mitp Anwendungen

Kinder sicher im Netz

Das Elternbuch

von
Sigrid Born

1. Auflage

Thematische Gliederung:

Internet

mitp/bhv 2013

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 8266 9471 4

Inhaltsverzeichnis: Kinder sicher im Netz – Born

mitp

Sigrid Born

Kinder sicher im Netz

Das Elternbuch

Inklusive CD-ROM

Kapitel 1

Die größten Gefahren im Internet – für Kinder und Erwachsene

Sicherheit im Internet ist in erster Linie eine Elternaufgabe: Sie setzen die Sicherheitsstandards, Sie zeigen, wie man bewusst und verantwortungsvoll mit dem Computer umgeht. Und Sie sind diejenigen, die die Gefahren des WWW kennen sollten.

Der Hightech-Verband BITKOM hat zu Beginn des Jahres 2013 eine Hitliste der zehn größten Gefahren aus dem Internet herausgebracht. Bei diesen Hauptgefahren handelt es sich ausschließlich um Programme mit dem Ziel, Schaden auf Ihrem Rechner anzurichten. Und die wichtigsten lernen Sie hier in einem Überblick kennen. Außerdem erfahren Sie etwas über Ihre Datenspuren im Netz – und das sind nicht wenige.

1.1 Ohne Netz und doppelten Boden – Erwachsene surfen sorglos

Beginnen wir mit einigen Tatsachen: Nach einer Cybercrime-Studie des amerikanischen Sicherheitsdienstleisters Norton aus dem Jahr 2012 werden jeden Tag 1,5 Millionen Menschen Opfer einer Attacke aus dem Internet – 18 Opfer pro Sekunde.

Laut der polizeilichen Kriminalstatistik ist der Schaden aller Cybercrime-Delikte im Jahr 2011 um 16 Prozent auf insgesamt 71,2 Millionen Euro gestiegen (2010: 61,5 Millionen Euro).

Das Sicherheitssoftware-Unternehmen Symantec zeigt in seinem Cybercrime-Report, wie sorglos Erwachsene sich im WWW bewegen. 4.500 erwachsene Internetnutzer in Europa wurden dazu befragt, das Ergebnis ist ziemlich erschreckend: Drei von fünf Erwachsenen nutzen ungesicherte lokale Funknetzverbindungen – die fast überall üblichen WLANs (Wireless Local Area Network). Fast die Hälfte von ihnen macht sich zwar Sorgen um die Sicherheit ihrer Verbindung, doch 43 Prozent rufen ihre E-Mails ab, 38 Prozent loggen sich bei sozialen Netzwerken ein und 18 Prozent sogar bei ihrer Bank – wohlgemerkt, öffentlich und ungesichert. Ebenso gut könnten sie lauthals ihre PIN- und TAN-Nummern verkünden oder ihr Schlüsselbund mit genauen Adressangaben auf einer Parkbank liegen lassen.

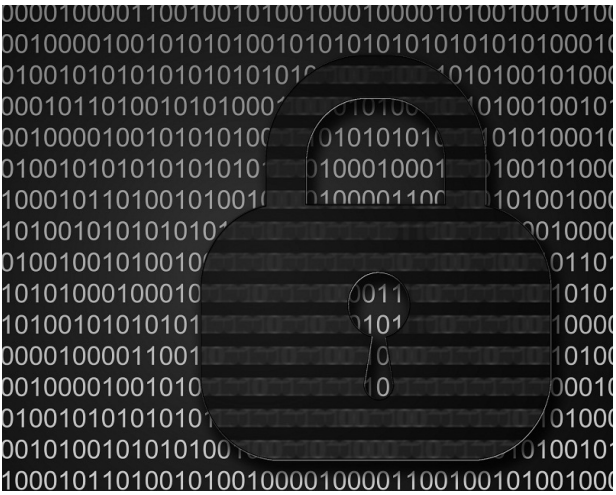


Abb. 1.1: Datenschutz hat oberste Priorität. Foto: Gerd Altmann, pixelio

Auch außerhalb von WLANs sind Smartphone- und Tablet-Besitzer erstaunlich risikobereit: Ein Drittel schützt das Mobilgerät nicht mit einem Passwort, 40 Prozent der Anwender laden Apps aus unsicheren Quellen herunter. Dabei zeigt die Symantec-Studie große Unterschiede zwischen einzelnen Ländern. So speichern nur vier Prozent der Deutschen ihre Bankdaten auf Mobilgeräten, während dies in Dänemark 13 Prozent der Befragten tun.

