Betriebssicherheit im pädagogischen Netz

Verbindliche IT-Standards und Empfehlungen

05.01.2015
Version 1.1

Im Zuge des Projektes SIP2010 haben die meisten Schulen bereits jetzt eine durchgängige schulinterne Vernetzung im pädagogischen Bereich sowie eine leistungsfähige Anbindung an das Internet erhalten. Einige Schulen werden in Rahmen von Sanierungsmaßnahmen die Vernetzung erhalten. Damit können die Lernprozesse der Schülerinnen und Schüler mit zeitgemäßen Methoden und digitalen Medien unterstützt werden. Es ist ein schulübergreifendes pädagogisches Netz entstanden, das verlässlich nutzbar und sicher sein soll. Aber nicht nur das Netzwerk, das durch Viren und Schadprogramme gefährdet ist, auch der Datenschutz selbst rückt stärker in den Fokus, je mehr Daten sich im Netz befinden.

Vor diesem Hintergrund sind technische Standards entwickelt worden, die eine angemessene Netzwerksicherheit herstellen und den Datenschutz berücksichtigen. Die Standards wurden ergänzt durch Empfehlungen, die eine sinnvolle Ergänzung in Ihrer Schule sein können.

Bei der Entwicklung war uns bewusst, dass die Herstellung der Netzsicherheit für viele Schulen eine Herausforderung ist. Die Standards und Empfehlungen geben daher einen Rahmen, mit dem die Verantwortung der Schulleitung für die IT-Sicherheit in der Schule ausreichend wahrgenommen werden kann.

Die Standards sind verpflichtend. Bitte prüfen Sie daher, was in Ihrer Schule bereits umgesetzt wurde bzw. was noch umzusetzen ist. Sollten Sie noch Fragen haben, können Sie sich an die pädagogisch-technische Beratung im Landesinstitut für Lehrerbildung und Schulentwicklung wenden. Ansprechpartnerin ist Frau Traub (ingeborg.traub@li-hamburg.de).

Die Standards und Empfehlungen sind im Folgenden beschrieben.

1 Verbindliche Standards

1.1 Netzinfrastruktur

1.1.1 Pädagogisches LAN (lokale Festvernetzung)

Im Rahmen des Projektes SIP2010 bzw. von Sanierungsvorhaben haben bzw. erhalten die Schulen eine standardisierte Festvernetzung in der Pädagogik. Mit Abschluss dieser Maßnahme ist das Netzwerkmanagement in die Verantwortung von Dataport übergegangen. Störungen etc. werden von dem Dienstleister behoben.

Der nachfolgende Standard gilt für Schulen, die bereits standardisiert vernetzt sind.

Standard

Das standardisierte Netz darf nicht durch die Schule oder Beauftrage der Schule verändert etc. werden. Dazu gehört auch, dass das Netz nicht selbstständig durch Netzwerkkomponenten erweitert werden darf. Dies betrifft sowohl die Fest- als auch die Funkvernetzung.

Netzwerkänderungen und Erweiterungen können beim Kundenzentrum Schul-IT beantragt werden (schul-it@bsb.hamburg.de).

Schulen, die durch einen Eingriff das pädagogische Netz verändern etc., tragen ggf. hierdurch entstehende Kosten.

1.1.2 Pädagogisches WLAN (lokales Funknetz)

Ein nicht gesichertes WLAN kann leicht durch unberechtigte Personen genutzt werden. Urheberrechtsverletzungen dieser Personen würden zu Lasten der Schule gehen. Es ist daher erforderlich, die WLAN-Router / Accesspoints ausreichend zu schützen.

Da Schulen zukünftig verstärkt auch WLAN nutzen werden, wird zurzeit ein Standard für die WLAN Nutzung konzipiert, um neben dem zentralen LAN-Management auch einen zentralen Support für den WLAN Bereich aufzubauen. Voraussetzung dafür sind einheitliche WLAN-Accesspoints, die die Anforderungen an ein zentrales Management erfüllen.

Standard

Notwendige Ergänzungen durch WLAN-Accesspoints müssen daher über das Kundenzentrum Schul-IT bestellt werden (schul-it@bsb.hamburg.de).

