Einbruch – Computerdiebstahl – Datenschutzverletzung

Das Katholische Datenschutzzentrum in Dortmund ist als Datenschutzaufsicht der kirchlichen Einrichtungen in NRW u.a. für die Entgegennahme von Meldungen von Datenschutzverletzungen zuständig, bei denen eine Gefahr für die Rechte und Freiheiten natürlicher Personen zumindest nicht ausgeschlossen werden kann. Eine solche Gefahr könnte z.B. in der illegalen Verwendung sensibler Gesundheits- oder Sozialdaten bestehen oder auch einfach in dem unrechtmäßigen Zugriff auf ein fremdes Bankkonto.

Durchschnittlich zweimal pro Monat werden bundesweit den Katholischen Datenschutzaufsichten Diebstähle von PC oder Laptops aus kirchlichen Einrichtungen in Form einer „Meldung einer Datenschutzverletzung“ angezeigt, d.h. die meldende Einrichtung hat bereits festgestellt, dass nicht nur ein wertvolles Inventargut gestohlen wurde, sondern dass auch personenbezogene Daten von Betroffenen in falsche Hände gelangt sind.

Leider sind auch Kindertageseinrichtungen häufig von Einbruchdiebstählen betroffen. Wenn wir annehmen, dass sich auf einem gestohlenen Computer z.B. Adressen und Kontoverbindungen von Eltern, kommentierte Bildungsdokumentationen zu Kindern, sensible Korrespondenz mit Jugendämtern und Sozialbehörden, aber auch Personalinformationen und Arbeitszeugnisse der Mitarbeitenden befinden, kann man sich unschwer ausmalen, welche materiellen und immateriellen Schäden im schlimmsten Fall angerichtet werden können. Diese Überlegungen gelten im Übrigen nicht nur für „teure“ Computer, sondern auch für „billige“ Datenträger (z.B. USB-Memorysticks), auf denen sensible Daten gespeichert sind.

Wie können Schäden vermieden werden?

Bei vielen Diebstählen wird es dem Angreifer unnötig leichtgemacht. Deshalb möchten wir zuerst zum wiederholten Mal auf die Notwendigkeit eines ausreichenden Einbruchs- und Diebstahlschutzes hinweisen. Dazu gehört, dass die Einrichtung und ihre Büros (Türen, Fenster) mit einigem Aufwand mechanisch gesichert werden. Durch Organisationsanweisungen ist sicherzustellen, dass vorhandene Sicherungsmöglichkeiten (abschließbare Schränke, Kabelschlösser etc.) auch wirklich genutzt werden. Mobile Geräte sind besonders zu sichern und zu beaufsichtigen, z.B. niemals in abgestellten Fahrzeugen zu belassen. Wir empfehlen den Verantwortlichen, sich z.B. durch die Einbruchs-Präventionsstellen der örtlichen Polizei beraten zu lassen.

Aber leider lässt sich ein Diebstahl immer nur erschweren, aber niemals völlig verhindern, wenn der Einbrecher ausreichend Zeit und Mittel zur Verfügung hat. Deshalb sind unbedingt Maßnahmen zu treffen, die es dem unberechtigten Besitzer eines Gerätes unmöglich machen, auf die gespeicherten Daten zuzugreifen.

Schützt da nicht das Anmeldepasswort?

Um es ganz klar zu sagen: Die Absicherung eines Arbeitsplatz-PC oder Laptop durch ein Anmelde-Passwort hilft vielleicht gegen beiläufiges Offenlegen von Daten, solange sich das Gerät in der normalen Arbeitsumgebung (auf dem Schreibtisch, in der Einrichtung) befindet. Eigentlich ist es nur dazu geeignet, den Zugriff verschiedener Personen mit unterschiedlichen Rechten über Benutzerkonten abzusichern. Im Fall eines Diebstahls, wenn der Angreifer uneingeschränkten körperlichen Zugriff auf das Gerät und seine Komponenten hat, hilft ein Anmelde-Passwort gar nicht mehr gegen ein gezieltes Auslesen aller Daten aus den lokalen Speicherkomponenten (z.B. Festplatten): Der Angreifer baut die Datenträger aus und schließt sie z.B. als externe Festplatte an einen anderen Computer an. Für den oben erwähnten USB-Memorystick ist das Szenario offensichtlich.

