Kategorie Übermitteln personenbezogener Daten

Datenübermittlung bei Übergabe einer Präsentation auf einem USB-Stick

Der Praxisfall: Ein potenzieller Kunde bietet die Möglichkeit der Präsentation unserer Leistung vor Ort. Der zuständige Vertriebsmitarbeiter übergibt den USB-Stick, auf dem sich die Präsentation befindet, einem IT-Mitarbeiter beim potenziellen Kunden, damit dieser die Präsentation auf den kundeneigenen Systemen vornehmen kann. Auf dem Stick befinden sich auch zahlreiche andere personenbezogene Daten aus dem Vertrieb, unter anderem Kontakte von Ansprechpartnern bei andern Kunden.

Die Gefahr: Alle auf dem USB-Stick befindlichen Daten werden mit dessen Weitergabe „übermittelt“ (Näheres hierzu unter „Rechtliches“). Alle Dateien auf dem Stick können in kürzester Zeit kopiert werden und sind damit in die Hände eines unbefugten Dritten gelangt.

Rechtliches: „Übermitteln (ist) das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
a) die Daten an den Dritten weitergegeben werden oder
b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft.
Hier ist vor allem a) von Bedeutung, denn die Weitergabe von Daten an einen Dritten wird auch durch die Übergabe eines Datenträgers, auf dem sich die Daten ohne zusätzliche Sicherung befinden, vollzogen. Hierbei ist entscheidend, dass der Dritte die Möglichkeit hat, die Daten zur Kenntnis zu nehmen, nicht ob er das auch tatsächlich tut. Damit liegt auch ein Verstoß gegen die Weitergabekontrolle vor: Hier gilt es „zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können“. Wer unbefugt personenbezogene Daten weitergibt, begeht laut § 43 Abs. 2 Satz 1 Ziff. 1 eine Ordnungswidrigkeit, die mit Bußgeld bis 300.000 Euro geahndet werden kann.

Gefährdung bewusst machen: Alle Beschäftigten eines Unternehmens, die Daten auf einem Datenträger aus dem Unternehmen mitnehmen oder diese Datenträger im Unternehmen Dritten (Besuchern) zugänglich machen, müssen verlässlich darüber informiert sein, dass sie sich vor der Weitergabe des USB-Sticks noch einmal davon überzeugen müssen, dass außer den zur Übermittlung vorgesehenen Daten sich keine weiteren personenbezogene Daten auf dem Datenträger befinden dürfen. Der Übermittler trägt im Zweifelsfall die Verantwortung für die Handlungen, auch was das Bußgeld betrifft. Dies alles gilt auch für die Geschäftsleitung.

Technische Maßnahmen: Hier gibt es eigentlich nur eine einzige Möglichkeit. Diese besteht darin, dass für Zwecke der Präsentation eigene Sticks verwendet werden, auf denen keine weiteren Dateien gespeichert sind.

Unternehmenseigene Sticks bieten weitere Möglichkeiten: Hier können Anordnungen der Geschäftsleitung leichter umgesetzt werden, wenn Präsentationen nur auf unternehmenseigenen Sticks gespeichert werden. Geschieht dies noch durch die IT, kann durch geeignete technische Maßnahmen sichergestellt werden, dass keine weiteren Dateien mehr aufgespielt werden können.

VPN nutzen: Gerade für Präsentationen in unsicheren Drittländern (beispielsweise in Asien) kommt auch noch eine andere Möglichkeit in Betracht. Es gibt die Möglichkeit, über einen zweiteiligen USB-Stick einen VPN-Tunnel mit dem eigenen Rechner im Büro oder mit einem anderen System im Unternehmen aufzubauen. Dazu muss der eine Teil des Sticks im heimischen Büro verbleiben, der andere wird in den USB-Port des Präsentationsrechners gesteckt. Dann baut sich ein VPN-Tunnel auf, über den dann die Originalpräsentation vom heimischen Rechner aus vorgeführt werden kann. Achtung: das funktioniert nur, wenn die Kontrolle über den VPN-Stick vollständig beim Präsentierenden bleibt!

Verschlüsselte Verzeichnisse sind nicht immer sicher: Wenig zielführend ist es hingegen, wenn auf Sticks verschlüsselte Verzeichnisse eingerichtet werden, in denen die weiteren Dateien auf dem Stick untergebracht sind. Untauglich deshalb, weil diese Daten im geschilderten Fall einfach mitkopiert werden können. Dann hat der potenzielle Angreifer alle Zeit dieser Welt, die Verschlüsselung zu knacken.

Organisatorische Maßnahme kombiniert mit Verschlüsselung: eine andere taugliche Maßnahme ist es, bei der Vereinbarung des Termins schon die vorgesehene Präsentation zu übermitteln, diese kann mit einem Passwort verschlüsselt sein, wenn die Präsentierenden nicht möchten, dass sich die Zuhörer die Datei zuvor schon einverleiben können. PowerPoint

verfügt ab der Version 2007 über eine hinreichend Sichere AES256-Verschlüsselung. Wird für das Passwort eine Länge von mindestens 16 Zeichen gewählt, das alle Zeichenmöglichkeiten ausschöpft (Groß-, Kleinbuchstaben, Zahlen, Sonderzeichen), sind die Möglichkeiten, die Datei zu knacken, stark eingeschränkt.

Maßnahme bekannt machen: Hat die Geschäftsleitung die Gefährdungen erkannt und entsprechend Maßnahmen beschlossen, müssen diese in geeigneter Weise bekannt gemacht werden. 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. Dies kann aber auch im Rahmen der regelmäßigen Datenschutzunterweisungen erfolgen.

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