Die Geräte werden durch folgende Einstellungen geschützt:

- Es muss mind. WPA2-Verschlüsselung eingesetzt werden.
- Es ist ein komplexer Schlüssel zu verwenden, der mind. 20 Zeichen umfasst. Ist dies technisch nicht möglich, so müssen mind. 16 Zeichen verwendet werden.
- Das Standard-Administrationskennwort wird in ein komplexes Passwort geändert (mind. 8 Zeichen, die einen Großbuchstaben und ein Sonderzeichen enthalten).
- Die Administration des Routers / des Access-Points erfolgt über eine gesicherte Verbindung oder aber drahtgebunden.
- Es wird eine nichtssagende SSID verwendet, die es nicht zulässt, auf den WLAN-Betreiber zu schließen (z.B. eine 10-stellige Zahlenkolonne).
- Der WLAN-Router / der Access-Point wird zeitlich auf die tatsächliche Nutzung eingeschränkt.

Optionale Verbesserung

Insbesondere fest installierte WLAN-Router, die nicht nur temporär genutzt werden, eröffnen einen leichten Zugang. Der Schutz wird daher erheblich verbessert, wenn die MAC-Adressen der zugelassenen Rechner hinterlegt werden.

1.1.3 Jugendschutzfilter

Der Jugendmedienschutz erfordert, dass bei Zugriffen auf das Internet eine vorgeschaltete inhaltliche Filterung eingesetzt wird.

Standard

Im Rahmen der Netzanbindung erhalten die Schulen einen Schulrouter mit integriertem Jugendschutzfilter von Time-for-Kids. Dieser Filter arbeitet mit Kategorien, die gesperrt oder freigegeben werden können. Die Kategorisierung von Internetseiten wird laufend aktualisiert.

Die Schulrouter werden mit einer Grundeinstellung ausgeliefert. Es muss aber betont werden, dass die Grundfilterung nicht prinzipiell davor schützt, dass dennoch ggf. unangemessene oder für den Unterricht unerwünschte Seiten im Internet aufgerufen werden können. Andererseits ist nicht auszuschließen, dass in Einzelfällen Seiten geblockt werden, die im Unterricht benötigt werden.
Die Grundeinstellung kann daher bei Bedarf von der Schule nach den jeweiligen pädagogischen Erfordernissen angepasst werden, auch temporär und auf einzelne Rechner bezogen.

1.1.4 Firewall

Um die Netzwerksicherheit zu erhöhen, ist es erforderlich, ungewollte Zugriffe auf Netzwerkdienste zu unterbinden – von innen und von außen. Eine Firewall dient dazu, den Netzwerkzugriff zu beschränken, basierend auf Absender- oder Zieladresse und genutzten Diensten. Sie überwacht den durch sie hindurch laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht. Auf diese Weise kann das Risiko eines unerlaubten Zugriffs minimiert werden.

Standard

Es ist erforderlich, eine Firewall einzurichten. An Schulen, die einen Schulrouter von Time for Kids haben, ist diese bereits vorkonfiguriert.

Policy

Ausgangspunkt für die Firewall ist die Festlegung der Policy, d.h. die Festlegung welche Ports freigegeben werden. Als Startkonfiguration wird folgende Einstellung festgelegt:

„deny from all“ mit der expliziten Freigabe folgender Ports:

Zugriffe in das Internet	Zugriffe aus dem Internet
TCP 80 und 8080 http - Internetrecherche TCP 443 und 445 https (u.a. Microsoft-Dienste) TCP 25, 110, 143, 993 und 995 - E-Mail-Dienste TCP 21 ftp ICMP 8 und 30 ping	Keine

Schulen, die eine lokale Firewall betreiben, können die Startkonfiguration bei Bedarf verändern.

Darüber hinaus ist die Firewall des Endgeräts zu aktivieren.

1.1.5 Fernzugriff / Fernwartung

Es ist erforderlich, den Personenkreis, der einen Zugriff von außen erhält (d.h. außerhalb des behördenweiten FHH-Netzes, z.B. von zuhause aus oder durch eine Wartungsfirma), einzuschränken und nachvollziehbar zu machen.

