Berliner Schule

IT-Sicherheitshandbuch für die Verwaltungen in Berliner Schulen

Handreichung für den sicheren Einsatz von Informationstechnologie

Version 2.2

Historie

Version	Datum	Bearbeiter	Änderungen
0.1	14.09.2009	M. Pravida/BuDru	Erstanlage des Dokuments
0.2	16.09.2009	M. Pravida/BuDru	Einarbeitung der Ergebnisse des Workshops vom 15.09.2009
0.3	18.09.2009	M. Pravida/BuDru	Einarbeitung der fehlenden Informationen nach Rücksprache mit Hrn. Gollanek
0.4	18.09.2009	H. Rieger/BuDru	Review; Vorabversion
0.5	14.10.2009	Oliver Gollanek	Überarbeitung und Punkt Phishing eingeführt
1.0	25.11.2009	Oliver Gollanek	Finalisiert
1.0.1	04.12.2009	Oliver Gollanek	QS
1.0.1a	19.02.2010	Oliver Gollanek	QS
1.0.2	12.03.2010	Oliver Gollanek	
1.0.3	20.03.2012	Team Regionale IT-SiBe	QS
1.0.4	20.08.2013	Oliver Gollanek	Anpassung Kontaktdaten und Stellenzeichen; Thema Diebstahl ergänzt
1.1	18.02.2015	Horst Daniel (Zuarbeit von Ch. Schromm/BuDru)	Allgemeine Datenpflege, Einfügen des Datenschutzes in Abschnitt 4, Absenderfälschung bei E-Mail, Ergänzung eKlaBu-relevanter Aspekte, Erstellung Laptop-Nutzungsrichtlinie
2.0	14.06.2015	Oliver Gollanek	völlige Überarbeitung neues Layout
2.1	28.12.2016	Team Regionale IT-SiBe	Aktualisierung / Deckblatt
2.2	11.10.2017	Mischa Hengst	Umzug SSZB / ZSVU

Inhaltsverzeichnis

Sie sind gefordert! Und wir helfen Ihnen dabei …

Liebe Kolleginnen und Kollegen,

nicht nur durch die großen Datenskandale der letzten Jahre ist das Thema Sicherheit in der Informationstechnik oben auf der Tagesordnung angekommen. Im Zeitalter einer alle Lebensbereiche umfassenden Digitalisierung und einer immer noch weit verbreiteten Sorglosigkeit im Umgang mit eigenen und den persönlichen Daten anderer, ist es immer wichtiger, dass Sie, als Verantwortliche und Wächter über sensible personengebundene Daten, Ihren Anteil zu deren Schutz leisten.

Dabei können die Bedrohungen für die IT-Landschaft Ihrer Schule vielfältigster Ausprägung sein. Bei der missbräuchlichen Nutzung Ihres Internetanschlusses oder der Rechenleistung Ihrer Clients geht es in erster Linie um Ihre IT-Infrastruktur und Ihre Arbeitsfähigkeit. Es können aber auch persönliche Daten der Schüler, Eltern oder Lehrkräfte Ihrer Schule Ziel missbräuchlicher Nutzung werden.

Leider werden immer noch häufig, zumindest im privaten Bereich, Anschauungen vertreten wie beispielsweise: „Ich habe doch nichts zu verbergen.“, oder „Wen interessieren diese Daten schon.“ Nicht nur durch die Möglichkeit inzwischen große Datenmengen maschinell auszuwerten, scheinbar belanglose Daten automatisiert zu aussagekräftigen Datensätzen zu verknüpfen und diese missbräuchlich einzusetzen, ist eine erhöhte Aufmerksamkeit geboten.

Wir wollen Sie, unter anderem durch dieses IT-Sicherheitshandbuch, beim sicheren Einsatz von Informationstechnologie an Ihrer Schule unterstützen. Dieses Handbuch soll Ihnen eine verbindliche Sammlung wirkungsvoller Werkzeuge und Verhaltensweisen zum Schutz von IT und persönlicher Daten an Ihrer Schule geben und Sie im täglichen Umgang mit Informationstechnologie unterstützen.

Da nicht alle Ihre Fragen und Sorgen im Umgang mit persönlichen Daten in diesem Rahmen abschließend geklärt werden können, stehen Ihnen die IT-Sicherheits-beauftragten Ihrer Region gerne unterstützend für Fragen und Beratung zum sicheren und vor allem rechtssicheren Umgang mit Daten und Informationstechnologie zur Verfügung.

Dieses Handbuch wird permanent fortgeschrieben. Da seine Qualität auch von Ihren Erfahrungen und Verbesserungsvorschlägen abhängt, sind wir Ihnen für Anregungen oder Verbesserungsvorschläge sehr dankbar.

Organisation der IT-Sicherheit an den Schulen

Team der Regionalen Beauftragten für IT-Sicherheit

Die Regionalen IT-Sicherheitsbeauftragten, deren Aufgabengebiet sich über die öffentlichen Schulen von jeweils zwei Bezirken erstreckt, sind in der Regel Ihre Ansprechpartner und unterstützen Sie bei allen Fragen und Anforderungen rund um die IT-Sicherheit an Ihrer Schule.

Reinickendorf Spandau	Herr Kirk	alexander.kirk@sima.schule.berlin.de
Charlottenburg-Wilmersdorf Steglitz-Zehlendorf	Herr van Gemmern	michael.vangemmern@sima.schule.berlin.de
Friedrichshain-Kreuzberg Neukölln	Herr Hengst	mischa.hengst@sima.schule.berlin.de
Mitte Tempelhof-Schöneberg	Frau Röhr	kathrin.roehr@sima.schule.berlin.de
Lichtenberg Pankow	Herr Koll	andreas.koll@sima.schule.berlin.de
Marzahn-Hellersdorf Treptow-Köpenick	Herr Ullsperger	volker.ullsperger@sima.schule.berlin.de

Die Namen und Kontaktdaten der Regionalen IT-Sicherheitsbeauftragten finden Sie auch aktuell im Internet: https://www.egovscohool-berlin.de/IT-Sicherheit-Kontakt.

Falls Sie die genannten Personen nicht direkt erreichen, wenden Sie sich bitte an unsere zentrale Hotline.

zentrale Hotline (Schulservicezentrum-Berlin - SSZB):

030/ 90 214 666 oder

sszb@schule.berlin.de

Sicherer Umgang mit Computern und Informationen

Wie verbindlich ist das IT-Sicherheitshandbuch?

Das IT-Sicherheitshandbuch enthält verbindliche Regelungen und Maßnahmen, die für den sicheren Umgang mit der Informationstechnologie im Umfeld von eGovernment@School notwendig sind und beachtet werden müssen.

Das Sicherheitshandbuch ist interessant, aber ich habe andere oder darüber hinausgehende Fragen zur IT-Sicherheit. An wen kann ich mich wenden?

