Gefahrenzone

Risiken im Internet für Kinder und Jugendliche

Kinder und Jugendliche surfen nicht nur am heimischen PC. Viele mobile Geräte haben heute einen WLAN-Zugang und einen eingebauten Browser. Die Eltern haben kaum noch Kontrolle darüber, wann und wie ihre Kinder ins Internet gehen. Das kann böse Folgen haben.

Katja S. fiel aus allen Wolken, als sie Post bekam. Eine Anwaltskanzlei mahnte sie wegen eines Urheberrechtsverstoßes ab und garnierte das Schreiben mit einer deftigen Kostennote. Schlucken musste die Mutter von zwei Söhnen im Alter von 14 und 16 Jahren ob der Titelliste der zum Download angebotenen Werke – ganz offenbar handelte es sich um Pornografie. Der Haussegen im Hause S. hängt nun gründlich schief, auch weil bislang keiner der beiden zur Rede gestellten Söhne zugeben wollte, die Filme über eine Tauschbörse heruntergeladen zu haben. Einen Partner, der wohl auch unter Verdacht geraten wäre, hat Katja S. derzeit nicht. Möglicherweise hat aber auch einer der Nachbarn das nur mit WEP gesicherte WLAN gehackt und darüber die Filme gezogen – rekonstruieren lässt sich das nicht, S. bleibt auf dem Schaden sitzen.

Jugendliche sitzen häufig dem Irrglauben auf, Herunterladen sei vollkommen legal. Doch Tauschbörsen-Software wie Bittorrent oder eDonkey bietet schon während des Downloads Fragmente der heruntergeladenen Dateien im Upload an – das ist auf jeden Fall verboten, wenn es um geschützte Inhalte geht. Wenn Kinder und Jugendliche unbedingt Lieder für ihren MP3-Player kopieren möchten, sollte man sie auf Mitschnitte von Internetradios verweisen, dazu kann man Programme wie Streamripper, Phonostar Player oder radio.fx einsetzen. Die Tonspur aus YouTube-Videos extrahiert der Webdienst „YouTube mp3“.

Bei der Nutzung von Tauschbörsen ins Visier von Abmahnanwälten der Film- und Musikindustrie zu geraten ist längst nicht das einzige, was Kindern und Jugendlichen bei der Internet-Nutzung zustoßen kann. Die Blümchenwiese kindgerechter Internet-Angebote liegt nur ein paar Mausklicks von Hasspropaganda, harter Pornografie, Happy-Slapping-Videos und Splatter-Filmen entfernt. Tipps, wie man Kinder und Jugendliche auf diese Gefahren vorbereitet, damit sie mit den neuen Medien souverän umgehen, lesen Sie ab **S. 126 in c't 21/11[1]**.

Auch auf mobilen Geräten gibt es erste Web-Inhaltsfilter, die jugendgefährdende Seiten aussperren.

Besondere Sorgen bereiten Eltern die Möglichkeiten anonymen Mobbings. Mit pseudonymen Accounts und in der scheinbar irrealen Parallelwelt sozialer Netzwerke gewinnen Mobbing-Attacken möglicherweise erheblich an Schärfe im Vergleich zu denen im realen Leben.

Der Urheber einer Cyber-Mobbing-Attacke lässt sich nur dingfest machen, sofern einige Voraussetzungen erfüllt sind. Über den Weg einer Strafanzeige bei der Polizei lässt sich die Identität des Täters ermitteln, wenn sich feststellen lässt, von welcher IP-Adresse aus die Inhalte ins Netz gestellt wurden und anschließend die Zuordnung der Adresse zu einem Anschlussinhaber erfolgreich ist. Zwar ist die Vorratsdatenspeicherung unzulässig, die Provider

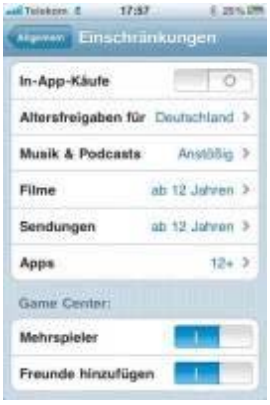
speichern aber dennoch die Daten eine ganze Weile für Abrechnungszwecke.

