Handreichung über den Datenschutz beim Umgang
mit personenbezogenen Daten
(Datenschutzrecht in der Schule)

I. Einführung, Grundbegriffe und Prinzipien

1. Was ist „Datenschutz“?

Unter Datenschutz versteht man alle Maßnahmen zur Sicherung gespeicherter personenbezogener Daten vor Missbrauch durch andere Personen oder öffentliche Stellen bei der Erfassung, Verarbeitung und Weitergabe.

2. Warum gibt es den Datenschutz?

Nach Artikel 2 Absatz 1 des Grundgesetzes hat jeder das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt. Zu diesem allgemeinen Persönlichkeitsrecht gehört auch das „Recht auf informationelle Selbstbestimmung“, d. h. das Recht einer jeden Person, grundsätzlich selbst über die Preisgabe und Verwendung ihrer persönlichen Daten zu bestimmen. Weiterhin ist jeder Einzelne davor zu schützen, dass er im Freistaat Sachsen durch Behörden und sonstige öffentliche Stellen bei der Verarbeitung personenbezogener Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird (vgl. auch § 1 des Gesetzes zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen - Sächsisches Datenschutzgesetz - SächsDSG). Dieses Recht darf nur auf Grund einer verfassungsgemäßen gesetzlichen Grundlage eingeschränkt werden. Gefährdungen des Rechts auf informationelle Selbstbestimmung ergeben sich insbesondere durch die zunehmende Nutzung von Informations- und Kommunikationstechnik in allen Bereichen des täglichen Lebens und deren wachsender Vernetzung.

3. Was hat der Datenschutz mit der Schule zu tun?

Die Schule hat als öffentliche Stelle mit vielen Personen (Schülerinnen und Schüler, Lehrpersonal, Erziehungspersonal, Erziehungsberechtigte) zu tun. Daraus ergibt sich zwangsläufig, dass in Schulen eine Vielzahl personenbezogener Daten anfällt, und zwar sowohl im Rahmen der Verwaltung als auch innerhalb des Unterrichts. Auch minderjährige Schülerinnen und Schüler können das Recht auf informationelle Selbstbestimmung für sich in Anspruch nehmen. Die vielfältigen Formen der Verarbeitung personenbezogener Daten in den Schulen bedürfen darum einer rechtlichen Ordnung.

4. Was sind „personenbezogene Daten“?

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse von bestimmten oder bestimmbaren natürlichen Personen (§ 3 Absatz 1 SächsDSG). Dazu gehören u. a. auch Bilder.

Für die Anwendung des Datenschutzrechts ist es nicht erforderlich, dass es sich um besonders schützenswerte Daten handelt. Dem Datenschutz unterliegen also grundsätzlich auch Daten wie Namen und Anschriften.

5. Was ist „Datenverarbeitung personenbezogener Daten“?

Datenverarbeitung ist das

- Erheben (= beschaffen),
- Speichern (= erfassen oder aufbewahren),
- Verändern (= inhaltlich umgestalten),
- Anonymisieren (= zuordnen zur konkreten Person kaum noch möglich),
- Übermitteln (= Weitergabe an, Einsichtnahme, Abruf durch Empfänger),
- Nutzen (= jede sonstige Verwendung),
- Sperren (= kennzeichnen zur Einschränkung der weiteren Verarbeitung) und
- Löschen (= unkenntlich machen)

von Daten (§ 3 Absatz 2 SächsDSG).
Ob die Verarbeitung automatisiert (mit Hilfe eines Computers) oder nicht automatisiert (zum Beispiel auch mündlich im Gespräch) erfolgt, ist grundsätzlich unerheblich.

6. Wann ist die Datenverarbeitung erlaubt?

Die Verarbeitung personenbezogener Daten muss erforderlich sein. Sie ist nur zulässig, wenn sie das SächsDSG oder eine andere Rechtsvorschrift erlaubt oder der Betroffene eingewilligt hat (§ 4 Absatz 1 SächsDSG). Die Einwilligung muss in der Regel schriftlich erfolgen und ist nur dann wirksam, wenn der betroffenen Person hinreichend deutlich gemacht worden ist, was mit ihren Daten geschieht (vgl. § 4 Absätze 3 und 4 SächsDSG).

Unter diesen Voraussetzungen ist die Einwilligung am besten geeignet, das Recht auf informationelle Selbstbestimmung zu wahren. Wenn also Zweifel bestehen, ob eine Datenverarbeitung rechtlich zulässig ist, sollte immer geprüft werden, ob die Einwilligung der betroffenen Person eingeholt werden kann (vgl. hierzu insbesondere Abschnitt II Punkt 3 „Schulen im Internet“).

7. Was bedeuten die Grundsätze der Erforderlichkeit und Zweckbindung?

Sie besagen, dass das Erheben personenbezogener Daten nur dann zulässig ist, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist (§ 12 Absatz 1 SächsDSG). Dies ist dann der Fall, wenn diese Stelle im konkreten Einzelfall ihre Aufgaben andernfalls gar nicht, nicht vollständig, nur unter unverhältnismäßig großen Schwierigkeiten oder nicht rechtzeitig erfüllen kann. In jedem Einzelfall muss also geprüft werden, ob die Aufgabe ohne die Verarbeitung personenbezogener Daten erfüllt

werden kann. Eine vorsorgliche Sammlung von Daten, z. B. weil diese als Hintergrundinformation oder später evtl. einmal gebraucht werden könnten (sog. Vorrats-Datenhaltung), ist unzulässig.

Der Grundsatz der Zweckbindung besagt, dass personenbezogene Daten grundsätzlich nur im Rahmen der Zweckbestimmung weiterverarbeitet werden dürfen, für die sie erhoben (= beschafft) worden sind. Ausnahmen von der Zweckbindung gibt es nur in gesetzlich geregelten Fällen.

8. Was gehört zu den Maßnahmen für die Gewährleistung des Datenschutzes?

Öffentliche Stellen, also auch Schulen, die personenbezogene Daten verarbeiten, haben alle personellen, technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um einen angemessenen Schutz der Daten zu gewährleisten.

Werden personenbezogene Daten verarbeitet, sind nach dem jeweiligen Stand der Technik Maßnahmen zu treffen (§ 9 Absatz 2 SächsDSG), die geeignet sind zu gewährleisten, dass

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),
3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),
5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

Die vorstehenden Grundsätze gelten auch für die nicht-automatisierte Datenverarbeitung.

Werden personenbezogene Daten in Akten verarbeitet, sind ebenso geeignete Maßnahmen zu treffen, um zu verhindern, dass Unbefugte bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung auf die Daten zugreifen können.

Beispielgebend sei auf das Datenschutzkonzept und das Einsatzkonzept „Betriebsstätte Schule“ im Rahmen von SaxSVS verwiesen.

9. Kontrolle des Datenschutzes und Konsequenzen bei Verstößen

Wenn eine Behörde die für ihr Handeln erforderlichen Informationen über Personen verarbeitet, muss sie sich dazu auf eine gesetzliche Grundlage stützen können. Die Datenflüsse müssen überschaubar bleiben (Transparenzgebot). Die Schule hat auf die Einhaltung der Datenschutzbestimmungen zu achten. Bestellte Datenschutzbeauftragte können die Dienststelle beraten. Datenschutzaufsichtsbehörde ist der Sächsische Datenschutzbeauftragte, der die öffentlichen Stellen kontrolliert. Der Sächsische Datenschutzbeauftragte ist für Schulen, Behörden und Bedienstete Ansprechpartner. Datenschutzhinweise zur Datenverarbeitung im Schul- und im Kultusbereich enthalten auch die vom Sächsischen Datenschutzbeauftragten regelmäßig veröffentlichten Tätigkeitsberichte.

