkret: Drucker auf der Fensterbank – vom Winde verwehte Ausdrucke

Der Praxisfall: Im Personalbüro in einem der oberen Stockwerke eines mehrgeschossigen Gebäudes war ein Drucker unmittelbar neben dem Fenster aufgestellt. Während die Gehaltslisten gedruckt wurden, war das Fenster zum Lüften geöffnet. Der Wind blies an diesem Tag kräftig. Es kam wie es kommen musste. Mehrere kräftige Windstöße folgten aufeinander. Die Lohnabrechnungen wurden ungewollt zur Luftpost. Die gesamte Personalabteilung schwärmte aus um die vertraulichen Unterlagen wieder einzusammeln.

Die Gefahr: Wenn Drucker neben geöffneten Fenstern platziert sind, kann es bei geöffnetem Fenster (auch wenn nur kurz gelüftet werden soll) passieren, dass im Drucker liegende Ausdrucke mit personenbezogenen Daten vom Wind mit fort genommen werden. Dadurch können personenbezogene oder sonstige vertrauliche Daten von unbefugten Dritten eingesehen werden.

Gefährdung bewusst machen: Wenn alle Beteiligten die Gefahren kennen, können geeignete Gegenmaßnahmen getroffen werden. Die Gefährdung kann am ehesten bei Ortsbegehungen erkannt werden. Wenn die Gefährdung mit den Beteiligten besprochen wird, ist darauf zu achten, dass verlässlich alle Beteiligten in die Gefährdungsunterweisung einbezogen wurden. Dies gilt auch für Abwesende, genauso wie für Beschäftigte, die nur vorübergehend im Bereich eingesetzt werden, wie Auszubildende, Praktikanten, Vertretungen.

Technische Maßnahmen: Es sollte geprüft werden, ob die Drucker an anderer Stelle aufgestellt werden können, wenn das Fenster geöffnet werden soll (beispielsweise für eine Stoßlüftung). Sollte das nicht möglich sein, beispielsweise weil die Anschlusskabel im Kabelkanal unter dem Fenster langlaufen, dann ist zu prüfen, ob es Schutzmaßnahmen wie Gitter oder ähnliches gibt, mit deren Hilfe die Windstöße ohne Folgen bleiben. Denkbar ist auch, für den Drucker eine Stromzufuhrtaste in Fensternähe anzubringen, die bei Öffnung des Fensters betätigt werden muss. So könnte sichergestellt werden, dass immer dann, wenn die betreffenden Fenster geöffnet sind, die Drucker nicht betätigt werden können. Gegebenenfalls haben auch die dort Arbeitenden eine Idee.

Bauliche Maßnahmen: Denkbar wäre auch eine bauliche Maßnahme, die eine Öffnung des Fensters künftig verhindert. Dies kann einfach durch Abschrauben des Fenstergriffes erfolgen. Oder das Anbringen einer Vorrichtung, dass die Fenster nur noch gekippt werden können. Alle genannten Möglichkeiten sollten bei einem Vorortttermin zusammen mit den Verantwortlichen geprüft werden.

Organisatorische Maßnahmen: In Ergänzung oder als Alternative zu technischen Maßnahmen können auch organisatorische Maßnahmen erforderlich sein. So kann beispielsweise angeordnet werden, dass nur gedruckt werden darf, wenn die betreffenden Fenster geschlossen sind. Die hier vorgestellten Maßnahmen gehören in den Bereich der allgemeinen Organisationsverpflichtung, die in § 9 BDSG sowie in anderen datenschutzrechtlichen Vorschriften wie den Landesdatenschutzgesetzen verbindlich geregelt ist.

Maßnahmen bekannt machen: Ist die Entscheidung gefallen, welche Maßnahmen ergriffen werden sollen, dann sind diese Maßnahmen allen Beteiligten in geeigneter Weise bekannt zu machen. Das kann über eine Arbeitsanweisung geschehen, die beispielsweise in Form einer Rundmail an die Betroffenen versandt wird. Mit einer Lesebestätigung ist dann auch der Nachweis erbracht, dass die Anordnung zur Kenntnis genommen wurde. Die Maßnahmen sollten dann auch Bestandteil der regelmäßigen Schulungen zum Datenschutz oder der allgemeinen Gefährdungsunterweisungen sein.

Regelmäßige Kontrollen: Regelmäßige angekündigte und nicht angekündigte Kontrollen sollen sicherstellen, dass vor allem organisatorische Maßnahmen auch eingehalten werden. Bei technischen Maßnahmen sollte kontrolliert werden, ob die Technik tatsächlich funktioniert. Kontrollen sind zu protokollieren. Aufgedeckte Mängel sollten zeitnah abgestellt werden.

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 Datenschutzsoft-

ware DATSIS und der Lernplattform Optilearn (Pflichtschulungen für Datenschutzbeauftragte) am Markt aktiv ist. Sein Lieblingsprojekt ist datenschutzkabarett.de