Besonders verheerend ist es, wenn Videos die Runde machen, die für den Betroffenen peinlich sind. Der wohl bekannteste Fall ereignete sich vor fast zehn Jahren. Ein kanadischer Schüler nahm sich selbst auf Video auf, als er einen Lichtschwert-Kämpfer aus einem der Star-Wars-Filme imitierte. Das übergewichtige Kind wirkte dabei in seiner Unbeholfenheit unfreiwillig komisch. Ein Mitschüler fand das Band einige Monate später und stellte es ins Internet. Der Schüler wurde als „Star Wars Kid“ weltbekannt und gleichzeitig Opfer übelster Schmähungen.

Mit Filtersoftware lässt sich sehr fein einstellen, welche Seiten Kinder zu sehen bekommen sollen.

Dabei können Aufnahmen für die Abgebildeten noch viel unangenehmer sein als die unbeholfenen Tanzschritte des Star Wars Kid. Einige Jugendliche haben Spaß daran, sich dem Partner per E-Mail und MMS leicht oder gar nicht bekleidet zu präsentieren, es gibt dafür sogar einen eigenen Begriff, das „Sexting“. Für sich genommen ist das harmlos. Eine Katastrophe wird daraus erst, wenn diese Bilder im Internet landen und Freunden und Bekannte dort über sie stolpern. In Umlauf kommen solche Bilder meist nach einem Streit oder wenn Speichermedien oder Zugangsdaten für Medienserver in falsche Hände geraten, etwa weil man das Handy mit den Filmen und Fotos darauf verliert oder es gestohlen wird. Auch in solchen Fällen ist der Verbreiter häufig nur schwer auszumachen.

Anzügliche Bilder können jedoch auch heimlich entstehen. Früher bohrten Spanner Löcher durch Sperrholzwände und linsten in die Mädchen-Umkleide. Heute verschaffen sie sich per Schadsoftware Zugriff auf die Webcam des PCs im Kinderzimmer und beobachten im Schutze der Anonymität, was dort vor sich geht. Solche Schadprogramme können mit jeder Installation von Software, auch als Dateianhänge an E-Mails, oder sogar beim bloßen Öffnen einer Webseite auf den PC gelangen. Bei gezielten Attacken bekommen die Opfer die Links zur Installation der Schadsoftware beispielsweise in einem Online-Chat präsentiert.



Im iPhone lassen sich grundlegende Jugendschutzeinstellunge vornehmen. Um diese zu umgehen, muss man einen PIN-Code eingeben.

Virenscanner sollten auf Kinder-PC aktiv **[1][2]** sein, Updates zeitnah, am besten automatisch installiert werden. Ein eingeschränkter Benutzer-Account für die jüngeren Nutzer hilft dabei, die Kontrolle über installierte Programme zu behalten, verhindert aber nicht, dass Schadsoftware den Weg auf den Rechner findet. Streamt die Webcam ungewollt Bilder ins Internet, lässt sich das über den Ressourcenmonitor von Windows feststellen. Dort sollte man prüfen, ob ein kontinuierlicher und lang anhaltender Datenstrom unklarer Herkunft im Upstream auftaucht und welche TCP-Verbindungen für den Versand dieser Daten verantwortlich sind. Erhärtet eine Prüfung den Verdacht, dass jemand die Webcam fernsteuert, sollte man umgehend die Polizei informieren. Solange eine Datenverbindung besteht, ist es für die Polizei in vielen Fällen möglich, den Täter dingfest zu machen. Sicherheitshalber schließt man die Webcam nur an, wenn man sie benötigt. Wenn sie beispielsweise in einem Notebook fest eingebaut ist, kann man sie bei Nichtgebrauch abdecken. Das eingebaute Mikrofon lässt sich jedoch nicht so einfach deaktivieren. Ist der Rechner heruntergefahren, stellt aber auch eine Wanzen-Software ihren Betrieb ein.