Datenschutzverstöße Einzelner können Ordnungswidrigkeiten oder gar Straftaten darstellen (§§ 38, 39 SächsDSG). Verstöße können auch dienst- und disziplinarrechtliche Folgen haben. Beispielsweise handelt ordnungswidrig, wer unbefugt vom SächsDSG geschützte personenbezogene Daten, die nicht offenkundig sind,
a) verarbeitet,
b) zum Abruf bereithält oder
c) für sich oder einen anderen abruft oder sich auf andere Weise verschafft.

II. Datenschutz in der Schule

1. Erforderlichkeit und Zweckbindung

Nach den Schulordnungen der einzelnen Schularten dürfen personenbezogene Daten der Schülerinnen und Schüler und ihrer Erziehungsberechtigten verarbeitet werden, soweit dies zur Erfüllung des Bildungsauftrags der Schule und der Fürsorgeaufgaben sowie zur Erziehung und Förderung der Schülerinnen und Schüler erforderlich ist (Zweckbindung). Das entbindet die Schulen und die am Schulwesen beteiligten Stellen von der Verpflichtung, für jede Datenerhebung eine spezielle Zweckbestimmung festzulegen.

Sofern Rechtsnormen oder Erlasse Festlegungen zum Datenschutz beinhalten, werden nicht nur die Organe und Funktionsträger der Schulen verpflichtet; letztlich wird jede einzelne Lehrkraft bei ihrer dienstlichen Tätigkeit zur Beachtung angehalten.

Die Verarbeitung der personenbezogenen Daten der Beschäftigten an den Schulen richtet sich nach der Rahmendienstvereinbarung zur „Elektronische Datenverarbeitung personenbezogener Daten durch die Schulen“ (RDV-EDVpD-Schule, Az. 12-0270.91-01/7/8 vom 27. Juli 2006).

2. Schulspezifische Fragen

a) Verarbeitung personenbezogener Daten

Schulen dürfen personenbezogene Daten von Schülern und deren Erziehungsberechtigten, von Lehrern, Referendaren und sonstigem Personal verarbeiten, soweit es zur Erfüllung der Aufgaben erforderlich ist.

Es ist sicherzustellen, dass Personalakten und Personalaktendaten nur durch die Schulleitung verarbeitet werden.

Das Verarbeiten personenbezogener Daten ist nur zulässig, wenn die Schulen ohne die gespeicherten Daten ihren Erziehungs- und Bildungsauftrag sowie ihre Verwaltungs- und Fürsorgeaufgaben nicht oder nicht vollständig erfüllen können.

Bereits bei der Erhebung der Daten ist den Betroffenen Speicherungs- und Verarbeitungszweck mitzuteilen.

Personenbezogene Daten dürfen grundsätzlich nicht auf privateigenen Datenverarbeitungsanlagen oder Datenträgern verarbeitet werden (Ausnahmen regeln sich nach Abschnitt III).

Auf Datenverarbeitungsanlagen, die im Unterricht oder für unterrichtliche Zwecke eingesetzt werden, dürfen personenbezogene Daten nicht gespeichert werden.

Datenverarbeitungsanlagen mit Serverfunktion, auf denen personenbezogene Daten gespeichert sind, müssen die Trennung zwischen pädagogischer und verwaltungstechnischer Nutzung gewährleisten (vgl. Pkt. 5 „Verwaltungsnetz vs. Unterrichtsnetzwerke“).

Schülerdaten sind spätestens mit Ablauf der Aufbewahrungsfristen (VwV AusSchul) in der automatisierten Datei zu löschen.

b) Datenübermittlung an öffentliche Stellen

An den Jugendärztlichen Dienst, den Schulpsychologischen Dienst, die Organe der öffentlichen Jugendhilfe, die Gerichte, die Staatsanwaltschaft, die Bezügestelle, die Jugendgerichtshilfe und sonstige öffentliche Stellen dürfen personenbezogene Daten übermittelt werden. Es ist von der übermittelnden Stelle zu prüfen, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt.

An die Gesamtvertretungen der Schüler bzw. der Eltern dürfen die Namen und die Funktion von Mitgliedern der Schülervertretung bzw. der Elternvertretung übermittelt werden. Für die Weitergabe zusätzlicher Daten bedarf es der Einwilligung der Betroffenen.

c) Datenübermittlung an nicht-öffentliche Stellen

Datenübermittlung an nicht-öffentliche Stellen ist ohne Einwilligung der Betroffenen unzulässig.

d) Nutzung von Bewertungen

Bewertungen von Leistungskontrollen, persönliche Notizen von Lehrern, Referendaren und sonstigem pädagogischen Personal und die den täglichen Unterricht begleitenden Vermerke im Klassenbuch und in ähnlichen Unterlagen dürfen im Rahmen der täglichen Arbeit in den Bildungseinrichtungen genutzt werden. Pädagogische Besprechungen über Schüler sind gestattet.

Die Bekanntgabe von Noten vor der Klasse ist eine pädagogische Frage. Sie liegt im pflichtgemäßen Ermessen des einzelnen Lehrers. Die Aspekte der Benotung dürfen zwischen Lehrern und Schülern besprochen werden. Persönlichkeitsrechtliche Grenzen sind zu beachten.

Bei Schülerwettbewerben ist bereits in der Ausschreibung die geplante Veröffentlichung der Namen der Teilnehmer zu formulieren.

3. Schulen im Internet

Schulen kommunizieren über das Internet, meist im Rahmen von Unterrichtsveranstaltungen oder besonderen pädagogischen Projekten. Dies ist ausdrücklich erwünscht und wird von der Staatsregierung gefördert. Darüber hinaus präsentieren sie sich auf eigenen Homepages. Darin werden häufig auch die Schulleitung, das Kollegium, Schülervertreterinnen und Schülervertreter, manchmal auch Elternvertreterinnen und Elternvertreter, Inhaberinnen und Inhaber besonderer Funktionen und Teilnehmerinnen und Teilnehmer an besonderen Veranstaltungen mit Namen, Vornamen, ggf. Dienstbezeichnung und weiteren "Kommunikationsdaten", manchmal sogar mit Foto präsentiert.

Dass dies im datenschutzrechtlichen Sinne "erforderlich" ist, ist nur schwer zu begründen. Das Sächsische Staatsministerium für Kultus hat Regelungen zu dieser Frage bisher nicht getroffen. Es ist zulässig, die Daten (Namensbezeichnungen, Dienstbezeichnungen und Funktionen) der Schulleiter und der stellvertretenden Schulleiter, soweit sie für die Repräsentation der Stelle nach außen erforderlich sind, bekannt zu geben.

Dennoch ist dringend zu empfehlen, sämtliche weitergehende Daten nur auf Einwilligungsbasis im Internet zu verarbeiten (vgl. § 4 SächsDSG).

Minderjährige Schülerinnen und Schüler sind in Bezug auf die Erhebung und Verarbeitung ihrer Daten selbst einwilligungsfähig, wenn sie die Bedeutung und Tragweite der Einwilligung und deren rechtliche Folgen erfassen können und ihren Willen hiernach zu bestimmen vermögen. Das wird jedenfalls bei Schülerinnen und Schülern des Sekundarbereichs II regelmäßig der Fall sein. Bei nicht-einwilligungsfähigen Schülern kann die Einwilligung durch die Elternsorgeberechtigten erfolgen.

Darüber hinaus sind Fragen des Urheberrechts, Jugendschutzes, der Verantwortung für Inhalte (auch bei Verlinkung auf andere Seiten z. B. durch Gestaltung von Impressum und Disclaimer) usw. von besonderer Bedeutung (vgl. z. B. http://www.lehrer-online.de/dyn/9.asp?url=350826.htm, http://arthur.sn.schule.de/medios/beratung/ghoerz.php3).

4. Beratung und Service

Fragen zum Datenschutzrecht sind an die Regionalschulämter (ab 1. Januar 2007 an die Sächsische Bildungsagentur) als nachgeordnete Schulaufsichtsbehörden zu richten.

