Datenschutz und Datensicherheit in Erziehungsberatungsstellen beim Einsatz von Personalcomputern

Der PC hat in den Erziehungsberatungsstellen längst Einzug gehalten. Es gibt kaum eine Beratungsstelle, die ihren Schriftverkehr oder die Adressdaten nicht auf dem eigenen PC verwaltet. Mit der Verbreitung des PC als “ganz normalem” Arbeitsmittel sind viele der anfänglich formulierten Bedenken verschwunden oder verstummt. Die regelmäßige Nutzung hat die einst kritische Distanz zur Technik verringert. Über das Internet entstehen jedoch neue Bedrohungen für die gespeicherten Daten.

Die Verschwiegenheit der Beratungsfachkraft ist in Zeiten globaler Vernetzung nicht ausreichend, um den Schutz personenbezogener Daten zu gewährleisten. Erforderlich ist zudem die gesetzeskonforme Verarbeitung der über die Ratsuchenden gesammelten Daten. Die Speicherung und Verarbeitung personenbezogener Daten auf Personalcomputern ohne besondere Sicherungsvorkehrungen stellt einen Verstoß gegen geltende Datenschutzvorschriften dar.

Inhaltliche Grundlagen des Datenschutzes

Stellenleitung und (Gesamt)Verantwortung

Zunächst stellt sich die Frage, welche Verantwortung Träger und Stellenleitung übernehmen, wenn ein PC in der Beratungsstelle aufgestellt wird. Es können drei Szenarien unterschieden werden:

- Die Beratungsstelle ist Teil eines administrativen Ganzen (z.B. Beratungsstelle eines Jugendamtes), innerhalb dessen die Beschaffung, die Aufstellung sowie die Administration ausschließlich von dazu spezialisierten Verwaltungseinheiten verantwortet wird.
- Die Beratungsstelle ist einem Träger angeschlossen, der die Beschaffung und Installation der Technik begleitet und technisches Personal zur Administration vorhält. Eine Betriebsvereinbarung regelt den Betrieb der Datenverarbeitung.
- Die Beratungsstelle ist bei der Beschaffung wie beim Betrieb der Technik auf sich alleine gestellt.

Die letzte Alternative belässt die Verantwortung bei der Stellenleitung, die alleine und ohne kompetente Fremdhilfe sicherstellen soll, dass der Betrieb der Datenverarbeitung die einschlägigen Vorschriften zu Datenschutz und Datensicherheit erfüllt.

Die Sicherstellung zureichender Datenschutzmaßnahmen wird durch mehrere Faktoren erreicht:

- Die Verantwortlichen sind hinreichend über die einschlägigen Datenschutzbestimmungen des Sozialgesetzbuches (SGB), des Strafgesetzbuches (StGB)

bke-Hinweis

und des Bundesdatenschutzgesetzes (BDSG) informiert.
- Die Verantwortlichen sind in der Lage, die gesetzlichen Auflagen auf die technische Verarbeitung von Daten zu übertragen.
- Die Verantwortlichen verfügen über hinreichende Technikkenntnisse zur Ableitung der erforderlichen technischen Konsequenzen („organisatorische Umsetzung").
- Und die Verantwortlichen sind in der Lage, aus den vorhandenen Erkenntnissen eine Verarbeitungsrichtlinie zu gestalten, die den erkannten Risiken Rechnung trägt und den Betriebsalltag „angemessen" regelt (Betriebsvereinbarung).

Sowohl im Bundesdatenschutzgesetz wie auch in den einschlägigen Vorschriften der beiden Kirchen ist von "angemessenem" Datenschutz die Rede. Die Relativierung auf den am Einsatzzweck orientierten Aufwand entlastet die Verantwortlichen nicht von der Verpflichtung, kontinuierlich zu prüfen, ob die getroffenen Maßnahmen angemessen bleiben. Nicht alleine sich ändernde Regelungen des Straf- oder Sozialgesetzbuches beeinflussen diese Norm, auch die schnelle technische Entwicklung macht deren Einhaltung nicht eben leicht. So kann der neu beschaffte PC mit seinem aktuellen Betriebssystem und den dort enthaltenen Erweiterungen ein (verstecktes) Problem mit sich bringen, das durch die bisherige Verfahrensvorschrift nicht abgedeckt ist.

Teile der hier skizzierten Verantwortung der Stellenleitung können delegiert werden – im Nahbereich an kundige Mitarbeitende beim Träger, im Fernbereich an eine spezialisierte Firma, was jedoch wegen der auf dem PC gespeicherten sensiblen Daten nicht unproblematisch ist. Letztlich bleibt die Stellenleitung für die „Angemessenheit" der Vorgehensweise und die korrekte Umsetzung der betrieblichen Vereinbarung verantwortlich.

Datenschutz – Qualitätsmerkmal der Beratung nach § 28 SBG VIII

Es gibt eine Vielzahl einschlägiger rechtlicher Bestimmungen über Schweigepflicht und Datenschutz für Fachkräfte freier und öffentlicher Träger der Jugendhilfe. Sie alle sind auch im Zusammenhang mit der Nutzung von Personalcomputern einzuhalten.

Für Fachkräfte der Jugendhilfe öffentlicher und freier Träger wichtige Regelungen enthält das Strafgesetzbuch, hier insbesondere § 203 StGB (Verletzung von Privatgeheimnissen). Diese Vorschrift stellt die unbefugte Offenbarung anvertrauter fremder Geheimnisse u. a. durch Ehe-, Familien-, Erziehungs- oder Jugendberater in einer (anerkannten) Beratungsstelle (Abs. 1 Nr. 4) und deren berufsmäßige Gehilfen (Abs. 3) unter Strafe. Durch § 203 StGB wird die persönliche Vertrauensbeziehung zwischen Angehörigen bestimmter Berufe und den Menschen geschützt, die Rat und Hilfe suchen. Der Staat setzt zum Schutz dieser Beziehung sein stärkstes Mittel ein: die Androhung von Geld- oder Freiheitsstrafe.

