

Wegen der vom Internet ausgehenden Gefahren für Datenbestände war es zunächst strittig, ob an den Schulen an Verwaltungsrechnern mit Zugriffsmöglichkeit auf personenbezogene Daten ein Internetzugang zulässig sei. Die Frage wurde mittlerweile beantwortet. Gleichzeitig wurde ein Katalog von Schutzmaßnahmen vor unerwünschten Zugriffen erarbeitet.

Datenschutzverpflichtungen der Schulen:

Die Schulen haben technische und organisatorische Maßnahmen dafür zu treffen, dass die bei ihnen gespeicherten personenbezogenen Daten (Schülerdatei, Kollegstufendatei, Lehrerdatei, aber auch Schulkorrespondenz mit personenbezogenen Daten) vor Verlust und vor Missbrauch geschützt werden. (Erläuternde Hinweise, Abschnitt 6.1a, Fundstelle s.u.)

Besondere Schutzmaßnahmen vor unerwünschten Zugriffen sind bei einem Internetzugang eines Rechners mit Zugriffsmöglichkeit auf personenbezogene Daten zu treffen. Die Verantwortung hierfür liegt bei der Schule. (Erläuternde Hinweise, Abschnitt 6.1c)

Technische Schutzmaßnahmen:

Technische Schutzmaßnahmen können beispielsweise darin bestehen, dass

- der Internetzugang für die Schulverwaltung mit einem eigenen Mail-Server für die Schulverwaltung abgewickelt wird, der mit einem nur der Schulverwaltung bekannten Passwort hochzufahren ist und nur über einen festen Port mit dem Verwaltungsrechner bzw. dem Verwaltungsserver kommunizieren kann;
- programmmäßig nur eingeschränkte Dienste zugelassen werden (z.B. nur E-Mails);
- der gesamte Datenverkehr zwischen Internet und Verwaltungsbereich protokolliert wird (also alle tatsächlichen und alle versuchten Zugriffe von innen und außen) und diese Protokolle gezielt stichprobenweise sowie anlassbezogen (z.B. bei Verdacht auf missbräuchliche oder sicherheitsgefährdende Nutzung des Internet-Zugangs) überprüft werden (die am Verwaltungsrechner arbeitenden Personen sind darüber zu informieren, s.u.);
- der gesamte Datenverkehr zwischen Internet und Verwaltungsbereich geprüft wird (z.B. durch Virens Scanner);
- programmmäßig der Zugriff auf als sicher bekannte Adressen beschränkt wird (also z.B. auf Schulaufsichtsbehörden, Landesamt für Statistik und Datenverarbeitung, Akademie für Lehrerfortbildung und Personalführung Dillingen, Institut für Schulpädagogik und Bildungsforschung, bestimmte andere Schulen) und jeweils eine Authentifizierung des Kommunikationspartners erfolgt (z.B. durch eine kryptierte Kennung);
- Dateien mit Anhängen eines nicht als sicher bekannten und zuverlässig identifizierten Absenders programmmäßig zurückgewiesen oder auf den Mail-Server des Unterrichtsnetzes umgelenkt werden (vor einer anschließenden eventuellen Übernahme ins Verwaltungsnetz sind derartige Anhänge sorgfältig auf Viren und sonstige unerwünschte Nebenwirkungen hin zu untersuchen);
- der Verwaltungsrechner nicht rund um die Uhr online ist, sondern vielmehr die Verbindung zum Provider nur bei Bedarf aufgebaut wird (z.B. zeitlich begrenzter Wahl-Zugang);
- keine nach außen bekannte, feste IP-Adresse verwendet wird (Auswahl eines Providers mit dynamischer IP-Adressverwaltung);
- Verwaltungsrechner mit Internetzugang mit einem eigenen Passwort vor unbefugter Inbetriebnahme geschützt werden; zusätzlich durch geeignete Software vor unbefugter

Inbetriebnahme schützen;

- ActiveX und Java-Funktionalität am Web-Browser standardmäßig ausgeschaltet werden. (Erläuternde Hinweise, Abschnitt 6.1c)

Organisatorische Schutzmaßnahmen:

Organisatorische Schutzmaßnahmen können etwa darin bestehen, dass

- die Verwaltungskräfte und ggf. gelegentlich an einem Verwaltungsrechner arbeitende Lehrkräfte durch eine Dienstanweisung verpflichtet werden, dort ausschließlich für die Schulverwaltung erforderliche dienstliche Internetzugriffe vorzunehmen (s.u.) und Downloads nur von E-Mails bestimmter explizit vorgegebener Stellen vorzunehmen.
- Sofern den Lehrern allgemein an einem ins Verwaltungsnetz integrierten Rechner ein lesender Zugriff auf Schülerdaten zur Verfügung gestellt wird (z. B. an Berufsschulen zur Abwicklung von Mahnungen), soll an diesem Rechner kein Internetzugang möglich sein.
- Ebenso soll an Rechnern des Unterrichtsnetzes kein Internetzugang möglich sein, wenn sie im Rahmen der Zeugniserstellung zur Erfassung von Zeugnisdaten verwendet werden.

