Betriebssicherheit im pädagogischen Netz

Verbindliche IT-Standards und Empfehlungen

für die staatlich allgemeinbildenden Schulen

07.2019
Version 2.0

Die Hamburger Schulen haben eine durchgängig standardisierte schulinterne Vernetzung im pädagogischen Bereich erhalten, sowie eine leistungsfähige Anbindung an das Glasfasernetz der Stadt Hamburg. Im Rahmen von Sanierungs- /Baumaßnahmen wird eine standardisierte Vernetzung umgesetzt. Damit können die Lernprozesse der Schülerinnen und Schüler mit zeitgemäßen Methoden und digitalen Medien unterstützt werden.

Es ist ein schulübergreifendes pädagogisches IT-Netzwerk entstanden, das verlässlich nutzbar und sicher sein soll. Aber nicht nur das Netzwerk, das durch Viren und Schadprogramme gefährdet ist, sondern auch Datenschutz und Informationssicherheit selbst rücken stärker in den Fokus, je mehr Endgeräte, Server und Daten sich im Netz befinden. Die Umsetzung von Datenschutz und Informationssicherheit sind nicht nur eine Frage der Technik, sie sind in erheblichem Maße von den organisatorischen und personellen Rahmenbedingungen abhängig.

Vor diesem Hintergrund sind **verpflichtende technische Standards** entwickelt worden, die eine angemessene Netzwerksicherheit herstellen und den Datenschutz berücksichtigen. Ergänzend zu den Standards stellen die Empfehlungen eine sinnvolle Ergänzung für die IT-Infrastruktur in Ihrer Schule dar. Sowohl die verpflichtenden Standards, als auch die Empfehlungen, die im Folgenden beschrieben werden, geben einen Rahmen, mit dem die Verantwortung der Schulleitung für die IT-Sicherheit in der Schule ausreichend wahrgenommen werden kann.

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).

Inhaltsverzeichnis

Anlagen

A. Verbindliche Standards

1. Netzinfrastruktur

1.1 Pädagogisches LAN (lokale Festvernetzung)

Die staatlich allgemeinbildenden Schulen haben eine standardisierte, schulinterne IT-Vernetzung (LAN = **L**ocal **A**rea **N**etwork) mit einheitlicher Konfiguration in den unterrichtlich genutzten Räumen. Die Verantwortung für den Betrieb und die Administration dieser schulpädagogischen Netzwerke wurde dataport übertragen. Dataport übernimmt das Netzwerk-Management mit Fehler- und Störungsbehebung. Dazu gehören nicht die lokalen Server, Netzwerkspeicher und Clients an den Schulen.

Standard

- Das standardisierte IT-Netzwerk darf nicht durch die Schule oder Beauftragte der Schule eigenständig verändert werden, so z.B. . Erweiterung mit Netzwerkkomponenten erweitert werden. Dies gilt für die **Fest- und Funkvernetzung**.
- Netzwerkänderungen und Erweiterungen müssen bei der BSB beantragt werden (schul-it@bsb.hamburg.de).
- Schulen, die durch einen selbständigen Eingriff das pädagogische Netz verändern, tragen die hierdurch entstehende Folgekosten (u.a. nachträglcihe Anpassungen an den Standard, Dokumentation).

1.2 Pädagogisches WLAN (Funknetz)

1.2.1 Allgemein

Die Nutzung mobiler IT-Endgeräte erfordert die Bereitstellung einer funkbasierten Vernetzung: WLAN (**W**ireless LAN). Ein nicht gesichertes WLAN kann leicht durch unberechtigte Personen abgehört und missbraucht werden, um z.B. Daten auszuspähen oder zu manipulieren. Unerlaubte Zugriffe auf ungesicherte IT-Endgeräte sowie die Verbreitung von Schadsoftware (Malware) in dem WLAN wären möglich. Urheberrechtsverletzungen würden zu Lasten der Schule gehen. Es ist daher erforderlich, die WLAN Accesspoints ausreichend zu schützen.
Von daher ist ein WLAN-Standard in Schulen konzipiert worden, 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

Von der Schule gewünschte Ergänzungen von WLAN-Accesspoints müssen daher über die BSB beschafft werden (schul-it@bsb.hamburg.de).