Ebenso wichtige Regelungen enthält das Sozialgesetzbuch. Hier ist hinzuweisen auf die bereichsspezifischen Regelungen für die Träger der öffentlichen Jugendhilfe im SGB VIII (§§ 61 - 68), auf § 35 SGB I sowie auf die §§ 67 - 85a SGB X. Der Schutz des Bürgers durch die Vorschriften des Sozialgesetzbuches geht weiter als der Schutz durch das Strafgesetzbuch. Während § 203 StGB den Bürger gezielt gegen die unbefugte Weitergabe von anvertrauten oder sonst bekannt gewordenen Geheimnissen an Dritte schützt, ist Schutzgegenstand des Sozialgesetzbuches das Erheben, Verarbeiten (Speichern, Verändern, Übermitteln, Sperren, Löschen) und das Nutzen von Sozialdaten (vgl. auch *bke* 1995a, 1995b).

Die Datenschutzbestimmungen des Sozialgesetzbuches verpflichten die Träger der freien Jugendhilfe nicht unmittelbar. Jedoch obliegt es dem Träger der öffentlichen Jugendhilfe nach § 61 Abs. 4 SGB VIII sicherzustellen, dass der Träger der freien Jugendhilfe den Schutz von Sozialdaten bei ihrer Erhebung, Verarbeitung und Nutzung in entsprechender Weise gewährleistet, wenn seine Einrichtungen und Dienste in Anspruch genommen werden. Für die Träger der freien Jugendhilfe gelten direkt die Bestimmungen des allgemeinen Datenschutzrechts (Bundesdatenschutzgesetz und Länderdatenschutzgesetze). Die Kirchen haben sich zudem eigene Datenschutzregelungen gegeben. Dies ist für die Evangelische Kirche das „Kirchengesetz über den Datenschutz", für die Katholische Kirche die „Anordnung über den kirchlichen Datenschutz". Ziel des Datenschutzes ist ein (formalrechtlich) korrektes Verfahren bei der Erhebung und im Umgang mit personenbezogenen Daten.

Das Vertrauen der Ratsuchenden in die Erziehungs- und Familienberatung ergibt sich nicht alleine aus der Unterstellung, die Beratungsfachkraft beachte ihre Pflicht, anvertraute Daten nicht an Dritte weiter zu geben, sondern ebenso aus der Erwartung, dass in Beratungsstellen personenbezogene Daten unter Beachtung der geltenden Datenschutzbestimmungen erhoben, gespeichert, verarbeitet, gelöscht und ggf. übermittelt werden.

Technischer und inhaltlicher (nichttechnischer) Datenschutz

Es ist die Form der Datenverarbeitung, die sicherstellt, ob die Daten vor dem Zugriff Unbefugter geschützt sind. Denn in jeder Beratungsstelle werden die gesammelten Daten auch außerhalb des „geschützten Dialogs" zwischen Ratsuchendem und Beratungsfachkraft aufbereitet (Berichte und Stellungnahmen, Adressdatenbank usw.). Die elektronische Erfassung der personenbezogenen Daten der Ratsuchenden definiert dabei keinen neuen Tatbestand, sondern eine neue Qualität. Denn die Sammlung von sensiblen (persönlichen) Daten auf Papier unterscheidet sich von der in elektronischer Form durch den Aufwand, der getrieben werden muss, um an bestimmte Informationen zu gelangen.

Die Zugangswege zu papiergebundenen und elektronischen Daten sind unterschiedlich:

- Der Zugang zu den Akten der Beratungsstelle erfordert den Zugang zum Aufbewahrungsort (Stahlschrank nach DIN-Norm). Ein Unbefugter muss dafür sorgen, dass er bei der Entnahme der Akten unentdeckt bleibt. Die Gefahr, dass der Verlust der Akte wie der Entwender entdeckt werden können, stellt ein potenzielles Hindernis für den Angriff auf sensible Daten dar.

- Der Zugang zu elektronischen Daten kann über einen mobilen Datenträger (z.B. Diskette) erfolgen. Wegen der Schnelligkeit der Übertragung können wahllos komplette Datenbestände kopiert werden. Der Kopiervorgang wird bei den handelsüblichen Betriebssystemen nicht protokolliert. Nicht zu vernachlässigen ist der Fall, dass der komplette PC aus der Stelle entwendet wird (Diebstahl).

Die Angemessenheit des zu gewährleistenden Datenschutzes ist in beiden Fällen unterschiedlich:

- Die Papierakte gilt als geschützt, wenn sie sorgsam unter Verschluss gehalten wird und nur den dazu bestimmten Personen zur Einsicht zur Verfügung steht.
- Elektronische Daten gelten als geschützt, wenn weder das Duplizieren (Kopieren) noch das Sichtbarmachen (Anzeigen, Entschlüsseln) durch Unbefugte möglich ist.

Zwar konstatiert der Gesetzgeber, dass ein hundertprozentiger Schutz der elektronisch zu verarbeitenden Daten nicht möglich sein wird, formuliert jedoch hohe Anforderungen an die „Angemessenheit“, die im Umgang mit persönlich anvertrauten Daten erforderlich ist. Diese Anforderungen sind in so genannten „Organisationskriterien“ zusammengefasst, die nachfolgend zitiert werden:

1. Der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, ist Unbefugten zu verwehren (Zugangskontrolle)
2. Es ist zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle)
3. Die unbefugte Eingabe personenbezogener Daten in den Speicher sowie deren Löschung ist zu verhindern (Speicherkontrolle)
4. Es ist zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle)
5. Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle)
6. Es ist zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch die Einrichtung zur Datenübertragung übermittelt worden sind (Übermittlungskontrolle)
7. Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle)
8. Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)
9. Es ist zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert verändert oder gelöscht werden können (Transportkontrolle)
10. Die innerbehördliche oder innerbetriebliche Organisation ist den besonderen Anforderungen des Datenschutzes entsprechend zu gestalten (Organisationskontrolle).

