Blaue Reihe

5

ULD

Internet: Alltag online

Surfen, Chatten, E-Mails und Soziale Netze
Was muss ich wissen?

Inhaltsverzeichnis

Impressum:
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Holstenstraße 98, 24103 Kiel, www.datenschutzzentrum.de

Stand: Mai 2015

Vorwort

Das Internet hat sich in den letzten Jahren nicht zuletzt durch die Verbreitung von Smartphones und Tablets zu einem nicht mehr aus dem Privatleben wegzudenkenden Medium entwickelt.

Nicht nur die Erwachsenen, sondern in zunehmendem Maße auch Kinder und Jugendliche nutzen das Internet. Insbesondere für die letztgenannte Gruppe stellt das Internet nicht nur ein Informationsinstrument dar. Dieses Medium dient den Kindern und Jugendlichen zur Kommunikation (Chat, Instant Messaging), als Kontaktbörse (Soziale Netzwerke) und zum Austausch von Dateien.

Dabei ist vielen PC- und Internetnutzern nicht bekannt und oftmals auch nicht bewusst, dass sich hieraus auch Risiken für Ihre Privatsphäre, ihre Persönlichkeitsrechte und für ihre privaten Daten ergeben können.

Der Inhalt dieser Broschüre gibt einen ersten Überblick über diese Risiken und nennt Tipps, wie man diesen begegnen kann. Diese Tipps orientieren sich an den Anforderungen, die ein verantwortungsvoller Internetnutzer – egal ob erwachsen oder nicht – unbedingt beachten sollte.

Was erfährt eine Webseite denn beim Surfen über mich?

Beim Aufruf einer Webseite werden an den Webserver (das ist der Computer, auf dem die Seiten gespeichert sind) diverse Informationen gesendet. Neben der eigentlichen Anfrage nach einer bestimmten Seite sind dies vor allem technische Informationen über den eigenen Computer oder das eigene Smartphone sowie die Adresse, an die die Seite geschickt werden soll, die sog. Internetprotokoll- oder IP-Adresse. Jeder mit dem Internet verbundene Rechner muss solch eine weltweit eindeutige Adresse haben, damit er mit anderen Rechnern kommunizieren kann.

Die Betreiber einer besuchten Webseite können anhand der IP-Adressen, die auf ihren Servern gespeichert werden, zumindest erkennen, aus welchem Land und über welchen Provider der Kontakt erfolgte. Auch der Ballungsraum ist in der Regel ortbar. Genauere Daten, etwa die Anschrift oder gar der Name des Nutzers, kann der Webseiten-Betreiber jedoch nicht aus der IP-Adresse entnehmen, sofern es sich nicht um eine fest zugewiesene Adresse handelt (die eher Firmen etc. haben).

Der Betreiber einer Webseite kann aber – abhängig von den Einstellungen im Browser – diverse Zusatzinformationen über den Nutzer bekommen. So kann unter Umständen die zuvor besuchte Webseite ermittelt oder die Zugriffe auf einzelne Webseiten über Monate und Jahre hinweg protokolliert werden.

Der sog. Referrer teilt dem Ziel-Server beim Anklicken eines Links mit, von welcher Webseite der Besucher kommt. Klickt der Nutzer einen Ergebnislink einer Suchmaschine an, kann die Zielseite mit Hilfe des Referrers auch die Suchbegriffe sehen, die zuvor eingetippt wurden.

Neben der IP-Adresse und dem Referrer verrät der eigene PC jeder angesurften Webseite noch eine Reihe von technischen Statusinformationen. Diese geben Auskunft darüber, welche Inhalte der eigene Rechner verarbeiten kann, ob also bestimmte Videos angezeigt oder Programme verarbeitet werden können.

Zu den übertragenen Daten gehören unter anderem:

- Verwendeter Webbrowser (Versions-Nr.)
- Eingeschaltete Steuerelemente des Browsers (Java, JavaScript, ActiveX)
- Betriebssystem des PC (Versions-Nr.)

Unter dem folgenden Link können Sie sich ein Bild dieser technischen Informationen machen: http://www.browsercheck.pcwelt.de/

Welche Möglichkeiten Sie haben, Ihren Browser nach Ihren Bedürfnissen möglichst sicher einzustellen, zeigt Ihnen diese Seite https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/WegInsInternet/DerBrowser/derbrowser_node.html

Was bedeuten „Cookies" für meine Privatsphäre?

