Datenschutz im Bereich der elektronischen Datenverarbeitung

*Christof **Radewagen**, Osnabrück; Karsten **Violka**, Hannover*

Im Bereich der ambulanten und stationären Kinder- und Jugendhilfe erhalten die Fachkräfte freier Träger oft sehr persönliche Einblicke in die Lebenssituation ihrer Adressatinnen und Adressaten. Sie erfahren von erzieherischen Fragestellungen, persönlichen oder familiären Geheimnissen, kindeswohlgefährdenden Aspekten, sowie Wünschen und Ängsten.

Um die geleistete Arbeit inhaltlich reflektieren zu können, ist es unter anderem notwendig theoretische Erklärungsansätze und das daraus abgeleitete methodische Vorgehen zu dokumentieren. Das gilt auch für den Nachweis gegenüber Vorgesetzten und Kostenträgern, die jeweilige Aufgabe gemäß verabredeter Qualitätsstandards erfüllt zu haben. Im Zeitalter der Digitalisierung wird zunehmend am Computer dokumentiert, ganzgleich, ob mit Hilfe einer speziellen Software oder aber in standardisierten Textverarbeitungsprogrammen.

Während papierne Akten wie selbstverständlich in verschlossenen Schränken aufbewahrt werden, stehen Computer offen in Büros beziehungsweise werden Tablets und Laptops in Autos, Arbeitstaschen der Mitarbeiter/innen mitgeführt und lagern zum Teil auch in ihren Privatwohnungen. Die gespeicherten Daten sind somit vielfältigen Gefahren durch einen unbefugten Zugriff Dritter, einer Zerstörung, dem Verlust oder Diebstahl ausgesetzt.

Das Bundesdatenschutzgesetz (BDSG) beschreibt in § 9 und der dazugehörigen Anlage, wie der Schutz elektronisch verarbeiteter Daten in der Praxis zu organisieren ist. Im Einzelnen sind folgende Anforderungen zu erfüllen:

Anforderung	Ziel
Zutrittskontrolle	Es ist sichergestellt, dass der Zutritt zu den Datenverarbeitungsanlagen vor Unbefugten geschützt ist.
Zugangskontrolle	Es ist sichergestellt, dass Daten weder unbefugt gelesen, kopiert, verarbeitet noch entfernt werden können. Dafür wird gewährleistet, dass Unbefugte die DV/ IT-Anlagen nicht nutzen und berechtigte Benutzer ausschließlich auf die für ihre Aufgabenerfüllung notwendigen Daten zugreifen können.
Zugriffskontrolle	
Weitergabekontrolle	Bei der elektronischen Übermittlung von Dateien ist gewährleistet, dass die Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es kann überprüft werden, an welche Stelle eine Datenübermittlung vorgesehen ist.
Eingabekontrolle	Es ist sichergestellt, dass festgestellt werden kann, wer wann welche Datenbestandveränderungen vorgenommen hat.
Auftragskontrolle	Es ist sichergestellt, dass Daten durch Auftragnehmer nur nach Weisung des Auftraggebers verarbeitet werden.
Verfügbarkeitskontrolle	Es ist sichergestellt, dass die Daten vor einer zufälligen Zerstörung und vor Verlust geschützt sind.
Trennungskontrolle	Es ist sichergestellt, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Verstöße gegen diese Datenschutzanforderungen können nicht nur dazu führen, dass die oft sehr sensiblen Informationen Unbefugten zugänglich werden und dadurch das Ansehen der betroffenen Adressat/innen in der Öffentlichkeit gefährdet ist. Sie sind darüber hinaus auch ein schwerwiegender Imageschaden für die betreffenden Einrichtungen und können von den zuständigen Kontrollbehörden auch geahndet werden, wie ein Beispiel aus Schleswig-Holstein zeigt:

Wegen eines Datenlecks, bei dem rund 3.600 Dokumente psychisch Kranker mit sensiblen Daten ungeschützt gespeichert und so von Unbefugten abrufbar waren, wurden vom Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) gegen die Einrichtung und ihre hundertprozentige Tochter Bußgelder von insgesamt 18.000 Euro verhängt. Die Bescheide sind mittlerweile rechtskräftig.

