

B. Richtlinien Internet-Sicherheit

Version 0.52

0.1 Grundsätzliches

Diese Richtlinie beschreibt die pädagogischen, technischen und organisatorischen Vorgaben für die Umsetzung der Internet-Sicherheit an den Zürcher Schulen. Sie basieren auf der kantonalen Gesetzgebung (IDG, IDV und ISV) und auf den Erfahrungen im Umgang mit Internet-Sicherheit der letzten Jahre.

Aufgrund der rasanten Entwicklungen im ICT-Bereich sollten diese Richtlinien in der Regel alle 4 bis 5 Jahre überprüft und gegebenenfalls den veränderten Gegebenheiten angepasst werden.

0.1.1 Ziele

Das Ziel dieser Internet-Sicherheits-Richtlinien ist es, die Schulen bei der Anwendung und Umsetzung einer guten Praxis betreffend der Sicherheit bei der Internet-Nutzung durch Schüler/innen, Lehrer/innen oder andere an der Schule tätige Personen zu unterstützen. Folgende drei Grundsätze sind dabei massgebend:

Es wird sowohl auf massvolle pädagogische als auch auf technische Massnahmen gesetzt.

Die Internet-Sicherheits-Infrastruktur soll schulspezifisch sein und ein semiprofessionelles Niveau erreichen.

Es wird eine Balance zwischen Sicherheitsrisiken, technischen Massnahmen und pädagogisch, didaktischem Mehrwert eines einfachen Netzzugangs angestrebt.

0.1.2 Definition von Internet-Sicherheit

Internet-Sicherheit ist ein sehr weiter Begriff. Er umfasst Themen wie

1. **Computer- und Netzsicherheit**, der Schutz der Infrastruktur vor Angriffen (Hacken, mutwillige automatisierte Überlastung, sowie Viren und anderem Schadcode)
2. **Datensicherheit**, der Schutz der Daten vor unerlaubtem Zugriff, Manipulation oder Verlust (Verschlüsselung, Datensicherung, etc.)
3. **Datenschutz**, der Schutz personenbezogener Daten vor Missbrauch (siehe Datenschutzgesetz)
4. **Schutz der Kinder, Jugendlichen und Lehrpersonen** vor problematischen Inhalten, problematischen Kontakten und Cybermobbing
5. **Schutz der Lehrer/innen und der Schule**, dass sie nicht in unangenehme und/oder rechtlich problematische Situationen geraten bzgl. der Internet-Nutzung in der Schule oder Internet-Einsatz im Unterricht (siehe Personalgesetz)
6. **Schutz der Schule** im Sinne, dass sie ihre Verantwortung bzgl. den obigen Punkten wahrnimmt.

0.1.3 Gültigkeitsbereich

- Diese Richtlinien betreffen alle von der Schule zur Verfügung gestellten Internetzugänge. Sie betreffen nicht die privaten Internetzugänge (via Handy etc.) der Schüler/innen und Lehrer/innen. Diese sind im Verantwortungsbereich der Nutzer/innen resp. deren Eltern. Die Nutzung der privaten ICT-Geräte auf dem Schulareal und im Unterricht ist in der *Internet-Nutzungsvereinbarungen* mit den Schüler/innen und Lehrer/innen geregelt.
- Schulen, die über eine umfassende ICT-Konzeption verfügen, können begründet auf die Umsetzung einzelner Richtlinien verzichten, falls diese anderweitig abgedeckt werden.
- Stufenspezifische Richtlinien sind folgendermassen gekennzeichnet: KGU (Kindergarten/Unterstufe), M (Mittelstufe), S1 (Sekundarstufe 1), S2 (Sekundarstufe 2).

0.2 Pädagogische Richtlinien

0.2.1 Gelebte Kultur der Internet-Nutzer/innen

- (a) In der Schule wird eine offene Kultur und ein Diskurs über den Umgang mit Internet-relevanten Themen gepflegt (z.B. Copyright, Sicherheit, Personen- und Datenschutz, Qualität von Informationsquellen, etc.).

0.2.2 Verhaltenskodizes mit Internet-Nutzer/innen

- (a) Jede Schule verfügt über eine *Internet-Nutzungsvereinbarung*, als Ergänzung zur Schulhausordnung oder als integraler Bestandteil dieser.
- (b) Die *Internet-Nutzungsvereinbarung* weist auf angemessenes, respektvolles Verhalten im Internet hin.
- (c) Die *Internet-Nutzungsvereinbarung* ist von allen Internet-Nutzer/innen resp. deren Eltern zur Kenntnis zu nehmen.