Mögliche Gefährdungen sind z.B. das Einschleusen von Viren und das Ausspähen von Passwörtern.

Standard

Organisatorisch:

Die Fernwartung durch eine externe Firma unterliegt den Bedingungen der Telekommunikationsrichtlinie der Stadt Hamburg. Unabdingbare Voraussetzung ist daher, dass die Einhaltung dieser Bedingungen mit der Firma schriftlich vereinbart wird. In der Anlage ist ein entsprechendes Formular angefügt.

Technisch:

Die direkte Vergabe der öffentlichen IP-Adresse für eine Fernwartung oder einen Fernzugriff durch Lehrkräfte oder Schülerinnen und Schüler ist nicht zulässig.

Soll eine externe Firma die Geräte der Schule per Fernzugriff warten, kann ein Zugriff über den zentralen VPN-Sprungserver eingerichtet werden. Der Zugriff kann im Kundenzentrum Schul-IT (BSB - V112) beantragt werden (per E-Mail an schul-it@bsb.hamburg.de mit dem unterschriebenen und eingescannten Formular der Anlage). Für den Schul-Support-Service 3S ist kein gesonderter Antrag nötig, da die Bedingungen für den Fernzugriff bereits mit dem Kontrakt vereinbart wurden.

Bei Schulen, die lokale Mail- oder Webserver betreiben, ist es erforderlich, eine DMZ (Demilitarisierte Zone) auf dem Schulrouter einzurichten, über die der Zugriff in das pädagogische Netz erfolgt (orangene Schnittstelle). Die öffentliche IP-Adresse wird in diesem Fall der DMZ zugewiesen. Für die Einrichtung einer DMZ sind ggfs. Konfigurationsänderungen Ihres Netzes durch Dataport erforderlich. Bitte beantragen Sie dieses per E-Mail beim Kundenzentrum Schul-IT schul-it@bsb.hamburg.de.

Schulen, bei denen derzeit Schüler von zuhause aus auf den Schulserver zugreifen, ist eine Migration auf eine andere Lösung erforderlich (z.B. Datenablage in Commsy oder ebenfalls die Nutzung einer DMZ).

1.2 Server und Endgeräte

1.2.1 Virenschutz

Das Eindringen von Schadprogrammen (Malware, Viren, Würmer, Trojaner, …) kann auf den Endgeräten, den Servern und im Netz erheblichen Schaden verursachen. Dazu gehören z.B. eingeschleuste Programme, die massenhaft SPAM versenden und in der Folge eine Abschaltung der Schule vom Internet erforderlich machen.

Standard

Für die Endgeräte- und Netzwerksicherheit ist es daher unerlässlich, dass auf allen Endgeräten und Servern ein aktuelles Virenschutz-Programm installiert wird.

Produkt-Empfehlungen finden Sie auf der Website des Kundenzentrums Schul-IT in der Rubrik Software-Beschaffung: http://schul-it.hamburg.de/software-beschaffung-paedagogik/

1.2.2 Private Endgeräte

Mit der Nutzung privater Endgeräte sind insbesondere die folgenden Risiken verbunden:

- die Verbreitung von Viren durch ungeschützte Rechner,
- der unkontrollierte Zugriff im pädagogischen Netz (z.B. Einsatz von ungewünschten Programmen wie das Ausspähen der Passworte),
- bei privaten Geräten von Lehrkräften der Zugriff auf Personen bezogene Daten.

Standard

Private Geräte der Schülerinnen und Schüler

Mit der Nutzung von privaten Geräten der Schülerinnen und Schüler kann aktuell keine Datensicherheit gewährleistet werden – insbesondere kann ein aktueller Virenschutz auf diesen Rechnern nicht überprüft und der Einsatz von Programmen wie z.B. zum Ausspähen der Passworte nicht verhindert werden. Es ist daher derzeit nicht zulässig, diese Geräte in das pädagogische Netz einzubinden. Es werden Lösungen erarbeitet, die zukünftig auch Schülerinnen und Schüler die Nutzung ihrer privaten Endgeräte ermöglichen sollen.

