Sicherheit und Nutzung

Jugendschutz

Der Schutz von Kindern und Jugendlichen in der Nutzung digitaler Lernmittel, digitaler Lernumgebungen und des Internets muss auf verschiedenen Ebenen erfolgen. Grundlage dafür liefern das Jugendschutzgesetz und der Jugendmedienschutz-Staatsvertrag. In diesen ist geregelt, unter welchen Bedingungen bestimmte Inhalte für Kinder und Jugendliche zugänglich gemacht werden dürfen. Neben den rechtlichen Aspekten für den Kinder- und Jugendschutz müssen die technischen Rahmenbedingungen so eingerichtet sein, dass diese vollständig umgesetzt werden können.

Die Umsetzung eines wirksamen Schutzes von Kindern und Jugendlichen muss einerseits deren Nutzungsverhalten betrachten und andererseits die möglichen Risiken, mit denen diese konfrontiert werden können. Deshalb wird eine alleinige technische Sicherung kaum möglich sein. Ebenso wichtig ist, die Kinder und Jugendlichen in ihrer Medien- und Internetnutzung zu sensibilisieren, ihre Kompetenzen in der kritischen Reflektion und des Selbstschutzes zu stärken.

Aus heutiger Sicht sollte die technische Sicherung von Internetzugängen so aufgesetzt sein:

- Schulserver (Schul-UTM-System) mit aktiver Content Filterung
- Inklusive Campuslizenz ISCA-Inhaltsfilter
- Firewall: Authentifizierung auf Nutzer- und Gruppenebene (Rollenkonzept)
- Kompletter Schutz angeschlossener lokaler Netze
- Virenscan und Angriffserkennung
- inklusive Umsetzung von Datenschutzrichtlinien
- Verschlüsselung des Datenverkehrs

„Wirkung entfalten und verlässlich schützen können technische Schutzlösungen nur dann, wenn sie bei den beliebten Diensten und gängigen Geräten ansetzen und sämtliche Risiken berücksichtigen, die sich aus der Interaktion ergeben.“[1]

Firewall

Eine physische oder virtuelle Firewall ist so konfiguriert, dass sie einerseits den Server und das schulische Netzwerk vor Angriffen von außen schützt. Darüber hinaus ist sie ein wichtiger Teilaspekt im schulischen Sicherheitskonzept. Die Firewall regelt die Zugriffe auf Datenbereiche und Funktionalitäten innerhalb des schulischen Netzwerkes und schützt die Zugriffe ins Internet durch geeignete Filter, entsprechend eines schulischen Rollenkonzeptes. Dadurch kann der Kinder- und Jugendschutz sichergestellt werden. Zudem schützt die Firewall vor unberechtigten Zugriffen über das Internet von außen.

[1] Bootz, Marx: Bericht Technischer Jugendmedienschutz, jugendschutz.net, Mainz 2019; S.19, https://www.jugendschutz.net/fileadmin/download/pdf/Bericht_ 2019_Technischer_Jugendmedienschutz.pdf

Filtertechniken

Diese Systeme müssen die Herausforderung meistern, dass sie alle Interaktionsrisiken kennen, die verschlüsselten Übertragungen sichern, aber auch vor unangemessenen Inhalten schützen.

Es wurden verschiedenen Techniken entwickelt, um gefährdende Inhalte von angemessenen Inhalten zu unterscheiden. Gerade junge Menschen sind noch nicht in der Lage, Unterscheidungen zu treffen und reagieren besonders im Internet mit Neugier und Grundvertrauen. Dieser Naivität kann mit einer ständigen Aufklärung über schädigende Inhalte, An- und Übergriffe begegnet werden. Doch bereits durch die Nutzung der möglichen technischen Mittel soll ein ausreichender Jugendschutz geboten sein.

Diese Filtertechniken können Teil eines umfassenden Sicherheitskonzeptes sein. Und so funktionieren sie:

Altersklassifizierung

Anbieter von Webseiten und Social Media hinterlegen ihren Inhalten ein Altersstufenlabel. Beim Aufruf der Website wird dieses Label gelesen und die Filtersoftware entscheidet, ob der Inhalt angezeigt wird. Das Label „age-de“ wird nur in Deutschland genutzt und ist leider nicht weit verbreitet.