Soziale Netzwerke

Kinder können bei der Nutzung von sozialen Netzwerken noch schlechter als ihre Eltern einschätzen, welche Daten schutzwürdig sind und welche nicht. Partyeinladungen auf Facebook etwa können durch ein falsch gesetztes Häkchen direkt in die Katastrophe führen. Nicht immer kommt der Polizeischutz dann rechtzeitig so wie im Fall Thessa, deren Party in einem Hamburger Vorort 1500 Teenager stürmen wollten. In ihrem Fall hatten Boulevardmedien durch eine identifizierende Berichterstattung für einen größeren Zulauf gesorgt, sodass sich die Polizei zum Eingreifen veranlasst sah. Die Schwelle, bei der Probleme

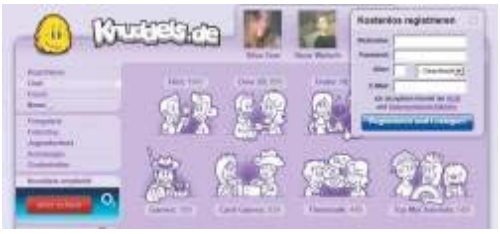
anfangen, liegt viel niedriger: Schon ein oder zwei Dutzend ungeladene Gäste können zum Alptraum werden, insbesondere wenn Jugendliche alleine zu Hause sind und nicht wissen, wie sie das Hausrecht durchsetzen sollen.

Die persönlichen Daten von Kindern sind ganz besonders schutzwürdig. Eine kleine Nachlässigkeit bereitete Markus D., seinen Eltern und Vereinskollegen viele schlaflose Nächte. Der 12-Jährige spielt in einem Fußballverein. Einer der erwachsenen Betreuer brachte die Kinder auf die Idee, sie sollten sich bei Facebook anmelden. In einer für alle Facebook-Nutzer einsehbaren Gruppe verabredeten sie sich zu Trainingsterminen und veröffentlichten Fotos vom Trainingsplatz. Mit den Einstellungen für die Privatsphäre setzten sie sich nicht weiter auseinander.

Der Jugendschutz von Windows 7 wertet die USK-Angaben installierter Spiele aus, um sicherzustellen, dass nur für die jeweilige Altersgruppe des Nutzers geeignete Spiele ausgeführt werden können.

Auf Markus' Facebook-Konto gingen nach kurzer Zeit Nachrichten eines angeblich gleichaltrigen Jungen ein, zunächst harmlose Erkundigungen nach dem Verlauf des Trainings oder Terminen. Dann aber wurden die Nachrichten immer anzüglicher. Der Junge wusste zunächst nicht, was er damit anfangen sollte. Als der Unbekannte dann schließlich auf seinem Handy anrief – die Daten standen ebenfalls auf Facebook – und ihn fragte, ob denn der eine oder andere der Jungen schon Schamhaare habe, schrillten bei seinen Eltern die Alarmglocken. Auch zwei Wochen nach dem Vorfall stehen die Fotos einiger Kinder der Gruppe noch im Netz; viele Eltern haben die Facebook-Accounts ihrer Kinder aber schleunigst gelöscht. Für sein Handy hat Markus nun eine neue Rufnummer, zum Training begleiten ihn stets Vater oder Mutter. Die Angst vor dem unbekannten potenziellen Sexualstraftäter sitzt tief.

Wenn Kinder schon soziale Netzwerke nutzen sollen, muss man sich mit den Privacy-Einstellungen sehr grundlegend auseinandersetzen. Auf keinen Fall dürfen persönliche Daten wie die Anschrift für Fremde sichtbar sein, das kann für Kinder sehr gefährlich werden. Diesen Kreis sollten Kinder nur um Personen erweitern, die sie auch in der realen Welt kennen. Eine Anleitung für Facebook finden Sie im c't-Link.



Bei einem Chat-System wie Knuddels.de kann man sich quasi anonym registrieren.

Abzocke per Telefonrechnung

Eine Gefahr für den Geldbeutel lauert in Online-Communitys und -Spielen, die zwar grundsätzlich gratis nutzbar sind, bei denen aber Gegenstände in der virtuellen Welt auch gegen echtes Geld erworben werden können, etwa im sozialen Netzwerk Habbohotel oder im Online-Rollenspiel Metin 2. Solche virtuellen Güter üben auf Kinder oft eine geradezu magische Anziehung aus. Wenn das Taschengeld nicht reicht, können sich Kinder und Jugendliche an der Telefonrechnung der Eltern bedienen, indem sie Mehrwertdienste anwählen und damit Zahlungen auslösen oder den Betrag über die Handyrechnung abbuchen lassen. Und genau darauf setzen die Betreiber und bieten das als komfortable Zahlungsmethode an. Bei wiederholter Anwahl fallen schnell zwei- oder gar dreistellige Beträge an. Eltern sollten zur Vorbeugung 0900-, 0137- und 0180-Rufnummern an Festnetztelefonen sperren, ebenso alle Mehrwertdienste bei Mobilfunkverträgen, auf die Kinder Zugriff haben.