Die Einhaltung der einschlägigen Datenschutzvorschriften ist nicht nur eine der Grundvoraussetzungen für die Sicherstellung des informationellen Selbstbestimmungsrechts der Adressatinnen und Adressaten, sondern auch ein Qualitätsmerkmal professioneller sozialer Arbeit und der beste Schutz vor rechtlichen Konsequenzen für den Träger.

Welcher inhaltliche und organisatorische Schutzstandard eingehalten werden muss, bemisst sich allerdings nicht nur nach einschlägigen Rechtsvorschriften, sondern auch nach der jeweiligen Sensibilität der Daten.

Die im Bereich der Kinder- und Jugendhilfe verarbeiteten Daten unterliegen mindestens der Schutzstufe C.

Man unterscheidet zwischen Daten der Schutzstufen A, B, C, D und E. Der Schutzstufe A sind Daten zuzuordnen, die frei zugängig sind, zum Beispiel Angaben in Telefonbüchern. Sie unterliegen einem geringen Schutzniveau. Daten der Schutzstufe B sind solche, deren Missbrauch für die Betroffenen keine besonderen Beeinträchtigungen zur Folge hat, für eine Kenntnis die Einsichtnehmenden gegenüber der speichernden Stelle aber ein berechtigtes Interesse zum Ausdruck bringen müssen, beispielsweise sind dies Verteilerlisten innerhalb einer Organisation. Der Schutzstufe C unterliegen Daten, deren Missbrauch die gesellschaftliche Stellung der Betroffenen beeinträchtigt. Hierzu zählt unter anderem der Bezug von Sozialleistungen – also auch der Bezug von Hilfe zur Erziehung. Unter die Schutzstufe D fallen Daten, deren Missbrauch die Existenz der Betroffenen beeinflussen können. Beispiele dafür sind Straffälligkeiten, Schulden oder Pfändungen. Unter die Schutzstufe E schließlich fallen Daten, deren Missbrauch das Leben oder die Freiheit der Betroffenen gefährden kann.

Die im Bereich der Kinder- und Jugendhilfe verarbeiteten Daten unterliegen aufgrund ihrer Sensibilität mindestens der Schutzstufe C, teilweise sogar D oder auch E. An den Schutzstandard der elektronischen Datenverarbeitung sind deshalb in Organisation und Inhalt besonders hohe Anforderungen zu stellen. Wie dieser in der Praxis konkret umgesetzt wird, haben die Träger der freien Jugendhilfe in einem Datenschutzkonzept schriftlich festzuhalten. Es dient den Mitarbeiterinnen und Mitarbeitern als Orientierungshilfe für die tägliche Arbeit und ist den wachsenden Gefährdungspotentialen und dem technischen Fortschritt regelmäßig anzupassen.

Elektronische Datenverarbeitung in der Praxis

In der Praxis stehen Jugendhilfeträger dabei vor technischen und organisatorischen Herausforderungen: Einerseits sind Computer, Tablets und Smartphones nahezu allgegenwärtig und ein aus der Praxis nicht mehr wegzudenkendes Werkzeug, andererseits sind Datenschutzkonzepte nur selten vorhanden. Hinzu kommt, dass die mit dem System standardmäßig ausgelieferten oder frei im Internet verfügbaren Schutzprogramme oft nur oberflächliche beziehungsweise trügeri-

sche Sicherheit bieten. Der Schutz der verarbeiteten Daten vor Angriffen aus dem Internet ist somit oftmals reine Glückssache. Weitere Gefahren entstehen durch das Verhalten der Nutzer/-innen selbst. Auch durch die unverschlüsselte Kommunikation via E-Mails zum Beispiel sind die Daten einer nicht kalkulierbaren Gefahr vor Angriffen aus dem Netz ausgesetzt. Gleiches gilt für die Installation von frei verfügbarer Software, deren Systemeingriffe und Zugriff auf die Datenbestände den Anwender/innen nicht bekannt sind. Das denkbar schlechteste Szenario: Die IT-Landschaft einer Einrichtung wird nicht professionell betreut und besteht aus Computern mit Internetzugang, auf denen sensible Daten ungesichert verarbeitet und per Mail versendet werden. Gleichzeitig haben die Anwender uneingeschränkte Möglichkeiten in Nutzung und Administration des Systems.