Die Aufrechterhaltung der IT-Sicherheit ist eine Aufgabe, die uns alle angeht. Verbesserungen und Anregungen, die uns helfen, das Sicherheitsniveau in der IT-Schulumgebung auf hohem Niveau zu halten, bzw. weiter zu erhöhen, sind sehr willkommen. Gerne unterstützen wir Sie auch bei Ihren Fragen und Problemen.

Bitte wenden Sie sich dafür an Ihre/n Regionalen IT-Sicherheitsbeauftragte/n und teilen Sie Ihre Vorschläge mit.

Welche IT-Sicherheitsrisiken existieren an meinem Arbeitsplatz?

Grundsätzlich beinhaltet der Umgang mit IT-Systemen immer Risiken. Diese Risiken stellen sich für Nutzer unüberschaubarer dar, als dies im analogen Zeitalter der Fall war.

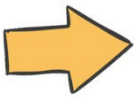
Oft sind für den Nutzer die Schwachstellen von IT-Systemen und dem eigenen Umgang mit ihnen nicht ersichtlich. Passwortdiebstahl und Schadsoftware (Viren, Trojanische Pferde, Würmer) erscheinen dabei noch am greifbarsten. Aber wer denkt schon an Phishing, Computersabotage, Datenveränderung oder gar „Social Engineering“?

Durch diese komplexen Bedrohungsszenarien für Ihre Informationstechnologie wird Nutzerverhalten zu einem nicht unerheblichen Risiko. Auf den folgenden Seiten werden deshalb nicht nur technische Sicherheitsmechanismen, sondern auch Nutzerverhaltensweisen dargestellt, die Ihnen einen größtmöglichen Schutz gewährleisten.

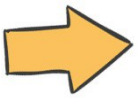
Welche Risiken den Datenschutz betreffend existieren an meinem Arbeitsplatz?

Personenbezogene Daten unterliegen dem Datenschutz. Deren Korrektheit (Integrität) und der Schutz vor Verlust (Vertraulichkeit, Verfügbarkeit) ist ein unabdingbares Recht eines jeden Betroffenen. Missbrauch von personenbezogenen Daten ist in jedem Fall zu vermeiden. Allein der unbefugte Zugang zu Anwendungen für die Datenverarbeitung (z.B. elektronisches Klassenbuch, Schuldistanzermittlung) kann einen immensen Schaden für die betroffenen Personen bedeuten, egal ob für Schüler, Erziehungsberechtigte oder Mitglieder des Lehrerkollegiums und der Schulleitung.

Damit sind die drei Grundpfeiler der IT-Sicherheit angesprochen:



Vertraulichkeit



Verfügbarkeit

Integrität

Einfach & Effektiv: Sicherheitsmaßnahmen

Im Folgenden werden Ihnen ein paar einfache aber effektive Sicherheitsmaßnahmen vorgestellt. Nicht nur in dienstlicher Umgebung sind diese sinnvoll, vieles kann auch im privaten Bereich verwendet werden.

Bildschirmsperre

Die Bildschirmsperre dient dazu, einen Rechner gegen die Benutzung durch Unbefugte zu sperren. Ein Weiterarbeiten ist erst möglich, wenn sich der angemeldete Benutzer mit seinem Passwort authentifiziert hat.

Ich will doch nur kurz Wasser holen!

Der Zeitraum Ihrer Abwesenheit ist nicht so erheblich. Mit der Bildschirmsperre wird nicht nur verhindert, dass zufällig anwesende oder gezielt suchende Personen Zugriff auf personenbezogene Daten und Anwendungen an Ihrem Rechner haben, sondern auch, dass andere mit Ihrer Kennung Tätigkeiten an Ihrem Rechner durchführen können, die auf Sie zurückgeführt werden. Einem versierten IT-Nutzer reichen schon wenige Sekunden, um Ihnen, dem Land Berlin oder einzelnen Personen (z.B. Schülern) während Ihrer Abwesenheit Schaden zuzufügen (zum Beispiel durch die Einsicht in ein Personaldokument, die Änderung von Schülerdaten oder das Drucken sensibler Dokumente).

Wenn Sie Ihren Arbeitsplatz verlassen, sperren Sie bitte immer manuell den Rechner.

Das erreichen Sie so:

- **PC in der ZSVU:** Klicken Sie wie beim Abmelden auf Ihren Namen und dort dann auf **Sperren**.
- **alle anderen PC:** + ***L*** (Windows- und L-Taste gleichzeitig drücken.) oder Sie drücken gleichzeitig die Tasten ***Strg*** + ***Alt*** + ***Entf*** und wählen ***Computer sperren***.

Die Sperre ist auch erforderlich, wenn Sie den Arbeitsplatz nur „kurz“ verlassen und/oder Kollegen noch im Raum sind!

Rechner, die Ihnen von eGovernment@School zur Verfügung gestellt worden sind, schalten die Bildschirmsperre nach 20 Minuten ein. Sollten Sie an einem anderen Rechner ohne diese Einstellung arbeiten, so bitten Sie Ihren Administrator, die Bildschirmsperre ebenfalls auf diesen Zeitabstand einzustellen. Eine automatische Bildschirmsperre entbindet allerdings nicht von der Verpflichtung den Bildschirm manuell zu sperren, sobald der Arbeitsplatz verlassen wird.

Passwörter – richtig auswählen und verwenden

Benutzernamen und Passwörter werden benötigt, um sich bei Computersystemen und Anwendungen zu authentifizieren. Individuelle Kennungen ermöglichen eine komplexe Rechtevergabe und eine Nachvollziehbarkeit von Handlungen.

Gelingt es einer Person mit böswilligen Absichten Ihr Passwort zu ermitteln, kann diese unter Ihrem Namen Daten zerstören, manipulieren und/oder ausspionieren.

Das individuelle Anmelden ist eine Datenschutzvorgabe. Es muss im Zweifelsfalle prüfbar sein, wer was getan hat. Das bedeutet keine ständige Überwachung, sondern dient dem Schutz der Nutzer.

Es gibt diverse Möglichkeiten fremde Passwörter zu ermitteln:

- Passwort erraten, aufgrund von persönlichen Informationen (Geburtsdatum, Familienangehörige, Reiseziele)
- Passwort mit Hilfsprogrammen ermitteln (Vergleich mit Wörterbüchern, Vornamenslisten, etc.)
- Programme probieren alle möglichen Kombinationen aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen aus (BrutForce-Programme).
- Notierte Passwörter auffinden
- Erfragen der Passwörter

Für Passwörter gelten folgende Grundsätze

- Länge: mindestens 8 Zeichen
- Lebensdauer: regelmäßig ändern, sofern nicht bereits vom System vorgegeben
- Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (sogenannte Komplexitätsanforderung)

Je länger und komplexer ein Kennwort ist, desto länger benötigen BrutForce-Programme zum Finden des Kennwortes. Bei mehr als 8 Zeichen werden es mehrere Jahre sein. **Benutzen Sie deshalb keine Passworte, die kürzer als 8 Zeichen sind.**

Passwörter sind persönlich und somit stets geheim zu halten. Dies gilt auch gegenüber vertrauenswürdigen Personen, wie dem IT-Sicherheitsbeauftragten, dem Administrator oder der Schulleitung. Passwörter dürfen nicht aufgeschrieben werden und leicht zugänglich abgelegt werden (z.B. „Post-it“ am Bildschirm oder unter der Tastatur).

