39. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

4.5.4 Beratung von Schulträgern bei der Einführung von Informationstechnik

Mit der Verordnung über die Verarbeitung personenbezogener Daten und statistische Erhebungen in Schulen aus dem Jahr 2009 sind auch die Schulträger, die ihren Schulen zentrale Dienstleistungen im IT-Bereich erbringen, mit neuen Fragestellungen konfrontiert worden. Einige Schulträger haben mich deswegen bei der Neugestaltung ihrer technischen Konzepte um eine enge datenschutzrechtliche Beratung gebeten und Einzelheiten ihrer technischen und organisatorischen Lösungen sehr intensiv mit mir diskutiert. Dabei sind in Detailfragen zum Teil beachtliche Fortschritte erzielt worden.

4.5.4.1 Ausgangslage

Zu der Wirkung der Verordnung über die Verarbeitung personenbezogener Daten und statistische Erhebungen in Schulen vom 4. Februar 2009 (ABl. 2009 S. 131) hatte ich bereits in meinem 38. Tätigkeitsbericht, Ziff. 4.5 und in der Broschüre „Datenschutz in Schulen“ detaillierte Ausführungen gemacht. Im Berichtszeitraum haben mich einige Schulträger um Beratung gebeten, damit sie bei der Entwicklung von Detailfragen ihrer Netzkonzepte alle datenschutzrechtlichen Fragestellungen schon frühzeitig berücksichtigen und Fehlentwicklungen vermeiden können.

Da die Ausgangslagen der Schulträger sowohl hinsichtlich der technischen Ausstattung als auch unter den Aspekten des möglichen Personal- und Sachmitteleinsatzes sehr verschieden sind und darüber hinaus sehr stark von der jeweiligen geografisch bestimmten Netzstruktur abhängen, entwickeln die Schulträger durchaus unterschiedliche Ansätze, um jeweils „ihre Lösung“ zu finden. Bei meiner Beurteilung und Begleitung der vorgelegten Lösungskonzepte habe ich unabhängig vom gewählten Weg feststellen können, dass die um Beratung nachsuchenden Schulträger sehr umfassend bemüht sind, die Umsetzung der neuen Erlasslage, das Schulgesetz und die datenschutzrechtlichen Vorgaben in ihren Konzepten vollständig zu berücksichtigen.

Einige nach den vorliegenden Erkenntnissen besonders gelungene Lösungen will ich an dieser Stelle als positive Beispiele – gerade auch für die Schulträger, die ihre Konzepte noch entwickeln – skizzieren.

4.5.4.2 Vorbildliches Gesamtkonzept des Main-Kinzig-Kreises

Der Main-Kinzig-Kreis hat mir bereits im vergangenen Jahr ein Gesamtkonzept vorgelegt, dem ich nach nur einem Abstimmungsgespräch uneingeschränkt zustimmen konnte.
Die Umsetzung wurde im Jahr 2010 fast vollständig abgeschlossen und die Schulen des Kreises sind im Bereich der Verwaltung mit einheitlicher Technik ausgestattet.

Die in der Kreisverwaltung vorhandene Infrastruktur erlaubte es der zuständigen Fachverwaltung einen Lösungsansatz zu wählen, bei dem jede Schule über ein geschlossenes Netzwerksegment mit eigenem VLAN-Bereich an die Kreisverwaltung angeschlossen ist und

am Standard-Arbeitsplatz weder ein Betriebssystem und die Anwendungssoftware noch die Daten vorgehalten werden müssen. Über die modernen Systeme ist es möglich, dass ein sog. Thin Client ohne eigene Festplatten sich das notwendige Betriebssystem aus dem Netz lädt. Die Anwendungen werden im Wesentlichen auf den Servern des Kreises betrieben und dem Benutzer über eine Terminalserver-Emulation zur Verfügung gestellt.

Je nach Schultyp und -größe wird zusätzlich mindestens ein vollwertiger Rechner mit verschlüsselten Festplatten als Datenaustauschstation und für bestimmte erweiterte Funktionen in den Schulen eingesetzt. Mit diesen Geräten können darüber hinaus bei einem Netzwerkausfall auch wichtige Aufgabenstellungen, wie z. B. die Vertretungsplanung, sichergestellt werden.