Ein umfangreiches Angebot an Informationen, Merkblättern, Checklisten, Arbeitshilfen und Broschüren bietet der Sächsische Datenschutzbeauftragte an, der wie folgt zu erreichen ist:

- Internet: http://www.datenschutz.sachsen.de/
- Post: Bernhard-von-Lindenau-Platz 1, 01067 Dresden
- Telefon: (03 51) 4 93 54 01
- Fax: (03 51) 4 93 54 90
- E-Mail: saechsdsb@slt.sachsen.de

Weitere Quellen und Links sind im Abschnitt IV aufgelistet.

5. Technisch-organisatorische Empfehlungen

- Datenträger / Aufbewahrung von Datenträgern

Als Datenträger kommen je nach technischer Ausstattung der Computer vorrangig Disketten, CD, DVD, USB-Sticks, mobile Festplatten, Chip-Karten, Foto-Karten usw. in Betracht. Wegen ihrer Handlichkeit ist darauf zu achten, dass sie nicht achtlos liegengelassen werden. Sie sind grundsätzlich so aufzubewahren, dass unautorisierte Personen keinen Zugriff erhalten. Soweit personenbezogene Daten auf mobilen Datenträgern gespeichert werden, sind diese mindestens mit einem Passwortschutz zu versehen; besser ist eine zusätzliche Verschlüsselung.

Sicherungskopien sind zweckmäßigerweise in einem sicher verschlossenem Behältnis des Schulleiters aufzubewahren. Soweit Daten gemäß Abschnitt III von Lehrern mit nach Hause genommen werden, ist durch diese ein adäquater Schutz zu gewährleisten.

- Belehrungen zum Datenschutz

Die Beschäftigten an Schulen sind mindestens einmal jährlich zum Thema Datenschutz zu belehren. In diesem Zusammenhang ist von den Beschäftigten die in Anlage 1 beigefügte Erklärung abzugeben.
Die Belehrung der Schulleiter erfolgt zu Beginn des Schuljahres durch die Regionalschulämter (ab 1. Januar 2007 die SBA).

- Datenschutzbeauftragter (DSB)

An Schulen können behördliche Datenschutzbeauftragte ernannt werden. Ab einer Zahl von 30 Beschäftigten oder 500 Schülern ist diese Ernennung Pflicht. Die Ernennung erfolgt auf Vorschlag der Schulleitung durch die RSÄ (ab 1. Januar 2007 die SBA). Ein DSB kann auch für mehrere Schulen ernannt werden. Der DSB ist Ansprechpartner in allen Fragen des Datenschutzes an der Schule. Zur Qualifizierung hat der DSB entsprechende Fortbildungsmaßnahmen wahrzunehmen.

Verwiesen wird in diesem Zusammenhang auf die Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Bestellung eines Datenschutzbeauftragten öffentlicher Stellen nach § 11 SächsDSG sowie auf die Anlage zur Bekanntmachung unter (http://www.datenschutz.sachsen.de).

- Datensicherung

Im Serverbetrieb ist eine zentrale Datensicherung durch ein am Server angeschlossenes bzw. eingebautes Datensicherungslaufwerk (z. B. Band, CD, DVD) zweckmäßig. Die folgenden Sicherungszyklen können empfohlen werden:

<u>Inkrementelle Datensicherung - Tagessicherungen</u>
Es werden nur die Änderungen seit der letzten Sicherung gesichert bei denen das Archivierungsbit gesetzt wurde

<u>Vollständige Sicherung - Wochensicherung und/oder Monatssicherung</u>
Es werden alle Daten des Servers gesichert und das Archivierungsbit gesetzt.

Je nach Datenaufkommen und Sicherungsmedium kann für die inkrementelle Sicherung ein Datenträger für mehrere Tage verwendet werden. Im Rahmen der Ausfallsicherheit ist jedoch zu empfehlen für jede Sicherung ein eigenes Medium zu verwenden.

Eine vollständige Sicherung zum Ende des Schuljahres sollte als Jahressicherung gesondert aufbewahrt werden.

Auch an Einzelplatzsystemen sollten regelmäßige Sicherungen (mindestens wöchentlich) durchgeführt werden.

Im Rahmen von SaxSVS wird zusätzlich ein Backup auf dem Server im Rechenzentrum des StLA angeboten. Bei umfangreichen täglichen Arbeiten sollte dies auch täglich genutzt werden. Verantwortlich für die Datensicherung ist der Schulleiter bzw. sein von ihm beauftragter Stellvertreter.

- E-Mail

E-Mails sind ein immer stärker genutztes Kommunikationsmittel. Der ungesicherte (nicht verschlüsselte) Versand von personenbezogenen Daten via E-Mail ist nicht gestattet.

- Entsorgung von Datenträgern und Ausdrucken

Ausgemusterte Datenträger wie Disketten, USB-Sticks und Platten, auf denen vormals personenbezogene Daten gespeichert/gesichert wurden, sind neu zu formatieren und gegebenenfalls mehrfach zu überschreiben oder physikalisch zu zerstören.

Ein mehrfaches Überschreiben (mindestens zweimal, besser drei- bis siebenmal) geschieht mit einer zufälligen Zeichenfolge. Dazu können Löschfunktionen von Dienstprogrammen genutzt werden, die teilweise auch als Freeware (kostenlose Software) im Internet zur Verfügung stehen.

EDV-mäßig erstellte Papierunterlagen (Computerausdrucke) mit personenbezogenen Daten sind in gleicher Weise wie manuell erstellte derartige Unterlagen so zu entsorgen, dass Unbefugten eine Einsichtnahme nur mit unverhältnismäßig großem Aufwand möglich wäre.

- Internet

Sind Verwaltungscomputer an das Internet angeschlossen, sind zur Sicherung der darauf befindlichen Daten dem aktuellen technischen Entwicklungsstand entsprechende Sicherheitsvorkehrungen zu treffen (Antivirensoftware, Firewall, Spamschutz usw.) und regelmäßig zu überprüfen.

- Löschung von Daten und Löschfristen

Personenbezogene Daten sind zu löschen, wenn sie zur Erfüllung der Aufgaben der Schule nicht mehr benötigt werden. Schülerdaten sind spätestens mit Ablauf der Aufbewahrungsfristen (VwV AusSchul) in der automatisierten Datei zu löschen.
Soweit personenbezogene Daten der Schüler durch Lehrer auf deren privaten Computern verarbeitet werden (vgl. Abschnitt III), sind diese zu löschen, wenn sie zur Erfüllung der Aufgaben des Lehrers nicht mehr benötigt werden, spätestens jedoch nach Ende des Schuljahres.

- Passwörter

Die folgenden Regeln für die Vergabe von Passwörtern sollten beachtet werden.

Parameter	**Einstellung**	**Bemerkung**
Passwort muss Komplexitätsanforderungen entsprechen	Aktiviert	Erzwingt die Benutzung von Kombinationen aus Buchstaben, Ziffern und/oder Sonderzeichen im Passwort
Passwortchronik erzwingen	2	Verhindert, dass der Benutzer bei Passwortwechseln auf das alte Passwort wieder zurückgreifen kann
Minimale Passwortlänge	8 Zeichen	Verhindert, dass Leer-Passwörter oder zu einfache Passwörter vergeben werden
Minimales Passwortalter	2 Tage	Verhindert, dass ein Benutzer durch mehrfachen aufeinander folgenden Passwortwechsel das alte Passwort wieder einstellen kann

Passwörter sind in regelmäßigen Abständen zu wechseln und weder auf oder unter Tastatur, Bildschirm oder an weiteren von Dritten zugänglichen Lokationen anzubringen. Eine Notfallliste mit Administratorpasswörtern ist in einem fest verschlossenem Umschlag in einem sicher verschlossenem Behältnis des Schulleiters zu deponieren.

Die Weitergabe von Passwörtern ist nicht zulässig. Da der Versuch, sich im Netz als ein anderer Nutzer auszugeben und Passwörter auszuprobieren, dann nicht bemerkt wird, wenn Fehlanmeldungen nicht protokolliert werden, wenn nach einer bestimmten Zahl von Fehlversuchen die Benutzerkennung nicht gesperrt wird oder Log-Protokolle nicht regelmäßig ausgewertet werden, ist die Sicherheit des Passwortverfahrens durch eine praktikable Begrenzung möglicher Fehlversuche zu schützen.