Die Geräte werden u.a. durch folgende Einstellungen geschützt:

- Der WLAN Access Point wird durch IT-Dienstleister der BSB vorkonfiguriert an die Schule übergeben.
- Ein aktuelles Protokoll zur Authentifizierung und Verschlüsselung der WLAN-Verbindung wird genutzt; z.Zt. WPA2-Verschlüsselung mit 128bit AES Verschlüsselung.
- Es ist ein komplexer Schlüssel zu verwenden, der mind. 20 Zeichen umfasst. Alternativ kann eine Authentifizierung und Autorisierung durch Zertifikatsberechtigung an einem RADIUS-Server (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) erfolgen.
- Die Administration des WLAN Access-Points erfolgt über eine gesicherte Verbindung oder aber drahtgebunden.
- Es wird eine nichtssagende SSID verwendet, die es nicht zulässt, auf die WLAN-Hardware zu schließen (z.B. eine 10-stellige Zahlenkolonne).

Optionale Verbesserung

- Fest installierte WLAN Access Points, die dauerhaft ihr Funknetz senden, eröffnen einen leichten Zugang. Der Schutz wird daher erheblich verbessert, wenn Zertifikate genutzt oder die MAC-Adressen der zugelassenen Rechner hinterlegt werden.
- Portabel genutzte Access Points sollten in regelmäßigen Abständen mit dem Netz verbunden werden, damit Sicherheitsupdates und nötige Firmware eingespielt werden können.

1.2.2 WLAN Netzarten

An den staatlich allgemeinbildenden Schulen gibt es zwei getrennte WLAN Netze für unterschiedliche Einsatzkontexte:

a) WLAN für schulische IT-Endgeräte (Schulnetz = grünes Netz:) Dieses WLAN Netz dient unterrichtlichen Zwecken und darf nur von schuleigenen IT-Endgeräten genutzt werden. Die Nutzung mit privaten Endgeräten ist in diesem WLAN Netz ausgeschlossen; siehe nachfolgenden Punkt.

b) WLAN für private IT-Endgeräte (BYOD-Netz[1] = blaues Netz): Um Lehrkräften und Schülerinnen und Schülern (SuS) die Nutzung Ihrer privaten IT-Endgeräte zu ermöglichen, wurde im dieses separate WLAN Netz eingeführt. Für die Nutzung dieses WLAN Netzes ist eine Benutzerauthentifizierung (eduPort-Account) an dem zentralen WLAN Management (RADIUS-Server) erforderlich.

Bezüglich der eingesetzten privaten IT-Endgeräte sind die Vorgaben dieses Dokumentes sowie etwaige übergeordnete Vorordnungen (Gesetze, Richtlinien u.a.) einzuhalten.

1.3 Jugendschutzfilter

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

Standard

- Im Rahmen der Anbindung an das Glasfasernetz der Freien und Hansestadt Hamburg erhalten alle Schulen einen Schulrouter mit integriertem Jugendschutzfilter. 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 aufgrund der Schnelllebigkeit der Internetinhalte es dazu kommen kann, 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.

1.4 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 und zu aktivieren. Router enthalten i.d.R. eine Firewall.

[1] BYOD = bring your own device

Sicherheitsregeln (Policy)

Ausgangspunkt für die Firewall ist die Festlegung der Sicherheitsregeln (policy). Diese beinhaltet u.a. die explizite Freigabe und Sperrung von Ports. Als Grundkonfiguration werden folgende Einstellungen festgelegt:

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

Zugriffe in das Internet über das pädagogische Netz (LAN) und WLAN (grünes Netz)					
Ports	**Dienst**	**Verwendung**	**Ports**	**Dienst**	**Verwendung**
8	ICMP	PING	995	TCP	POP3 (SSL/TLS)
30	ICMP	PING (Traceroute)	1194	UDP	OpenVPN
53	TCP + UDP	DNS	1900	TCP	Bonjour-Dienst
80	TCP	HTTP, App Store, Itunes ,	2195	TCP	Apple MDM
443	TCP	HTTPS + Apple MDM	2196	TCP	Apple MDM
445	TCP	SMB-Freigaben,	3689	TCP	Itunes
		Active Directory,	4500	UDP	IPSec VPN
		Windows Freigaben	5223	TCP	Apple MDM
465	TCP	SMTP (SSL/TSL)	5228	TCP + UDP	Google Play Store
500	UDP	IPSec VPN	5350	UDP	Bonjour-Dienst
587	TCP	SMTP (STARTTLS)	5351	UDP	Bonjour-Dienst
989	TCP + UDP	FTPS	8080	TCP + UDP	Microsoft Store
990	TCP + UDP	FTPS			
993	TCP	IMAP (SSL/TLS)			

Zugriffe aus dem Internet
keine

Zugriffe in das Internet über WLAN für private Endgeräte (blaues Netz)					
Ports	**Dienst**	**Verwendung**	**Ports**	**Dienst**	**Verwendung**
53	TCP + UDP	DNS	995	TCP	POP3 (SSL/TLS)
80	TCP	HTTP, App Store, Itunes ,	1900	TCP	Bonjour-Dienst
443	TCP	HTTPS + Apple MDM	3689	TCP	Itunes
465	TCP	SMTP (SSL/TSL)	5228	TCP + UDP	Google Play Store
587	TCP	SMTP (STARTTLS),	5350	UDP	Bonjour-Dienst
		FTPS,	5351	UDP	Bonjour-Dienst
		FTPS	8080	TCP + UDP	Microsoft Store
993	TCP	IMAP (SSL/TLS)			

Zugriffe aus dem Internet
keine

Zugriffe in das Internet über LAN (orangenes Netz)					
Ports	**Dienst**	**Verwendung**	**Ports**	**Dienst**	**Verwendung**
8	ICMP	PING	989	TCP + UDP	FTPS
30	ICMP	PING (Traceroute)	990	TCP + UDP	FTPS
53	TCP + UDP	DNS	993	TCP	IMAP (SSL/TLS)
443	TCP	HTTPS + Apple MDM	995	TCP	POP3 (SSL/TLS)
445	TCP	SMB-Freigaben, Active Directory, Windows Freigaben, SMTP (SSL/TSL)	1194	UDP	OpenVPN
			2195	TCP	Apple MDM
			2196	TCP	Apple MDM
			4500	UDP	IPSec VPN
500	UDP	IPSec VPN	5223	TCP	Apple MDM
587	TCP	SMTP (STARTTLS)	8080	TCP + UDP	Microsoft Store

Zugriffe aus dem Internet
keine

Empfehlung

Zusätzlich Schutz bieten die individuellen Firewalls der jeweiligen IT-Endgeräte

1.5 Benutzerauthentifizierung

Durch eine Authentifizierung der Benutzer am Netzwerk wird sichergestellt, dass nur Berechtigte hierauf Zugriff erhalten. Neben den Möglichkeiten einer differenzierten Rechte-Zuordnung der jeweiligen Benutzer können auch etwaige missbräuchliche Verwendungen (z.B. Urheberrechtsverletzungen durch das Nutzen von Filesharing-Börsen), nachverfolgt werden. Kann der Benutzer, der eine Urheberrechtsverletzung begangen hat, nicht nachvollzogen werden, haftet die Schulleitung.

Standard

a) Weiterführende Schulen
- Durchgehende Benutzerverwaltung
- Keine Admin-Kennungen für Schüler
- Keine Einrichtung eines Gast-Kennungen

b) 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

1.6 Fernzugriff / Fernwartung

Aus Sicherheitsgründen ist der 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 Schadsoftware (Malware, z.B. Viren, Würmer, Trojaner, Spyware), das Ausspähen von (personenbezogenen) Daten und Passwörtern sowie das Öffnen des Netzwerkes für unerlaubten Zugriff.