Eine kleine Hilfestellung zu Passwörtern

- Wählen Sie Passwörter, die Sie sich leicht merken können.
- Verwenden Sie eine Kombination aus Buchstaben, Zahlen und Sonderzeichen.
- Einfach zu merken sind Sätze, die dann entsprechend für das Passwort verwendet werden.

Beispiel: „**Ein Esel hat 2 Ohren und 4 Beine.“**. Für das Kennwort verwendet man nur die Anfangsbuchstaben der Wörter. Statt des Wortes **und** wird das Sonderzeichen **&** benutzt.

Das Kennwort würde bei diesem Satz lauten: „**EEh2O&4B.**“

Solch ein Passwort ist kaum zu erraten und nicht über Vergleiche mit Wörterbüchern usw. ermittelbar.

Hinweis: Nutzen Sie bitte nie dieses Kennwort. Denken Sie sich einen eigenen Satz aus!

Was kann ich tun, wenn ich mein Passwort vergessen habe?

Wenden Sie sich an Ihren Administrator oder, falls Sie schon in der sicheren Verwaltungsinfrastruktur von eGovernment@School (ZSVU) arbeiten, einfach an die zentrale Hotline (030/ 90 214 666).

Was ist, wenn ich im Urlaub bin und meine Kollegen mich vertreten sollen?

Zugangskennungen und Passwörter dürfen grundsätzlich nicht anderen Personen mitgeteilt werden. Um Zugriff auf Daten wirksam zu regeln, ist es notwendig, dass jeder Benutzer unter seiner eigenen Kennung und eigenem Passwort Zugang zum System hat. Werden Passwörter von mehreren Anwendern gemeinsam genutzt, besteht die Gefahr, dass nicht mehr nachvollziehbar ist, welche Personen unter einer bestimmten Benutzerkennung arbeitet.

Benötigen Sie Zugang zu einem Rechner, so wenden Sie sich an Ihren Administrator oder, falls Sie schon in der sicheren Verwaltungsinfrastruktur von eGovernment@School (ZSVU) arbeiten, einfach an die zentrale Hotline (030/ 90 214 666). Diese wird Ihnen dann ein eigenes Passwort erstellen.

Sichere Nutzung des Internets

Die Nutzung des Internets (WWW, FTP usw.) ist immer mit Sicherheitsrisiken verbunden. Sie übernehmen die entsprechende Verantwortung für den ordnungsgemäßen Umgang mit dem zur Verfügung gestellten Internetzugang.

Um die Internetnutzung so sicher wie möglich zu machen, gelten die folgenden Grundsätze

- Die Internetnutzung ist nur mit den installierten Programmen (Browser) und über die zur Verfügung gestellten Anschlüsse zulässig.
- Die private Nutzung des Internets ist grundsätzlich nicht zulässig (Siehe [1])
- Unterlassen Sie das Herunterladen von ausführbaren Programmen bzw. das Speichern von ausführbaren Dateien. Diese können Computerviren oder „Trojanische Pferde“ beinhalten oder die Stabilität Ihres Computers beeinträchtigen.
- Benutzen Sie keine Speicherdienste im Internet (sogenannte Clouds). Ihre Daten gehören nur auf den zur Verfügung gestellten Schulserver oder auf den Rechner, an dem Sie arbeiten.
- Benachrichtigen Sie die zentrale Hotline (030/ 90 214 666), falls Sie an Ihrem Rechner ungewöhnliche Effekte oder Datenverluste feststellen.
- Inzwischen sind aktive Webinhalte erlaubt (ausführbare Codes, die vom Webbrowser heruntergeladen, und auf dem lokalen Computer ausgeführt werden). Allerdings sollte bei der Ausführung von z.B. JavaScript-, ActiveX- und Java-Inhalten grundsätzlich erhöhte Aufmerksamkeit geboten sein.
- Meiden Sie unseriöse Seiten und „wilde Downloads“.
- Denken Sie daran, dass Sie mit einer IP-Adresse des Berliner-Landes-Proxy-Servers im Internet unterwegs sind. Von außen ist Ihr Surfverhalten, insbesondere wenn Seiten berechtigt sind, sog. *Cookies* in Ihrem Browser abzulegen, zurück verfolgbar. Damit repräsentieren Sie das Land Berlin im Internet.
- Geben Sie niemals Ihre persönlichen Daten (wie beispielsweise Adresse und Geburtsdatum) an, wenn Sie nicht wissen, wofür diese Daten verwendet werden sollen.

Verstöße gegen diese Grundsätze können unter Umständen arbeits- bzw. dienstrechtliche sowie strafrechtliche Konsequenzen haben.

Sicherer Datenaustausch (Wechselmedien & E-Mail)

Datenaustausch ist eine Grundvoraussetzung für Zusammenarbeit. Dementsprechend ist es unvermeidbar Daten mit Kollegen oder Behörden auszutauschen, sei es per E-Mail oder über ein Wechselmedium (USB-Stick, Festplatte, CD, etc.). Der Datenaustausch birgt jedoch einige Risiken, wie beispielsweise der Verlust von Wechseldatenträgern oder das Einschleusen von Schadsoftware auf einem Dienstrechner. Deshalb wurden hierfür klare Vorgaben definiert.

Folgende Vorgaben gelten beim Datenaustausch:

- Ein Datenaustausch darf nicht von einem unsicheren Netz (z. B. edukatives Netz) in ein sicheres Netz erfolgen. Als sicher betrachten wir das Netz, das eGovernment@School Ihnen zur Verfügung stellt (ZSVU) oder ein Netz, welches durch Ihren eigenen Administrator in Ihrem Verwaltungsbereich gut gepflegt ist.

Korrekte Verwendung von Wechselmedien

- Lassen Sie Wechseldatenträger nie unbeaufsichtigt liegen.
- Die USB-Sticks müssen in einem abschließbaren Schrank aufbewahrt werden, um den Zugriff durch Unbefugte zu verhindern.
- Daten dürfen nur auf definierten USB-Sticks mit Verschlüsselungstechnik gespeichert werden.
- Booten Sie Ihren Dienstrechner nicht von Wechseldatenträgern.