Fast jeder vierte deutsche PC ist infiziert: Das ergab die Malware-Statistik des Antivirensoftware-Herstellers Panda Security in seinem Bericht für das erste Quartal 2013. Von Januar bis März seien weltweit über 6,5 Millionen neue Schädlinge gefunden worden. Die Rangliste der Staaten mit den meisten infizierten Rechnern führt mit 53,4 Prozent China an. Deutschland liegt zwar unter den Top Ten der weniger belasteten Länder, dennoch ist hier fast jeder vierte PC (22,9 Prozent) mit Schadsoftware belastet.

Und Kaspersky Lab berichtet in seinem Quartalsbericht, dass jeder infizierte Rechner im Durchschnitt acht Sicherheitslücken aufweise.

1.2 Schadprogramme über Downloads

»Einem herumschweifenden Jäger begegnet ein herumschweifendes Tier.« Dieses Sprichwort aus Afrika trifft wohl auf jeden zu, der sich im Internet bewegt. Das Tier aber hört oder sieht man vielleicht noch, aber wenn Sie von einem Schadprogramm im Internet erwischt werden, merken Sie erst einmal nichts.

Wie aber sehen die Gefahren konkret aus? Damit hat sich BITKOM, das Sprachrohr der IT-, Telekommunikations- und Neue-Medien-Branche, beschäftigt.

Abb. 1.2: Die zehn größten Gefahren im Internet, ermittelt von BITKOM

Wichtig

Viren – Würmer – Schadprogramme

Vor nicht allzu langer Zeit hießen schädliche Programme meistens »Viren«. Heute sprechen Experten ganz allgemein von »Schadprogrammen« – auch »Malware« genannt. Damit sind alle bösartigen Programme gemeint, die auf den Computern, die sie infizieren, unerwünschte Funktionen ausführen. Nach einer Definition des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sind viele dieser Schädlinge »... modular aufgebaut und können darum häufig nicht eindeutig einer bestimmten Kategorie – etwa Virus oder Wurm – zugeordnet werden«. Diese Programme sind so schlau programmiert, dass sie über das Internet automatisch weitere Funktionen aktualisieren und sich ständig verändern können. Und dann machen sich diese Schadprogramme auf, um weitere Rechner im Internet zu infizieren. Dazu nutzen sie zum Beispiel Schwachstellen im Browser. Weitere Infos dazu finden Sie auf den Webseiten des BSI (`www.bsi-fuer-buerger.de`).

Die größte Bedrohung für Internetnutzer, so zeigt es die Studie der BITKOM, sind sogenannte *Drive-by-Downloads*. Das sind Webseiten, die mit schädlichem Code

infiziert werden. Wenn Ihr Rechner Schwachstellen hat, reicht es also aus, eine solche Internetseite nur zu besuchen. Das ist besonders fies, denn Sie müssen nicht einmal mehr auf einen Link klicken oder gar eine Datei herunterladen. Die Schadprogramme fangen Sie sich ganz nebenbei ein. Ein Bericht der European Network and Information Security Agency erklärt die Drive-by-Downloads für besonders tückisch, weil sie kaum zu erkennen sind.

Und das trifft zu allem Überfluss auch auf einige Apps zu. Immer mehr setzt sich das mobile Bezahlen durch, und so ist es nicht weiter verwunderlich, dass schädliche Apps programmiert werden, um an Ihr Geld zu gelangen. Es trifft vor allem Android-Geräte: Für das mobile TAN-Verfahren taucht inzwischen eine Variante für unterschiedliche Banken auf. Der Trojaner fordert den Benutzer auf, Handyhersteller, Modell und Handynummer anzugeben. Gelingt es den Betrügern, auf diese Weise Smartphones mit Schadcode zu infizieren, können sie in Kombination mit so erwischten Zugangsdaten beliebig Überweisungen ausführen.

1.3 Trojaner und Würmer

Auf dem zweiten Platz liegen Würmer und Trojaner. Trojaner führen auf infizierten Computern unbemerkt gefährliche Funktionen aus, und digitale Würmer verbreiten sich selbst über das Internet.

Hinweis

Die Computerversion des Trojanischen Pferdes funktioniert nach demselben Prinzip wie das Vorbild aus der griechischen Mythologie. Ein scheinbar nützliches Programm hat ein anderes böswilliges Programm sozusagen im Bauch, das dann unbemerkt eindringt und sich auf dem PC installiert. So können beispielsweise Passwörter und andere vertrauliche Daten ausgespäht, verändert, gelöscht oder bei der nächsten Datenübertragung an den Angreifer verschickt werden. Dieser Datendiebstahl bleibt in der Regel unbemerkt, weil im Gegensatz zum Diebstahl materieller Dinge nichts fehlt. Anders als Computerviren können sich Trojanische Pferde jedoch nicht selbstständig verbreiten.

So ähnlich funktionieren die als Trojaner bekannten Schadprogramme. Sie tarnen sich als harmlose Dateien und beinhalten schädliche Software, die Ihren Rechner oder Ihr Handy infiziert.