Neben den oben beschriebenen technischen Informationen gibt es weitere Mechanismen, die Informationen über den Internetnutzer liefern können. So ist es Webseiten möglich, auf dem PC des Nutzers Informationen zu speichern und bei einem späteren Besuch wieder abzurufen. Die so gespeicherten Informationen bezeichnet man als „Cookies". Das Verfahren ist wichtig und notwendig, um Nutzer zum Beispiel in einem Online-Shop für die Dauer des Einkaufs wiederzuerkennen. Normalerweise kann ein Server zwei verschiedene Aufrufe seiner Webseite nicht zweifelsfrei einem Computer zuweisen. Die

technischen Informationen, die er erhält, sind hierfür zu allgemein. Auch die IP-Adresse ist kein eindeutiges Unterscheidungsmerkmal, da sie nicht statisch einem einzigen Rechner zugewiesen ist. Um nun einen Nutzer über einen längeren Zeitraum wiederzuerkennen, kann ein Server eine Identifikationsnummer in einem Cookie ablegen und diese Nummer abfragen, wenn der Kunde sich durch den Shop klickt. So ist es möglich, dem Kunden stets seinen Warenkorb mit den dort abgelegten Produkten anzuzeigen.

Nach dem Einkauf ist der Cookie dann eigentlich überflüssig. Viele Webseiten speichern jedoch Cookies, die nicht nur für die aktuelle Sitzung gelten, sondern eine Lebensspanne von mehreren Tagen bis hin zu mehreren Jahren besitzen. Das bedeutet, dass ein Computer über Jahre hinweg von einer Webseite anhand der Identifikationsnummer stets als derselbe Computer wiedererkannt werden könnte. So können Besuche auf einer einzelnen Webseite miteinander verkettet und Nutzungsprofile erstellt werden. Im Falle von Google bedeutet dies beispielsweise, dass alle Besuche eines Nutzers auf allen Google-Seiten und Google-Diensten miteinander verknüpft werden können. Suchbegriffe können demselben Nutzer zugeordnet werden. Meldet sich dieser Nutzer irgendwann bei einem Google-Dienst an, sind alle bislang anonym zusammengeführten Informationen schlagartig einer Person zuzuordnen.

Darüber hinaus gibt es auch Werbefirmen, die mit Hilfe von Bannereinblendungen Cookies erzeugen, die seitenübergreifend funktionieren. Diese sog. Drittanbieter- oder Third-Party-Cookies haben keinen anderen Zweck als die Profilbildung. So dürfte jeder schon beobachtet haben, dass er plötzlich Werbung für ein Produkt eingeblendet bekommt, das er sich vorher (ggf. sogar Tage vorher) auf einer ganz anderen Seite angesehen hatte. Derartige Werbenetzwerke sind heute die Regel und ermöglichen,

das Surfverhalten eines Menschen über weite Teile des Internets hinweg zu beobachten.

Die einfachste Methode, sich vor derlei Aufzeichnungen zu schützen, ist die Deaktivierung von Langzeit-Cookies im Webbrowser. Das vollständige Abschalten von Cookies ist jedoch kaum zu empfehlen, da viele Seiten auf das vorübergehende Speichern angewiesen sind und dies auch sinnvoll ist. Stattdessen sollte der Browser so konfiguriert werden, dass Cookies grundsätzlich akzeptiert, beim Beenden des Browsers jedoch vollständig gelöscht werden. Hinweise für die Einstellungen bei verschiedenen Browsern finden Sie im Internet unter der Adresse www.datenschutzzentrum.de/tracking.

Welche Bedeutung hat die IP-Adresse?

Betreiber von Webseiten können mit der IP-Adresse meist wenig anfangen, da die Adresse sich regelmäßig ändert und keinen konkreten Rückschluss auf Personen zulässt. Anders ist es jedoch, wenn Sie bewusst eine feste IP-Adresse beantragt haben. Der Provider jedoch, der die Adresse vergibt (z. B. Telekom, 1&1, Arcor u. a.), speichert die Zuordnung, welcher Kunde zu welchem Zeitpunkt eine bestimmte IP-Adresse hatte. Abhängig von der Vertragsgestaltung ist die Speicherdauer unterschiedlich.

Das bedeutet faktisch, dass innerhalb dieser Speicherdauer jeder Klick im Internet zugeordnet werden kann – wenn auch oft nur mit Hilfe des Internetproviders und auf richterliche Anordnung.

Anhand der IP-Adresse kann ein Webseitenaufruf allerdings nur einem Anschlussinhaber zugeordnet werden. Nutzen mehrere Personen einen Internet-Anschluss (z. B. in der Familie), geht aus der IP-Adresse nicht hervor, welche Person gerade online war.

Normalerweise ändert sich die IP-Adresse täglich, so dass für Webseitenbetreiber die IP-Adresse der Besucher wenig Aussagekraft hat. Es gibt allerdings inzwischen auch Provider in Kabelnetzwerken, die ihren Kunden eine IP-Adresse über einen längeren Zeitraum zuweisen. Hier bleibt die IP-Adresse über mehrere Tage identisch, wodurch auch Besuche auf Webseiten in diesem Zeitraum mit ein und derselben Absenderadresse festgestellt werden können. In solchen Fällen kann eine Anonymisierung der IP-Adresse wünschenswert sein.