- Private Hard- und Software

Die Nutzung von privater Hard- und Software in der Schule ist grundsätzlich nicht zulässig. In Ausnahmefällen sind alle in dieser Handreichung beschriebenen Maßnahmen auch für diese Technik sicherzustellen.
Zur Verarbeitung personenbezogener Daten auf privaten Computern vgl. Abschnitt III.

- Verfahrensverzeichnis

Soweit an der Schule personenbezogene Daten verarbeitet werden, führen sie gemäß § 10 SächsDSG ein Verzeichnis automatisierter Verarbeitungsverfahren (Verfahrensverzeichnis). Die Führung dieses Verzeichnisses kann auch nach § 8 RDV-EDVpD-Schule durch eine andere Stelle (Schule, RSA – ab 1. Januar 2007 die SBA) geführt werden.

- Verschlüsselungssysteme

Ein optimaler Zugriffsschutz erfolgt mit der Verschlüsselung von Daten bzw. Datenträger. Nähere Information können zu diesem Thema beim Betreiber von SaxSVS, dem Rechenzentrum des StLA erfragt werden.

- Verwaltungsnetz vs. Unterrichtsnetzwerke

Es ist sicherzustellen, dass kein unautorisierter Zugriff auf personenbezogene Daten und die zugehörenden Programme erfolgen kann. Ein optimaler Schutz wird dabei nur in der physikalischen Trennung der Verwaltungs- und der Unterrichtsrechner gesehen. Vor dem Hintergrund der realen Situation an Schulen sind Netze für Schulverwaltung und Unterricht aber zumindest logisch zu trennen (z. B. Teilnetze mit gesicherten Übergängen).

- Virenschutz

Verwaltungsrechner sind mit geeigneter Software vor schädlichen Programmen (Viren, Trojanern usw.) zu schützen. Dabei ist sicherzustellen, dass diese Software regelmäßig aktualisiert wird (mindestens wöchentlich; zu empfehlen ist aber täglich). Weitere Informationen zu diesem Thema sind als Anlage 2 beigefügt.

III. Hinweise zur Verarbeitung personenbezogener Daten auf privaten Computern von Beschäftigten an Schulen

Lehrerinnen und Lehrer (im Folgenden "Lehrer") nutzen Computer im häuslichen Umfeld zur Unterstützung ihrer Unterrichtsvor- und -nachbereitung zur Verwaltung ihrer Schülerdaten (Erstellung von Klassenlisten, Führung eines EDV-gestützten Notenbuches, Unterstützung bei der Bewertung von Klassenarbeiten, Schreiben von Zeugnissen usw.). Inwieweit eine derartige Verarbeitung personenbezogener Daten auf privaten Computern der Lehrer zulässig ist, hat das Sächsische Staatsministerium für Kultus in Zusammenarbeit mit dem Sächsischen Datenschutzbeauftragten wie folgt geklärt.

1. Grundsätzliches

Der Einsatz privater Computer in der Verwaltung zur Erledigung dienstlicher Aufgaben ist im Allgemeinen nicht zulässig und aus Gesichtspunkten der Datensicherheit riskant. Er ist daher nur in Ausnahmefällen zugelassen.

Lehrern steht in der Schule regelmäßig kein Arbeitsplatz für die Erledigung von Verwaltungsarbeiten zur Verfügung. Daher ist es schon immer erforderlich, dass sie Unterlagen mit personenbezogenen Schülerdaten zu Hause bearbeiten. Sie sind dabei als Teil der Behörde „Schule“ tätig.

Im Rahmen der Bewältigung der dienstlichen Verwaltungsaufgaben ist der Einsatz privater Computer von Lehrern als ein zulässiger Ausnahmefall anzusehen. Sie unterliegen dabei den gleichen Datenschutzbestimmungen, die auch für ihre Schule gelten (vgl. Absatz 3.5 „Rechtsgrundlagen“). Aus diesen Bestimmungen werden im Folgenden die für die Datenverarbeitung am privaten Computer besonders Wichtigen näher erläutert.

2. Datenrahmen

Es dürfen lediglich Daten jener Schüler verarbeitet werden, die der bearbeitende Lehrer selbst unterrichtet bzw. deren Klassenleiter oder Kollegstufenbetreuer er ist. Art und Umfang der Daten hat sich an den herkömmlich etwa in einem Notenbuch geführten oder bei der manuellen Zeugniserstellung benötigten Daten zu orientieren. Sie werden für das jeweils aktuelle Schuljahr als Basisdaten aus dem Schulverwaltungsprogramm SaxSVS bereitgestellt. Die in der Regel verwendeten Datenträger, wie USB-Sticks, dürfen ausschließlich für dienstliche Zwecke verwendet werden. Der Datentransfer ist zu dokumentieren. Die verwendeten Datenträger müssen passwortgeschützt sein. Ein datensicherer Transportweg ist zu gewährleisten. Sicherzustellen ist auch, dass nicht über E-Mail Daten transferiert werden. Verantwortlich für die Datenweitergabe ist der Schulleiter bzw. sein von ihm beauftragter Stellvertreter.

Der Datenrahmen beinhaltet:

- Name, Vornamen

- Geschlecht
- Geburtsdatum
- Klasse / Gruppe / Kurs
- Ausbildungsrichtung bzw. Ausbildungsberuf
- Fächer, in denen der Lehrer den Schüler unterrichtet
- Leistungen in den vom Lehrer erteilten Fächern (einschließlich Datum der Notengebung und Art der Leistungserhebung)
- Zeugnisdaten (insbesondere Noten und Bemerkungen).

Bei jedem Merkmal hat der Lehrer im Einzelnen zu prüfen, ob die Verarbeitung zur Erfüllung seiner dienstlichen Aufgaben erforderlich ist.

Mit diesem Datenrahmen ist es beispielsweise möglich,
- Klassenlisten mit verschiedenen Sortierungen und Rasterungen zu erstellen (Fachlehrer, Klassensprecher, Klassenleiter können dabei als Bestandteil des Listenformats - etwa des Listenkopfes - geführt werden; die Führung derartiger Daten in einer Datei ist aber nicht zulässig),
- ein Notenbuch EDV-gestützt zu führen, das automatisch den Gesamtstand des Schülers oder den Einfluss einer anderen Gewichtung der einzelnen Prüfungen zeigt,
- die Notengebung bei Prüfungsaufgaben zu unterstützen (Umrechnung von Korrekturpunkten in Noten, Auswirkungen der Wahl eines anderen Fehlerschritts, Umsetzung von Sportleistungen in Noten, Durchschnittsberechnung, usw.)
- Zeugnisbemerkungen (Veranlagung, Verhalten, Mitarbeit sowie Bemerkungen über die Teilnahme am Wahlunterricht, über ausgefallenen Unterricht usw.) zu Hause zu entwerfen und Zeugnisse mit dem externen Zeugnismodul von SaxSVS zu schreiben.

Nicht zulässig hingegen ist es beispielsweise,
- vom Schulverwaltungsprogramm SaxSVS (oder einem anderen z. B. kommerziellen Programm) der Schule die gesamten Daten aller Schüler zur Weiterverarbeitung in einem privaten Programm mit nach Hause zu nehmen,
- in einem EDV-mäßig geführten Notenbuch Ordnungsmaßnahmen, häusliche Verhältnisse der Schüler und dgl. zu führen (diese sensiblen Daten dürfen auch in einem Schulverwaltungsprogramm der Schule nicht geführt werden),
- Programme einzusetzen, die über einen umfangreichen Datensatz verfügen, und dabei nicht alle Merkmale zu führen (Ausnahme: die nicht geführten Merkmale sind im Datensatz nicht zugänglich und wurden aus den Erfassungsmasken gelöscht).