Zahlreichen Gefahren für die Sicherheit der Daten kann bereits durch einfache Maßnahmen entgegengetreten werden:

Grundsätzliche Gefahren und erste Lösungen

Als weltweit am häufigsten eingesetztes Betriebssystem ist Windows vielen Hackerangriffen ausgesetzt. Dabei sind die Daten auf einem Windows-PCs vor allem durch Viren und Trojaner bedroht, die in der Regel Lücken in veralteter Software missbrauchen. Das System sollte deshalb so konfiguriert sein, dass neu veröffentlichte Sicherheitsupdates automatisch installiert werden. Das kann Windows XP allerdings nicht mehr leisten. Dieses Betriebssystem wird von Microsoft nicht mehr mit Sicherheitsupdates versorgt. Rechner mit diesem Betriebssystem dürfen deshalb zum Schutz der Daten auf keinen Fall mit dem Internet verbunden sein. Der Support vom XP-Nachfolger Windows Vista endet am 11. April 2017, der von Windows 7 am 14. Januar 2020. (Quelle: http://windows.microsoft.com/de-de/windows/lifecycle). Hier gilt es, rechtzeitig auf ein anderes Betriebssystem umzusteigen.

Auch alternative Browser wie Mozilla Firefox müssen regelmäßig aktualisiert werden

Bei der Recherche im Internet gilt es zu beachten, dass vor allem der Microsoft Internet-Explorer immer wieder Sicherheitslücken aufweist und somit ein beliebtes Angriffsziel für Schadprogramme ist. Um hier vorzubeugen, ist der Einsatz eines alternativen Browsers, etwa Mozilla Firefox, zu empfehlen. Allerdings muss auch dieser regelmäßig aktualisiert werden, um stetig auftauchende Sicherheitslücken zu schließen. Angriffsanfällige Browser-Plugins, insbesondere Java und Flash, sollten zum Schutz vor Hackerangriffen deinstalliert werden, auch wenn dadurch einige Anwendungen nicht mehr in gewohnter Qualität laufen.

Windows-PCs benötigen zudem einen aktuellen Virenscanner mit gültiger Lizenz. Wie Tests in unterschiedlichen Computermagazinen zeigen, bieten nicht alle Scanner-Produkte ein identisches Schutzniveau. Kostenlose Antivirus-Pakete wie Microsofts »Security Essentials« beispielsweise schneiden oft mit ungenügendem Ergebnis ab.

Um unbefugten Nutzerinnen und Nutzern Datenzugriffe zu erschweren, sollte jede/r Mitarbeiter/in ein separates Benutzer-Konto mit eingeschränkten Nutzerrechten und individuellem Passwort erhalten. Zusätzlich sollten auf der Anwenderebene zwischen »normalen« Nutzern und Administratoren unterschieden werden. »Normalen« Anwendern ist es dabei zu verwehren, Programme auf dem PC zu installieren oder notwendige Sicherheitseinstellungen zu verändern. So beugt man dem Einsatz von eventueller Schadsoftware vor und kann zudem unterbinden, dass nicht lizensierte Software verwendet wird. Einrichtungen, die einen eigenen Server betreiben, können hierfür leicht Benutzergruppen abbilden und so Zugriffsberechtigungen flexibel konfigurieren.

Auch eine regelmäßige – automatisierte - Datensicherung ist unbedingt notwendig. PC-Festplatten können jederzeit ausfallen beziehungsweise gestohlen, versehentlich gelöscht oder überschrieben werden. Da auch Backup-Medien gestohlen werden können, sollten sie an einem sicheren Ort – am besten außerhalb des Büros - aufbewahrt werden.

Gefahren durch E-Mail

Beim Versenden von Mails besteht unter anderem die Gefahr, dass die Daten in unbefugte Hände gelangen. Unverschlüsselte E-Mails sind auf ihrem Weg durchs Internet auf allen Zwischenstationen im Klartext einsehbar. Der Text einer Standard-E-Mail ist daher so wenig vor fremden Blicken geschützt, wie der auf einer Postkarte.