Ich möchte anonym im Internet surfen. Ist das möglich?

Wichtig zu wissen: Es ist in Deutschland noch erlaubt bzw. vom Gesetz sogar gewollt, sich anonym im Internet zu bewegen.

Beim Surfen ist man gegenüber dem Betreiber einer Webseite nicht anonym. Er kann die IP-Adresse sowie technische Informationen des eigenen Rechners sehen, kann diese jedoch nicht ohne Weiteres zu einer konkreten Person auflösen. Dies ist nur mit Hilfe des Providers und der Strafverfolgungsbehörden möglich. Will man nicht erkennbar sein (also auch nicht mit Hilfe des Providers), muss die eigene IP-Adresse verschleiert werden. Erst dann entspricht der Besuch eines Online-Shops dem Besuch eines großen Kaufhauses, wo niemand nach Verlassen des Ladens (bzw. der Webseite) rückwirkend die eigene Identität ermitteln kann.

Es gibt verschiedene technische Möglichkeiten, die Identität des eigenen PCs und seine IP-Adresse zu verschleiern. Dabei handelt es sich um Software, die sich mit einem einzelnen Computer oder einem Netz von Rechnern im Internet verbindet, über die der eigene Datenverkehr beim Surfen umgeleitet wird. Die umleitenden Computer rufen an Stelle des eigenen Rechners die Seiten im Internet ab. So wird die eigene IP-Adresse verschleiert,

da sie gegenüber Web-Servern etc. nicht mehr in Erscheinung tritt.

Die bekanntesten Anonymisierungsdienste sind JonDonym und TOR:

JAP/JonDonym: Der JAP (im Rahmen der kommerziellen JonDonym-Anonymous-Proxy-Server JonDo genannt) ermöglicht, beim Internet-Surfen eine feste IP-Adresse zu nutzen, die man sich mit vielen anderen JAP-Nutzern teilt. Dadurch erfährt weder der angefragte Server noch ein möglicher Lauscher auf der Verbindung, welcher Nutzer welche Webseite aufgerufen hat. Es können kostenlose und kostenpflichtige Server für diesen Dienst genutzt werden. Mehr Informationen über JAP/JonDo finden Sie unter http://www.anonym-surfen.de/.

Tor: Tor ist eine freie Software und ein offenes Netzwerk, das Internetverbindungen der Nutzer durch ein verteiltes Netzwerk von Servern leitet. Dadurch will es vor Webseitenbetreibern schützen, die Interessensprofile der Nutzer erstellen, und vor Lauschern, die den Datenverkehr abhören. Mehr Informationen über Tor finden Sie unter http://www.torproject.org/.

Daneben gibt es kommerzielle Software im Handel zu kaufen.

Welche Datenspuren, die mein Surfverhalten verraten, sind eigentlich auf meinem PC gespeichert?

Browser speichern eine ganze Menge Informationen über die Webseiten, die der Nutzer aufgerufen hat. Im Allgemeinen geschieht dies, um die Ladegeschwindigkeit der Seiten zu optimieren oder um dem Nutzer bestimmte Funktionen zur Verfügung stellen zu können.

Zur Optimierung werden beispielsweise Elemente von Webseiten auf der Festplatte abgelegt. Das können Grafikelemente sein oder der HTML-Text der Seite selbst. Diese Dateien werden im sog. Cache abgelegt, damit sie bei einem erneuten Aufruf schnell zur Verfügung stehen und nicht erst erneut über das Netz geladen werden müssen. Der Cache ist bei modernen Browsern leicht 50 MB und mehr groß. Dort lassen sich ohne großen Aufwand die angesurften Seiten rekonstruieren. Allerdings gilt dies nur für Nutzer, die direkt am PC sitzen. Der Cache lässt sich nicht über das Internet auslesen. Neugierigen Familienmitgliedern oder Kollegen, die Zugriff auf den eigenen PC haben, steht er jedoch offen.

Ähnlich verhält es sich mit der sogenannten History, der Liste der zuletzt besuchten Webseiten. Diese soll unnötige Tipperei ersparen, indem zum Beispiel schon nach Eingabe weniger Buchstaben einer Webadresse diese angezeigt wird oder alle anderen Adressen, die diese Zeichen enthalten. Hat man die Adresse einer besuchten Seite vergessen, kann man auch eine Liste aller in den letzten Tagen und Wochen aufgerufenen Webseiten anzeigen lassen, um so die gesuchte Adresse wiederzufinden. So praktisch das alles ist, so unangenehm kann es unter Umständen sein, wenn diese Daten von anderen eingesehen werden. Daher kann es sinnvoll sein, die History ab und an zu löschen oder ihre Speicherung sogar vollständig zu unterbinden.