Standard

Organisatorisch:

Die Fernwartung unterliegt den Bedingungen der Telekommunikationsrichtlinie der Stadt Hamburg. Unabdingbare Voraussetzung ist daher, dass die Einhaltung dieser Bedingungen mit demjenigen, der die Fernwartung durchführen will, 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 IT-Endgeräte der Schule per Fernzugriff warten, kann ein Zugriff über den zentralen VPN-Sprungserver eingerichtet werden. Der Zugriff muss über die BSB (schul-it@bsb.hamburg.de) mit dem unterschriebenen und eingescannten Formular der Anlage beauftragt werden. 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 Server (z.B. E-Mail- / Webserver oder Lernplattformen) betreiben, die von außerhalb erreichbar sind (d.h. außerhalb des schulinternen pädagogischen Netzes (LAN/WLAN), ist es erforderlich, eine DMZ (Demilitarisierte Zone) auf dem Router einzurichten, über die der Zugriff in das pädagogische Netz erfolgt (sog. 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. Diese sind bei der BSB (schul-it@bsb.hamburg.de) zu beantragen.

2 Server und IT-Endgeräte

2.1 Allgemeine Schutzmaßnahmen

2.1.1 Betriebssystem und Softwareanwendungen

Neben der zentralen Netzwerkinfrastruktur sind Firmware, Betriebssysteme, Internet-Browser und Softwareanwendungen ein häufiges Ziel von Angriffen. Die Internet-Browser sind die zentralen Anwendungen für die Nutzung von Onlineangeboten im Internet und stellen damit einen wesentlichen Angriffspunkt für Schadsoftware und gefährlichen Webseiten dar.

Standard

Für einen sicheren Betrieb der IT-Endgeräte (Server, Desktop, Notebook, Tablet, Smartphones etc.) und sonstigen internetfähigen Geräte (z.B. Internet of Things) ist es erforderlich, dass die aktuellen Sicherheitsupdates und Fehlerbehebungen des Betriebssystems (z.B. Microsoft Windows, iOS, Android) zeitnah eingespielt werden. Dieses gilt auch für die Internet-Browser. Softwareanwendungen sollten auch regelmäßig aktualisiert werden.

2.1.2 Virenschutz

Schadprogramme gefährden sämtliche IT-Endgeräte (Server, Desktop, Notebook, Tablet, Smartphones etc.) und sonstigen internetfähigen Geräte (z.B. Internet of Things). Aufgrund der Vielseitigkeit der Schadprogramme lassen sich diese nicht mehr singulär einer Malware-Kategorien (z.B. Virus, Wurm, Trojaner, Spyware) zuordnen. Sie erfüllen meist mehrere Funktionalitäten. Das Eindringen von Schadprogrammen kann auf den Endgeräten, den Servern und im Netz erheblichen Schaden verursachen.

Standard
Für die Endgeräte- und Netzwerksicherheit ist es daher unerlässlich, dass auf allen Endgeräten und Servern, sofern verfügbar, ein aktuelles Virenschutz-Programm installiert und die aktuellen Updates eingespielt sind.

Produktempfehlungen finden Sie auf der Website Schul-IT der BSB in der Rubrik Software-Beschaffung: https://schul-it.hamburg.de/software-beschaffung-paedagogik/

2.1.3 Benutzerkonto

Betriebssysteme bieten die Möglichkeit Benutzerkonten mit unterschiedlichen Rechten einzurichten. Das Administratorenkonto bietet die größten Eingriffsmöglichkeiten in das System; z.B. um Programme zu installieren oder Einstellungen zu ändern. Wird ein IT-Endgerät mit Schadprogrammen infiziert, sind die Eingriffsmöglichkeiten des Schadcodes (u.a. Manipulationen am Endgerät, Datendiebstahl, Nutzer blockieren) mit den Berechtigungen eines Administratorkontos um so gravierender.

Standard
Der Zugriff auf das Internet soll ausschließlich über ein Benutzerkonto mit eingeschränkten Rechten, keinesfalls ein Administrator-Konto, erfolgen.