Mit der Festlegung des Datenrahmens soll einerseits einer Verwaltungsverlagerung von der Schule nach Hause und andererseits einer unnötigen bzw. datenschutzrechtlich nicht zu vertretenden Datenansammlung durch einzelne Lehrer vorgebeugt werden.

Die Verarbeitung personenbezogener Daten der Erziehungsberechtigten der Schüler, der Ausbildungsbetriebe (bei berufsbildende Schulen) und des Lehrpersonals der Schule auf privaten Computern ist grundsätzlich nicht gestattet.

Die Verarbeitung nicht personenbezogener Daten (Arbeitsblätter, Übungsaufgaben, Bücherverzeichnis usw.) auf privaten Computern der Lehrer ist uneingeschränkt zulässig. Bei der Erstellung von Prüfungsunterlagen und dgl. ist dabei ggf. in besonderer Weise (Datenträger wegschließen usw.) für die Geheimhaltung der Unterlagen zu sorgen.

3. Richtlinien

Als "Richtlinien" sind bei der Verarbeitung von Schülerdaten auf privaten Computern der Lehrer zu beachten:

- Die Schülerdaten dürfen Dritten nicht zugänglich gemacht werden. Eine Datenübermittlung an Dritte ist nicht zugelassen. Selbstverständlich finden auch in diesem Rahmen die Regelungen zum Datengeheimnis bzw. zur Verschwiegenheitspflicht von Beamten und Angestellten Anwendung. In diesem Zusammenhang wird insbesondere auf die Gefahren bei Vernetzungen und Online-Zugängen hingewiesen.
- Die Datenträger sind nach ihrer Verwendung wegzuschließen. Bei der Speicherung auf Festplatte sind die Daten passwortgeschützt abzuspeichern.
- Es ist geeignete Vorsorge zu treffen, dass alle gespeicherten Daten beim Ausfall des Computers trotzdem jederzeit zur Verfügung stehen.

Als Dritte zählen auch Ehepartner, Kinder, Freunde des Lehrers. Sollten diese den privaten Computer des Lehrers ebenfalls nutzen können (Textverarbeitung, Spiele, Surfen im Internet usw.), so ist von einer Speicherung von Schülerdaten auf einer Platte abzusehen.

Bei der Abwehr von Gefahren aus dem Internet kann eine Orientierung an dem Maßnahmenkatalog sinnvoll sein, der für die Schulverwaltung zusammengestellt wurde (vgl. Absatz 3.5 „Rechtsgrundlagen“; Abschnitt IV und Anlage 1).

Bei einer Speicherung von Schülerdaten auf externe Datenträger hat die Löschung durch eine Formatierung des Datenträgers zu erfolgen. Ausgemusterte Datenträger wie Disketten, USB-Sticks und Platten, auf denen vormals personenbezogene Daten gespeichert/gesichert wurden, sind neu zu formatieren und gegebenenfalls zu überschreiben oder physikalisch zu zerstören (vgl. auch Abschnitt II Punkt 5 „Datenträger / Aufbewahrung von Datenträgern“).

EDV-mäßig erstellte Papierunterlagen mit personenbezogenen Daten sind in gleicher Weise wie manuell erstellte derartige Unterlagen so zu entsorgen, dass Unbefugten eine Einsichtnahme nur mit unverhältnismäßig großem Aufwand möglich wäre.

Eine Vorführung eines Programms zur Verwaltung von Schülerdateien ist mit Echtdaten nur gegenüber Kollegen der eigenen Schule zulässig.

Die Vorsorge, dass alle gespeicherten Daten (insbesondere Noten) beim Ausfall des Computers trotzdem jederzeit zur Verfügung stehen, kann etwa dadurch getroffen werden, dass die erfassten Daten von Zeit zu Zeit ausgedruckt werden oder auf sonstige schriftlich geführte Unterlagen zurückgegriffen werden kann.

3.1 Verpflichtung

Einer erneuten Verpflichtung auf das Datengeheimnis nach § 6 SächsDSG bedarf es nicht. Jedoch sollte dokumentiert werden, wenn ein privater Computer zur Verarbeitung von Schülerdaten genutzt wird, dass sich die Lehrkraft datenschutzgerecht zu verhalten hat und dass Verstöße auch dienstrechtliche Konsequenzen nach sich ziehen können.

Anlage 1 enthält eine zu unterzeichnende Erklärung zum Datenschutz an Schulen und insbesondere zur Nutzung von Schülerbasisdaten auf Datenverarbeitungsanlagen von Lehrkräften für das jeweilige Schuljahr. Zu Revisions- und Datenschutzkontrollzwecken ist diese Erklärung in der Schule zur Akte zu nehmen.

3.2 Genehmigung

Die Nutzung eines privaten Computers für die Verarbeitung von Schülerdaten unter Wahrung des o. g. Datenrahmens (vgl. Abschnitt III Punkt 2) und der o. g. Richtlinien bedarf keiner gesonderten Genehmigung.

3.3 Datenschutzfragen

In Datenschutzfragen, die bei der Bearbeitung personenbezogener Schülerdaten am privaten Computer auftreten, sollen sich die Lehrer zunächst an den Datenschutzbeauftragten ihrer Schule (soweit ein Datenschutzbeauftragter bestellt wurde) bzw. an ihren Schulleiter wenden. Weitere Beratungsstellen in Datenschutzfragen vgl. Abschnitt "Rechtsgrundlagen".

3.4 Kontrolle

Berechtigte Personen können Lehrer, die Schülerdaten auf ihren privaten Datenverarbeitungsanlagen verarbeiten, auffordern, ihre privaten Datenverarbeitungsanlagen (PC, Notebook, externe Datenträger) zu datenschutzrechtlichen Kontrollen in den Räumlichkeiten der Schule oder zuständigen Schulaufsichtsbehörde bereitzustellen.
Berechtigte Personen sind u. a. der Sächsische Datenschutzbeauftragte, der Schulleiter des betroffenen Lehrers oder der Leiter der zuständigen Schulaufsichtsbehörde.
Diese Kontrollen sind im Beisein des betroffenen Lehrers durchzuführen und zu protokollieren. Der Lehrer hat das Recht, zu dieser Kontrolle eine Person seines Vertrauens hinzuzuziehen.

3.5 Rechtsgrundlagen

Die voranstehenden Ausführungen stützen sich auf die Datenschutzbestimmungen für Schulen (vgl. Abschnitt I und II). Die „Erläuternden Hinweise“ sind auf der CD der Sächsischen Schulverwaltungssoftware SaxSVS enthalten und können auf der Homepage der Sächsischen Schulverwaltungssoftware (www.saxsvs.de) aufgerufen werden.

IV. Rechtliche Grundlagen sowie weitere Quellen und Links

Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz - SächsDSG) vom 25. August 2003

Schulgesetz für den Freistaat Sachsen – SchulG vom 16. Juli 2004

Schulordnungen der jeweiligen Schulart

Rahmendienstvereinbarungen:

- Rahmendienstvereinbarung „Elektronische Datenverarbeitung personenbezogener Daten durch die Kultusverwaltung“ zwischen SMK und HPR Verwaltung - RDV-EDVpD-HPR vom 27. Juli 2006
- Rahmendienstvereinbarung „Elektronische Datenverarbeitung personenbezogener Daten durch die Kultusverwaltung“ zwischen SMK und Lehrerhauptpersonalrat (LHPR) - RDV-EDVpD-LHPR vom 27. Juli 2006
- Rahmendienstvereinbarung „Elektronische Datenverarbeitung personenbezogener Daten durch die Schulen“ zwischen SMK und Lehrerhauptpersonalrat (LHPR) - RDV-EDVpD-Schule vom 27. Juli 2006

Weitere nützliche Links:

Datenschutz und Datensicherheit allgemein und speziell an Schulen

http://www.sn.schule.de/index.php?auswahl=recht
http://www.lehrer-online.de/url/grundlagen-datenschutz
http://www.lehrer-online.de/url/linksammlung-datenschutz
http://www.lehrer-online.de/dyn/9.asp?url=350826.htm
http://www.bildungsserver.de/zeigen.html?seite=1525
http://www.bildungsserver.de/zeigen.html?seite=289
http://www.bfdi.bund.de/DE/Home/homepage__node.html
http://www.dfn.de/content/beratung/rechtimdfn/rz-checkliste/
http://www.bsi.bund.de/gshb/deutsch/index.htm
http://www.datenschutz-berlin.de/recht/de/rv/index.htm
http://www.rittershofer.de/info/linux/isich.htm
http://www.datenschutz.de/

Viren, Würmer, Trojaner usw. (vgl. auch Anlage 1)

http://www.microsoft.com/germany/athome/security/viruses/default.mspx
http://www.microsoft.com/germany/athome/security/spyware/default.mspx

V. Abkürzungen

DSB	Datenschutzbeauftragter
RDV-EDVpD-HPR	Rahmendienstvereinbarung „Elektronische Datenverarbeitung personenbezogener Daten durch die Kultusverwaltung“ zwischen SMK und HPR Verwaltung vom 27. Juli 2006
RDV-EDVpD-LHPR	Rahmendienstvereinbarung „Elektronische Datenverarbeitung personenbezogener Daten durch die Kultusverwaltung“ zwischen SMK und Lehrerhauptpersonalrat (LHPR) vom 27. Juli 2006
RDV-EDVpD-Schule	Rahmendienstvereinbarung „Elektronische Datenverarbeitung personenbezogener Daten durch die Schulen“ zwischen SMK und Lehrerhauptpersonalrat (LHPR) vom 27. Juli 2006
RSA	Regionalschulamt
SächsDSG	Sächsisches Datenschutzgesetz (Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen vom 25. August 2003
SaxSVS	Sächsische Schulverwaltungssoftware
SBA	Sächsische Bildungsagentur
SBI	Sächsisches Bildungsinstitut
SchulG	Schulgesetz für den Freistaat Sachsen vom 16. Juli 2004
SMK	Sächsisches Staatsministerium für Kultus
StLA	Statistisches Landesamt

VI. Anlagen

1. Erklärung zum Datenschutz an Schulen und insbesondere zur Nutzung von Schülerbasisdaten auf Datenverarbeitungsanlagen von Lehrkräften
2. Anmerkungen zu schädlicher Software (Viren, Trojaner usw.)

Anlage 1: Erklärung zum Datenschutz an Schulen und insbesondere zur Nutzung von Schülerbasisdaten auf Datenverarbeitungsanlagen von Lehrkräften

Lehrkraft: _____

Erklärung zum Datenschutz an Schulen und insbesondere zur Nutzung von Schülerbasisdaten auf Datenverarbeitungsanlagen von Lehrkräften

Ich bin darauf hingewiesen worden, dass es mir gemäß § 6 Abs. 1 SächsDSG untersagt ist, personenbezogene Daten zu einem anderen als dem meiner rechtmäßigen Aufgabenerfüllung erforderlichen Zweck zu verarbeiten, insbesondere diese Daten unbefugt dritten Personen bekannt zu geben oder zugänglich zu machen. Dies gilt auch nach Beendigung meiner Tätigkeit fort.

Die Verarbeitung personenbezogener Daten im Schulbereich darf nur auf der gesetzlichen Grundlage des Schulgesetzes und einschlägiger Rechtsverordnungen der Sächsischen Staatsregierung erfolgen.

Soweit ich personenbezogene Schülerdaten auf meinem privaten PC verarbeite, habe ich durch geeignete, auch technische Sicherungsmaßnahmen, dafür Sorge zu tragen, dass unbefugte Dritte nicht auf den Datenbestand zugreifen oder ihn anderweitig einsehen können. Dies gilt gleichermaßen für Computerausdrucke.

Diese personenbezogene Daten der Schüler sind zu löschen, wenn ich sie zur Erfüllung meiner Aufgaben nicht mehr benötige, spätestens jedoch nach Ende des Schuljahres. Computerausdrucke mit personenbezogenen Daten sind in gleicher Weise wie manuell erstellte derartige Unterlagen so zu entsorgen, dass Unbefugten eine Einsichtnahme nur mit unverhältnismäßig großem Aufwand möglich wäre.

Mir ist bekannt, dass Verstöße gegen die genannten Bestimmungen Dienstvergehen darstellen und entsprechende dienst- und arbeitsrechtliche Konsequenzen nach sich ziehen können.

Ich verpflichte mich, vorstehende Bestimmungen einzuhalten und, soweit ich personenbezogene Schülerdaten auf meinem PC verarbeite, auf Anforderung der berechtigten Personen (gemäß Teil III, Punkt 3.4 der Handreichung) meine Datenverarbeitungsanlage (PC, Notebook, externe Datenträger) zu datenschutzrechtlichen Kontrollen in den Räumlichkeiten meiner Schule oder Schulaufsichtsbehörde bereitzustellen.

Schuljahr	Ort, Datum	Unterschrift der verpflichteten Lehrkraft	Unterschrift des Schulleiters

Original zur Personalnebenakte
Kopie für den Unterzeichner

Anlage 2: Anmerkungen zu schädlicher Software (Viren, Trojaner usw.)

(aktuelle Informationen dazu unter:
http://www.microsoft.com/germany/athome/security/viruses/default.mspx und
http://www.microsoft.com/germany/athome/security/spyware/default.mspx)

Was ist ein Virus?

Ein Virus ist programmierter Code, der sich rasch vervielfältigt. Er heftet sich an ein Programm oder eine Datei und infiziert Computer, auf denen das Programm oder die Datei verwendet wird. Viren können Software, Hardware und Dateien beschädigen.
So, wie sich verschiedene Viren wie Ebola oder Schnupfen beim Menschen unterschiedlich schlimm auswirken, variiert auch die Wirkung von Computerviren von lästig bis zerstörerisch. Ein echter Virus vermehrt sich nicht ohne Benutzeraktionen wie die gemeinsame Verwendung einer Datei oder das Versenden einer E-Mail.
Wenn Sie eine E-Mail mit einer Anlage von einem unbekannten Absender erhalten, löschen Sie diese Mail sofort. Leider können selbst Anlagen von bekannten Absendern nicht mehr sicher geöffnet werden, denn möglicherweise hat sich das Virus über das Adressbuch Ihres Bekannten selbst an Sie versandt. Sollten Sie also von einem bekannten Absender eine E-Mail-Nachricht mit einer nicht erwarteten Datei erhalten, kontaktieren Sie den Absender, um sich über den Inhalt der Anlage zu vergewissern, bevor Sie die Anlage öffnen.

Was ist ein Wurm?

Ein Wurm ist eine Unterkategorie von Computerviren. Auch ohne Zutun von Benutzern kann er sich von Computer zu Computer selbstständig vermehren. Die große Gefahr von Würmern ist ihr Dominoeffekt: Ein Wurm kann sich z.B. an alle im Adressbuch enthaltenen E-Mail-Adressen versenden und sich dabei als Anhang einer E-Mail von einem vertrauenswürdigen Bekannten tarnen. Auf den PCs der Empfänger kann sich der Wurm auf gleiche Weise unkontrolliert vermehren. Ein Wurm kann viel Arbeitsspeicher beanspruchen, Netzwerke blockieren und das Anzeigen von Webseiten verlangsamen oder Ihren PC komplett lahm legen.
Da Würmer zur Vermehrung kein Programm und keine Datei als „Wirt“ benötigen, können sie sich in Ihrem System niederlassen und einer fremden Person die Fernsteuerung Ihres PCs ermöglichen.

Was ist ein Trojanisches Pferd?