Viele moderne Browser haben eine eigenen Privat- bzw. Privacy-Modus. Dieser unterbindet, dass Daten über das Surfverhalten auf dem eigenen Rechner über das Beenden des Browsers hinaus gespeichert werden. Gegenüber dem Webseitenanbieter bietet dieser Modus allerdings keinen vollständigen Schutz vor Beobachtbarkeit

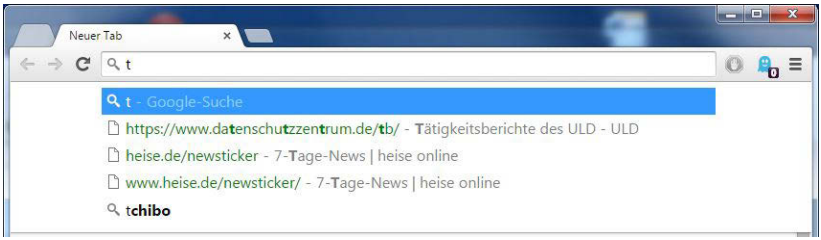

Abbildung 1: Vorschläge des Browsers bereits aufgerufene Seiten nach Eingabe des Zeichens "t", hier unter Google Chrome

Darüber hinaus speichert der Browser unter Umständen auch Eingaben in Webformulare. So merkt er sich zum Beispiel die Eingabe der E-Mail-Adresse auf der Login-Seite von E-Mail-Anbieten. Bei einem erneuten Besuch der Seite schlägt der Browser dann die entsprechende Adresse schon vor und erspart dem Nutzer so ein wenig Tipparbeit. Auch Passwörter lassen sich so bequem abspeichern. Jeder Nutzer muss selbst entscheiden, ob er den Browser solche Informationen speichern lassen möchte oder nicht. Reine Formulardaten stellen dabei das kleinere Problem dar. Passwörter bedeuten hingegen oftmals den Zugriff auf Webseiten und Dienste. Ein Missbrauch kann hier ernsthafte Konsequenzen nach sich ziehen. Wie schon im Falle des Browser-Cache kann auch hier die aufgerufene Webseite nicht auf die gespeicherten Informationen zugreifen. Eventuelle Mitbenutzer des Rechners können es aber sehr wohl.

Wie sicher ist E-Mail?

Die Kommunikation per E-Mail ist mit dem Versenden einer Postkarte zu vergleichen. Es ist ohne weiteres möglich, diese Informationen zu lesen. E-Mails unterliegen zwar auch dem Schutz des Fernmeldegeheimnisses und des Briefgeheimnisses (Art. 10 Grundgesetz), aber es ist möglich, E-Mails auf ihrem Transportweg durch das Internet abzufangen, zu kopieren und sogar zu verändern.

Kann ich dafür sorgen, dass die Inhalte meiner E-Mails nicht gelesen werden?

Ja, dafür gibt es Verschlüsselungs-Programme, die für Privatanwender kostenfrei nutzbar sind. Die bekanntesten sind PGP (Pretty Good Privacy) und GNUPG. Die Nutzung dieser Verschlüsselungstechnik setzt voraus, dass alle Kommunikationspartner eines der beiden (beide sind untereinander kompatibel) Programme benutzen.

Eine Einführung in das Thema E-Mail-Verschlüsselung finden Sie im Internet unter https://www.bsi.bund.de/DE/Themen/ProdukteTools/Gpg4win/gpg4win_node.html sowie auf der Seite www.gpg4win.de.

Was kann ich gegen Spam unternehmen?

Unter Spam versteht man unaufgefordert zugesandte E-Mail-Werbung im Internet. Spam stellt seit Jahren eine der größten Belästigungen der Internetnutzer dar. Bis heute ist es nicht gelungen, das Spamaufkommen zu minimieren. Die Tendenz ist, dass das Aufkommen eher noch im Steigen begriffen ist. So lange Sie sich an die folgenden Regeln halten, können Sie die Bedrohung für Ihre Daten und Ihren PC in Grenzen halten.

Die einfachste und sicherste Regel ist: Spam ungelesen sofort löschen! Für alle, denen dieser Rat zu einfach ist:

- Nicht auf Spam-Mails antworten

  Absender lassen sich in E-Mails leicht fälschen. Daher ist die als Absender genannte E-Mail-Adresse in den seltensten Fällen auch der Urheber der Werbemail. Eine Antwort an die Absenderadresse ist also sinnlos.

Nicht auf in Spam-Mails enthaltene Links und Anhänge klicken.

Klicken Sie auf einen solchen Link, werden Sie auf Webseiten gelenkt, die im besten Fall lediglich Inhalte anzeigen, die Sie nicht interessieren. Im schlimmsten Fall wird von dieser Seite oder dem Anhang Schadcode auf Ihren Rechner übertragen, um diesen mit Viren oder Trojanern zu infizieren.

- Bei unverlangter E-Mail-Werbung niemals auf einen „Abmelden"-Link klicken!