(Erläuternde Hinweise, Abschnitt 6.1c)

E-Mails mit personenbezogenen Daten:

Die Versendung von Schulkorrespondenz mit personenbezogenem oder sonstigem vertraulichen Inhalt mittels E-Mail ist wegen der offenen Struktur des Internets nur unter Anwendung einer Verschlüsselung zulässig, die den Schutz der Vertraulichkeit, Integrität und Authentizität ausreichend sicherstellt. (Erläuternde Hinweise, Abschnitt 6.1c)

Protokolldatei der Internetzugriffe:

Eine Protokollierung der von der Schule aus getätigten Internetzugriffe macht letztlich nur dann Sinn, wenn auch festgestellt werden kann, wer den Zugriff vorgenommen hat. Da damit eine Verarbeitung personenbezogener Daten der Rechnernutzer verbunden ist, war zu klären, ob eine derartige Datei datenschutzrechtlich zulässig ist, insbesondere auch in aus dem Blickwinkel der Verhältnismäßigkeit. Die Antwort auf diese Frage ist folgendermaßen ausgefallen:

Die Pflicht der Vorsorge gegen unerwünschte Einwirkungen aus dem Internet auf Verwaltungsrechner mit personenbezogenen Daten macht dort die Führung einer personenbezogenen Protokolldatei der Internetzugriffe sogar erforderlich. Die Lehrer und Verwaltungsangestellten sind darauf in geeigneter Weise hinzuweisen, etwa im Rahmen einer Belehrung, dass außerdienstliche bzw. nicht schulisch veranlasste Internetzugriffe am Verwaltungsrechner ausnahmslos unzulässig sind. (Erläuternde Hinweise, Abschnitt 4.1)

Schulverwaltung und Intranet:

Sollen die in der Schulverwaltung eingesetzten Rechner und Rechner für Unterrichtszwecke (insbesondere auch in Hinblick auf einen gemeinsamen Zugang zum Internet) an ein und dasselbe Intranet der Schule angeschlossen werden, so muss in besonderer Weise sichergestellt sein, dass aus dem Intranet unautorisierten Personen ein Zugriff auf personenbezogene Daten und die zugehörigen Programme nicht möglich ist. Die Verantwortung hierfür liegt bei der Schule. Ein optimaler Schutz wird nur in der physikalischen Trennung der Verwaltungs- und der Unterrichtsrechner gesehen. Netze für Schulverwaltung und Unterricht sind aber zumindest logisch zu trennen (z.B. Teilnetze mit gesicherten Übergängen).

Bei EDV-mäßiger Verwaltung von Lehrerdaten ist gemäß der Dienstvereinbarung mit dem Hauptpersonalrat die Einbindung von Rechnern für Verwaltungs- und Unterrichtszwecke in

ein einziges Netz nicht zulässig. (Erläuternde Hinweise, Abschnitt 6.1b)

Rechtsgrundlagen:

Die voranstehenden Ausführungen stützen sich auf die Datenschutzbestimmungen für Schulen. Diese sind in den „Erläuternden Hinweisen für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes“ zusammengestellt und erläutert (KWMBI I Nr. 9/2001 S. 112 und KWMBI I Nr. 20/2002 S 354). Die „Erläuternden Hinweise“ sind auf der CD der bayerischen Schulverwaltungsprogramme enthalten und können auf der Datenschutz-Homepage der bayerischen Schulverwaltungsprogramme (www.schule.bayern.de/winsv) aufgerufen werden.

Weitere Informationen:

Weitere Informationen zur „Sicherheit im Schulnetz“ können der gleichnamigen Broschüre der Akademie für Lehrerfortbildung und Personalführung in Dillingen entnommen werden, die auf der CD der bayerischen Schulverwaltungsprogramme enthalten ist, und den Artikeln und Beiträgen, die auf der Datenschutz-Homepage der bayerischen Schulverwaltungsprogramme (www.schule.bayern.de/winsv) aufgerufen werden können.