Black-/Whitelists

Diese listenbasierte Filterung wird z. B. über die Bundesprüfstelle für jugendgefährdende Inhalte erstellt und gepflegt. Der Liste sind indizierte URLs hinterlegt. Das ist die Blacklist. Die Whitelist listet insbesondere für jüngere Kinder geeignete Inhalte auf. Hier können die Filterprogramme nur Seiten dieser Liste anzeigen.

Hash-Werte

Hash-Verfahren erkennen Dateien eindeutig wieder (auch Fotos und Videos). Dazu wird ein Wert aus der Datei errechnet, der wie ein Fingerabdruck einmalig ist. Die Hash-Werte werden ebenso in einer Liste geführt.

„Ein zukunftsfähiges Schutzkonzept muss Kinder und Jugendliche schützen und ihnen gleichzeitig eine unbeschwerte digitale Teilhabe ermöglichen.“
(Quelle: ebenda, S.24)

Keywords

Keywords sind eine Anwendung aus dem Bereich der Mustererkennung. Diese textbasierte Katalogisierung von Webseitentexten kann ungeeignete und schädliche Inhalte in Texten indizieren und in eine Blacklist füllen. Das Verfahren ist nicht fehlerfrei, da auch Seiten, die sich mit indizierten Themen aufklärend auseinandersetzen, als schädlich erkannt werden.

Künstliche Intelligenz

Die Zukunft wird in den Verfahren liegen, die das maschinelle Lernen zur Analyse von Lernverhalten und -erfolgen einsetzen. Hier werden Algorithmen darauf trainiert, Texteingaben und Interaktionen zu analysieren. Die Trefferquote liegt sehr hoch, wenn die Trainingsmaterialien und der verknüpfte Lernalgorithmus optimal zusammenspielen.

Verschlüsselung

Eine Verschlüsselung „verpackt“ die im Internet zu übertragenden Daten in einer Form, die nur von den bekannten Systemen entschlüsselt werden können. Damit werden keine Klardaten übertragen, die von Dritten „mitgelesen“ werden könnten. Damit können die Daten von Teilnehmenden, die aus dem schulischen Netzwerk ins Internet kommunizieren, geschützt werden.

Medienkompetenzen

„Ein zukunftsfähiges Schutzkonzept muss Kinder und Jugendliche schützen und ihnen gleichzeitig eine unbeschwerte digitale Teilhabe ermöglichen.“ [2]

Deshalb muss ein wirksamer Schutz von Kindern und Jugendlichen auch darauf aufbauen, diese entsprechend ihres Alters für die Gefahren im Internet zu sensibilisieren und sie zu stärken. Dazu sollten sie geeignete Handlungsmethoden erlernen, um in geeigneter Weise mögliche Gefahren zu erkennen und sich zu schützen.

Die Bundesländer haben diese Medienkompetenzentwicklung in ihren Rahmenlehrplänen aufgenommen. Dennoch sind weiterhin verschiedene Gefährdungen im Internet festzustellen.

[2] https://www.vielfalt-mediathek.de/wp-content/uploads/2021/08/Hass-im-Netz_Technischer-Jugendmedienschutz.pdf, S.25

Risiken und Gefahren im Internet und in Messenger-Diensten

Phishing

Über Instant Messenger, Mail und in Chatrooms wird versucht, persönliche Daten über den Wohnort, Lebensverhältnisse etc. zu erhalten. Das können kriminelle Personen sein, die sich über lohnende Ziele für Einbrüche informieren wollen. In anderen Situationen (Gewinnspiele, Preisversprechen) werden geschickt Abonnementabschlüsse getarnt. Man kann das durch die Art der Informationen, die abgefragt werden, erkennen.

Cybermobbing

Als Cybermobbing bezeichnet man das Phänomen, dass Chatgruppen oder Einzelnen über Andere lästern und diese diffamieren.

Hier wird absichtlich und vorsätzlich über einen längeren Zeitraum schikaniert. Die ausführenden Personen machen sich dabei die Anonymität des Internets zu Nutze und haben die persönliche Schädigung der Zielperson zum Ziel.