Ein bekanntes Beispiel: der Trojaner des Bundeskriminalamtes (BKA) – ausgerechnet! Europäische Strafverfolger haben inzwischen eine Gruppe Cyberkrimineller verhaftet, die auf diese Weise Internetnutzer betrogen hat. Sie hatten einen Trojaner programmiert und in Umlauf gebracht, der die befallenen Rechner sperrte, indem sie über das Programm verschlüsselt wurden. Auf dem Bildschirm

erschien eine Meldung, der Computer sei wegen mutmaßlich illegaler Aktivitäten von den Behörden gesperrt worden – etwa weil User Webseiten mit Kinderpornografie besucht hätten.

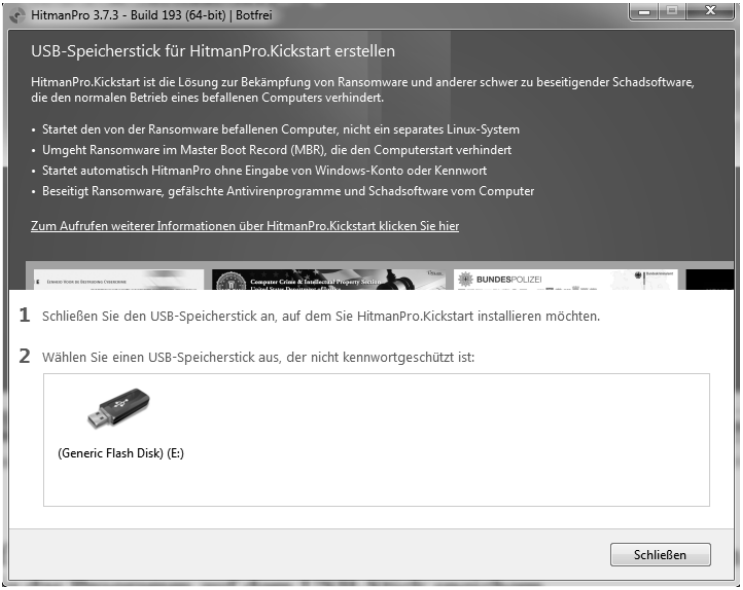
Abb. 1.3: Beispiel für den Trojaner, der angeblich von der Bundespolizei verschickt wurde

Gegen die Zahlung einer Strafe in Höhe von 100 Euro – eine Art Lösegeld – werde der Rechner wieder freigegeben. Ein Logo einer Strafverfolgungsbehörde wie der Bundespolizei oder des Bundeskriminalamtes war natürlich eingebaut. Selbstverständlich passiert nach dem Zahlen dieser Strafe nichts, der Computer ist weiterhin gesperrt.

Sollte sich bei Ihnen einmal dieser Trojaner einschleichen, kann das Programm *HitmanPro.Kickstart* vom Anti-Botnet-Beratungszentrum helfen (`http://blog.bot-frei.de`). Sie sollten sich das Programm auf einem USB-Stick speichern und es als Notfallprogramm dann anwenden, denn es lässt sich vom USB-Stick booten. Windows wird bereits während der Startsequenz auf Malwarebefall untersucht, und das Schadprogramm wird auch entfernt.

Unten auf dem Bild befindet sich ein kleiner Kickboxer. Wenn Sie den anklicken, können Sie das Programm auf dem USB-Stick speichern.

Abb. 1.4: Das Programm HitmanPro stellt Ihren gesperrten Computer wieder her.



Sie folgen nun den Anweisungen, die Ihnen das Programm gibt. Bei weiteren Fragen hilft Ihnen das Servicecenter des Bundesamtes für Sicherheit in der Informationstechnik, das unter 01805 274100 oder `mail@bsi-fuer-buerger.de` erreichbar ist. Informationen finden Sie auch auf den Seiten des eco-Verbandes der deutschen Internetwirtschaft e. V. (`www.bka-trojaner.de`).

Vorsicht

Auch stolze Besitzer von Apple-Rechnern sind nicht mehr sicher. Der Blog des Anti-Botnet-Beratungszentrums warnt, dass mittlerweile die ersten Mac-Rechner Opfer einer FBI-Ransomware geworden sind. Beim Öffnen des Safari-Browsers wurden sie mit einer Warnung des FBI überrascht, das angeblich den Mac gesperrt hat und wegen einer Urheberrechtsverletzung einen Betrag in Höhe von 300 Dollar fordert.

Immer wieder tauchen neue Varianten dieser bereits seit 2011 bekannten Schadsoftware auf. Um Glaubwürdigkeit vorzutäuschen, missbrauchen die Erpresser offizielle Logos von bekannten Unternehmen und Behörden. Neben dem Logo der Bundespolizei werden die Nutzer mit den Logos des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e. V. (GVU) getäuscht.