Damit verbunden ist die Empfehlung, den Zugriff auf das pädagogische Netz durch private Geräte derzeit entbehrlich zu machen; z.B. durch die Nutzung von Plattformen wie SchulCommsy oder die Verwendung von USB-Sticks.

Nicht betroffen von dieser Regelung sind von der Schule initiierte sogenannte Notebookklassen, bei denen die Schülerinnen und Schüler ein Gerät sowohl in der Schule als auch zuhause nutzen, weil hier seitens der Schule die beschriebenen Sicherheitsanforderungen berücksichtigt werden müssen.

Private Geräte der Lehrkräfte

Die derzeit gültige Richtlinie zur Verwendung privater Geräte durch Lehrkräfte erlaubt keine Einbindung in das pädagogische Netz.

Derzeit wird eine neue Richtlinie erarbeitet, die eine Verwendung der privaten Geräte der Lehrkräfte unter bestimmten Voraussetzungen im pädagogischen Netz erlaubt. Mit Inkrafttreten der neuen Richtlinie werden die Betriebssicherheitsstandards angepasst und Ihnen neu zugesendet.

2 Empfehlungen

2.1 BIOS-Schutz

Ein BIOS-Schutz ist zu empfehlen, um ein Umgehen der Sicherheitsmaßnahmen, die auf den Endgeräten implementiert wurden (z.B. die Wächterkarte), zu verhindern.

Standard

- Das BIOS wird Passwort geschützt. Dabei werden die systemtechnischen Möglichkeiten für die Komplexität ausgenutzt.
- Im BIOS wird eingestellt, dass der Start nur über Festplatte oder PXE (z.B. für Softwareupdates erforderlich) möglich ist.
- Die Einstellung USER ACCESS wird auf NO gesetzt.
- Das BIOS-Passwort ist nur dem/der IT-Verantwortlichen der Schule und seiner/ihrer Vertretung bekannt.

2.2 Rechnerauthentifizierung

Die Rechner-Authentifizierung ermöglicht einen kontrollierten Zugriff auf das pädagogische Netz; d.h. der Zugriff kann auf Rechner eingeschränkt werden, die den Sicherheitsstandards entsprechen. Darüber hinaus wird eine Nachvollziehbarkeit – zumindest der Rechner - bei Urheberrechtsverletzungen hergestellt.

Empfehlung

Schulen, die einen Schulrouter von Time-for-Kids haben, sollten die Möglichkeit der MAC-Registrierung nutzen. Die Router werden mit der Einstellung „Registrierung: ja“ und „Internet nur für registrierte Geräte: nein“ ausgeliefert, damit die Inbetriebnahme des Filters nicht zum Ausfall der Endgeräte führt. Die Schule kann die Internetsperre für nicht registrierte Geräte in einer konzertierten Aktion nachholen und dann „Internet nur für registrierte Geräte: ja“ setzen.

2.3 Benutzerauthentifizierung

Urheberrechtsverletzungen (z.B. das Nutzen einer Musiktauschbörse) können nur dann sicher nachverfolgt werden, wenn eine Benutzerauthentifizierung eingesetzt wird. Kann der Benutzer, der eine Urheberrechtsverletzung begangen hat, nicht nachvollzogen werden, haftet die Schulleitung.

Da mit einer Benutzerverwaltung auch einiger Einrichtungs- und Pflegeaufwand verbunden ist, wird es hier nur als Empfehlung genannt. Nichtsdestotrotz wird es insbesondere weiterführenden Schulen sehr empfohlen, diese aufzusetzen.

Empfehlung

Weiterführende Schulen	- Durchgehende Benutzerverwaltung - Keine Admin-Kennungen für Schüler - Keine Einrichtung eines Gastaccounts
Grundschulen	- Zumindest eine minimale Benutzerverwaltung, die auf dem PC zwischen Admin und Benutzer unterscheidet - Einen besseren Schutz bietet das Aufsetzen eines kleinen Servers mit einer Benutzerverwaltung über LDAP

2.4 Protokollierung der Internetzugriffe

Bei Urheberrechtsverletzungen wird eine Nachvollziehbarkeit der Zugriffe benötigt. Dieser Punkt ergänzt die Einrichtung einer Benutzerverwaltung.