Nur wenn der Schutz der Daten auf der Ebene der Datenträger eingerichtet ist, also unabhängig davon, an welchem Rechner der Datenträger angeschlossen wird, läuft das beschriebene Angriffsszenario ins Leere.

Nur Verschlüsselung hilft!

Was sich vielleicht wie Spezialwissen für IT-Experten anhört, ist in Wahrheit recht einfach und nur ganz wenig unbequem: Der Schutz der Daten auf Ebene der Datenträger wird durch eine passwortgeschützte Verschlüsselung erreicht.
In der Praxis ist der Ablauf wie folgt: Auf dem PC/Laptop wird eine Verschlüsselungssoftware installiert, bzw. eine schon im Betriebssystem (z.B. Windows 10 Professional oder Enterprise) vorhandene Verschlüsselungskomponente aktiviert. Die Festplatte des PC/Laptop wird während einer Initialisierung komplett verschlüsselt. Dabei wird ein Passwort festgelegt, evtl. auch ein Master-Passwort, welches der Admin unter Verschluss nimmt.

Ab jetzt wird bei jedem Systemstart, also vor dem ersten Zugreifen auf den lokalen Datenträger, das Passwort der Verschlüsselung abgefragt und erst dann das Betriebssystem mit Benutzerkonto und Anmeldepasswortabfrage gestartet. Im weiteren Arbeitsverlauf läuft die Entschlüsselung (beim Lesen der Daten) und die Verschlüsselung (bei Schreiben) vom

Anwender unbemerkt im Hintergrund solange der Computer eingeschaltet bleibt. Erst wenn der Rechner stromlos wurde oder neu gestartet wird, muss das Passwort der Festplattenverschlüsselung neu eingegeben werden.

Die „kleine Unbequemlichkeit“ liegt also darin, dass nach einer Festplattenverschlüsselung der Start des Systems die Eingabe von zwei Passwörtern verlangt: Eines für die Ver- und Entschlüsselung des Datenträgers und ein anderes für die Anmeldung am Betriebssystem.

Verschlüsselungsprogramme für mobile Datenträger, z.B. USB-Memorysticks, arbeiten auf die gleiche Art oder legen versteckte und verschlüsselte Verzeichnisse an, die nur nach Eingabe eines Passworts sichtbar, lesbar und beschreibbar sind.

Wird ein Computer entwendet, dessen Datenträger verschlüsselt und dessen Verschlüsselungsprogramm mit einem starken Passwort gesichert wurde, kann man davon ausgehen, dass der Angreifer keine Kenntnis über die gespeicherten Daten erlangen wird. In diesen Fällen ist deshalb in der Regel auch keine meldepflichtige Datenschutzverletzung gegeben. Natürlich sollten Sie auch solche Diebstähle u.a. Ihrem betrieblichen Datenschutzbeauftragten anzeigen.

Was nicht da ist, kann nicht gestohlen werden

Noch ein Hinweis: Der beste Schutz für Daten ist der Verzicht auf eine lokale Speicherung. Wann immer möglich, sollte eine Verarbeitung und Ablage auf zentralen Systemen, z.B. in KiTaPLUS oder anderen Verwaltungsplattformen oder auch in zentralisierten Ordnern bei Ihrem IT-Dienstleister stattfinden. Wenn ein professioneller Dienstleister auf Grundlage von geprüften Auftragsverarbeitungsverträgen für eine gesetzeskonforme und sichere Datenhaltung sorgt, wird damit die örtliche KiTa-Leitung von vielen Risiken entlastet. Fazit: Sorgen Sie zuerst für einen möglichst weitreichenden Diebstahlschutz, um die wertvollen Investitionsgüter Ihrer Einrichtung zu schützen. Vermeiden Sie dann soweit wie möglich die Speicherung von personenbezogenen Daten auf lokalen Geräten und richten Sie schließlich zusammen mit Ihrer IT-Betreuung unbedingt eine Verschlüsselung Ihrer Datenträger ein, damit auch in den Fällen, in denen ein Diebstahl oder ein anderer Verlust der Hardware nicht verhindert werden konnte, Ihre Daten nicht offengelegt werden und Sie damit eine Gefährdung der Rechte und Freiheiten natürlicher Personen wirkungsvoll verhindern.

MICHAEL TEGETHOFF
Referent im Katholischen Datenschutzzentrum Dortmund

Weitere Informationen:
www.katholisches-datenschutzzentrum.de