Insgesamt deckt das Konzept neben allen rechtlichen Vorgaben die Forderungen meines Eckpunktepapiers
„DV-Dienstleistungen für Schulen durch Schulträger und deren Auftragnehmer (Stand: 22. August 2008)“ ab:

- Trennung der Netze durch VLAN und den Einsatz von Firewalls,
- Schutz der Daten bei Gerätediebstahl durch eine zentrale Datenhaltung bzw. eine Verschlüsselung bei lokaler
  Speicherung,
- Umsetzung eines tagesaktuellen Virenschutzes,
- Kontrolle externer USB-Geräte durch den Einsatz einer entsprechenden Software,
- Einführung einer sicheren plattformbasierten Lösung für den häuslichen Arbeitsplatz (s. Ziff. 4.5.4.3),
- Zwischen dem Schulträger und den kreiseigenen Schulen wurden die Leistungen und wechselseitigen Verpflichtungen verbindlich geregelt.
- Der Schulträger hat ein Verfahren vorgesehen (s. Ziff. 4.5.4.4), das die notwendige Transparenz und Revisionssicherheit bei der Administration der Schulverwaltungsrechner bzw. Daten sicherstellt.

4.5.4.3 Plattformbasierte Zugriffe auf die Daten der Schulverwaltung am Heimarbeitsplatz

Die beschriebene Terminalserver-Lösung für die Verwaltungsarbeitsplätze macht sich der Schulträger auch bei der Gestaltung der Heimarbeitsplätze zunutze. Für die Einrichtung eines häuslichen Arbeitsplatzes ist nur die Installation eines Software-Clients auf dem Rechner erforderlich. Die Verbindung wird über einen verschlüsselten Zugriff (SSL) auf die Terminalserver-Plattform des Kreises hergestellt und zur Authentisierung der Benutzer wird zusätzlich zu dem verwendeten Passwort ein Token nach dem OTP-Standard eingesetzt. Da eine Anmeldung an den Servern der Kreisverwaltung über das Internet ohne das durch den Token generierte Einmal-Passwort nicht möglich ist, sind unbefugte Zugriffe auf diesem Weg sicher ausgeschlossen. Dennoch besteht auch bei dieser Konstellation für den Benutzer des Heimarbeitsplatzes die Verpflichtung, durch einen aktuellen Virenschutz sein System gegen Angriffe zu schützen und die anderen Vorgaben zum häuslichen Arbeitsplatz (s. Ziff. 4.5.3) zu erfüllen.

Eine Übertragung der Daten auf das lokale System am Heimarbeitsplatz wird durch entsprechende Einstellungen an den zentralen Systemen ausgeschlossen. Damit wird eines meiner wesentlichen Anliegen erfüllt, dass die Daten, die im Rahmen des § 3 Abs. 2 der Verordnung und deren Anlage 1, Ziff. 6 am häuslichen Arbeitsplatz verarbeitet werden, nicht

durch technische Fehler oder ein Versehen des Benutzers auf das lokale System übertragen werden und dort zu einem späteren Zeitpunkt unbefugten Personen zugänglich sind. Auch der Ausdruck von Unterlagen ist nur an den zugewiesenen Druckern in der Schule möglich, die entweder in nicht allgemein zugänglichen Bereichen der Schulverwaltung stehen müssen oder bei denen die Funktion „vertrauliches Drucken“ – der Druck kann dadurch an den Geräten erst nach Eingabe einer PIN erfolgen – genutzt wird. Im Ergebnis ist in jedem Fall sichergestellt, dass die Ausdrucke nicht in unbefugte Hände gelangen.

Anlage 1 Ziff. 6.1 bis 6.13 Verordnung über die Verarbeitung personenbezogener Daten und statistische Erhebungen in Schulen

6. Datensatz bei der Verarbeitung personenbezogener Schülerdaten auf privaten Datenverarbeitungseinrichtungen der Lehrkräfte