  Oft stehen am Ende einer Spam-Mail Sätze wie dieser: „Wenn Sie unsere kostenlosen Informationen nicht mehr erhalten wollen, klicken Sie bitte auf diesen Link!". Mit der vermeintlichen Abmeldung wird oftmals jedoch nur geprüft, ob die Mailadresse auch benutzt wird. Klickt man auf Abmelden, bestätigt man dem Spammer, dass es sich bei der eigenen Mailadresse um eine garantiert aktive Adresse handelt – und die lassen sich teuer weiterverkaufen.

Verwenden Sie Abmeldelinks daher nur bei Newslettern oder ähnlichen Mails, für die Sie sich irgendwann einmal bewusst eingetragen haben.

Wie kann ich mich gegen schädliche Software schützen?

Ein hundertprozentiger Schutz gegen Viren, Würmer und Trojaner (sog. Malware) ist nicht zu erreichen. Das Risiko kann aber schon dadurch minimiert werden, indem man sich im Internet umsichtig bewegt. D. h. man sollte sich die Webseiten, die man aufsucht genau anschauen und keinesfalls ohne nachzudenken Programme herunterladen und installieren. Dasselbe gilt für Anhänge an E-Mails (s. o.).

Bei der Installation neuer Software ist darauf zu achten, was genau die Installationsroutine auf den PC spielen möchte. Häufig wird – insbesondere bei kostenloser Software – neben dem eigentlichen Programm noch eine Reihe von Werbeprogrammen auf den Computer geschmuggelt. Im Verlauf der Installation wir dies zwar oft angekündigt, die Häkchen zum Deaktivieren dieser heimlichen Installation übersehen viele Nutzer jedoch.

Auch sollte die Software auf dem eigenen PC stets auf dem neuesten Stand gehalten werden. Sicherheitslücken in Programmen ermöglichen schädlicher Software sonst unter Umständen auf den eigenen PC zu gelangen. Aktualisierungen (sog. Patches) für das Betriebssystem sind Pflicht und sollten so schnell wie möglich eingespielt werden. Lassen Sie hierzu das automatische Update eingeschaltet. Aber auch Anwendungen, die auf dem Computer installiert sind, müssen auf dem neuesten Stand sein. Hierzu zählen insbesondere Browser, Mail- und Chatprogramme sowie alles, was aktiv mit dem Internet kommuniziert. Aber auch andere Software, die nicht direkt mit dem Internet zu tun hat, muss aktuell sein. Hierzu zählt insbesondere der Acrobat Reader zur Anzeige von PDF-Dokumenten.

Einen weitergehenden Schutz bieten Antivirenprogramme, die als Freeware oder gegen Entgelt erhältlich sind. Dabei ist es weniger wichtig, welchen Scanner Sie genau einsetzen, als vielmehr diesen auch aktuell zu halten. Virenscanner erkennen Schadsoftware anhand einer Vergleichsliste, der sog. Signaturliste. Befindet sich ein neuer Computervirus nicht in dieser Vergleichsliste, kann der Scanner ihn nicht erkennen. Darum sollten Virenscanner mehrmals täglich nach Signaturupdates suchen und diese einspielen. Ebenso wichtig ist es, heruntergeladene Dateien vor jeder weiteren Aktion unbedingt mit dem Scanner zu überprüfen.

Weitere Informationen erhalten Sie auch auf der Homepage des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unter www.bsi-fuer-buerger.de.

Meine Kinder nutzen auch das Internet. Welche Gefahren sind damit verbunden?

Kinder kommen bereits früh mit PCs, Smartphones und Internet in Berührung. Schon in den Grundschulen werden die Schülerinnen und Schüler langsam an den Umgang mit dem PC herangeführt. In der weiterführenden Schule wird diese Strategie fortgeführt und hier auch der Umgang mit dem Internet als Informationsmedium geübt. Während jedoch in der Schule sorgfältig darauf geachtet wird, welche Webseiten die Kinder aufsuchen, geschieht dies im häuslichen Umfeld leider nicht immer: Sehr früh erhalten Kinder heute unkontrolliert Zugang zum Internet über ein eigenes Smartphone oder einen eigenen PC. Viele Eltern wissen aber nicht, was ihre Kinder dort machen bzw. reglementieren die Nutzung nicht oder nicht ausreichend. Damit erkennen sie auch nicht, welche Seiten sich ihr Kind im Internet anschaut, mit wem es in welcher Weise kommuniziert und in welchen sozialen Netzwerken es sich aufhält.

Hat Ihr Kind bereits Zugang zum Internet oder soll es demnächst einen solchen erhalten, sollten Sie Folgendes wissen:

Das Internet bietet unendliche Möglichkeiten der Informationsbeschaffung und gibt Zugang zu einer unbegrenzten Zahl von Webseiten, die nützlich für Ihr Kind sein können. Es enthält aber auch Inhalte, die Ihr Kind nicht sehen sollte. Pornografische, Gewalt verherrlichende, rassistische und extremistische Inhalte finden sich ohne große Suche.