2.2 Private Endgeräte

Mit der Nutzung privater IT-Endgeräte im schulischen Umfeld müssen auch die allgemeinen IT-Sicherheitsrisiken und deren Schutzmaßnahmen betrachten werden. Es bestehen u.a. folgende IT-Risiken:

- die Verbreitung von Schadsoftware durch ungeschützte IT-Endgeräte,
- bei mobilen IT-Endgeräten (u.a. Smartphones) können Malware alles protokollieren, entwenden und veröffentlichen, was die Nutzer damit machen (z.B. ein-/ ausgehende Anrufe, SMS, Adressbücher, GPS-Standorte, Dateneingaben). Mit Rooter-Malware können Dritte Zugriff und Kontrolle über das IT-Endgerät übernehmen
- bei privaten IT-Endgeräten von Lehrkräften der unberechtigte Zugriff auf personenbezogene Daten ermöglichen
- der unkontrollierte Zugriff im pädagogischen Netz (z.B. Einsatz von ungewünschten Programmen, wie das Ausspähen der Passworte)

Standard:

- **Private Geräte der Lehrkräfte**
  Bei der Nutzung privater IT-Endgeräte durch Lehrkräfte im schulischen Einsatz sind zum einen die Vorgaben dieses Dokumentes, insbesondere die Sicherstellung der allgemeinen Schutzmaßnahmen (vgl. Punkt 2.1), zu erfüllen und einzuhalten. Zum anderen sind Maßnahmen zur Gewährleistung eines angemessenen Datenschutzstandards der gespeicherten Daten (z.B. personenbezogene Daten der Schülerinnen und Schüler) gemäß den geltenden datenschutzrechtlichen Bestimmungen umzusetzen. Genaueres regeln ergänzende Dienstanweisungen und Richtlinien (u.a. Richtlinie zur Verwendung privater IT-Endgeräte).
  Eine Nutzung des WLANs (BYOD/blaues Netz) für private Endgeräte der Lehrkräfte ist unter Einhaltung dieser Vorgaben möglich.

- **Private Geräte der Schülerinnen und Schüler**
  Eine Nutzung des WLANs (BYOD/blaues Netz) für private Endgeräte der Schülerinnen und Schüler ist dann möglich, wenn zum einen die Schule diesen WLAN explizit für die Schülerinnen und Schüler freigeben hat und zum anderen, wenn die Vorgaben dieses Dokumentes, insbesondere die Sicherstellung der allgemeinen Schutzmaßnahmen an den privaten Endgeräten (vgl. Punkt 2.1) sichergestellt werden.

2.3 Externe Datenspeicher

Soweit die Schule externe, nicht BSB-seitig zentral bereitgestellte Datenspeicher oder Webspeicher von Dritten für die Verarbeitung von Daten einsetzt, hat sie grundsätzlich vorab ein Verfahrensverzeichniss und die Datenschutz-Folgenabschätzung (DSFA) dem behördlichen Datenschutzbeauftragten zur Bewertung zuzuleiten.

B. Empfehlungen

1 UEFI-/ BIOS-Schutz

Schadprogramme können nicht nur Betriebssysteme und Softwareanwendungen angreifen, sondern auch die Firmware-Module UEFI (**U**nified **E**xtensible **F**irmware **I**nterface) bzw. dem Vorläufer BIOS (**B**asic **I**nput/**O**utput **S**ystem). Das Firmware-Modul läuft bereits, während das IT-Endgerät erst startet (bootet). Dadurch ist es möglich, Schutzmaßnahmen abzuschalten und vertrauliche Daten zu entschlüsseln. Um einen sicheren Systemstart zu gewährleisten, ist es erforderlich eine geschlossene Sicherheitsumgebung mittels Passwortschutz der Firmware-Module aufzubauen.