Diese Kriterien finden sich sinngemäß im Bundesdatenschutzgesetz (BDSG) sowie den Datenschutzgesetzen der beiden Kirchen. Die Umsetzung der Vorschriften richtet sich nach konkreten (technischen) Verhältnissen vor Ort und erfolgt somit individuell, weshalb die Aufstellung allgemeiner Richtlinien nur aufzeigt, welche organisatorischen Prozesse einer besonderen Beachtung bedürfen.

Vier Szenarien – zwei Verantwortliche

Die Verantwortung, die jede Stellenleitung für die Umsetzung und Einhaltung der Auflagen übernimmt, kann durch vier Szenarien skizziert werden:

1. Beratungsstelle mit PC, ohne administrative Fachkraft, ohne Netzwerk.
In dieser Variante liegt die Verantwortung für die Einhaltung des geforderten zureichenden („angemessenen“) Datenschutzes bei der Stellenleitung. Von ihr wird erwartet, dass die vom Gesetzgeber formulierten Schutznormen auf die technischen Gegebenheiten fehlerfrei übersetzt und gewährleistet werden (Gewährleistungspflicht nach § 61 Abs. 4 SGB VIII). Der Betrieb elektronischer Datenerfassungsanlagen im Umfeld von Leistungen des SGB muss den geltenden Bestimmungen (StGB, SGB I, VIII und X) entsprechen.
2. Beratungsstelle mit PC, ohne administrative Fachkraft, mit Netzwerk
In dieser Variante liegt die Verantwortung für die Einhaltung eines zureichenden Datenschutzes bei der Stellenleitung. Die Einrichtung und der Betrieb eines Netzwerkes ohne zureichende Kenntnisse darf, in Anbetracht der tief greifenden Zugriffsmöglichkeiten auf die Daten anderer im Netz befindlicher PC, juristisch als grob fahrlässig gewertet werden.
3. Beratungsstelle mit PC, administrativer Fachkraft und Netzwerk
In dieser Variante kann die Verantwortung für die Einhaltung eines zureichenden Datenschutzes von Stellenleitung und Netzwerk-Administration gemeinsam wahrgenommen werden oder einseitig bei der Administration liegen. Die tatsächliche Verantwortlichkeit muss durch eine Betriebsvereinbarung geregelt sein.
4. Sonderfall Internetzugang
Einen Sonderfall der Vernetzung stellt der Zugang zum Internet dar, also die Vernetzung des lokalen Rechners oder Netzwerkes mit dem weltweiten Internet. Verantwortlich ist die Stellenleitung, sofern die Abtretung an eine spezialisierte administrative Fachkraft nicht geregelt ist.

Die hieraus folgenden Gefahren bzw. notwendigen Vorkehrungen sind Thema der folgenden Ausführungen.

Datensicherheit und Internet

Die Vernetzung von Rechnern verlangt besondere Sicherheitsvorkehrungen, weil die lokalen Daten im Falle einer Vernetzung (insbesondere zum Internet) spezifischen Gefahren ausgesetzt sind:

- Durch das Einschleusen von Schadroutinen (das sind ausführbare Programme, die auf dem PC Schäden verursachen, dazu zählen Viren, Würmern, Trojaner) werden die Datenbestände gelöscht.

- Durch das Einschleusen von Schadroutinen können die Tastaturanschläge abgehört und an einen Rechner im Internet gesendet werden (d.h. alles, was auf dem befallenen PC geschrieben wird, wird von sogenannter SpyWare oder einigen spezialisierten Trojanern „mitgeschrieben“ und an die Autoren der Schadroutinen gesendet).
- Durch das Einschleusen von Schadroutinen (z.B: sogenannte Remote-Software wie SubSeven) kann der Rechner ferngesteuert werden, womit der uneingeschränkte Zugriff auf den befallenen PC gelingt und alle darauf vorhandenen Datenbestände über das Internet eingesehen und übertragen werden können (Datendiebstahl) sowie die Funktionsfähigkeit des PC eingeschränkt werden kann (z.B: ferngesteuertes Abschalten von Schutzmaßnahmen).

Bei bestehender Verbindung zum Internet kann den oben beschriebenen Gefahren durch die beiden nachstehend genannten Verfahrensvarianten begegnet werden:

- Ein (alter) PC wird exklusiv zur Verbindungsaufnahme mit dem Internet abgestellt, auf diesem PC befindet sich keinerlei sensibles, personenbezogenes Datenmaterial.
- Der PC wird durch eine Kombination technischer Maßnahmen vor (lesenden und schreibenden) Zugriffen aus dem Netzwerk (oder dem Internet) geschützt (z.B. durch Einsatz einer Firewall, Antivirensoftware, restriktive Browsereinstellungen etc.).

Betriebsvereinbarungen als Richtlinien zu Datenschutz und Datensicherheit

Eine Betriebsvereinbarung regelt nicht nur den Betrieb der Verarbeitung sensibler und/oder personenbezogener Daten auf Personalcomputern, sondern auch die Zuständigkeiten von Personen innerhalb der betrieblichen Organisation. Der Vorteil einer Betriebsvereinbarung besteht vor allem darin, dass

- die verantwortlichen Personen mit ihren Zuständigkeiten benannt sind,
- die Organisation der Datenerfassung beschrieben ist,
- die Vereinbarung regelmäßig angepasst werden muss,
- die Mitarbeitenden hinsichtlich der Einhaltung der geltenden Schutznormen abgesichert sind.