Was kann ich tun, um zu verhindern, dass mein Kind auf solche Seiten gelangt?

Einen vollständigen Schutz gibt es nicht. Für jüngere Kinder gibt es spezielle Portale wie z. B. www.blinde-kuh.de, die den Einstieg ins Netz begleiten. Werden die Kinder älter (und neugieriger), besteht die Möglichkeit, den Zugang zu jugendgefährdenden Webseiten am PC durch spezielle Programme zu sperren. Diese Programme gibt es in Kombination mit Personal-Firewalls. Dort lassen sich Filter aktivieren, die automatisch versuchen, den Zugang zu solchen Webseiten zu unterbinden. Allerdings gelingt dies nie vollständig und kann von technikkundigen Jugendlichen ggf. wieder umgangen werden, weshalb Filter allenfalls als zusätzliche Maßnahme, niemals jedoch als alleinige Schutzmaßnahme betrachtet werden sollten. Wichtig ist es deshalb, nicht nur das Surfverhalten Ihres Kindes zu reglementieren und zu kontrollieren sondern vor allem mit Ihrem Kind über die Gründe für diese Reglementierung zu sprechen und über die Risiken aufzuklären.

Ist das Kind mit einem Smartphone mit Internetzugang ausgestattet, bestehen keine realistischen Möglichkeiten, den Aufruf von Webseiten präventiv zu kontrollieren. Hier kommt es umso mehr auf den Dialog zwischen Eltern und Kind an.

Besteht eine Gefahr durch Chats und Messenger?

Chats und insbesondere Messenger auf dem Smartphone ergänzen bzw. ersetzen inzwischen die Kommunikation über das Telefon oder SMS. Besonders Jugendliche nutzen diese Angebote, um gleichzeitig mit mehreren Bekannten und Freunden in Kontakt zu bleiben. Am beliebtesten sind Dienste wie WhatsApp und Skype. Über diese Dienste können auch Fotos und Videos ausgetauscht werden.

Die Vorteile von Messengern sind neben der Ersparnis von

Telefongebühren, dass viele Nutzer quasi gleichzeitig miteinander unbegrenzt durch Kosten und Ländergrenzen kommunizieren können.

Messenger wie WhatsApp sind teilweise an die Telefonnummer des Smartphones gebunden, auf dem sie installiert sind. Nachrichten werden von WhatsApp anhand dieser Nummer zugestellt. Im Falle eines Rufnummernwechsels (bspw. nach dem Ende des Mobilfunkvertrags) kann es so allerdings zu Fehlzustellungen kommen, wenn die Kommunikationspartner noch die alte Nummer gespeichert haben.

Inhalte von Chat- und Messenger-Kommunikation (also neben Textnachrichten auch versendete Bilder und Videos) sind selten ausreichend gegen unbefugtes Mitlesen geschützt. Zumindest die Betreiber der Dienste, die ihren Sitz oft in den USA haben, können meist vollständig Zugriff auf die Inhalte nehmen. Sogenannte Ende-zu-Ende-Verschlüsselung, bei der Nachrichten ausschließlich für die beteiligten Nutzer lesbar sind, ist leider selten. Eine Ausnahme stellt hier der Messenger Threema dar, der plattformübergreifend verfügbar ist. Auf Apple Geräten bietet iMessage eine entsprechende Verschlüsselung, stellt jedoch eine plattformabhängige Insellösung dar. WhatsApp bietet derzeit (Mai 2015) keine durchgängige, plattformübergreifende Ende-zu-Ende-Verschlüsselung.

Online-Chats ohne Bindung an die Mobilfunknummer bergen ein anderes Risiko: Es ist möglich, in diesen Diensten eine falsche Identität vorzugaukeln. Es ist bekannt, dass fremde Personen in diesen Internet-Chats versuchen, unter Vorspiegelung falscher Identitäten, Kontakt zu Kindern und Jugendlichen aufzunehmen, um diese über ihre private Lebenssituation auszuhorchen. Im schlimmsten Fall handelt es sich um Personen, die auch kriminelle Handlungen planen.

Sie sollten deshalb Ihr Kind auch über diese Gefahren aufklären und ihm raten, nur mit Personen zu chatten, die ihnen auch im „richtigen" Leben bekannt sind. Ferner sollten Sie Ihrem Kind empfehlen, nicht seinen echten Namen zu benutzen, sondern ein Pseudonym (Nickname) zu wählen. Die Verwendung eines solchen Nicknames ist in Chatrooms ziemlich verbreitet und damit erst recht nicht auffällig. Auch andere persönliche Informationen wie Anschrift, Telefonnummer oder der Name der eigenen Schule sollten niemals im Chat preisgegeben werden. Auch sollte Ihrem Kind klar sein, dass Zugänge der Freunde von Dritten übernommen oder Namen gefälscht werden können. Es ist wichtig, sensibel dafür zu sein, Änderungen im Verhaltensmuster von vermeintlich bekannten Kommunikationspartnern zu erkennen und stets vorsichtig zu sein.