Bei Postfächern, die von externen Mail-Providern gemietet werden (etwa 1&1, GMX, Microsoft oder Google) und Cloud-Diensten gilt: sämtliche Daten liegen dem Anbieter im Klartext vor. Man gibt also mit der Nutzung solcher Postfächer die Kontrolle darüber ab, wer die Daten einsehen und weitergeben kann.

Mittels Transportverschlüsselung (»TLS«) lässt sich ein wirksam geschützter Kanal zu Partnerorganisationen etablieren

Zur Absicherung des Mail-Verkehrs ist es daher für Organisationen ratsam, einen eigenen Mailserver zu betreiben, der E-Mails ohne Umweg über externe Dienstleister entgegennimmt (»MX«).

Mit einem eigenen Mailserver stellen Einrichtungen sicher, dass Mails zwischen ihren eigenen Mitarbeitern den geschützten »internen« Bereich des Netzwerks erst gar nicht verlassen. Zudem lässt sich mittels Transportverschlüsselung (»TLS«) ein wirksam geschützter Kanal zu Partnerorganisationen etablieren, ohne dass sich Anwender selbst um Mail-Verschlüsselung sorgen müssen.

Die Verschlüsselung von Mails mittels des kostenlosen Programms GnuPG (»GNU Privacy Guard«) ist vor allem für technisch versierte und geschulte Mitarbeiter geeignet. Richtig angewendet ist GnuPG ein sehr sicheres Mittel – leider ist die Hürde für Anwender relativ hoch und es wird in der Praxis eher selten eingesetzt. Für größere Organisationen lohnt sich deshalb der Einsatz spezieller Mail-Gateways, die ein- und ausgehende E-Mails automatisch verschlüsseln.

Das Problem mit dem Datenaustausch

Bei der Zusammenarbeit mit Kolleg/innen und Dritten ist es oft notwendig, (sensible) Daten zu übermitteln. Gängige Kommunikationswege sind etwa E-Mail, USB-Sticks, externe Festplatten und zentrale Server.

E-Mails sind nicht immer der richtige Weg, um Dokumente an Kollegen und Dritte zu übertragen: Haben sie eine Größe von vielen Megabyte oder sind sie an viele Empfänger zugleich gerichtet, bringen sie die Postfächer auf dem Mailserver schnell an ihre Kapazitätsgrenzen. Hinzu kommen die schon beschriebenen Sicherheitsprobleme beim Übertragen.

Cloud-Dienste wie beispielsweise Dropbox oder iCloud sind aus Datenschutzsicht nicht akzeptabel.

USB-Sticks und externe Festplatten eigenen sich nur dann als Transportmittel, wenn sie mit einem geeigneten Werkzeug verschlüsselt sind, etwa mit dem kostenlosen Werkzeug Truecrypt oder Microsofts Bitlocker. In der Praxis ist die Nutzung von USB-Sticks und anderen externen Datenträgern allerdings äußerst problematisch: Ihr Gebrauch ist für Einrichtungen schwer zu kontrollieren, sie gehen leicht verloren und dienen mitunter als Übertragungsweg für Schadsoftware. In vielen Einrichtungen ist ihr Einsatz deshalb aus gutem Grund verboten.

Ein aus Datenschutzsicht ebenfalls nicht akzeptabler Weg zum Dokumentenaustausch, sind

Cloud-Dienste wie beispielsweise Dropbox oder iCloud. Auch hier gibt man seine Daten in »fremde« Hände, da in der Regel jede Datei vollständig auf den Server des Anbieters kopiert und gespeichert wird. Die installierten Programme halten dazu eine ständige Datenverbindung zum Server des Anbieters aufrecht.

Um Dokumente sicher via Internet auszutauschen, ist deshalb der Einsatz eines eigenen Dateiservers zu empfehlen, auf den die Mitarbeiter/innen über eine verschlüsselte Netzwerkverbindung zugreifen können (VPN, Virtual private network). Ein solcher zentraler Server, an dem sich die Anwender anmelden, hat auch den Vorteil, dass sich Zugriffsrechte und Arbeitsgruppen abbilden lassen und man Dokumente zentral und strukturiert einsortieren kann. So ist sichergestellt, dass jeder Mitarbeiter nur Zugriff auf die für ihn notwendigen Dokumente erhält.