0.2.3 Medienkompetenz der Internet-Nutzer/innen

- (a) Alle Internet-Nutzer/innen verfügen über ihrer Stufe entsprechenden Internet-Nutzungs-Kompetenzen.
- (b) Alle Internet-Nutzer/innen verfügen über eine ihrer Stufe entsprechenden Medienkompetenz bezüglich Internet-Nutzungs.
- (c) Alle Internet-Nutzer/innen sind sich den ihrer Stufe entsprechenden Problemen bei der Internetnutzung bewusst.
- (d) Lehrpersonen und Schulverwaltungspersonal sind mit dem Umgang von personenbezogenen Daten vertraut.

0.3 Umgang mit Daten

Die Internet-Nutzer/innen beachten das Datenschutzgesetz, insbesondere

- (a) personenbezogene Daten sind zurückhaltend zu erfassen.

- (b) personenbezogene Daten dürfen nur mit Zustimmung der Betroffenen im Internet veröffentlicht werden.
- (c) qualifizierende personenbezogenen Daten sind verschlüsselt zu speichern und zu versenden.

0.4 Technische Richtlinien

0.4.1 Anforderungen an die ICT-Nutzergeräte

Unter ICT-Nutzergeräte zählen Workstations, Desktops, Notebooks, Subnotebook, Netbooks, Tablets, E-Book-Reader, Handys, Smartphones, Musikgeräte, Videogeräte, etc. mit der Möglichkeit des Internetzugangs.

- (a) Alle in der Schule verwendeten ICT-Geräte für die Schadcode in Umlauf ist, müssen über einen aktuellen Schadcodeschutz (Virenschutz etc.) verfügen.
- (b) Alle in der Schule verwendeten ICT-Geräte, für die Sicherheitsupdates angeboten werden, müssen regelmässig aktualisiert werden.

0.4.2 Anforderungen an das IT-Netzwerk

- (a) Das Netzwerk ist dokumentiert zum Beispiel als *Netzwerkplan und/oder Inventarliste*.
- (b) Der Netzverkehr vom Schulnetz zu Internet-Anwendungen wird maximal 6 Monate protokolliert.
- (c) Der Netzverkehr vom Schulnetz zu Internet-Anwendungen (Web, Mail, FTP, etc.) wird überprüft bezüglich
 - welche Art von Internet-Anwendungen erlaubt, resp. ausgeschlossen werden (Firewall),
 - welche Internet-Quellen erlaubt, resp. ausgeschlossen werden (Ressourcen-Filterung).
 - wer den Internet-Zugang nutzen darf, resp. ausgeschlossen wird (Authentifizierung/Autorisierung),
- (d) Die Einstellung von Firewall, Ressourcen-Filterung und Authentifizierung/Autorisierung ist dokumentiert in einer *Sicherheitspolicy*.
- (e) Firewall, Ressourcen-Filterung und Authentifizierung/Autorisierung kann von der Schule selbst oder in Auftrag betrieben werden.
- (e) Eine Firewall soll die Schule gegen unberechtigte An- und Zugriffe von und nach aussen schützen.
- (f) Eine Ressourcen-Filterung beschränkt den Zugang zu problematischen Inhalten auf allen den Schüler/innen zugänglichen Geräten mit Internetzugang der Schule. Das Ressourcen-Filterung kann auf URL-Verbotslisten und/oder Inhaltsüberprüfung aufbauen. Ressourcen-Filterung ist verpflichtend für KGU, M und S1 und empfohlen für S2.
- (g) Die Authentifizierung/Autorisierung beschränkt den Internet-Zugang auf bekannte Nutzer/innen. Authentifizierung/Autorisierung ist verpflichtend für S2 und empfohlen für S1, M.
- (h) Anonyme Internetzugänge können aus pragmatischen Gründen weiter angeboten werden, unter der Bedingung einer restriktiven Ressourcen-Filterung und einer restriktiven Firewall.
- (i) Detailanforderungen zu (FW) Firewall, (RF) Ressourcen-Filterung und (AA) Authentifizierung/Autorisierung sind im Anhang zu finden.

0.5 Organisatorische Richtlinien

0.5.1 Verantwortliche Personen

- (a) Es ist eine Person zu bestimmen, die für die Umsetzung der Internet-Sicherheit verantwortlich ist, sich informiert und bei Fragen als Ansprechperson gilt.
- (b) Die Schule hat ein mehrstufiges pädagogisches und technisches Support-Konzept eingerichtet, das auch bei Fragen zu Internetnutzung und Internetsicherheit greift.

0.5.2 Sicherzustellende Vorgehen

- (a) In der Schule ist ein Vorgehen sicherzustellen, wie bei Angriffen von aussen und bei Missbrauch von innen die notwendigen Gegenmassnahmen (z. B. Informationswege, Sichern von Beweisen, etc.) eingeleitet werden.
- (b) In der Schule ist ein Vorgehen sicherzustellen zur Auswertung personenbezogener Logdaten.
- (c) In der Schule ist ein Vorgehen sicherzustellen, wie das Sperren oder Freigeben von Internetinhalten bzgl. der Ressourcen- oder Inhalts-Filterung geregelt ist.