Die folgende Aufstellung gibt einen Überblick über Regelungen, die Inhalt einer Betriebsvereinbarung sein sollten:

- Die Regelung der Aufbewahrungs- und Löschvorschriften für papiergebundene Dateien.
- Die Regelung der Aufbewahrungs- und Löschvorschriften für elektronische Dateien.
- Die Regelung der Kriterien der Aufstellung von Personalcomputer in den Dienst- und Kontakträumen (Sichtschutz, Zugangssperre etc.).
- Die Regelung von Vorschriften zur technischen Sicherung von Daten (Datenträgerkontrolle, Zugriffskontrolle, Eingabekontrolle etc.).
- Die formale Verpflichtung der Mitarbeitenden auf die in der Institution geltenden Datenschutzvorschriften.
- Die Regelung der Vernichtung elektronischer Datenträger (nicht mehr gebrauchte Disketten, Festplatten, CD, Magnetbänder oder andere Massenspeicher).
- Die Darstellung der Gefahren der elektronischen Datenverarbeitung bei lokal vernetzten Arbeitsplätzen,
- Die Darstellung der Gefahren bei mit dem Internet vernetzten Arbeitsplätzen.
- Die Regelung der Nutzung des Internet während der Arbeitszeit sowie die private Nutzung, sofern diese erlaubt ist (z.B. Verbot des Aufrufs gewaltverherrlichender, rassistischer und pornografischer Inhalte etc.).
- Die Regelung der Nutzung von speziellen Anwendungen (z.B. Online-Beratung, Online-Statistik etc.).

Technische Grundlagen der Datensicherheit

Zur Verdeutlichung, welche Implikationen mit der Wahl der Technik verbunden sind, sei an dieser Stelle auf häufig verwendete Begriffe und deren Definitionen hingewiesen:
Mit Datensicherheit in der Informationstechnik (IT) wird allgemein der technische Schutz von Daten bezeichnet, der verschiedene Anforderungen erfüllen muss hinsichtlich...

Vertraulichkeit: Vertrauliche Informationen müssen vor unbefugter Einsicht geschützt sein.
Verfügbarkeit: Dem Benutzer stehen die Dienstleistungen und Funktionen des IT-Systems zum erforderlichen Zeitpunkt (z.B: während der gesamten Arbeitszeit oder nur zu festgelegten Zeiten) zur Verfügung.
Integrität: Die Daten stehen vollständig und unverändert zur Verfügung. Der Verlust der Integrität von Informationen bedeutet, dass diese entweder unerlaubt verändert oder Angaben zum Autor verfälscht wurden oder der Zeitpunkt der Erstellung oder letzten Änderung manipuliert wurde.

Die drei zentralen Grundlagen werden durch weitere Kriterien ergänzt:

Authentisierung: Bei der Anmeldung an einem System wird im Rahmen der Authentisierung die Identität der Person geprüft und verifiziert (Kennwort und Passwort, evtl. weitere Kennwörter usw.).
Autorisierung: Bei einer Autorisierung wird geprüft, ob eine Person, IT-Komponente oder Anwendung zur Durchführung einer bestimmten Aktion berechtigt ist, d.h. diese Form der Sicherstellung betrifft auch technische Geräte oder Prozesse.
Datensicherung (engl. Backup): Bei einer Datensicherung werden zum Schutz vor Datenverlust Sicherungskopien der vorhandenen Datenbeständen von dazu berechtigten Personen erstellt.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt ein umfassendes, detailliertes, fortlaufend aktualisiertes Grundschutzhandbuch (www.bsi.de/gshb/deutsch/menue.htm) heraus. Dort sind die konkreten Gefährdungslagen verschiedener IT-Systeme aufgelistet, differenziert nach höherer Gewalt, organisatorischen Mängeln, technischem Versagen, menschlicher Fehlhandlungen und vorsätzlicher Handlungen. Es werden geeignete Maßnahmen empfohlen, um die jeweilige Gefährdung auszuschalten oder das Gefahrenrisiko erheblich zu minimieren.

Das Grundschutzhandbuch richtet sich an Fachleute und fortgeschrittene Anwender. Die Realisierung der einschlägigen Empfehlungen des Grundschutzhandbuchs erhöht die Datensicherheit um ein Vielfaches und gewährleistet einen weitestgehend sicheren Betrieb.

Darüber hinaus veröffentlicht das BSI einen Leitfaden „IT-Sicherheit – IT-Grundschutz kompakt“ (www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf). Er listet die häufigsten Versäumnisse auf und empfiehlt wichtige Sicherheitsmaßnahmen, welche auch für Laien übersichtlich und verständlich dargestellt sind. Im Anhang dieses Leitfadens befinden sich übersichtliche Prüflisten zur IT-Sicherheit. Durch Ankreuzen der gestellten Fragen ergibt sich schnell ein Überblick, welche Verbesserungen notwendig sind, und welche Maßnahmen gegebenenfalls durchgeführt werden müssen. Normales Anwendungswissen reicht aus, um bei den jeweils eingesetzten IT-Systemen anhand dieses Leitfadens eine bereits weit reichende Sicherheit zu gewährleisten.

PC-Systeme

Der PC wird in in aller Regel in einem Zustand ausgeliefert, bei dem zahlreiche für die Sicherheit erforderlichen Einstellungen deaktiviert sind. Bereits bei der ersten Inbetriebnahme müssen notwendige Sicherheitseinstellungen aktiviert werden. Empfohlen wird die Aktivierung des so genannten „BIOS-Passwort“ (ohne Eingabe des Passwortes kann der Rechner nicht hoch gefahren werden), das Deaktivieren oder Beschränken einzelner Hardware-Geräte im BIOS oder im Betriebssystem (zum Beispiel das Abschalten von Diskettenlaufwerken, wenn das Kopieren von Datenbestände auf diesen Datenträger verhindert werden soll), das Einrichten einer differenzierten Benutzer-, Verzeichnis- und Datenverwaltung (besonders im Netzwerk), das Einschränken oder Abschalten einzelner Dienste (z.B. der Dienst zur Übermittlung interner Nachrichten) oder das Anlegen automatisch verschlüsselter Dateisysteme für vertrauliche Daten, um nur einige der in Frage kommenden Maßnahmen zu nennen.