Datenaustausch per E-Mail

- Die Schulleitungen haben die Möglichkeit Ihre Mails zu verschlüsseln. Bei vertraulichen Daten muss diese Möglichkeit unbedingt genutzt werden. Dafür wurden die Signatur- und Verschlüsselungszertifikate von der Senatsverwaltung zur Verfügung gestellt.

Dienstliche E-Mail-Nutzung

Der interne E-Mail-Dienst ist zur behördlichen Kommunikation gedacht.

Für die E-Mail-Nutzung gelten folgende Grundsätze

- Die E-Mail-Nutzung ist nur mit den installierten E-Mail-Programmen zulässig.
- Die private Nutzung der E-Mail-Dienste ist grundsätzlich nicht zulässig (Siehe [1])
- Arbeiten Sie nur unter Ihrer eigenen Benutzerkennung und geben Sie diese nicht weiter.
- Öffnen Sie keine Anhänge, welche Sie nicht erwartet haben und die Ihnen zweifelhaft erscheinen.
- Benachrichtigen Sie die zentrale Hotline (030/ 90 214 666), falls Sie an dem Rechner ungewöhnliche Effekte bzw. Datenverluste feststellen.
- Leiten Sie nicht leichtfertig E-Mails an eine große Zahl von Empfängern weiter. Kettenmails etc. sind dringend zu vermeiden.

Verstöße gegen diese Grundsätze können unter Umständen arbeits- bzw. dienstrechtliche sowie strafrechtliche Konsequenzen haben.

Sichere Berliner Schulmail für die Schulleitung

Ihnen wurde für Ihr Schulmailkonto die Möglichkeit zur Verfügung gestellt**,** E-Mails rechtssicher digital zu unterschreiben und zu verschlüsseln.

Nutzen Sie diesen Service, denn er schafft Ihnen Rechtssicherheit.

- Mit einer signierten Mail bestätigen Sie Ihre Identität als Schulleitung. Dies kann in bestimmten Fällen sogar Ihre Unterschrift ersetzen.
- Mit einer verschlüsselten Mail haben Sie die Möglichkeit ein mächtiges Instrument zu verwenden, das verhindert, dass die von Ihnen versendeten Informationen von Dritten mitgelesen werden.

Diese, Ihnen bereitgestellten Werkzeuge können Ihren Arbeitsalltag erleichtern. Nutzen Sie sie!

Vertrauliche Dokumente

Die Infrastruktur im Verwaltungsnetz muss besonders geschützt werden, da eine Vielzahl von personenbezogenen Daten verarbeitet werden. Jedoch sind auch Ausdrucke dieser Daten zu schützen. Daher besteht für alle Dokumente, deren Inhalt besonders schutzbedürftig ist, eine Kennzeichnungspflicht nach den Regelungen der GGO I (vertraulich, persönlich, verschlossen, nur für den Dienstgebrauch).

Lassen Sie die Dokumente nicht offen oder unverschlossen liegen und geben Sie diese nicht weiter. So verhindern Sie eine Einsichtnahme Dritter und/oder Unbefugter. Lesen Sie zu diesem Thema auch das Kapitel „Druckernutzung im Verwaltungsbereich“.

Entsorgung von Datenträgern und Papierdokumenten

Datenträger und Papierdokumente mit vertraulichen oder personenbezogenen Inhalten müssen in jedem Fall sicher entsorgt werden, um nicht in die Hände von Dritten zu geraten.

- Werfen Sie vertrauliche Dokumente und Datenträger auf keinen Fall in den Papierkorb!
- Papierdokumente müssen durch eine geeignete Methode unlesbar gemacht werden, beispielsweise mit Hilfe eines Aktenvernichters.
- Optische Datenträger (CDs und DVDs) können nur physisch zerstört werden.
  Entweder müssen Sie in möglichst kleine Teile zerbrochen oder die Beschichtung großflächig abgekratzt werden.
- Festplatten werden durch das einmalige Formatieren nicht sicher gelöscht. Sie müssen mehrmals überschrieben werden. Verwenden Sie dazu am besten ein geeignetes Programm.

Hinweise zum richtigen Löschen finden Sie auf unserem Portal

https://www.egovschool-berlin.de/node/940

- Personenbezogene Daten müssen immer verschlüsselt transportiert werden. Das betrifft Daten auf externen Datenträgern aber auch in E-Mail-Anhängen.
  Man kann verschlüsselte Datenträger zum Transport benutzen oder die Dateien vor dem Versand als E-Mail-Anhang verschlüsseln.

Die Anleitungen mit Download und Installation der benötigten Software finden Sie hier:

https://www.egovschool-berlin.de/node/957

Schutz vor gefährlicher Schadsoftware

Bei Schadsoftware handelt es sich um Computerviren, „Trojanische Pferde“, Computerwürmer u. ä. Diese Software kann Rechnern, Netzwerken, Behörden, Unternehmen und (durch Informationsabfluss) auch Dritten hohen Schaden zufügen.

Wie erkenne ich, dass mein Rechner infiziert ist?

Mögliche Indizien einer Rechnerinfizierung:

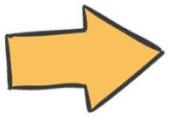
- Der Rechner verfügt über eine deutlich reduzierte Leistung. Eventuell reagiert er manchmal sogar gar nicht mehr.
- Der Zugriff auf bestimmte Laufwerke oder Datenträger ist nicht mehr möglich.
- Es werden nicht vorhersehbare Bilder, Meldungen und Dialogfenster auf dem Bildschirm angezeigt.
- Beim Öffnen eines Mailanhangs werden Dialogfenster angezeigt und/oder die Systemleistung nimmt sofort stark ab.
- Ihr Browser verfügt plötzlich über zusätzliche Icons und Symbolleisten.
- Es werden Warnungen angezeigt, dass bestimmte Programme versuchen eine Verbindung mit dem Internet herzustellen, obwohl Sie dies nicht veranlasst haben.
- Die Virensoftware ist deaktiviert und kann nicht mehr gestartet werden.
- Sie erhalten viele E-Mails mit dem Betreff "Undelivered Mail Returned to Sender“
- Es passieren Vorgänge (Verschwinden von Programmen etc.) auf Ihrem Computer ohne Ihr Zutun.