0.6 Unterstützung durch das VSA/MBA

Die Schulen werden bei der Umsetzung dieser Richtlinien unterstützt:

- Beim Kanton (VSA und MBA) sind für die in den Richtlinien erwähnten Dokumente Beispieldokumente verfügbar.
- Der Kanton (VSA und MBA) unterstützt die Evaluation/Entwicklung von semiprofessionellen Angeboten/Lösungen, die die technischen Anforderungen dieser Richtlinien erfüllen.
- Der Kanton (VSA und MBA) koordiniert die Lizenzierung von Sicherheits-Software wo möglich und notwendig.
- Der Kanton (VSA und MBA) oder/und der Bund (educa) stellt den Schulen regelmässig (wöchentlich) aktualisierte URL-Sperrlisten zu den wesentlichen Kategorien als Grundlage für die Ressourcenfilterung bereit.
- Der Kanton (VSA und MBA) oder/und der Bund (educa) stellt den Schulen ein föderiertes Authentifizierungs- und Autorisierung-System zur Verfügung.

0.7 Inkrafttreten

Diese Richtlinie tritt ab sofort in Kraft. Für bestehende Lösungen gilt eine Übergangsfrist bis Ende Schuljahr 2010/11.

unterzeichnet

Regierungsrätin Regina Aepli

0.8 Anhang

Dieser Anhang beschreibt eine technische Sichtweise und gilt als Orientierung für die technische Umsetzung, der Richtlinien.

0.8.1 Detailanforderung an die Netzwerkkomponenten

- Alle zentralen Netzwerkkomponenten müssen IPV4 und IPV6 behandeln können.

0.8.2 Detailanforderung an eine Firewall (FW)

Eine Firewall muss folgende Minimalanforderungen erfüllen:

- (a) in einer *Sicherheitspolicy* ist zu definieren, welcher Netzverkehr nach bestimmten Regeln zugelassen oder verhindert werden soll. Diese *Sicherheitspolicy* muss für eine gesamte Schule Gültigkeit haben.
- (b) Diese *Sicherheitspolicy* muss in regelmässigen Abständen überprüft und den aktuellen Umständen angepasst werden.
- (c) Die Firewall muss den Traffic protokollieren. Es muss in sinnvollen Abständen geprüft werden, ob die Zugriffsbeschränkungen eingehalten werden und funktionieren. Nur durch eine hohe Analyse-Frequenz können Angriffe wie Port Scans, Smurf, Ping of Death, oder Teardrop in nützlicher Zeit erkannt und abgewehrt werden.
- (d) Die Logdaten der Firewall müssen mindestens 6 Monate lang archiviert werden.
- (e) Die Software-Komponenten müssen in regelmässigen Abständen ein Update erfahren. Es ist ein Qualitätsmerkmal der eingesetzten Lösung, wie häufig solche Updates zur Verfügung gestellt werden.
- (f) Sämtliche Anpassungen der Konfiguration auf der Firewall müssen im System rückverfolgbar sein. Der Zugriff zum Ändern der Konfiguration muss eingeschränkt werden.
- (g) Die Firewall muss wirksam die eigene Netzwerkstruktur verbergen. Nur nötige, öffentliche IP-Adressen sollen nach aussen (Internet) sichtbar sein
- (h) Funktioniert die Firewall aufgrund von Hardware- oder Software-Problemen nicht oder nicht einwandfrei, muss der Zugang zum Internet unterbrochen werden können. Nur so kann die Sicherheit aufrecht erhalten werden.
- (i) Im Fall eines Ausfalls des Systems oder wichtiger Komponenten davon, muss Ersatz-Material verfügbar sein, und das System muss mittels Backup/Restore-Funktion innert nützlicher Frist wiederhergestellt werden können.

0.8.3 Details zu den Anforderungen an Ressourcen-Filterung (RF)

Die RF muss folgende Bestimmungen erfüllen, wenn sie wirksam und effizient sein soll:

- (a) Die Schule definiert selber oder auf Empfehlung des Kantons, welche Kategorien unerwünschten Inhalts (Pornographie, Gewaltdarstellungen, etc.) sie blockieren will.
- (b) Entweder verfügt die RF über einen leistungsfähigen Service, der laufend die Kategorisierung von Web-sites aktualisiert und mit der RF synchronisiert (URL-Filtering) oder es wird ein Inhaltsüberprüfungssystem (Content-Screening-System) eingesetzt, welches vermög den Inhalt zur Laufzeit zu scannen.
- (c) Wird URL-Filtering (Ressourcenfilterung) eingesetzt, so muss die zugrundeliegende Datenbank regelmässig aktualisiert werden.
- (d) Wird ein Scanning zur Laufzeit eingesetzt (Inhaltsüberprüfung), muss insbesondere auf eine genügende Performanz-Reserve geachtet werden.
- (e) Anfragen via URL und via IP-Adressen müssen gleichermassen geprüft und allenfalls abgewiesen werden können.