Trojanische Pferde sind Programme, die sich als nützliche Software tarnen, aber Computern großen Schaden zufügen können. Vor kurzem gab ein Trojanisches Pferd vor, eine E-Mail mit Anlagen für Microsoft-Sicherheitsaktualisierungen zu sein. Tatsächlich aber enthielt es Viren zur Deaktivierung von Antivirus- und Firewall-Software.
Trojanische Pferde vermehren sich, wenn Benutzer ein Programm öffnen, das scheinbar von einer legitimen Quelle stammt, z.B. können sie in kostenlos heruntergeladener Software enthalten sein. Downloaden Sie deshalb niemals Software von einer nicht ver-

trauten Quelle. Downloaden Sie Microsoft-Updates und -Patches nur von Microsoft Windows Update oder Microsoft Office Update.

Spam

Spam ist der Begriff für unerwünschten, den gewünschten Mailverkehr behindernden, Massenversand von Werbemail.
Spam kann in verschiedenen Variationen auftreten, das geht von den - wohl geläufigsten - Massenmails mit Werbung, bis hin zu virenverseuchten Mails, die Würmer vom eigenen, infizierten, Rechner aus verschicken.

Im Groben können folgende Varianten unterschieden werden:

Hoaxes: Hoaxes enthalten in der Regel Virenwarnungen oder Spendenaufrufe. Damit einher geht auch der Aufruf, dieses Mail an so viele Bekannte wie möglich weiterzuleiten, um eine möglichst große Verbreitung zu gewährleisten.
Kettenbriefe: Kettenbriefe folgen einem ähnlichen Schema wie Hoaxes, unterscheiden sich aber inhaltlich von diesen. Auch hier geht es darum, die Empfänger dazu zu bringen, sie an möglichst viele Bekannte weiterzuleiten.
Kommerzielle Werbemails: Hier werden von kommerziellen Versendern Werbemails in großen Mengen versandt.
Von Würmern erzeugter Spam: Einige bekannte Mailwürmer installieren auf dem Wirtssystem einen eigenen Mailhost, über den sie Kopien von sich selbst an alle Mailadressen versenden, welche sie in den auf dem Wirtssystem vorhandenen Dokumenten und Mailclients finden.

Woher bekommen Spammer ihre Adressen?

Scanning: Beim Scanning, auch Harvesting genannt, wird Software, oft auch Bot (von Robot) genannt, eingesetzt um Mailadressen aus öffentlich zugänglichen Quellen zu beschaffen. Hier scannen diese Bot´s Webseiten und Newsgroups nach Mailadressen ab und tragen diese in die Datenbanken der Spammer ein.
Adresshandel: Hier werden Adressen, die oft durch Freemailanbieter, Newsletterversender oder Anbietern von Maildiensten gesammelt wurden, weiterverkauft, wodurch diese Firmen ihre in der Regel kostenlosen Dienste refinanzieren.
Brut Force: Spammails werden an Standardadressen wie z.B. info@ oder zufällig generierte Adressen verschickt

Maßnahmen gegen Spam

Die Gefahr seine Mailadressen an Spammer zu geben besteht meistens bei:
Eingabeformularen auf Webseiten: Sehr viele Webseiten verlangen eine Registrierung. Hier wird in der Regel auch die Mailadresse als Pflichtinformation abgefragt. Hier sollte ein Blick auf das „privacy statement“ geworfen werden, in welchem die Anbieter oft eine Weitergabe der Adressen einschließen. Grundsätzlich muss hier damit gerechnet werden dass die Adresse für Spam missbraucht wird. Abhilfe schafft für so etwas einen oder mehrere Freemaileraccounts zu betreiben, die nicht für den täglichen Mailverkehr verwendet werden, sondern nur gezielt bei Bedarf.

Einträgen in Mailinglisten oder Newsletter: Hier sollte man, neben der Hauptmailadresse, eine oder mehrere Adressen bei Freemailern nutzen, die für so etwas angegeben werden. Wenn so ein Postfach zu sehr von Spam belastet wird, kann es gelöscht werden und ein neues eingerichtet werden.
Webseiten: Von Einträgen der eigenen Mailadresse auf Webseiten in einem üblichen Mailformat (adresse@domain.de) sollte man tunlichst absehen, da es automatisierte Software gibt, die solche Adressen ausliest. Besser sind hier Schreibweisen wie „adresse [at] domain [dot] de“
Bekannte die Mailadressen unwissentlich weitergeben Oft werden Mails an eine Gruppe von Empfängern gesendet, die allerdings alle im Feld „an“ eingetragen wurden. Das hat den Effekt, dass jeder der Empfänger im Klartext in der Adresszeile eingetragen wird und die Adressen so, z.B. von Mailwürmern, auch leicht ausgelesen werden können. Hier hilft nur, das Feld „BCC“ zu verwenden. Sollte man so eine Mail empfangen ist es gut den Absender zu informieren und auf die damit - auch ihn betreffenden - Probleme hinzuweisen.

Wie sollte man auf Spammails reagieren?

Spammails sollte man einfach löschen. Auf keinen Fall sollte man darauf antworten, oder gar versuchen sich über die meist angegebenen Links aus der Verteilerliste auszutragen. In der Regel dienen diese Links nur dazu, Adressen auf ihre Echtheit hin zu verifizieren, so dass sie dann noch teurer weiterverkauft werden können. Zudem sind die Absenderadressen in der Regel gefälscht um eine Verfolgung der Spammer zu erschweren.

Teilen Sie nicht jedem Ihre E-Mail-Adresse mit

Einige Spammer erhalten Adressenlisten von Websites, auf denen Sie sich für kostenlose Angebote eingetragen, eine Onlinebestellung aufgegeben oder an einem Preisausschreiben teilgenommen haben. Ihre Adresse kann auch in Telefonbüchern, Newsgroups, Jobbörsen und Chaträumen gefunden werden.

Beachten Sie die folgenden Tipps:
Richten Sie eine nur für Webtransaktionen bestimmte E-Mail-Adresse ein. Erwägen Sie ein E-Mail-Konto bei einem kostenlosen Anbieter für Ihre Onlinetransaktionen. Auf diese Weise bleibt Ihre tatsächliche E-Mail-Adresse geheim.
Teilen Sie Ihre Haupt-E-Mail-Adresse nur Leuten mit, die Sie kennen. Vermeiden Sie den Eintrag Ihrer E-Mail-Adresse in Verzeichnissen von Internetadressen. Geben Sie Ihre E-Mail-Adresse auch nicht auf Ihrer Website an.
"Tarnen" Sie Ihre E-Mail-Adresse. Verwenden Sie eine getarnte E-Mail-Adresse, wenn Sie sie in einer Newsgroup, einem Chatraum oder an einem schwarzen Brett veröffentlichen. Sie können beispielsweise bei der Adressenangabe anstatt des Buchstabens "o" Nullen (0) verwenden (z. B. s0me0ne@beispiel.c0m). Ihre Adresse kann von einer Person korrekt gelesen werden. Spammer dagegen verwenden automatische Verfahren zum Auslesen von E-Mail-Adressen. Eine getarnte Adresse ist daher für Spammer nutzlos.
Achten Sie auf markierte Ankreuzfelder. So mancher Onlinehändler fügt seinen Formularen ein (bereits markiertes!) Ankreuzfeld hinzu, das Ihr Einverständnis zur Weitergabe

Ihre E-Mail-Adresse an Dritte bestätigt. Klicken Sie auf das Ankreuzfeld, um es zu deaktivieren.

Lesen Sie die Richtlinien zum Datenschutz von Websites

Lesen Sie beim Beantragen von webbasierten Diensten wie Online-Banking, Online-Shopping oder Rundschreiben sorgfältig die Richtlinien zum Datenschutz, bevor Sie Ihre E-Mail-Adresse preisgeben. Aus diesen geht hervor, ob und wenn ja, wie Ihre auf der Website angegebenen Daten weitergegeben werden. (Wenn Sie die Richtlinien nicht lesen, erklären Sie sich u. U. mit der Weitergabe Ihrer Informationen einverstanden, ohne es zu wissen.)
Schweigt sich die Website darüber aus, sollten Sie sich die Angabe dieser Daten genau überlegen: Zahlreiche Firmen - darunter auch namhafte Unternehmen - verwerten Ihre Informationen auf eine Weise, der Sie evtl. nicht zustimmen.