6.1 Name einschließlich Geburtsname,
6.2 Vorname,
6.3 Geschlecht,
6.4 Geburtsdatum,
6.5 Klasse/Jahrgangsstufe, Kurs,
6.6 Schüleraktenzeichen und Gesamtschülerverzeichnis,
6.7 LUSD-ID der Schülerin oder des Schülers,
6.8 Unterrichtsfächer,
6.9 Bildungsgang, Ausbildungsrichtung/Ausbildungsberuf, gegebenenfalls Schwerpunkt,
6.10 Fächer, in denen die Lehrkraft Schülerinnen und Schüler unterrichtet,
6.11 selbst erteilte Zeugnisnoten und Ergebnisse und Teilergebnisse schriftlicher, mündlicher und praktischer Leistungsüberprüfungen sowie Verhaltensbewertungen in dem von der Lehrkraft erteilten Unterricht sowie Art und Datum der Leistungserhebung beziehungsweise der Bewertung,
6.12 Zeiten des Fernbleibens vom Unterricht in den Fächern, in denen die Lehrkraft die Schülerinnen und Schüler unterrichtet,
6.13 Mitglieder der Schulleitung, gegebenenfalls weitere mit Leitungsaufgaben betraute Lehrkräfte und Klassenlehrer dürfen soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, darüber hinaus die folgenden Schülerdaten verarbeiten:
6.13.1 Halbjahresnoten in allen Fächern der betreffenden Schülerinnen und Schüler,
6.13.2 alle zeugnisrelevanten Leistungsangaben,
6.13.3 zeugnisübliche Bemerkungen,
6.13.4 Telefonnummer, Telefaxnummer und E-Mail-Adresse der Schülerinnen und Schüler sowie deren Eltern, sofern der Erhebung nicht widersprochen wird

In einem weiteren Schritt beabsichtigt der Main-Kinzig-Kreis eine geeignete, für die Verarbeitung der sonderpädagogischen Gutachten unerlässliche Verschlüsselung einzuführen. Wenn sich hier eine geeignete Lösung findet, lassen sich auch diese besonders zu schützenden Daten im Rahmen der rechtlichen Vorgaben an den häuslichen Arbeitsplätzen verarbeiten.

Anlage 1 Ziff. 6.14 Verordnung über die Verarbeitung personenbezogener Daten und statistische Erhebungen in Schulen

6. Datensatz bei der Verarbeitung personenbezogener Schülerdaten auf privaten Datenverarbeitungseinrichtungen der Lehrkräfte
...

6.14 Förderschullehrkräfte und Berufsschullehrkräfte mit sonderpädagogischer Zusatzausbildung dürfen zur Erstellung von sonderpädagogischen Gutachten außerdem folgende personenbezogene Daten verarbeiten:
6.14.1 zur Anamnese der Schülerin oder des Schülers in ihrer oder seiner Familie,
6.14.2 zu den Entwicklungsbedingungen der Lernumwelt,
6.14.3 zu Faktoren und Merkmalen hinsichtlich der Vorgeschichte,
6.14.4 zu Lernvoraussetzungen und den individuellen Fähigkeiten in ihrem Zusammenhang mit der aktuellen Lernsituation,
6.14.5 zum Lernverhalten,
6.14.6 zur sprachlichen Entwicklung,
6.14.7 zur körperlichen und motorischen Entwicklung,
6.14.8 zum emotionalen und sozialen Verhalten,
6.14.9 zur kognitiven Entwicklung,
6.14.10 zur Handlungsfähigkeit in Situationen der täglichen Erfahrung,
6.14.11 zu zusammenfassenden Beurteilungen,
6.14.12 zu Förderempfehlungen und zu Hinweisen für den zu entwickelnden Förderplan.

4.5.4.4 Revisionssichere Protokollierung

Die vollständige Protokollierung beim Betrieb von IT-Systemen umfasst unter dem datenschutzrechtlichen Blickwinkel alle automatisierten und ggf. manuellen Aufzeichnungen, die dazu geeignet sind festzustellen, wer wann mit welchen Mitteln auf Daten zugegriffen hat. Ergänzend dazu kann mit den Protokollen und Dokumentationen nachvollzogen werden, wer wann über welche Berechtigung in den Systemen verfügte und ob diese Berechtigungen den in diesen Zeiträumen vorgegebenen Aufgabenstellungen entsprachen. Leider werden die automatisierten Protokolle in Standardsystemen oft nicht manipulationssicher erzeugt und abgelegt. Ein höheres Maß an Revisionssicherheit ist nur durch den Einsatz von speziellen Software-Paketen zu erreichen, die die anfallenden Protokolle schützen und sicher ablegen sowie alle dazu notwendigen Prozesse überwachen (s. 38. Tätigkeitsbericht, Ziff. 10.1).

In der Prüf- und Beratungspraxis der vergangenen Jahre wurde ich vereinzelt gebeten, den Inhalt und die Integrität von Protokolldaten zu bewerten. In aller Regel waren im Vorfeld in einer Daten verarbeitenden Stelle vertrauliche Informationen aus Schriftstücken, Patientendatensätzen oder nicht öffentlichen Sitzungen bzw. deren Protokollen, bekannt geworden und es galt festzustellen, ob mit den Zugriffsprotokollen der IT-Systeme unbefugte Zugriffe nachzuweisen wären.