Besonders hinterlistig sind sogenannte Abo-Fallen **[2][3]** . Deren Betreiber spiegeln dem Kunden ein kostenloses Angebot vor und veranlassen ihn, seine persönlichen Daten zu hinterlassen. Irgendwo im Kleingedruckten auf der Seite geben sie gut getarnt einen Preis für die Dienstleistung an, die in aller Regel andernorts in besserer Qualität und obendrein kostenlos erhältlich ist.

Die so gewonnenen Daten nutzen sie, um dem Kunden eine Rechung zuzuschicken. Häufig sind das 96

Euro pro Jahr bei einer Laufzeit von zwei Jahren. Mit Briefen in rüdem Ton und ständig eskalierenden Drohungen drängen sie den Kunden zur Zahlung, auf die sie in der Regel aber keinen Anspruch haben. Um zu verhindern, dass Kinder in solche Abo-Fallen gehen, sollte man sie dazu anhalten, keinesfalls persönliche Daten wie Name, Geburtsdatum, Anschrift und E-Mail-Adresse in Web-Formularen zu offenbaren. Das schützt nicht nur vor Abo-Abzocke, sondern auch vor Nachstellungen durch Unbekannte. Bei Bedarf sollte man dem Nachwuchs zeigen, wie sich Wegwerf-Email-Adressen mit wenigen Handgriffen einrichten lassen, beispielsweise bei Spamgourmet.

Sobald für einen Download persönliche Daten abgefragt werden, sollte man genau schauen, wo sich der Pferdefuß versteckt. Hier treibt jemand mit dem guten Namen von OpenOffice Schindluder.

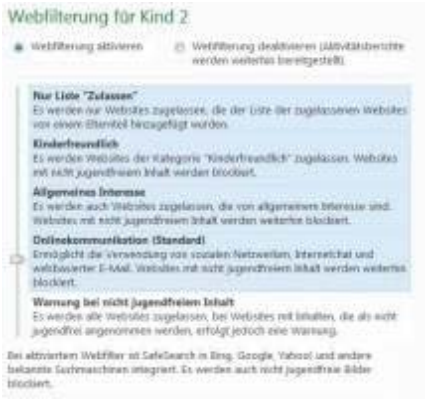
Noch gemeiner sind Abo-Fallen auf Werbebannern in Smartphone-Applikationen **[3][4]** . Hier reicht manchmal ein einziger falscher Fingertipp, um ein kostenpflichtiges Abonnement abzuschließen. Die Daten des Kunden benötigen die Anbieter nicht, sie haben direkten Durchgriff auf die Rechnungen. Reklamationen geprellter Kunden bearbeiten die Mobilfunkanbieter oft nur widerwillig.

Virtuelles Kindermädchen

Bisher konzentrierten sich Eltern und Sicherheitsindustrie auf technische Lösungen, den Internetzugang auf von Kindern genutzten PCs unter Kontrolle zu bringen **[4][5]** . Für kleinere Kinder eignet sich dafür eine Whitelist-Lösung wie FragFinn, die nur geprüfte und von einem Redaktionsteam oder den Eltern freigegebene Seiten zugänglich macht. Die Linksammlungen sind allerdings nicht allzu umfangreich, denn jede Freigabe will zuvor sorgfältig geprüft sein. Halten Eltern Seiten für unbedenklich, die nicht in der Whitelist enthalten sind, müssen sie jede einzelne manuell freigeben. Im besten Falll geschieht das direkt im Browser über die Eingabe eines Passworts.

Für ältere Kinder, die auch mal auf eigene Faust nach Aufklärungsbroschüren oder Material für Referate suchen müssen, eignet sich eine Blacklist-Lösung, die genau umgekehrt arbeitet, über eine Liste inkriminierter Inhalte den gröbsten Schmutz ausfiltert und bekannte Gewalt-, Hass- und Pornoseiten sperrt. Der Schutz von Blacklists ist nicht allzu zuverlässig; probiert das Kind Dutzende von Seiten durch, wird es früher oder später auf eine stoßen, die der Filter durchlässt, weil sie noch nicht erfasst ist.