Empfehlung

a) UEFI
- Zur Absicherung des Betriebssystemstarts wird UEFI Secure Boot verwendet. Dieser garantiert die Echtheit bzw. Unverfälschbarkeit von wichtigen Software-Teilen der Firmware.
- Die vorinstallierten Schlüssel sollten auf Vertrauenswürdigkeit überprüft werden

b) BIOS
- 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 Geräteauthentifizierung

Die Geräte-Authentifizierung ermöglicht einen kontrollierten Zugriff auf das pädagogische Netz (LAN und WLAN); d.h. der Zugriff kann auf Geräte eingeschränkt werden, die den Sicherheitsstandards entsprechen. Darüber hinaus wird eine Nachvollziehbarkeit – zumindest der Geräte – bei Urheberrechtsverletzungen hergestellt. Die MAC-Adresse (**M**edia-**A**ccess-**C**ontroll-Adresse) ist die eindeutige Identifikation eines Netzwerkadapters eines IT-Endgerätes im Netzwerk.

Empfehlung

Der Zugriff auf das pädagogische Netz sollte mittels MAC-Registrierung der IT-Endgeräte an dem Router gesteuert werden. Die Router mit Jugendschutzfilter werden mit der Einstellung „Registrierung: ja“ und „Internet nur für registrierte Geräte: nein“ ausgeliefert, damit die Inbetriebnahme des Filters nicht zur Zugriffsverweigerung der noch unregistrierten IT-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.

3 Protokollierung der Internetzugriffe

Um sich gegen missbräuchliche Nutzung des pädagogischen Netzwerkes (LAN und WLAN) zu schützen (z.B. Malware-Aktivitäten, Urheberrechtsverletzungen), ist es erforderlich, die Zugriffe nachzuvollziehen. Dieser Punkt ergänzt die Einrichtung einer Benutzerverwaltung.
Nach Rücksprache mit der behördlichen Datenschutzbeauftragten ist eine Protokollierung zulässig, wenn

- Regeln definiert wurden, wann die Protokolldateien im Vier-Augen-Prinzip ausgewertet werden dürfen (z.B. nur bei einem begründeten Verdacht)

- und die Protokolldateien nur 2 Monate aufbewahrt werden.

Empfehlung

Wird die Firewall auf dem Schulrouter genutzt, sollte dort auch die Protokollierung aktiviert werden. Zu beachten sind dabei die o.g. Bedingungen.

4 Datensicherungen

Um Datenverluste, insbesondere auf Servern und NAS-Laufwerken (Network Attached Storage), zu verhindern, sollten regelmäßig Datensicherungen durchgeführt werden.

Empfehlung

Erstellung und Umsetzung eines Datensicherungskonzeptes, in dem u.a. Zeitintervall, Zeitpunkt der Datensicherung, die Anzahl der aufzubewahrenden Generationen, Umfang der zu sichernden Daten sowie die Zuständigkeit für die Durchführung, Überwachung der Sicherung und Rückspielung der Daten enthalten sind. Vertrauliche Daten sollten vor der Sicherung möglichst verschlüsselt werden.