Bezüglich Schadsoftware gibt es folgende Sicherheitsvorgaben

- Schutz durch Antivirensoftware auf jedem PC. Das Schulservicezentrum hält für die von der Senatsverwaltung bereitgestellten Rechner eine Lizenz der Anti-Virensoftware McAfee für Sie bereit. Sollten Sie diesbezüglich Bedarf haben, so wenden Sie sich an das Schulservicezentrum: sszb@schule.berlin.de.
- Starten Sie Ihren Arbeitsplatzrechner nicht von Wechseldatenträgern (USB, CD etc.)
- Vor der Installation von zusätzlicher Software muss diese auf mögliche Gefährdungen hin untersucht werden. Deshalb erfolgt die Installation solcher Software durch den Systemadministrator.
- Öffnen Sie keine Dateien, die mit einer E-Mail mitgeschickt wurden und nicht von Ihnen erwartet werden, bzw. nicht dem üblichen E-Mail-Verkehr mit dem Absender entsprechen. Bei Anhängen mit den Dateiendungen .zip, .exe und .js sollten Sie besonders misstrauisch sein.
- Weitere Hinweise zum Umgang mit E-Mail-Anhängen finden Sie im Dokument auf der Plattform von eGovernment@School:
  https://www.egovschool-berlin.de/sites/default/files/Anhang_auf_Schadsoftware_pruefen-Version_01.pdf
- Klicken Sie nicht auf Links in einer E-Mail, die nicht von Ihnen erwartet wurde, bzw. nicht dem üblichen E-Mail-Verkehr mit dem Absender entspricht.
- Geben Sie keine Benutzerdaten bekannt, wenn Sie in E-Mails unbekannter Herkunft dazu aufgefordert werden.

Bei Vorfällen (Virenwarnungen, ungewöhnliches Verhalten o.ä.) gelten folgende Vorgaben:

- Keine Panik!
- Jegliche Tätigkeiten am PC einstellen, um ein Infizieren weiterer Dateien zu vermeiden. Den Rechner durch langes Drücken des Anschaltknopfes hart herunterfahren und sowohl vom Stromnetz als auch vom Netzwerk trennen.
- Bitte informieren Sie sofort die zentrale Hotline des SSZB (030/ 90 214 666).
- Virensuche und Virenbeseitigung darf nur durch für Viren zuständige Mitarbeiter der Informationstechnik erfolgen.
- „Falsche“ Virenbeseitigung kann zu größerem Schaden führen!



Auch bei Einhalten aller Vorsorgemaßnahmen kann ein Virus ins System gelangen, z.B. weil der Virus so neu ist, dass er von den Virenprüfprogrammen noch nicht erkannt wurde.

Bleiben Sie ruhig, wenn Sie einen Virus oder ungewöhnliches Verhalten Ihres Rechners bemerken und wenden sich an das Schulservicezentrum (030/ 90 214 666).

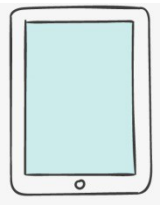
Nur so ist der Schaden gering zu halten.

Druckernutzung im Verwaltungsbereich

Die Funktionalitäten von Druckern sind in den letzten Jahren erheblich gestiegen. Oft bringt die erhöhte Funktionalität Vereinfachungen im Arbeitsablauf mit sich. Auf einige Funktionen, die inzwischen bei Druckern weit verbreitet sind, sollten Sie jedoch besonderes Augenmerk richten:

- Speicher von Druckern: Drucker verfügen über einen Speicher, der in manchen Fällen sogar das erneute Drucken von Dokumenten direkt über die Tasten an dem Drucker ermöglicht. Die Drucker die im Rahmen des eGovernment-Projektes an Ihre Schule ausgegeben worden sind, wurden so konfiguriert, dass dies nicht möglich ist. Bei schuleigenen Geräten sollten Sie ggf. prüfen, ob Ihr Drucker so konfiguriert wurde, dass dies möglich ist.
- Sie sollten auch einen Augenmerk auf die Webserverfähigkeiten vieler Drucker richten, da Sie so eventuell vertrauliche Daten im Netz verfügbar machen.
- Für den Druck der Schülerdaten steht ein separater Drucker in einem geschützten, verschlossenen Verwaltungsraum zur Verfügung. Sie dürfen ausschließlich diesen Drucker dafür benutzen.
- Sollte der Drucker defekt sein, verständigen Sie bitte die zentrale Hotline (030/ 90 214 666). Baugleiche Ersatzgeräte stehen in ausreichender Stückzahl zur Verfügung und schadhafte Geräte können somit ohne Komplikationen ausgetauscht werden.
- Weiterhin dürfen die Ausdrucke nicht unbeaufsichtigt gelassen werden. Auf Grund der Vorgaben des Berliner Datenschutzgesetzes (BlnDSG) sind die Schülerdaten als personenbezogene Daten besonders zu schützen. Lassen Sie die Ausdrucke nicht im Drucker liegen, sondern entnehmen Sie diese sofort. Damit geben Sie Dritten nicht die Möglichkeit, unbefugt Einsicht in diese Daten nehmen zu können.

Nutzung von mobilen Endgeräten



Einerseits verwenden Schulleitungen Laptops für Verwaltungstätigkeit und z.B. bei Konferenzen, andererseits werden Laptops im unterrichtlichen Zusammenhang (z.B. eKlaBu, s.u.) verwendet. Dies hat neben den unterschiedlichen Möglichkeiten zur Gestaltung der Verwaltungstätigkeiten auch sicherheitsrelevante Aspekte.

- Der heimliche Zugang und Zugriff durch Unbefugte (z.B. Schüler) darf nicht möglich sein. Sorgen Sie für die diebstahlsichere Aufbewahrung der Geräte.
- Die Sicherheitsbetrachtung von Klassenräumen ist erheblich vereinfacht, da keine IT-Systeme dauerhaft und unbeaufsichtigt dort betrieben werden. Wird statt eines kabelgebundenem Netzwerks ein gesichertes, verschlüsseltes eigenes WLAN betrieben, reduziert dies weiterhin das Gefahrenpotenzial von (ungesicherten) Netzwerkanschlüssen.
- Das heimliche Aufbringen von Schadsoftware (Viren, Key-Logger…) über ungesicherte USB-Ports unbeaufsichtigter Computer darf nicht möglich sein.

Folgende Vorgaben gelten bei der Nutzung von Laptops

- Der Laptop darf niemals von der dafür verantwortlichen Lehrkraft in einer unsicheren Umgebung (Klassenzimmer, Lehrerzimmer etc.) unbeaufsichtigt gelassen werden.
- Passwörter sind stets geheim zu halten.
- Die automatische Bildschirmsperre darf nicht deaktiviert werden.
- Der Anschluss eines Präsentationsgeräts (Beamer) darf erst erfolgen, wenn alle Passwörter eingegeben wurden.
- Der Laptop darf nicht als Wireless Access Point betrieben werden und somit weiteren Drahtlosgeräten (z.B. Smartphones) Zugang zum Schulnetzwerk verschaffen.

Elektronisches Klassenbuch (eKlaBu)

Das Elektronische Klassenbuch ist ein Pilotprojekt, das momentan nur an wenigen Schulen stattfindet.

Mit der Klassenbuch-Anwendung wird das Papierklassenbuch abgelöst. Das elektronische Klassenbuch wird zur Erfassung von Fehlzeiten, Klassenarbeiten und erteiltem Unterricht verwendet. Die Vorteile, die sich aus dieser Anwendung ergeben sind u.a.