Mein Kind nutzt Facebook. Was sollte ich da beachten?

Facebook ist ein sogenanntes Soziales Netzwerk, in dem sich Menschen aller Altersstufen zusammenschließen. Für viele Schülerinnen und Schüler ist Facebook inzwischen – zusammen mit WhatsApp (das von Facebook aufgekauft wurde) - „das Internet". Diese Plattform macht es möglich, mit vielen anderen zu kommunizieren, neue Kontakte zu knüpfen, sich zu verabreden oder einfach zu spielen. Dazu kann jeder Nutzer sein eigenes Profil erstellen, also eine Seite, auf der persönliche Angaben zu einem selbst gemacht werden. Facebook-Nutzer können sich untereinander austauschen, indem sie sich Nachrichten schicken (wie E-Mails) oder aber an der Pinnwand eines anderen Nutzers Mitteilungen hinterlassen. Darüber hinaus können Fotos und Videos veröffentlicht und kommentiert werden.

Wie bei einem sozialen Austausch und Kommunikation im Leben außerhalb des Internets können soziale Netzwerke zum gezielten Mobbing von Mitschülern genutzt werden. Hänseleien aus der

Schule werden über soziale Netzwerke in den privaten Rückzugsraum der Schülerinnen und Schüler getragen und weiten sich durch die indirekte Kommunikation und die herabgesetzte Hemmschwelle leicht aus. Wenn Ihnen ein solcher Vorgang durch Ihr Kind bekannt wird ist es wichtig, sofort zu reagieren. Sie haben die Möglichkeit, sich an die Betreiber der Plattform zu wenden, damit von dort dafür Sorge getragen wird, dass die Ihr Kind belastenden Inhalte entfernt werden. Ggf. kann es auch notwendig werden, sích an die Polizei zu wenden, um prüfen zu lassen, ob strafrelevante Tatbestände vorliegen.

Eine weitere Gefahr liegt in der Mitteilsamkeit der Jugendlichen. In vielen Fällen überblicken Kinder und Jugendliche nicht die Folgen, wenn sie allzu freigiebig mit ihren eigenen und auch fremden Daten sind. Als Mindestanforderung sollte gelten, das eigene Profil nur den eigenen akzeptierten Kontakten (den sog. Facebook-„Freunden") zugänglich zu machen. Veröffentlichungen im Rahmen des eigenen Profils werden so nicht mehr für die Öffentlichkeit sichtbar, sondern nur denjenigen Facebook-Nutzern, die auf der eigenen Freundesliste stehen. Allerdings besteht bei vielen Jugendlichen der Hang, möglichst viele Facebook-„Freunde" zu sammeln und jede Anfrage anzunehmen. Ein Missbrauch von Informationen kann somit auch bei Einschränkung der Öffentlichkeit nie ganz ausgeschlossen werden. Auch die Einstellung, dass „Freunde von Freunden" das eigene Profil sehen dürfen ist quasi als „öffentlich" zu verstehen, wenn man bedenkt, dass hunderte „Freunde" nicht selten bei Facebook-Nutzern sind.

Es ist bei Facebook auch möglich, Bilder von sich und anderen Personen bereitzustellen und damit anderen Besuchern von Profilseiten zugänglich zu machen. Wenn auf diesen Bildern andere Personen erkennbar sind und diese der Veröffentlichung nicht ausdrücklich zugestimmt haben oder sogar von dieser nichts

wissen, verstößt Ihr Kind gegen das Recht am eigenen Bild dieser Personen. Dies kann rechtliche Konsequenzen haben. Dabei muss man auch beachten, dass sich Facebook Rechte an den hochgeladenen Bildern und Videos einräumen lässt.

Sie sollten Ihr Kind in dieser Hinsicht also aufklären und dafür Sorge tragen, dass Sie Kenntnis von den Aktivitäten Ihres Kindes bei Facebook haben. Bitte beachten Sie zu diesem Thema auch unsere Broschüre Nr. 7 „Soziale Netzwerke". Diese finden Sie im Internet unter: www.datenschutzzentrum.de/blauereihe

Was ist mit anderen Online-Diensten wie WhatsApp und Snapchat?