C. Glossar

Begriff	Erläuterung
AES	Advanced Encryption Standard – effizienter und sicherer Algorithmus zum Verschlüsselung und Entschlüsseln von Daten, der 128, 192 oder 256 Bit Schlüssellängen verwendet
BIOS	Basic Input Output System – veraltetes Kernsystem aus den 1970er Jahren, welches zum Starten der Hardware (Boot-Vorgang) erforderlich ist. Beschränkungen liegen u.a. in 1024 KByte Arbeitsspeicher und 2,2 TByte Festplattengröße. Nachfolger: → UEFI
Datenschutz	Grundrecht auf informationelle Selbstbestimmung gewährleistet jedem das Recht, über Verwendung und Preisgabe seiner persönlichen Daten zu bestimmen. Seit dem 25.05.2018 gilt eine einheitliche Europäische Datenschutz-Grundverordnung (→ DSGVO)
DMZ	Demilitarisierte Zone - bezeichnet eine Pufferzone, die ein internes Netzwerk von öffentlichen Netzwerken trennt und so absichert. In der DMZ befinden sich u.a. E-Mail- oder Webserver, deren Kommunikation durch Firewalls überwacht wird
DSGVO	Datenschutz-Grundverordnung - EU-weit vereinheitlichte Verordnung der Europäischen Union zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen
DSFA	Datenschutz-Folgenabschätzung – In der → DSGVO ist in Artikel 35 die Pflicht verankert, vor Beginn einer geplanten Datenverarbeitung, die Folgen der Verarbeitung für den Schutz der personenbezogenen Daten abzuschätzen und zu dokumentieren
Firmware	In einem Speicherchip eingebettete Software, die die Grundfunktionalität eines Gerätes ermöglicht
http	Hypertext Transfer Protocol - ermöglicht die Kommunikation zwischen Browser und Webserver, d.h. den Datenaustausch über das Internet.
https	Hypertext Transfer Protocol Secure – ermöglicht ggü. dem → http die sichere, d.h. abhörsichere Kommunikationsübertragung im Internet
ICMP	Internet control message protocol - zur Übertragung von Statusinformationen und Fehlermeldungen in IP-, TCP- und UDP-Protokollen um die Übertragungsqualität zu verbessern. Für die Nutzer nicht direkt einsehbar.
Informationssicherheit	Schutzziele der (technischen) Verarbeitung von Informationen, dass diese vollständig, korrekt und verfügbar, aber vor dem unberechtigtem Zugriff geschützt sind
IoT	Internet of Things = Internet der Dinge – Oberbegriff für eine allgegenwärtige Technologie, die es ermöglicht, Geräte, Sensoren und Gegenstände miteinander zu vernetzen, damit diese autonom kommunizieren und agieren können
IT-Endgerät	Oberbegriff für alle Internet-fähigen Geräte in einem TCP/IP-Netzwerk; u.a. Desktop-Computer, Laptops, Tablets, Smartphones, Drucker sowie „Internet of things“-Geräten
Jugendmedienschutz	Oberbegriff für den Schutz von Kindern und Jugendlichen vor schädlichen Einflüssen durch Medien, u.a. Erwachsenenwelt, die nicht dem Entwicklungsstand der Minderjährigen entsprechen. Rechtliche Grundlage sind u.a. im Jugendschutzgesetz (JuSchG), im Jugendmedienschutz-Staatsvertrag (JMStV) und Verbreitungsverbote des Strafgesetzbuchs (StGB)

LAN	Local Area Network – lokales, örtliches Netzwerk
LDAP	Lightweight Directory Access Protocol – Verzeichniszugriffsprotokoll zur Durchführung von Abfragen und Änderungen in einem verteilten Verzeichnisdienst. Anwendungsfall für LDAP kann z.B. eine Benutzerverwaltung sein
MAC	Media Access Control – die MAC-Adresse ist eine 48-Bit lange physikalisch eindeutige Adresse einer Netzwerkschnittstelle und dienst als Identifikator eines IT-Endgerätes im Netzwerk.
Malware	Schadsoftware – Oberbegriff für alle Arten bösartiger Software, die versuchen ein IT-Endgerät zu infizieren, um u.a. persönlichen Daten und Kennwörter auszuspähen, Systeme versteuern oder zu blockieren und Geld zu erpressen. Malware-Kategorien sind z.B. →Virus, →Wurm, →Trojaner, →Spyware
NAS	Network Attached Storage – Dateiserver mit höherer Festplattenspeicherkapazität in einem Netzwerk. Je nach Ausführung können verschiedene Benutzer mit unterschiedlichen Berechtigungen angelegt werden
PXE	Preboot Execution Environment – Verfahren um Computer über das Netzwerk zu starten (booten).
RADIUS-Server	Remote Authentication Dial-In User Service – zentraler Authentifizierungsdienst, insbesondere in →WLAN Netzwerken, der Nutzer in einem Netzwerk authentifiziert und autorisiert.
SIP2010	Sonderinvestitionsprogramm 2010 – alle allgemeinbildenden staatlichen Schulen haben flächendeckend eine Netzinfrastruktur (→LAN) sowie eine breitbandige Internetanbindung über das stadteigene Glasfasernetz (WAN) erhalten
SMTP	Simple Mail Transfer Protocol – Netzwerk-Kommunikationsprotokoll für die Übertragung von E-Mails. Die Kommunikation (Senden und Weiterleiten) erfolgt zwischen einem E-Mail-Client und einem SMTP-Server. Dabei können die Daten auch zwischen zwei oder mehr Servern ausgetauscht werden
Sprungserver	Eine Fernwartung von Rechner im LAN über das Internet ist gefährlich. Daher wird hierfür eine verschlüsselte, nicht abhörbare Verbindung (via Remote Desktop) benötigt, die über einen gehärteten und überwachten Sprungserver via ssh-Verbindung hergestellt wird
Spyware	Spion-Software zählt zur Malware. Sie späht ohne Wissen der Nutzer Daten aus um diese entweder zu verkaufen oder gezielt Werbung und Produkte anzubieten. Hierzu werden ggf. Ports geöffnet und ungewollte Programme installiert, u.a. Keylogger (Aufzeichnen von Tastureingaben), Browser-Hijacking (Verändern von Standard-Einstellungen oder manipulierte Such-/ Symbolleisten)
SSID	Service Set Identifier – Name eines Funknetzwerkes (→WLAN)
TCP/IP	Transmission Control Protocol/Internet Protocol - Protokoll-Familie für die Vermittlung und den Transport von Datenpaketen in einem dezentralen Netzwerk (→LAN). Es erbringt zentrale Funktionen: Logische Adressierung (IP), Wegfindung (IP), Fehlerbehandlung und Flussteuerung (TCP), Anwendungsunterstützung (TCP) und Namensauflösung (DNS)
Trojaner	Zählt zur Malware und tarnt sich nach außen als harmloses Programm. Sie ermöglichen unberechtigten Dritten den Zugriff auf das infizierte IT-Endgerät und das Ausspähen von Daten
UEFI	(Unified Extensible Firmware Interface – ersatz für das veraltete → BIOS. UEFI kann verschlüsselte Treiber und Software verwenden