- ein einfaches Verfahren zur Erfassung von Fehlzeiten und die (automatische) Benachrichtigung von Erziehungsberechtigten und ggfs. Ausbildern,
- Verfügbarkeit der aktuellen Daten für alle Zugriffsberechtigten,
- Parallele Datenverarbeitung z.B. der Fehlzeiten durch den Lehrer bei der Anwesenheitskontrolle und dem Sekretariat bei eingegangener telefonischer Entschuldigung,
- Einfache Auswertung der aktuellen Daten durch die Zugriffsberechtigten.

Da die Daten, die im Rahmen des elektronischen Klassenbuchs erfasst werden, nicht in der IT-Umgebung der Schule gespeichert, sondern über das Internet an den externen Dienstanbieter übermittelt werden, gilt eine besondere Sorgfalt bei der Nutzung der IT-Systeme. Die Verarbeitung der Daten darf ausschließlich mit den dafür vorgesehenen Anwendungen geschehen, da nur so die Sicherheit und der Schutz der Daten gewährleistet werden kann. Aktive Schutzmechanismen, wie die Zugriffsregelungen, die physikalische Sicherheit (z.B. abschließbarer PC-Schrank) oder organisatorische Vorgaben zur IT-Sicherheit (z.B. Geheimhaltung der Kennwörter) dürfen nicht umgangen werden.

Sämtliche im Rahmen des eKlaBu erfassten Daten fallen unter das Berliner Datenschutzgesetz und sind somit besonders zu schützen!

Abiturdatenlieferung

Die alljährliche Lieferung von Abiturdaten findet in elektronischer Form statt.

Erstellung der Abiturdaten

Um zu gewährleisten, dass die Abiturdaten nicht personalisiert an die Senatsverwaltung geliefert werden und um Ihnen diesbezüglich Rechtssicherheit zu garantieren, werden die Abiturdaten vorher von einer Ihnen bereitgestellten Software (ADPSW) getrennt und auf formale Korrektheit überprüft.
Bei der Trennung werden die persönlichen Daten der Abiturienten (Name, Vorname, Geburtsdatum) anonymisiert und Ihnen eine Datei mit diesen anonymisierten Daten zur Verfügung gestellt, die Sie dann der Senatsverwaltung übermitteln sollen.

Abgabe der Abiturdaten

Die alljährliche Lieferung von Abiturdaten findet über die sichere Berliner Schulmail statt und wird durch Sie mit Ihrem lokalen Mailclient (Thunderbird oder Outlook) und der von SenBJF bereitgestellten Verschlüsselung an die entsprechende Stelle in der Senatsverwaltung geliefert.

Die Übermittlung der Daten erfolgt per signierter und verschlüsselter Mail, auch um Ihnen Rechtssicherheit bezüglich des Transportweges zu bieten.

Dadurch, dass Sie die Mail signieren, garantieren Sie grundsätzlich für die Korrektheit der versendeten Abiturdaten. Da die Mail verschlüsselt ist, wird zudem gewährleistet, dass die anonymisierte Abiturientendatei nicht von anderen eingesehen werden kann

Fragen und Antworten

IT-Infrastruktur und –organisation

Darf ich die Infrastruktur für meine privaten Zwecke nutzen?

Die vorhandene Infrastruktur der Informationstechnik wurde für dienstliche Zwecke zur Verfügung gestellt. Eine private Nutzung ist grundsätzlich nicht zulässig. Ebenfalls unzulässig ist ein Anschluss von privaten Geräten.

Mir fehlen Zugriffberechtigungen, was ist zu tun?

Bitte sprechen Sie mit Ihrer Schulleitung. Diese kann veranlassen, dass Ihnen fehlende Rechte erteilt werden.

Welche Ansprechpartner stehen mir bei Problemen oder Fragen seitens der Senatsverwaltung zur Verfügung?

Sollten Schwierigkeiten, Probleme oder sonstige Abweichungen vom Normalzustand auftreten, verständigen Sie bitte unverzüglich die zentrale Hotline (030/ 90 214 666). Versuchen Sie nicht, Probleme selbst zu lösen. Dies gilt insbesondere für einen vermuteten Befall mit Schadsoftware o.ä.

Datenspeicherung

Was ist bei der Datenspeicherung zu beachten?

Schülerdaten dürfen ausschließlich in den definierten Verzeichnissen auf dem Schulserver gespeichert werden. Da die Daten jedoch jederzeit verfügbar sind, ist auf Datensparsamkeit zu achten. Dies bedeutet, dass nicht unnötig jede Auswertung gespeichert werden muss, da sie erneut generiert werden kann. Achten Sie also darauf nicht unnötig Dateien zu erzeugen, bzw. zu speichern.

Was ist mit den Importen/ Exporten?

Da die Daten auf dem Client anfallen, ist eine temporäre Speicherung möglich und ggf. notwendig. Es ist aber darauf zu achten, dass bei positiver Ergebnismeldung des Portals, zu dem Sie die exportierten Daten gesendet haben, die Daten sofort vom Client gelöscht werden. Beispielsweise sollten Sie sich überlegen, in welchem Verzeichnis Sie die Daten der Abiturdatenerhebung speichern und wann Sie diese Daten nach erfolgreicher Übermittlung wieder löschen.

Denken Sie also bei jedem Speichern oder Exportieren von personenbezogenen Daten daran, dass Sie diese Daten nicht an für andere User zugänglichen Orten ablegen. Wenn die Zugriffsrechte zu Ihrem Schulverwaltungsprogramm klar definiert worden sind, Sie die Exporte aus diesem Programm allerdings an einem für jeden User zugänglichen Ort ablegen, sind trotz klarer Zugriffsrechte auf das Schulverwaltungs-programm ggf. persönliche Daten für nicht berechtigte User zugänglich.

Viren, Würmer & Co

Was sind Viren, Trojanische Pferde usw.?

Im allgemeinen Sprachgebrauch werden alle möglichen Schadprogramme als Viren bezeichnet. Das eigentliche Computervirus ist in Wirklichkeit nur ein kleiner Teil der im Umlauf befindlichen Schadprogramme. Zusammenfassend werden Schadprogramme deshalb auch als Schadsoftware bzw. Malware bezeichnet.

Häufig werden mehrere Schadprogramme miteinander vermischt, um eine schnelle und breite Verbreitung und einen vielfältigen Nutzen zu haben.

Wie wird Schadsoftware verbreitet bzw. wie gelangt sie in das System?