Bloßstellung

Durch einen unbedachten Upload, Teilen von z. B. einem vermeintlich lustigen Fotoschnappschuss oder Video kann eine Person bloßgestellt werden. Für die bloßgestellte Person kann der Schaden immens sein. Die Bloßstellung kann eine einmalige Aktion sein, im Internet ist diese aber nur schwer dauerhaft zu löschen.

Ausgrenzung

In Gruppen von Messenger-Diensten können Einzelpersonen ausgegrenzt werden. Die Ursachen können vielfältig sein. Oft steht ein Vorsatz dahinter.

Cyber-Grooming

In Chatrooms versuchen erwachsene Personen, sich das Vertrauen von Kindern und Jugendlichen zu erschleichen. Sie geben alles vor, um interessant zu wirken und ein vertrauensvolles Verhältnis aufzubauen. Ist dies gelungen, kehrt sich die Machtdynamik allerdings um: Das Vertrauen wird zu Straftaten wie etwa der Anfertigung kinderpornografischer Aufnahmen oder sexuellen Missbrauches missbraucht. Neben sexuellen Handlungen können Aufforderungen zu meist spielerisch angelegten „Mutprobe“-Challenges mit selbstzerstörerischen Aktivitäten bis hin zum verlangten Suizid folgen. Meist wird den Jugendlichen hierbei als Lohn für bestandene Challenges die Anerkennung des Cyber-Groomers und ein höherer „Coolness“-Faktor in Aussicht gestellt, was gerade für labile Jugendliche oder solche mit geringem Selbstwertgefühl attraktiv erscheinen kann.

Dieser meist niedrigschwellig beginnende und dann immer stärker eskalierende Prozess kann lange anhalten und ist schwer zu entdecken.

Sexuelle Belästigung/Missbrauch

Auch diese werden über Chatrooms oder direktes Anschreiben (die Kontaktdaten können von Freunden stammen, denen diese entlockt wurden) initiiert. Es werden direkte sexuelle Avancen gemacht, meist mit Versprechungen oder Belohnungen.

Sexting

Meint die anzügliche Kommunikation über sexuelle Themen. Ebenso ist das Versenden erotischer Bildaufnahmen des eigenen Körpers per Smartphone oder Internet gemeint. Oft durch die Betroffenen zunächst als harmloser und erregender Flirt wahrgenommen und begrüßt, liegt die Gefahr in der unkritischen Nutzung, die zur missbräuchlichen Weiterverbreitung der so erlangten intimsten Fotos. Diese Fotos sind im Internet nur schwer dauerhaft zu löschen und meist für einen großen Betrachterkreis aus allen Teilen des Lebens (alle Freunde und das soziale Umfeld, die ganze Schule, der Sportverein, etc.) sichtbar.

Hate Speech

„Hassrede“ meint als Oberbegriff alle Formen von pauschal gruppenbezogener Menschenfeindlichkeit und Diskriminierung im Netz und in sozialen Netzwerken. Ziel der Täter (Hater) ist es, ihren vermeintlichen Hass auszudrücken, in der Gesellschaft zu verbreiten sowie diese Gruppen oder einzelne Personen gezielt öffentlich abzuwerten oder auszugrenzen. Hate Speech ist somit von der allgemeinen Meinungsfreiheit abzugrenzen – und hat Folgen für die Opfer (psychosozial) wie auch für die Täter (Löschung der Posts/ ggf. strafrechtliche Verfolgung).

Cyber-Crime

Für den Begriff existiert keine allgemein gültige Definition. „Üblicherweise versteht man darunter alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik (IKT) oder gegen diese begangen werden.“[2] Der Jugendschutz beginnt hier mit der Sicherung der IKT gegen mögliche Angriffe, die Jugendliche aus Neugier und spielerischem Drang gegen die schulischen Einrichtungen richten könnten.

Kinder und Jugendliche müssen sich in den Softwarediensten, die eine digitale Schule für sie bereithält, sicher bewegen können. Sie müssen befähigt werden, Gefahren zu erkennen, lernen welche Reaktionen angemessen sind und wissen, dass sie bedingungslos angehört werden.

[2] https://bundeskriminalamt.at/306/