Die auf dem Markt erhältlichen Betriebssysteme sind in unterschiedlicher Weise in der Lage, die gestellten Anforderungen an die IT-Sicherheit zu erfüllen. Sofern notwendige Funktionen oder Fehlerkorrekturen fehlen, was insbesondere bei nicht mehr unterstützten (Alt)Versionen der Fall ist (z.B: Windows 95, 98, NT), müssen zusätzliche Programme installiert sein. Auch hier gibt das Grundschutzhandbuch des BSI die passenden Empfehlungen.

Neuerdings stellen alle Hersteller aufgrund des gewachsenen Sicherheitsbewusstseins regelmäßig Updates zur Verfügung, um bekannt gewordene Sicherheitslücken zu schließen. Es wird dringend empfohlen, das Betriebssystem regelmäßig zu aktualisieren. Allerdings stellt die Aktualisierung des Betriebssystems über das Internet selbst eine Sicherheitslücke dar, weil für diesen Vorgang dem Hersteller während der Updatezeit alle wichtigen Zugriffsrechte auf das lokale System und den dort gespeicherten Daten eingeräumt werden. Eine aktuelle Betriebsvereinbarung sollte deshalb auch den Aktualisierungsmodus regeln. Innerhalb lokaler Netzwerke kann dafür gesorgt werden, dass die angeschlossenen PC (Clients) die Sicherheitsupdates aus dem lokalen Netz beziehen und die Sicherheitslücke somit umgehen.

Lokales Netzwerk

Werden PCs innerhalb einer räumlich abgegrenzten Einheit (Wohnung, Haus, Betriebsgebäude) vernetzt, spricht man von einem LAN (Local Area Network). Netzwerke sind heute weit verbreitet, auch in Beratungsstellen. Die meisten Netze nutzen das Internet-Protokoll (TCP/IP-Netzwerk, auch Intranet genannt) zum Datenaustausch. Ein Protokoll ist eine Sammlung technischer Verfahrensregeln und Funktionen, mittels derer Rechner in der Lage sind, die gewünschten Aufgaben zu erledigen. Bestimmte Dienste oder Programme werden über einen so genannten „Server“ den angeschlossenen PC (Clients) zur Verfügung gestellt (Client-Server-Struktur). Sowohl Einrichtung wie Wartung eines Netzwerkes erfordern professionelle, einschlägige Fachkenntnisse. Für die Mitarbeitenden ist eine spezielle Einweisung (Schulung) in den Umgang mit den Netzwerkdiensten unverzichtbar.

Einerseits erhöht die Vernetzung die Gefährdungsmomente für die Datensicherheit, andererseits garantieren gut gewartete und professionell eingerichtete Server eine insgesamt höhere Datensicherheit als die Datenverarbeitung auf unvernetzten PC.

Internet

Durch den Internetzugang entstehen weitere, spezifische Gefährdungssituationen für die Datensicherheit, die technisch und organisatorisch zu bewältigen sind. Die einfachste Variante besteht darin, einen einzelnen (älteren) PC exklusiv für diese Aufgabe zu reservieren. Sobald aber Funktionalitäten wie Mail- oder Webserverdienste (WWW, auch umgangssprachlich Internet genannt) an mehreren Arbeitsplätzen erforderlich sind, müssen diese Internetdienste über das interne Netzwerk erreichbar sein. Die Abschottung des internen Netzwerkes (LAN) gegen die Gefahren aus dem Internet (WAN, Wide Area Network) übernimmt dabei eine Firewall, die ausschließlich die benötigten Dienste zulässt (z.B.: Mail, WWW) und dafür sorgt, dass ein PC im lokalen Netzwerk nicht direkt über das Internet erreicht werden kann. Die Einrichtung einer Firewall setzt einschlägige Fachkenntnisse voraus.

Doch auch der durch eine Firewall geschützte PC bleibt über die Inhalte der zugelassenen Dienste (Mail, WWW und Download (FTP)) weiterhin gefährdet. Anhänge eingehender Mails können Viren oder andere Schadroutinen enthalten, aufgerufene Internetseiten können einen präparierten Code enthalten, der Zugriff auf den Rechner erlaubt und vieles mehr. Grundsätzlich sollen Mailanhänge mit einem aktuellen Virenprogramm überprüft werden, am besten automatisiert und noch vor der Anzeige im Mailprogramm.

Auch der auf dem Rechner eingesetzte Browser kann fehlerhaft programmiert sein und gravierende Sicherheitslücken aufweisen. Deshalb ist bei der Konfiguration der Internetsoftware (Browser und E-Mail-Programm) besondere Sorgfalt angebracht und eine „restriktive“ Konfiguration zu bevorzugen. Alternativ zum gebräuchlichen Internet Explorer von Microsoft können die

Browser „Mozilla“ (Netscape) oder „Opera“ verwendet werden, gleiches gilt für alternative Mailprogramme.

Die Liste der Gefährdungsmomente zeigt, dass Anwender eine spezielle Schulung brauchen, um sicherheits- und verantwortungsbewusst zu arbeiten und in der Lage sind, eine vernünftige „angemessene“ Gefahreneinschätzung vorzunehmen.

Beratung über das Internet

Die Erbringung von Beratungsleistungen unter Einsatz der Dienste des Internet bedarf einer gesonderten Betrachtung. Derzeit stehen dafür zur Verfügung: E-Mail, Chat und Forum. Entsprechende Software ist leicht erhältlich; aus datenschutzrechtlicher Sicht ist ihre Nutzung aber nicht unproblematisch.