Mobile Geräte: Smartphone oder Tablet

In der Praxis ist es zum Teil notwendig, unterwegs und am Heimarbeitsplatz auf aktuelle Dokumente und E-Mails zuzugreifen. Wenn Geräte mit Adressaten-, Geschäfts- oder Betriebsdaten die Einrichtungsräume verlassen, sind zusätzliche Sicherheitsmaßnahmen notwendig.

Gängige Smartphones und Tablets mit den Betriebssystemen iOS und Android sind für die Verarbeitung sensibler Daten nicht geeignet – vor allem sollte der Einsatz privater Geräte verboten sein, da diese durch die Einrichtung nicht zu kontrollieren sind: Tablets und Smartphones sind eng mit den Online-Diensten der Anbieter verknüpft, private und dienstliche Adressbücher und Mailkonten lassen sich nicht sicher voneinander trennen. Zusätzlich installierte Apps von Drittherstellern können weitgehende Zugriffsrechte auf Adressat/innendaten erlangen.

Eine gute Möglichkeit für die mobile Datennutzung sind dienstliche Notebooks mit verschlüsselter Festplatte, die nach den Vorgaben der Organisation konfiguriert sind. Dabei muss die Festplatte mit speziellen Werkzeugen vollständig verschlüsselt sein (»Full disk encryption«), sodass beim Start des Gerätes zuerst das zusätzliche Verschlüsselungspasswort abgefragt wird. Damit sind die Daten auch dann geschützt, wenn das Gerät abhanden kommt.

Eine gute Lösung: Remote Desktops

Eine ständig wachsende Zahl von Computern in einer Organisation datenschutzkonform zu warten und zu sichern ist mit einem erheblichen Arbeitsaufwand verbunden. Ein sich stetig an die neuesten Gefahren anpassendes Sicherheitskonzept erhöht den Zeitaufwand zudem. Eine Alternative zu den herkömmlichen Computern sind sogenannte »Remote Desktops«. Dabei stellt ein zentraler Server die Desktop-Umgebung und alle Anwendungen bereit, mit denen die Mitarbeiter/innen arbeiten. Der Administrationsaufwand ist um Größenordnungen kleiner, die Umgebung lässt sich sehr sicher und vor allem einheitlich vorkonfigurieren.

Der Zugriff auf den Remote Desktop erfolgt über eine verschlüsselte VPN-Verbindung, die nach heutigem Stand der Technik äußerst sicher ist.

Mit Remote Desktops werden Mitarbeiter unabhängig von einem lokalen Arbeitsplatz: Ihre Arbeitsumgebung begleitet sie mit allen Programmen und Daten überall dort, wo sie Zugriff auf das verschlüsselte Netzwerk der Organisation haben. Soll eine neue Software eingeführt werden, genügt es, diese einmal auf dem zentralen Server zu installieren, damit sie allen Kolleg/innen zur Verfügung steht

Durch die Verwendung eines solchen Systems kann auf den Einsatz von »vollständigen« Computern verzichtet werden. Es reichen sogenannte Thin-Clients, Endgeräte, die lediglich den Zugang zum Remote Desktop herstellen und auf denen selber keine Daten gespeichert werden. Werden

diese Geräte gestohlen oder sind sie defekt, gehen deshalb auch keine Daten verloren. Der Zugriff auf den Remote Desktop erfolgt über eine verschlüsselte VPN-Verbindung, die nach heutigem Stand der Technik äußerst sicher ist.

Auf diese Weise können die datenschutzrechtlichen Vorgaben gemäß § 9 BDSG und der dazugehörigen Anlage sicher umgesetzt und zentral gesteuert werden. Änderungen werden einheitlich ins System eingepflegt und gelten dann für die gesamte Netzwerkumgebung. Auch mobile Geräte können ins System eingefügt werden. ❑

Prof. Dr.
Christof Radewagen
Hochschule Osnabrück
Postfach 1940
49009 Osnabrück
c.radewagen@hs-osnabrueck.de

Karsten Violka
Violka IT
Beratung,
Entwicklung, Netze
Eleonorenstr. 18
30449 Hannover
kav@violka-it.de
www.violka-it.de