Beispiele

- Download von Programmen aus dem Internet
- Öffnen von E-Mail-Anhängen
- Anklicken von Hyperlinks
- Nutzung von Wechseldatenträgern (diese werden häufig infiziert, wenn sie mit einem bereits infizierten System verbunden werden)
- Besuch infizierter Internetseiten
- Chatprogramme und Musik-, Video- und Spielebörsen

Beispiele für Folgen eines Befalls mit Viren oder anderen schadenstiftenden Programmen

- Verschlüsselung von Dateien
- Internetverbindungsversuche (meist im Hintergrund)
- hoher Netzwerkverkehr
- Abfluss vertraulicher Daten, wie z.B. Benutzerdaten, Dokumente, E-Mail-Adressen
- Ausspähen von Tastatureingaben
- Verringerte Rechnerleistung
- Zerstörung von vorhandenen Programmen
- Manipulation von Dateien
- unbekannte Meldungen auf dem Bildschirm
- Festplatte ist nicht mehr nutzbar

Vorsorgemaßnahmen

Sollten Sie eine E-Mail erhalten, die Ihnen verdächtig vorkommt, löschen Sie diese bitte nicht sofort, sondern informieren Sie die zentrale Hotline und den Regionalen IT-Sicherheitsbeauftragten. Bitte leiten Sie die verdächtige E-Mail nicht weiter. Solche E-Mails können uns Aufschluss darüber geben, ob eine neue Bedrohung vorliegt oder nicht.

Seien Sie aufmerksam, wenn Ihnen bestimmte Versprechungen im Internet oder auch per E-Mail gemacht werden. Die E-Mail in schlechtem Deutsch, die Ihnen das Blaue vom Himmel verspricht, ist Vergangenheit. Inzwischen werden Sie immer wieder auf gut designte Spam-Mails stoßen, die Ihnen beispielsweise mitteilen, dass ein Paket für Sie bereitliegt und Sie den aktuellen Status über einen Link in der Mail aufrufen können…

Grundsätzlich sollten Sie sich bei jeder nicht von Ihnen erwarteten Mail fragen: Kann das sein, habe ich das wirklich bestellt, erwarte ich ein Paket, würde mich meine Bank in einer so wichtigen Angelegenheit per Mail kontaktieren? Im Zweifelsfall: Löschen oder mit erhöhter Vorsicht (Links, etc.) betrachten.

Weitere Hinweise zum Umgang mit Anhängen und Links in E-Mails finden Sie in folgendem Dokument:
https://www.egovschool-berlin.de/sites/default/files/Anhang_auf_Schadsoftware_pruefen-Version_02.pdf

Fehler im Virenschutzprogramm melden Sie bitte der zentralen Hotline (030/ 90 214 666) !

Phishing – Wenn Datendiebe nach ihren Passwörtern angeln...

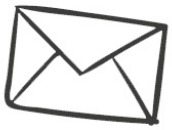
Phishing („Password Fishing“) stellt im Vergleich zu Viren oder Würmern eine relativ neue Gefahr dar. Mit den sogenannten Phishing-Mails locken Betrüger die Anwender z.B. auf gefälschte Internetseiten und fordern diese auf, ihre Passwörter und Zugangsinformationen dort einzugeben. Die Daten landen aber in den Händen der Betrüger und können so für Daten-Einbrüche genutzt werden.

Manche dieser Phishing E-Mails sind sogar so geschickt konstruiert, dass unmittelbar nach dem Öffnen der E-Mail im Hintergrund – und vom Nutzer unbemerkt – ein Programmcode ausgeführt wird, welches die Lesezeichen des Browsers so ändert, dass beim nächsten Aufruf einer bestimmten Seite nicht mehr das Original angesteuert wird, sondern die von den Betrügern manipulierte Seite.

Vor Phishing Attacken schützt nur vorsichtiges Verhalten. Bitte informieren Sie im Verdachtsfalle umgehend die zentrale Hotline (030/ 90 214 666)!

Absenderfälschung von Mails

Worin liegt die Gefahr eines falschen Absenders einer E-Mail?



Eine E-Mail hat, ähnlich einem Papierbrief, verschiedene Orte, an denen der Absender vermerkt werden kann. Beim Papierbrief sind dies beispielsweise der Umschlag und der Briefkopf des eigentlichen Schriftstücks.

Die Anzeige im E-Mailprogramm kann einen vertrauenswürdigen Absender vorgaukeln, während im „Antworten an“ Feld die Adresse eines Datendiebs stehen kann. Drückt man auf den Antworten-Knopf, so wird diese E- Mail an den Datendieb verschickt.

Woran erkenne ich einen gefälschten Absender?

Einen gefälschten Absender zu erkennen ist nicht immer ganz leicht. Bei Berücksichtigung folgender Punkte verhindern Sie leicht das unbeabsichtigte Verraten geheimer oder personenbezogener Daten:

- Entspricht der Schreibstil der E-Mail dem des Absenders sonst üblichen? (Grammatikalische Fehler, besondere Ausdrucksweisen etc.)
- Sensible Daten dürfen nie über einen unsicheren Kanal wie unverschlüsselte E-Mails verschickt werden. Werden solche Daten oder Auskünfte per E-Mail erfragt, könnte eine falsche Identität hinter dem Absender stecken. Greifen Sie zum Telefon und fragen Sie nach!
- Ist die E-Mail Adresse bei einer Antwort absolut identisch mit der, die als Absender bei der eingegangenen E-Mail zu sehen ist? Manchmal unterscheiden sich diese nur minimal, meistens im Adressteil nach dem @-Zeichen.

(Erika.Mustermann@b**ei**spiel.de vs. Erika.Mustermann@b**ie**spiel.de)

Warum werden E-Mails mit gefälschtem Absender verschickt?

Durch diesen einfachen Trick werden nicht nur Schädlinge in ein System eingeschleust, da man ja dem Absender vertraut und deshalb auch dem (bösartigen) Anhang der E-Mail. Durch gezielte Anfragen an bekannte Empfänger (Schulleitung, Lehrer etc.) können auf diese Weise auch sensible (Schüler-) Daten angefordert werden, ohne dass der Empfänger Verdacht schöpft. Dies ist eine Variante des Social Engineering (s.u.).

Außerdem werden gefälschte Absender gerne in Verbindung mit *Phishing* eingesetzt, um den Empfänger noch einfacher zum Öffnen eines in einer E-Mail enthaltenen Links zu verleiten – schließlich scheint der Absender ja vertrauenswürdig zu sein.

Worum geht es bei Social Engineering?

In der heutigen Zeit begegnen uns viele Gefährdungen der Informationssicherheit. Leider wird dabei nicht nur versucht, Systeme mit technischen Mitteln zu kompromittieren, sondern auch über die „Schwachstelle Mensch“ Informationen zu erhalten.

Bei den Angriffen gibt sich der Angreifer z.B. als Techniker oder anderweitig berechtigte Person aus und versucht auf diese Weise – unter Einsatz von 'Smalltalk' im direkten Gespräch am Telefon oder im Rahmen einer E-Mail – Vertrauen zu erlangen, um anschließend durch geschickte Fragen interne Informationen zu erhalten. Auch Schüler sind durchaus in der Lage, Informationsgewinnung mit Social Engineering zu betreiben.