E-Mail-Beratung

Ratsuchende nutzen die neuen technischen Möglichkeiten und bringen ihre Fragen zu Erziehungsproblemen auch per E-Mail zum Ausdruck, wenn Beratungsstellen auf diesem Wege erreichbar sind. Beratungsstellen die Beratungen mit gängigen E-Mail-Programmen (z.B. Outlook, Mozilla) durchführen, müssen in Rechnung stellen, dass diese Form der Kommunikation sowohl die Möglichkeit des Mitlesens des Datenverkehrs ermöglicht als auch die Reidentifikation des Senders zulässt.

Bei einer E-Mail wird nicht nur ein komplettes Dokument verschickt, es können auch zusätzlich Anlagen versandt werden. Beides kann im Internet durch unbefugte Dritte abgefangen und eingesehen werden, ohne dass der Empfänger bemerkt, dass seine Mail gelesen wurde. Die für den Mailaustausch benutzten Protokolle smtp und pop3 sind von Hause aus unverschlüsselt. Eine Verschlüsselung der Nachricht ist nur möglich, wenn beide Seiten (Sender und Empfänger) ein Schema zur Verschlüsselung vereinbaren und die zur Entschlüsselung notwendigen Schlüssel austauschen (z.B. pgp). Ein einseitiges Aufsetzen von Sicherheitsmaßnahmen greift nicht; in diesem Fall empfängt die Gegenseite die versandte Mail unverschlüsselt. Eine Verschlüsselung von E-Mails ist hochschwellig, weil beide Seiten vor dem Austausch der Inhalte zunächst die Sicherheitsstandards austauschen müssen. Zudem hat der Anbieter einer E-Mail-Beratung keine Garantie, dass der Ratsuchende die angebotenen Sicherheitsstandards auch auf seinem PC installiert.

Darüber hinaus erlauben Mailadressen häufig einen Rückschluss auf die reale Person durch Angabe von Vor- und Nachname als Adressteil; immer aber offenbart die Adresse den Besitzer des Postfachs (Account) beim jeweiligen Provider. Dies ist für einen Datenspion eine wichtige Information. In der Vergangenheit sind schon mehrfach durch Sicherheitslücken (z.B. entsprachen die Zugangsdaten den Adressdaten oder die Passwörter konnten erraten werden) die Daten der Konteninhaber ausgespäht wurden, die beim Provider im Klartext vorliegen (Name, Adresse, Telefonnummer, Geburtsdatum etc.). Mit anderen Worten: die Re-Identifikation des Senders ist bei keinem der Internetdienste ähnlich leicht zu bewerkstelligen wie beim E-Mail-Dienst.

Die Beratungsstellen bleiben aber datenschutzrechlich in der Pflicht, die Bedingungen einer Beratung so zu gestalten, dass das Privatgeheimnis der Ratsuchenden geschützt ist. Bei einer Beratung per E-Mail kann dies nicht garantiert werden. E-Mail-Beratung entspricht nicht den Anforderungen des Datenschutzes.

Eine Alternative bietet die so genannte webbasierte Mail. Hier loggt der Ratsuchende sich auf dem Server eines Beratungssystems ein und schreibt seine Anfrage in eine Maske innerhalb des Systems. Es wird daher physikalisch keine Nachricht von A nach B verschickt, sondern der Inhalt direkt auf dem Server abgelegt. Zwischen dem Ratsuchenden (technisch: dem Client) und der Beratungsfachkraft (technisch: der Serverseite) wird allerdings auch ein Datenstrom ausgetauscht. Technische Grundlage ist das http-Protokoll. Damit ein unbefugtes Mitlesen Dritter ausgeschlossen werden kann, muss dieser Datenaustausch verschlüsselt werden. Dafür steht die SSL-Verschlüsselung, wie sie heute bei Banken üblich ist, zur Verfügung. (SSL steht für Secure Socket Layer und beschreibt ein von der Firma Netscape entwickeltes Übertragungsprotokoll, mit dem verschlüsselte Kommunikation mittels so genanntem Tunneling möglich ist, d.h. SSL baut eine sichere Verbindung zwischen Server und Client auf. Die Verschlüsselung erfolgt über ein Zertifikat, das kostenpflichtig bei einer Zertifizierungsinstanz (einem Trust-Center) gekauft werden muss.) Für eine SSL-Verschlüsselung des http-Protokolls muss der Ratsuchende (Client) keinerlei zusätzliche Technik installieren. Das Beratungsangebot kann ohne technische Kenntnis allein durch Angabe eines frei wählbaren Nicknamens und eines selbstdefinierten Passworts in Anspruch genommen werden.

Beratung im Chat

Bei einem Chat werden zwischen den Teilnehmern in Echtzeit Datenströme ausgetauscht: Bei Nutzung des Standardprotokolls IRC werden diese Daten unverschlüsselt zwischen Server und Client übertragen. Die Datenströme können personenbezogene oder auf reale Personen beziehbare Angaben enthalten, die von Dritten mitgelesen werden können. Der Schutz des Privatgeheimnisses der Ratsuchenden kann hier nur gewährleistet werden, wenn die Daten verschlüsselt übertragen werden. Derzeit existiert jedoch kein verschlüsseltes Chat-Protokoll. Ein verschlüsselter Beratungschat muss daher auf der Basis des http-Protokolls unter Verwendung der SSL-Verschlüsselung grundständig programmiert werden (https = hyper text transfer protokoll over secure socket layer). Dies wird für einzelne Beratungsstellen kaum zu leisten sein. Beratung in einem Chat setzt professionell programmierte Software voraus.