Wie stelle ich eine Wurm- oder Virusinfektion fest?

Typische Anzeichen dafür, dass Ihr PC mit einem Virus infiziert ist, sind folgende Symptome:

- Möglicherweise arbeitet der Computer nur noch mit reduzierter Leistung, der Computer reagiert überhaupt nicht mehr oder er startet alle paar Minuten neu. Manche Viren greifen die zum Starten des Computers erforderlichen Dateien an. Ist Ihr Computer von einem Virus dieser Art befallen, erscheint nach dem Einschalten möglicherweise ein leerer Bildschirm.
- Sie erhalten eine E-Mail-Nachricht, die einen merkwürdigen Anhang enthält. Wenn Sie den Anhang öffnen, werden Dialogfenster angezeigt, oder die Systemleistung nimmt von einem Augenblick zum anderen plötzlich rapide ab.
- Ein Anhang, den Sie kürzlich geöffnet hatten, besitzt eine merkwürdige Dateinamenerweiterung wie beispielsweise .jpg.vbs oder .gif.exe.
- Ein Antivirenprogramm ist ohne ersichtlichen Grund deaktiviert und kann nicht neu gestartet werden.
- Auf dem Bildschirm werden merkwürdige Dialogfenster angezeigt.
- Aus Ihren Lautsprechern werden plötzlich merkwürdige Geräusche oder merkwürdige Musik wiedergegeben.
- Ein Programm verschwindet von Ihrem Computer, obwohl Sie das Programm nicht deinstalliert haben.
- Windows wird unerwartet neu gestartet.

Bitte beachten Sie, dass einige Symptome auch andere Ursachen (z.B. Hardware-Fehler) haben können. Nur mit Hilfe eines aktuellen Antivirusprogramms können Sie zuverlässig feststellen, ob Ihr Computer mit einem Virus infiziert ist oder nicht.

Was ist Spyware?

Spyware ist Software, die ohne Ihre Zustimmung und ohne Ihr Wissen Ihre persönlichen Informationen ausspioniert. Spyware-Angriffe drohen z. B. beim Herunterladen von Mu-

sik über Filesharing-Programme, kostenlosen Spielen oder anderer Software aus unbekannten Quellen. Spyware sammelt Informationen über die von Ihnen besuchten Websites oder vertraulichere Daten wie Benutzernamen und Kennwörter.
Spyware tritt häufig mit so genannter Adware auf, die einige Werbetreibende unbemerkt auf Ihrem Systeminstallieren. Adware erzeugt unerwünschte Werbeanzeigen, die oft auch pornografisches oder anderes unerwünschtes Material enthalten. Diese Anzeigen können auf Ihrem Desktop Speicherplatz belegen: Produktives Arbeiten ist nicht mehr möglich und die Leistung des PCs und des Systems werden beeinträchtigt.
Tipp: Nicht jede Software, die mit Anzeigen verbunden ist oder Ihre Onlineaktivitäten verfolgt, ist schlecht. Zum Beispiel kann ein kostenloser Musikservice mit gezielter Werbung ein faires Geschäft sein. Lassen Sie sich zur Sicherheit genau darüber informieren, was die Software bewirkt.

Was ist unerwünschte Software?

Spyware und nicht autorisierte Adware sind Beispiele "unerwünschter" Software. Gemeint sind Programme, die ohne Ihre Einwilligung die Kontrolle über Ihre Homepage oder Suchseite übernehmen. Es gibt mehrere Möglichkeiten, wie unerwünschte Software auf Ihr System gelangt. Häufig wird die Software während der Installation anderer Software, wie z. B. Musik oder Videos als Filesharing-Programm, unbemerkt installiert.
Im Folgenden zeigen wir Ihnen, wie Sie die Installation unerwünschter Software auf Ihrem Computer verhindern und was nach einer bereits erfolgten Installation zu tun ist.

Schritt 1: Passen Sie die Sicherheitseinstellungen von Internet Explorer 6 (Webbrowser) an

Im Internet Explorer von Microsoft können Sie die Sicherheitsstufe einstellen, mit der Sie sich im Internet bewegen. Wählen Sie eine mittlere oder hohe Sicherheitsstufe. Auf diese Weise können Sie kontrollieren, was auf Ihrem Computer installiert wird. Je höher die Sicherheitsstufe, desto geringer ist das Risiko, Opfer von Spyware zu werden. Bei Sicherheitsstufe „Niedrig“ können Websites ohne entsprechenden Hinweis Software auf Ihren Computer downloaden. Seien Sie mit dieser Einstellung daher vorsichtig.

Schritt 2: Laden Sie keine Dateien unbekannter Anbieter auf Ihren Computer

Im Folgenden sind einige nützliche Tipps aufgeführt, wie Sie sich vor unerwünschter Software schützen können.

- Installieren Sie Software nur von vertrauenswürdigen Websites Bevor Sie von einer Website etwas downloaden, sollten Sie sicher sein, dass Sie dieser Website vertrauen können. Ist dies nicht der Fall, sollten Sie die Software nicht downloaden. Wenn Sie sich nicht sicher sind, fragen Sie z. B. Ihre Freunde, oder ziehen Sie andere vertrauenswürdige Quellen zu Rate.
- Lesen Sie das Kleingedruckte Lesen Sie die Lizenzvereinbarung und die Datenschutzbestimmungen sorgfältig durch, bevor Sie Software aus dem Internet auf Ihrem Computer installieren. Klicken Sie erst dann auf „Ich stimme zu“ oder „OK“. Wenn Sie im „Kleingedruckten“ etwas finden, das Sie misstrauisch macht, sollten Sie die Installation abbrechen. Lässt sich das Fenster nicht schließen, wenn Sie den Li-

zenzvereinbarungen nicht zustimmen, klicken Sie niemals auf "Ja" oder "Ich stimme zu", sondern versuchen Sie stattdessen, das Fenster über das „X“ in der rechten oberen Fensterecke zu schließen.
- Seien Sie vorsichtig mit Musik und Filmen als "kostenlose" Filesharing-Programme Augen auf beim Download: Statistiken zufolge stammt ein Großteil der auf Systemen installierten unerwünschten Software von diesen Programmen.

Schritt 3: Suchen Sie nach Anzeichen für unerwünschte Software auf Ihrem Computer

Unerwünschte Software ist darauf ausgelegt, ohne Ihr Wissen ausgeführt zu werden. Folgende Merkmale sind typisch für eine Infektion:

- Beim Starten Ihres Internetbrowsers wird eine Seite angezeigt, die Sie noch nie zuvor gesehen haben.
- Über das Suchfeld werden Sie zu einer Seite weitergeleitet, die Sie nicht wieder erkennen.
- Es wird Werbung auf Seiten angezeigt, die Sie vorher dort nicht gesehen haben.
- Sie werden mit Popups konfrontiert - unabhängig von der besuchten Seite. Diese Popups können zum Teil auch anstößig sein.
- Ihr Computer ist ungewöhnlich langsam. Spyware nutzt die Ressourcen ihres Computers. Dies kann den Computer verlangsamen. Bugs in der Software können sogar zu einem Computerabsturz führen.

Schritt 4: Verwenden Sie ein Tool zur Erkennung und Entfernung unerwünschter Software

Trotz aktivierter Firewall, Antivirus-Programm und aktueller Software sind Sie nicht gänzlich vor unerwünschter Software gefeit. Mit spezieller Erkennungs- und Entfernungssoftware können Sie nach unerwünschter Software suchen und diese vom Computer entfernen. Denken Sie daran, dass danach evtl. ein kostenloses Programm nicht mehr genutzt werden kann, das mit der Software im Zusammenhang steht.
Tipp: Halten Sie Ihre Erkennungs- und Entfernungstools stets aktuell. Viele Hersteller bieten die Möglichkeit einer automatischen Suche nach Updates bei jeder neuen Internetverbindung an. Anderenfalls sollten Sie auf der Website des Herstellers regelmäßig nach Downloads suchen.