Wenn der Computer unter Windows 7 läuft, ist eine Kinderschutzlösung bereits vorinstalliert und muss unter dem Menüpunkt „Jugendschutz“ in der Systemsteuerung nur noch für die jeweiligen Benutzer aktiviert und konfiguriert werden. Damit lassen sich Zeitlimits einrichten und die Ausführung nicht von den Eltern autorisierter Programme sperren. Einen umfangreichen und qualitativ hochwertigen Inhaltsfilter für den Internet-Zugang, der sich von jedem beliebigen Internet-PC aus verwalten lässt, bietet Microsoft unter „Family Safety“ zum Download an. Weitergehende Funktionen bieten Programme wie die Kindersicherung von Salfeld, die eine deutlich flexiblere Zeitverwaltung bietet und bei Bedarf Nutzungsprotokolle erstellt.



Der Webfilter von Microsoft Family Safety lässt sich bei Bedarf aus der Ferne konfigurieren. So können die Eltern auch vom Büro aus Freigaben für bestimmte Seiten erteilen.

Das funktioniert aber nur solange die Kinder das Internet ausschließlich über den heimischen PC nutzen. In neueren AVM-Routern kann man für den Internet-Zugang eine Zeitbeschränkung vorsehen. Das verhindert, dass die Kinder mit mobilen WLAN-Geräten nachts unter der Bettdecke surfen. Im WLAN von Freunden oder in den Mobilnetzen greift die Sperre nicht mehr. Datentarife für den Mobilfunk gibt es inzwischen bei allen Providern zum Taschengeldpreis, teilweise auch ohne Prüfung des Geburtsdatums. Vielen Eltern ist gar

nicht klar, dass man mit einigen marktüblichen MP3-Playern ins Internet gehen kann. Immer mehr Geräte, die für den Anschluss eines Displays vorgesehen sind oder selbst ein Display haben, sind auch mit einem Web-Browser ausgestattet, etwa TV-Geräte, Blu-ray-Player oder Spielekonsolen, inzwischen bereits Handys der untersten Preisklasse. Kinder loten sehr schnell aus, was die Geräte alles können und entdecken Funktionen an Geräten der Unterhaltungselektronik, die den Eltern nicht bekannt sind. Damit verlieren Eltern vollständig die Kontrolle darüber, wann und wo die Kinder ins Internet gehen und was sie dort zu sehen bekommen. Und wenn es keinen WLAN-Zugang gibt, bringt eben ein Freund ein Smartphone mit und konfiguriert das Gerät als mobilen Hotspot.

Eine gewisse Zeit lang kann man jüngere Kinder von solchen Geräten noch fernhalten, doch mit zunehmendem Alter lässt sich die Anschaffung irgendwann nicht mehr hinauszögern, ohne die tatsächliche oder vermeintliche soziale Isolation des Sprösslings zu befördern. Immerhin bieten solche Geräte immer häufiger die Möglichkeit, bestimmte Funktionen durch ein Passwort zu schützen oder permanent und kindersicher abzuschalten.

Bei iOS-Geräten etwa lassen sich mit wenigen Klicks diverse Betriebssystemfunktionen – darunter Ortungsdienste, Installation und Löschen von Apps, iTunes, Änderungen an Mail-Accounts und In-App-Käufe – verbieten. Apps lassen sich gestaffelt nach den im iStore angegebenen Altersfreigaben sperren. Bei Browsern ist Apple sehr restriktiv; die Altersfreigabe liegt in der Regel bei 17 Jahren. Wer sein Kind dennoch auf iPhone, iPad und Co. surfen lassen will, muss eine kindersichere Browser-Lösung wie die kostenlose K9 Web Protection installieren.

Android bietet von Haus aus keine Kinderschutzfunktionen. Für diesen Zweck gibt es allerdings mehrere Apps, etwa Android Parental Control, Smart App Protector und KidsProof Launcher. Im Ersteren vergeben die Eltern einen Zugangscode. Anschließend können sie entweder eine Whitelist mit Programmen vorgeben, die das Kind ohne Zugangscode öffnen darf, oder sie sperren einzelne Programme.