Die Bedeutung von Facebook nimmt im Umfeld von Jugendlichen aktuell nach unserer Beobachtung ab. An seine Stelle treten neben WhatsApp Dienste wie Instagram, Snapchat oder auch YouNow. Die bereits angesprochenen Probleme beim Veröffentlichen von Fotos und Videos gelten auch hier. Problematisch ist hier insbesondere Snapchat. Dieser Dienst verspricht, dass der Empfänger ein erhaltenes Foto nur für eine festgelegte Zeitspanne sehen kann – danach ist es verschwunden. Viele Nutzer wähnen sich so vor Missbrauch sicher. Leider kann Snapchat diesen Anspruch nicht wirklich erfüllen. Mit wenig Hintergrundwissen kann ein Empfänger die Fotos aus der App extrahieren, ohne dass der Empfänger dies erfährt. Für Jugendliche, die auf Snapchat setzen, weil Sie um das Missbrauchsrisiko wissen, das von Fotos ausgeht, ist dieser Umstand oft nicht vorhersehbar. Bei Apps wie WhatsApp ist ein weiteres Problem, dass diese für ihre Nutzung den Zugriff auf das Adressbuch auf dem Smartphone benötigen. Wird dieses gewährt, so gibt man damit auch Daten von Freunden, Verwandten und Bekannten frei, was diese ggf. gar nicht wollen. Auf solche Dienste sollte besser verzichtet werden, wenn man seine Kontakt nicht einzeln um Erlaubnis fragen möchte.

Wie kann ich das Foto, Profil oder sonstige persönliche Informationen löschen lassen, die Dritte im Internet über mich veröffentlicht haben?

Je nach Intensität der Verletzung und Eilbedürftigkeit können Sie die folgenden Schritte nacheinander oder gegebenenfalls auch parallel einleiten.

- Sofern möglich, kontaktieren Sie denjenigen, der das Foto bzw. Ihre Informationen veröffentlicht hat und fordern Sie ihn auf, die verletzenden Inhalte sofort zu löschen. Weisen Sie dabei auf Ihre Persönlichkeitsrechte hin.
- Nehmen Sie Kontakt zum Anbieter des Internetangebots auf, auf dem die Persönlichkeitsverletzung begangen wird und fordern Sie vom Betreiber die sofortige Löschung der Informationen. Bei deutschen Anbietern sollten Sie die Kontaktdaten im Impressum bzw. unter „Kontakt" finden. Weisen Sie auch hier auf Ihr allgemeines Persönlichkeitsrecht hin und darauf, dass nach § 10 Telemediengesetz rechtswidrige Inhalte unverzüglich vom Betreiber des Internetangebots zu entfernen sind.
- Sollte kein Impressum auf der Webseite vorhanden sein, so können Sie ggf. Informationen über den Betreiber der Seite über die Registrierungsdaten des Domain-Namens (Teil der Internetadresse) erfahren. Bitte wenden Sie sich zu diesem Zweck an die jeweilige Registrierungsorganisation:
  - Für de-Domains (z. B. xzy.de) erhalten Sie Auskunft unter: http://www.denic.de
  - Für com-Domains erhalten Sie Auskunft unter: http://www.whois.com
  - Für net-Domain erhalten Sie Auskunft unter: http://www.whois.net
  - Für info-Domains erhalten Sie Auskunft unter: http://info.info/whois

- Wenn ein Straftatbestand vorliegt (z. B. Beleidigung), können Sie Anzeige bei Ihrer örtlichen Polizei stellen.
- Wenden Sie sich an den Landesbeauftragten für Datenschutz Ihres Bundeslandes. Es handelt sich hierbei um unabhängige Aufsichtsbehörden, die Sie als öffentliche Einrichtung in Datenschutzfragen kostenlos beraten und ggf. zumindest bei deutschen Anbietern direkt gegen diese bei Rechtsverletzungen vorgehen können.
  Die Kontaktdaten aller Datenschutzbeauftragten finden Sie unter http://www.datenschutz.de/institutionen/adressen/.
- Auch die örtlichen Verbraucherzentralen können Sie beraten. Informationen dazu finden Sie u. a. hier: http://www.surfer-haben-rechte.de.

Weitere Hinweise zum Umgang mit dem Internet durch Kinder finden Sie auch unter

- www.klicksafe.de
- www.secure-it.de
- www.bsi-fuer-buerger.de
- www.watchyourweb.de

Kontakt

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein (ULD)
Holstenstraße 98
24103 Kiel
Telefon: +49 (0) 431 988-1200
Telefax: +49 (0) 431 988-1223
E-Mail: mail@datenschutzzentrum.de
www.datenschutzzentrum.de

Broschüren zu den Themen

- Sozialhilfe, Grundsicherung und Arbeitslosengeld II
- Verbraucher-Scoring
- Videoüberwachung und Webkameras
- Internet: Alltag online
- Illegaler Datenhandel
- Soziale Netzwerke
- Datenschutz für Patienten

können Sie unentgeltlich bei uns bestellen oder von unserer Homepage unter www.datenschutzzentrum.de/blauereihe herunterladen.