Nach Rücksprache mit der behördlichen Datenschutzbeauftragten ist eine Protokollierung zulässig, wenn

- Regeln definiert wurden, wann die Protokolldateien durch den Administrator ausgewertet werden dürfen (z.B. nur bei einem begründeten Verdacht)
- und die Protokolldateien nur 2 Monate aufbewahrt werden.

Empfehlung

Wird die Firewall über den Schulrouter von Time-for-Kids realisiert, sollte dort auch die Protokollierung aktiviert werden. Zu beachten sind dabei die o.g. Bedingungen.

Anlagen

Vereinbarungen zum Fernzugriff im pädagogischen Netzwerk

zwischen der Schule _____

und dem Dienstleister _____

1. Der Fernzugriff ermöglicht die Fernwartung und die Fernsteuerung von Geräten im pädagogischen Netz der Schule.
   Zur Fernwartung gehören Administrationsarbeiten wie Softwareverteilung, Treiberaktualisierung und Fehlerbehebung. Davon abzugrenzen ist die Fernsteuerung, bei der die Anwenderin / der Anwender per Aufschalten auf das Gerät in der Bedienung unterstützt wird. Auswertungen über die Häufigkeit der Nutzung durch einzelne Anwender erfolgen nicht.

2. Der Fernzugriff wird dem Dienstleister von der Schule gewährt. Die Schule wird über den Fernzugriff vorab informiert.

3. Der Fernzugriff zum pädagogischen Netz der Schule darf ausschließlich durch autorisierte Personen über den zu diesem Zweck eingerichteten Zugangsserver erfolgen. Personenbezogene Accounts für den Zugangsserver können von der Schulleitung für den Dienstleister mit dem anliegenden Formular beim Kundenzentrum Schul-IT der BSB beantragt werden.

4. Daten, die im Rahmen der Fernwartung an die Supportfirma übermittelt werden, werden nur für die erforderliche Maßnahme verwendet und unmittelbar danach gelöscht.

5. Die Übermittlung von Dateien mit personenbezogenen Daten erfolgt nur nach explizierter Freigabe durch die Schule und wenn dies aus technischen Gründen oder zur Gewährleistung der Betriebssicherheit erforderlich ist.

6. Eine technische Geräteüberwachung, die Personenangaben enthält (z.B. die Benutzerkennung) oder Rückschlüsse auf Personen ermöglicht, erfolgt nur mit Zustimmung der Schulleitung.

7. Eine Fernsteuerung des Clients erfolgt nur nach explizierter Freigabe durch den Anwender / die Anwenderin in der Schule.

8. Alle Maßnahmen der Fernwartung und -steuerung sind - soweit es personenbezogene Daten betrifft - nachprüfbar zu dokumentieren.

9. Der Dienstleister ist zur Wahrung des Datengeheimnisses und der Verschwiegenheit verpflichtet. Eine Weitergabe von Daten ist nicht zulässig.

10. Die Vereinbarung gilt bis zur Aufhebung bzw. bis zur Löschung des Accounts auf dem Zugangsserver. Diese ist durch die Schulleitung beim Kundenzentrum Schul-IT der BSB mit dem anliegenden Formular zu beauftragen.

_____	_____
Schulleitung	Dienstleister

An das

Kundenzentrum Schul-IT

V112

Hiermit beantragt die Schule _____

☐ die Einrichtung eines personengebundenen Accounts auf dem Zugangsserver für den Fernzugriff in das pädagogische Netz.

Für den Dienstleister (Name der Firma):

_____

Die verantwortlichen Personen für den Fernzugriff sind:

_____

☐ die Löschung des Accounts auf dem Zugangsserver für den Fernzugriff in das pädagogische Netz.

Für die Personen:

_____

Schulstempel

Datum und Unterschrift der Schulleitung

_____