Leider war in fast allen Fällen ein sicherer, möglicherweise gerichtlich verwertbarer Nachweis nicht zu führen, da die Protokollierung einerseits oft nur unvollständig aktiviert war und andererseits die anfallenden Protokolle nicht hinreichend gegen Veränderungen geschützt wurden. Auch um die in solchen Situationen automatisch in den Kreis der Verdächtigen geratenen Administratoren zu schützen, ist es notwendig, mit speziellen Systemen die anfallenden Protokolle und die beteiligten Prozesse zu schützen bzw. zu überwachen.

Für den Main-Kinzig-Kreis war es neben diesen grundsätzlichen Überlegungen wichtig, die Administrationsarbeiten für die kreiseigenen Schulen revisionssicher und mit einer verbesserten Auswertbarkeit nachweisen zu können. Daher hat der Kreis ein Projekt auf den Weg gebracht, bei dem durch den Einsatz eines entsprechenden Systems alle sicherheitsrelevanten Vorgänge in der IT der Kreisverwaltung auf separaten Servern abgelegt werden.

Das nahezu fertig entwickelte Konzept steht vor seiner Umsetzung. Allerdings müssen die Fragen der Rollenverteilung bei der Überwachung der kritischen Prozesse noch mit der Personalvertretung abgestimmt und durch die zuständigen Gremien der Kreisverwaltung beschlossen werden. Wegen der übergreifenden Bedeutung für alle IT-Bereiche der Kommunal- und Landesverwaltung werde ich die Projektumsetzung im Laufe des Jahres 2011 weiter begleiten und erneut dazu berichten.

4.5.4.5 Mustersicherheitskonzept für die Schulen im Kreis Groß-Gerau

Im Wege der Beratungsgespräche zu den Konzepten des Kreises Groß-Gerau hat die zuständige Fachverwaltung besonderen Wert darauf gelegt, dass die Umsetzung in den Schulen die notwendige Akzeptanz erfährt und entsprechend mitgetragen wird. In diesem Zusammenhang wurde im Lauf des Jahres neben einer Sicherheitsrichtlinie zur IT-Nutzung, in der verbindliche Rahmenbedingungen zwischen Schulträger und Schulen verabredet werden, auch der Entwurf eines Mustersicherheitskonzeptes für die Schulen erarbeitet.

Alle staatlichen Schulen in Hessen sind durch den Erlass über IT-Sicherheit und Datenschutz in Schulverwaltungen des Hessischen Kultusministeriums vom 27. November 2009 (ABl. 2010 S. 11) im Zusammenhang mit § 10 HDSG dazu verpflichtet, ein Sicherheitskonzept zu erstellen, sehen sich aber dabei in aller Regel vor einer Aufgabe, die sie ohne die Unterstützung ihres Schulträgers nicht bewältigen können. Ich unterstütze daher alle Ansätze, bei denen der Schulträger mit seinen kreiseigenen bzw. städtischen Schulen ein Musterkonzept entwickelt und dabei alle Punkte abdeckt, für die er, als der zentrale „Dienstleister“, die fachliche Verantwortung trägt.

Im jüngsten, mir vorliegenden Entwurf des IT-Sicherheitskonzeptes des Kreises Groß-Gerau sind neben zentralen Vorgaben zur allgemeinen Systemnutzung und zum Grundschutz auch solche zum Netzmanagement, zur Datenhaltung/Sicherung, zum Virenschutz usw. enthalten. Die Schulen müssen dann bspw. noch die folgenden schulspezifischen Details ergänzen:

- Zutrittskontrolle zu Gebäuden und Räumen
- Schlüsselvergabe
- Aufbewahrung/Lagerung von Schülerakten
- Aufbewahrung externer Datenträger^
- Datensicherung lokaler Systeme2
- lokale Entsorgung von Akten und Datenträgern

Der Kreis Groß-Gerau hat damit die Voraussetzungen geschaffen, dass die kreiseigenen Schulen im Laufe des nächsten Jahres flächendeckend ihre Sicherheitskonzepte erstellen können. Zusätzlich beabsichtigt die zuständige Fachverwaltung ein erweitertes Sicherheitskonzept für die eigenen Zwecke zu erstellen, das den Schulleitungen zur Klärung von Detailfragen zur Einsicht vorgelegt werden kann. Sicherheitsrelevante Einzelheiten sind den Verantwortlichen in den Schulen auf diese Weise zugänglich, müssen aber nicht in die Konzepte der einzelnen Schulen übernommen werden.