Diskussionsforum

Das Forum ist vom Grundsatz her eine öffentliche Informationsplattform, die Beiträge werden von den Nutzern, die sich persönlich angemeldet haben (registrierte Mitglieder der Community) eingestellt und können gegenseitig aber meist auch von Nicht-Mitgliedern gelesen werden. Die erforderliche Software steht frei verfügbar und in verschiedenen Varianten in den Technik-Foren im Internet zur Verfügung. Auch wenn alle veröffentlichen Nachrichten (Postings)

vom Verfasser zum Mitlesen freigegeben sind, ergeben sich dennoch datenschutzrechtliche Themen: Wenn im Rahmen der Postings Informationen über dritte Personen gegeben werden, kann es erforderlich sein, zum Schutz des informationellen Selbstbestimmungsrechts dieser Personen solche Angaben zu löschen. Deshalb ist es erforderlich, im Vorspann des Angebotes auf die Teilnahmebedingungen und Spielregeln hinzuweisen. Um den Anforderungen des Datenschutzes gerecht zu werden (im Beratungskontext darüber hinaus auch aus fachlich-konzeptionellen Gründen) muss eine Moderation des Forums sicher gestellt sein. Auf die datenschützende „Eingriffspflicht" der Moderatorinnen muss in den Nutzungsbedingungen ebenfalls hingewiesen werden.

Spezielle Fachsoftware

In den Erziehung- und Familienberatungsstellen kommt spezifische Fachsoftware zum Einsatz – Klientenverwaltungen, diagnostische Testprogramme – in der höchst sensible Daten verarbeitet und gespeichert werden. Für diese Fachanwendungen wie deren Betrieb muss eine konkrete Risikoanalyse erstellt werden. Die Abnahme muss durch den zuständigen Datenschutzbeauftragten erfolgen, fast immer in Zusammenarbeit mit den Administrationskräften. Die beim Einsatz dieser Spezialsoftware zu treffenden Maßnahmen sind bereits bei der Organisationskontrolle benannt worden.

Begleitende Maßnahmen beinhalten unter anderem:

- Vereinbarung zu Wartung und Updates der Fachverfahren
- Ausführliche Dokumentation der Fachsoftware (auch die technischen Grundlagen betreffend)
- Betriebliche Vereinbarungen zum Betrieb der Fachsoftware (Installation, Benennung der zugangsberechtigten Personen, Speicherung der Daten, Sicherungskopien etc.)
- Schulungen zur Fachanwendung und besonderer Berücksichtigung der Aspekte „Datenschutz und Datensicherheit".

Die Realisierung dieser Aufgaben erfordert die enge Zusammenarbeit zwischen und Abstimmung mit der Stellenleitung, dem Träger, den Mitarbeitenden, der EDV-Abteilung sowie (fast immer) der Personal- oder Mitarbeitervertretung.

Alternative Anwendungen und Betriebssysteme

Alternative Betriebssysteme sind aktuell in aller Munde, weil die mehrheitlich eingesetzten Windows-Betriebssysteme immer wieder Opfer massiver und systemkritischer Attacken werden und von einem Teil der Sicherheitsexperten als „unsicher" eingestuft sind.

Wodurch lassen sich „sichere" von „unsicheren" Betriebssystemen unterscheiden?

Zunächst gilt, dass sichere Betriebssysteme Attacken über eine bestimmte Zeit (Stabilität) oder ohne Zugriffs- und Änderungsmöglichkeit auf systemkritische Datenbestände (Integrität) standhalten müssen. Bekannte Lücken des Betriebssystems müssen offen dokumentiert sein. Die Anwender müssen regelmäßig mit Ergänzungen (Patches) versorgt werden, die die bekannten Lücken schließen.

Alternative und im Büroalltag verwendbare Betriebssysteme sind Linux und MacOS (Apple MacIntosh). Beide Betriebssysteme kommen aus der Unix-Welt und gelten als sicher. Allerdings erfordert die Administration eines Linuxsystems spezielle Kenntnisse, weshalb Windows-Anwendern der Umstieg schwer fallen dürfte. Für diese Betriebssysteme gibt es ein ganzes Bündel von Office-Anwendungen (Textverarbeitung Tabellenkalkulation, Präsentation, Datenbanken etc.), die den Datenaustausch mit anderen Office-Produkten problemlos ermöglichen (d.h. Fremddateien können problemlos gelesen und im gleichen Format geschrieben werden).

Beim Einsatz der als unsicher eingestuften Betriebssysteme kompensieren alternative Verfahrensweisen die dort vorhandenen Mängel, wenn auch teilweise mit erheblichem Aufwand und technisch nicht immer zufriedenstellend. Eine der Möglichkeiten besteht in der Trennung der unsensiblen von den sensiblen Daten, erstere werden auf dem eigenen Rechner gelagert, letztere auf speziell abgesicherten Maschinen im Netzwerk (sofern vorhanden) unter Einsatz von Unix- oder Linux-Betriebssystemen. Die Kopplung verschiedener Betriebssysteme ist problemlos möglich, muss aber von spezialisiertem Personal eingerichtet und gewartet werden.

Ein anderer Weg führt über das „unsichere" Internet: mit Hilfe dieses weltweiten Netzwerkes können Datenbestände ebenfalls in der oben beschriebenen Weise getrennt werden. Allerdings muss die Übertragung der Daten verschlüsselt erfolgen, damit Unbefugte den übertragenen Inhalt nicht mitlesen können.

Während ein PC nur schlecht gegen Diebstahl gesichert werden kann, gelingt dies mit mobilen Datenträgern (Diskette, Wechselplatte, CD-RW) sehr einfach. Es muss geprüft werden, ob die zum Einsatz kommenden Klientenverwaltungsprogramme konfiguriert werden können, die erzeugten Datenbestände (ausschließlich) auf einem mobilen Datenträger zu speichern. Vielfach zeigt sich hier ein erstes Hindernis: Der durch das Spezialprogramm erzeugte Datenbestand ist größer als das Fassungsvermögen des mobilen Datenträgers. Gelegentlich sind auch Zugriffsprobleme (Geschwindigkeit, Datendurchsatz, eindeutige Kennung des Datenträgers) der Grund für ein Scheitern.

Letztlich bleibt der Nutzer das größte Anwendungsrisiko: Die Durchführung all der Vorschriften und Regeln liegt in seiner Hand; hängt von seinem Verständnis der Materie und seiner Sorgfalt ab.