	und bietet u.a. höhere Sicherheit in der Boot-Phase durch das Verhindern unautorisierter → Firmware, Betriebssysteme oder anderer UEFI-Treiber.
Verfahrensverzeichnis	Verzeichnis von Verarbeitungstätigkeiten - In der → DSGVO ist in Artikel 30 die Pflicht verankert, vor Beginn einer geplanten Datenverarbeitung, zu einem Verfahren zu beschreiben, wer verantwortlich, welche Informationen zu welchem Zweck verarbeitet, löscht und übermittelt.
Viren	Der Computervirus zählt zur Malware und kann sich selbst reproduzieren. Es gibt eine Vielzahl von unterschiedlichen Viren, u.a. Bootsektorviren, Skriptviren (Javascript oder Virtual-Basic-Script (VBS) auf Internetseiten), Programmviren, Makroviren (u.a. in Word- oder Excel-Dateien)
VPN	Virtual Private Network – Echtzeit verschlüsselte Verbindung zwischen zwei Stellen (z.B. Client – Server) zur Sicherung der Informationen gegen Ausspähen und Manipulationen
WAN	Wide Area Network – Netzwerk über größere Entfernungen um verschiedene →LANs, aber auch einzelne Rechner miteinander zu vernetzen
WLAN	Wireless Local Area Network - drahtloses lokales Funk-Netzwerk
WPA2	Wi-Fi Protected Access 2 – ist ein Sicherheitsstandard (IEEE 802.11i) für die Authentifizierung und Verschlüsselung von WLANs und basiert auf dem → AES
Würmer	Würmer zählen zur Malware und können sich ohne Hilfe der Benutzer selbstständig weiter verbreiten; klassischerweise per E-Mail. Diese können u.a. Daten zerstören und ausspähen.

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 bei der Behörde für Schule und Berufsbildung per E-Mail (Schul-IT@bsb.hamburg.de) 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. Die- se ist durch die Schulleitung bei der Behörde für Schule und Berufsbildung per E-Mail (Schul-IT@bsb.hamburg.de) mit dem anliegenden Formular zu beauftragen.

_____	_____
Schulleitung	Dienstleister

Anlage 2: Antrag zum Fernzugriff im pädagogischen Netzwerk

An

IT - Service - Pädagogik

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

_____