Interne Informationen können z.B. sein:

- Schülerdaten
- Passwörter/Zugangskennungen
- Rechnernamen
- Ablaufstrukturen
- Verzeichnispfade zu geheimen und/oder geschützten Dokumenten
- Interne Telefonnummern, Namen o. ä.

Vieles scheint trivial, doch können Angreifer mittels geschickter Maßnahmen durch diese Informationen weitere Angriffe starten, die sie dann zu ihrem eigentlichen Ziel führen. Auch können einige, jeweils für sich einzeln nutzlose, Informationen dem Angreifer wertvolle Hinweise geben (z. B. Klausuren etc.).

Wie kann ich mich schützen?

- Geben Sie nicht leichtfertig interne Informationen preis.
- Geben Sie keine Passwörter weiter! Ein Administrator wird Sie niemals – wirklich niemals – danach fragen!
- Kontrollieren Sie auch beim Schreiben einer E-Mail-Antwort die E-Mail-Adresse des Empfängers.
- Wenn Sie von einer Ihnen unbekannten Person nach internen Informationen gefragt werden, legen Sie gesundes Misstrauen an den Tag. Fragen Sie diese Person nach dessen Arbeitsstelle und prüfen sie ggf. (z. B. durch einen Rückruf) nach, ob diese Person wirklich Bedienstete des Landes Berlin ist.
- Geben Sie telefonisch keine internen Auskünfte an unbekannte Personen (Werbeanrufer, Vertriebsmitarbeiter etc.).
- Geben Sie auch im privaten Umfeld keine internen Informationen weiter.

Auch freundliche Schüler dürfen keine internen Daten erhalten und/ oder an Ihren Geräten arbeiten!

An wen kann ich mich wenden?

Es gibt auch über die hier dargestellten Methoden hinaus Möglichkeiten, durch die potenzielle Angreifer über Sie an interne Informationen gelangen können.

Haben Sie das Gefühl, dass sie ausspioniert worden sind, so melden Sie dies dem Regionalen IT-Sicherheitsbeauftragten.

Umgang mit Einbrüchen und Diebstahl

Bitte informieren Sie die Polizei über den Vorfall. Von dort erhalten Sie eine Vorgangs- bzw. Bearbeitungsnummer.

Jeder Rechner, Bildschirm, Drucker oder sonstige Hardware, die seitens der Senatsverwaltung im Verwaltungsbereich an Ihre Schule ausgegeben werden, ist inventarisiert. So wird unter anderem der Überblick über Bedarf und die Ausstattung der Verwaltungsbereiche von Schulen gewährleistet.

Sollte Hardware durch Einbruch und Diebstahl abhandenkommen, so melden Sie sich bitte umgehend mit der Vorgangsnummer der Anzeige beim SSZB (030/ 90 214 666). Dort werden alle weiteren Schritte veranlasst.

Sollten auch Kennwörter oder der Datenträger mit den elektronischen Zertifikaten für die Signatur und Verschlüsselung von dem Diebstahl betroffen sein, so melden Sie das bitte ebenfalls unverzüglich an das SSZB, damit die Sperrung veranlasst werden kann.

Bitte beachten Sie, dass es beim Abhandenkommen von persönlichen Daten gesetzlich vorgeschrieben ist, dies in jedem Fall Ihrem Datenschutzbeauftragten mitzuteilen.

Glossar

Abkürzung, Begriff	Erläuterung
ADPSW	Abiturdatenprüfsoftware – in dieser Software werden die Abiturdaten eingelesen und datenschutzkonform anonymisiert.
Cookie	Cookies sind kleine Textdateien in Web-Browsern. Die vom Webserver gesendeten Cookies, die auf dem Personal Computer des Web-Client hinterlegt werden, dienen dazu, das Nutzerverhalten zu speichern. Darüber können z.B. Passwörter, persönliche Daten des Nutzers, welche Webseiten er am häufigsten aufruft und wie lange die Besuchsdauer war, ausgelesen werden.
eKlaBu	Elektronisches Klassenbuch
GGO I	Gemeinsame Geschäftsordnung für die Berliner Verwaltung/ Allgemeiner Teil
IT	Informationstechnologie
IT-SiBe	Beauftragte / Beauftragter für IT-Sicherheit
SenBJF	Senatsverwaltung für Bildung, Jugend und Familie
Spam	Nicht angeforderte und unerwünschte E-Mails, welche von „Spammern“ an eine Vielzahl von Empfängern verschickt werden. Intention kann Werbung, Phishing oder Verbreitung von Schadsoftware sein.
Wireless AccessPoint	Ein Wireless Access Point ist ein Gerät, das als Schnittstelle für kabellose Kommunikationsgeräte fungiert. Endgeräte stellen per Wireless Adapter (Drahtlosadapter) eine drahtlose Verbindung zum Wireless Access Point her, der wiederum über ein Kabel mit einem fest installierten Kommunikationsnetz verbunden sein kann.
ZSVU	zentrale Schulverwaltungsumgebung – zentrale IT-Umgebung des ITDZ Berlin für die Verwaltungen der Berliner Schulen

Quellen

[1] Dienstvereinbarung über die Nutzung des Internets und anderer elektronischer Informations- und Kommunikationsdienste in der Berliner Verwaltung (Internet- DV)
Link: https://www.berlin.de/hpr/dienstvereinbarungen/artikel.299659.php

[2] Benutzungsrichtlinien der Senatsverwaltung für Bildung, Jugend und Wissenschaft für die Nutzung des Internets

[3] Sicherer Zugang zum Intranet und Internet in der Berliner Verwaltung
Link im Intranet:
http://www.verwalt-berlin.de/imperia/md/content/intranet/seninn/it-kompetenzzentrum/it-sicherheit/konzept_internet_intranet_zugang_aktuell.pdf

Ergänzende Dokumente

- Dokumente beim Bundesamt für Sicherheit in der Informationstechnik (BSI)
  - speziell BSI für Bürger (www.bsi-fuer-buerger.de)
- IT-Sicherheitsgrundsätze der Berliner Verwaltung
- Bundesdatenschutzgesetz (BDSG)Betriebsverfassungsgesetz (BetrVG)
- Sozialgesetzbuch (SGB)
- Telekommunikationsgesetz (TKG)
- Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV)
- Informations- und Kommunikationsdienste-Gesetz (IuKDK)
- Urheberrechtsgesetz (TDDSG)
- Leitfaden für eine sichere IT-Infrastruktur im Verwaltungsbereich der öffentlichen Berliner Schulen

Bildrechte:

Icons designed by:
freepik.com

Bild Titelseite: Andreas Koll