Literatur

bke (1995a): Datenschutz, Schweigefplicht und Zeugnisverweigerungsrecht. In: bke (1997): Rechtsfragen in der Beratung, Fürth, S. 16-22.

bke (1995b): Bedeutung der Datenschutzregelungen des KJHG für die Erziehungsberatungsstellen. In: bke (1997): Rechtsfragen in der Beratung, Fürth, S. 23-33.

www.bsi.de

Anhang: Drei Checklisten

1: Formale Voraussetzungen

- Wie lauten die Aufbewahrungs- und Löschvorschriften für papiergebundene Dateien?
- Wie lauten die Aufbewahrungs- und Löschvorschriften für elektronische Dateien?
- Wie lauten die Anweisungen zur (räumlichen) Aufstellung von Personalcomputern in den Dienst- und Kontakträumen?
- Wie lauten die Vorschriften zur Sicherung von auf dem Monitor angezeigter Daten bei Abwesenheit vom Arbeitsplatz (z.B. Passwort für das temporäre Verriegeln des Bildschirms etc.)?
- In welcher Form werden die Mitarbeitenden auf die in der Institution geltenden Datenschutzvorschriften verpflichtet?
- Wie lauten die Vorschriften zur Vernichtung elektronischer Datenträger (Disketten, Festplatten, CD, Magnetbänder oder andere Massenspeicher)?
- In welcher Form wird über die Gefahren der elektronischen Datenverarbeitung bei lokal vernetzten Arbeitsplätzen unterrichtet?
- In welcher Form wird über die besonderen Gefahren der elektronischen Datenverarbeitung bei mit dem Internet vernetzten Arbeitsplätzen unterrichtet?
- Wie lauten die Vorschriften zur inhaltlichen Nutzung des Internet während der Arbeitszeit und außerhalb der Arbeitszeit (z.B. Verbot des Aufrufs gewaltverherrlichender, rassistischer und pornografischer Inhalte etc.)?
- Wie lauten die Vorschriften zur beruflichen Nutzung des Internet bei Einsatz spezieller, über das Internet angebotener Software (z.B. Online-Beratung, Online-Statistik etc.)?

2: Technische Procedere

- Werden sensible Daten (so genannte Hilfsmerkmale) ausschließlich auf geschützte Datenträger gespeichert?
- Werden Berichte und Gutachten sowie andere Schriftstücke, die Merkmale einer realen Person enthalten, ausschließlich auf geschützte Datenträger gespeichert?
- Sind die in den Beratungsstellen verwendeten Statistik- und Klientenverwaltungssysteme so konfigurierbar, dass die erzeugten Datenbestände ausschließlich auf geschützte Datenträger oder (ausschließlich) auf speziell gesicherte Rechner im Netzwerk gespeichert werden können?
- Sind die in den Beratungsstellen benutzten Klientenverwaltungssysteme so konfigurierbar, dass Felder mit Hilfsmerkmalen (z.B. Geburtsdatum, PLZ und Ort usw.) unvollständige Angaben (z.B. nur das Geburtsjahr, nur dreistellige PLZ) ohne Fehlermeldung entgegennehmen können?
- Werden Datenträger regelmäßig ausgetauscht bzw. gewartet (um Löschung durch Verschleiß vorzubeugen)?
- Werden wichtige Daten redundant (mehrfach) vorgehalten und existieren festgelegte Procedere zur Erzeugung der erforderlichen Sicherungskopien?
- Werden mobile Datenträger (Disketten, CD, Magnetband, Kompaktdisketten wie z.B. ZIP) während des Zugangs zum Internet aus dem Rechner entfernt?
- Werden mobile Datenträger nach Beendigung der Arbeit aus dem Rechner entfernt und verschlossen?
- Werden mobile Datenträger in besonderer Weise gegen Diebstahl gesichert (Stahlschrank, Tresor etc.)?
- Ist der Zugang zu den mobilen Datenträgern gegenüber den Mitarbeitenden der Beratungsstelle geregelt?

3: Betriebliche Regelungen und Vereinbarungen

Über die mit dem Träger geschlossene Betriebsvereinbarung soll sichergestellt werden, dass

- der Träger für die insgesamt zu treffenden Sicherheitsvorkehrungen verantwortlich ist (und bleibt),
- geregelt wird, wer für den Schutz der in den Beratungsstellen verarbeiteten Daten verantwortlich ist,
- der Träger fachlich versiertes Personal zur technischen Administration vorhält,
- die Mitarbeitenden über (regelmäßige) Schulungen mit der Umsetzung der Vorschriften der betrieblichen Vereinbarung vertraut gemacht werden,
- Netzwerke nur dann zum Einsatz kommen, wenn sowohl beim Träger wie auch in der Beratungsstelle Personen mit speziellen Kenntnissen verfügbar sind,
- der Zugang zum Internet nur bei Einsatz einer Firewall erlaubt ist,
- in den Beratungsstellen nur Betriebssysteme zum Einsatz kommen, die den Sicherheitshinweisen des BSI (oder vergleichbarer Institutionen) entsprechen,
- der Datenzugriff über die Benennung der dafür berechtigten Personen geregelt ist.

Ziel der betrieblichen Vereinbarung ist – im Zusammenhang mit dem Betrieb einer sozialen Beratungsstelle – der Schutz der persönlichen Daten der Ratsuchenden. Die konkreten Anweisungen nehmen dabei Rücksicht auf die technischen Gegebenheiten vor Ort und leiten hieraus die erforderlichen (Schutz)Maßnahmen ab. Die Ableitungen müssen geeignet sein, das Verhalten der Mitarbeitenden konkret anzuleiten. Weiterhin müssen die Anleitungen so formuliert sein, dass sie von Laien verstanden und umgesetzt werden können.

Fürth, den 2. August 2004