Darüber hinausgehende Funktionen, wie es sie etwa für PCs gibt – etwa an bestimmte Zeiten gebundene Sperren oder Zeitkontingente –, bietet Android Parental Control nicht. Einen rudimentären Zeitplan bietet dagegen der Smart App Protector. Dort können die für alle zugriffsgeschützten Apps eine Aktivierungszeit festlegen. So lässt sich der Browser etwa für die Schul- und Nachtzeit sperren. KidsProof Launcher funktionierte in unseren Versuchen nicht zuverlässig und stürzte des Öfteren ab.

Für andere Geräte mit Internetzugang, etwa Spielkonsolen oder MP3-Player, gibt es häufig zwar einen pauschalen Zugangsschutz, aber keine darüber hinausgehende Kinderschutzfunktionen. Den Zugriff auf das Internet kann man nur zu Hause mit einer Filterlösung auf dem Router kontrollieren. Deshalb ist es unter Umständen besser, dem Kind ein passend konfiguriertes Smartphone in die Hand zu drücken statt einzelner Geräte, deren Funktionsumfang sich nicht einschränken lässt. Mit fortschreitendem Alter des Kindes kann man dann die Funktionen nach und nach freigeben, sofern das Gerät in Kinderhänden überhaupt so lange überlebt.

Laufen lernen

Eltern, die wenig Ahnung vom Internet haben, müssen zwangsläufig Angst vor der Technik bekommen. Angst ist aber ein schlechter Ratgeber, eine gesunde Skepsis und eine möglichst neutrale Einschätzung der Lage ist besser. Auch im wirklichen Leben muss man den Kindern beibringen, nicht auf die Straße zu laufen, keine Süßigkeiten von Fremden anzunehmen und ihre Freunde nicht zu mobben.

Kinder kann man vom Internet auf Dauer genauso wenig fernhalten wie vom öffentlichen Raum. Eine geschützte Zone auf Papas PC mit Whitelist-Filter mag für die ersten Gehversuche noch interessant sein, spätestens nach ein oder zwei Jahren werden die Kinder aber gezielt nach Löchern im Zaun suchen und die auch finden. Wenn sie zu diesem Zeitpunkt bereits wissen, welche Gefahren drohen, können sie diesen besser begegnen, als wenn man ihnen diese verschwiegen hat.

Die Probleme mit der neuen Technik lassen sich nicht durch den Einsatz von noch mehr Technik lösen,

sondern nur ein wenig mildern. Der Schlüssel zur Lösung liegt in der Kommunikation zwischen Eltern und Kindern; mehr dazu lesen Sie im Artikel auf den folgenden Seiten. (uma)

Literatur

[1] Gerald Himmelein, Schutzschirme für Windows, Die 2012er-Generation der Virenscanner, **c't 20/11, S. 112 [6]**

[2] Holger Bleich, Angelockt und abkassiert, Der Nepp mit Abo-Fallen im Netz floriert, **c't 11/09, S. 90 [7]**

[3] Holger Bleich, Inkasso auf Fingertipp, Tückische Abofallen in iPhone- und Android-Apps, **c't 22/10, S. 36 [8]**

[4] Urs Mansmann, Schmutzsieb, Webfilter für Kinder-PCs unter Windows, **c't 22/10, S. 138 [9]**

www.ct.de/1121122[10]

Kinder im Internet

Artikel zum Thema "Kinder im Internet" finden Sie in c't 21/2011:

Risiken im Internet für Kinder - **Seite 122[11]**
Medienerziehung mit Verständnis und Augenmaß - **Seite 126[12]**

URL dieses Artikels:
http://www.heise.de/ct/artikel/Gefahrenzone-1353628.html

Links in diesem Artikel:
[1] http://www.heise.de/artikel/archiv/ct/11/21/126/
[2] #lit
[3] #lit
[4] #lit
[5] #lit
[6] http://www.heise.de/artikel/archiv/ct/11/20/112/
[7] http://www.heise.de/artikel/archiv/ct/09/11/090/
[8] http://www.heise.de/artikel/archiv/ct/10/22/036/
[9] http://www.heise.de/artikel/archiv/ct/10/22/138/
[10] http://www.ct.de/1121122
[11] http://www.heise.de/artikel/archiv/ct/11/21/122/
[12] http://www.heise.de/artikel/archiv/ct/11/21/126/