1.3.1 Trojaner auf dem Smartphone

Apps – also Anwendungen (engl.: »applications«) für Smartphones sind – Software für Mobilgeräte oder mobile Betriebssysteme. Das sind manchmal wirklich sinnvolle Programme wie der Navigator der Deutschen Bahn oder Apps von Tageszeitungen oder für Kinder die App *First Words*, eine Art Vokabeltrainer fürs Englische. Aber immer mehr Trojaner werden über die Apps verschickt. Im April 2013 wurden Postbank-Kunden das Ziel der Angriffe: Die Nachricht trägt im Betreff »Extended Validation-Zertifikate (EV-SSL-Zertifikat) im Android«. Liest man diesen Betreff, denkt man, das sei wichtig für die Sicherheit des Gerätes. Nun wird man auf Deutsch dazu aufgefordert, eine App zu installieren. Die Nachrichten werden ungezielt als Spam verschickt und können deshalb in jedem Postfach landen. Als Absender erscheinen unter anderem Adressen wie »kundenservice@postbank.de« und »mobile-banking@postbank.de«.

Wer die E-Mail mit seinem Android-Smartphone öffnet und der Aufforderung nachkommt, lädt sich einen auf das Auslesen von Onlinebanking-Daten spezialisierten Trojaner auf sein Smartphone. Dies ergab eine Analyse des Branchendienstes heise Security. Mit den ausgespähten Informationen sei es für die Kriminellen ein Leichtes, die Bankkonten zu plündern, schreibt heise Security dazu.

Sicherheitsexperten beobachten seit Langem einen Anstieg von Trojaner-Angriffen auf mobile Betriebssysteme wie Android. So gelang es Onlinedieben, über einen kombinierten Angriff auf PC und Smartphones das zweistufige mobile TAN (mTAN)-Sicherheitsverfahren auszuhebeln und eine millionenschwere Beute einzufahren. Mehr als 30.000 Konten wurden 2012 mithilfe des *Zeus in the Mobile* (ZitMO)-Trojaners abgeräumt und deutsche Kontoinhaber insgesamt um etwa 12 Millionen Euro erleichtert.

1.3.2 Bausätze für Viren

Das Internet macht's möglich: Es gibt Anleitungen, wie man selbst Schadprogramme herstellen kann. Eine Gefahr für Kinder besteht insofern, als diese gerne herumexperimentieren und sehr neugierig sind – mit Feuer, mit Messern und auch mit Programmen. Und aus reiner Neugier besuchen sie solche Seiten, die dann gerne ihrerseits mit Viren oder Trojanern verseucht sind.

Hinweis

Das erste Werkzeug dieser Art war das *Virus Construction Set*. Entwickelt wurde es schon 1990 von einer Gruppe mit dem Namen »Verband Deutscher Virenliebhaber«. Bald folgten *NuKE's Randomic Life Generator, Odysseus, Senna Spy Internet Worm Generator* und viele, viele andere.

Abb. 1.5: Stoned ist ein Bootvirus, auch Bootsektorvirus genannt. Das Virus wurde erstmals 1987 in der Stadt Wellington, Neuseeland, entdeckt.

1.3.3 Nicht zu unterschätzen: Botnetze

Wenn Sie jemandem ins Netz gegangen sind, kann das auch ein Botnetz sein. »Bot« kommt von »robot«, das ist eigentlich etwas Gutes und heißt »arbeiten«. Im IT-Fachjargon ist mit »Bot« ein Programm gemeint, das ferngesteuert auf Ihrem PC arbeitet. Ihr Computer ist also gekapert worden. Botnetze basieren auf Viren, Trojanern und Würmern. Botnetze sind sehr viele Computer – meist mehrere Tausend, es können aber auch mehrere Millionen sein –, die per Fernsteuerung zusammengeschlossen und zu bestimmten Aktionen missbraucht werden.

Vielleicht ist auch Ihr Computer Teil eines Botnetzes? Der Rechner kann sich infizieren, wenn Sie im Internet unterwegs sind oder E-Mail-Anhänge öffnen. Meistens sind Bots zunächst ziemlich unauffällig, sodass Sie davon nichts bemerken. Doch der Schein trügt. Denn die Verursacher der Schadprogramme können diese per Knopfdruck aktivieren, zum Beispiel um E-Mails zu versenden. Dazu schicken sie entsprechende Kommandos an den befallenden PC. Eine einzige kriminelle Person kann alle Bots zentral in ihrem Netzwerk dirigieren und ihnen befehlen, die gleichen Aufgaben auszuführen. Voraussetzung dafür: Der PC muss online sein. Ihr PC scheint nun ganz normal zu arbeiten, während sich gleichzeitig im Hintergrund lauter unerfreuliche Dinge abspielen.

Wie erkennt man, dass der Rechner infiziert ist?

Das Bundesinnenministerium gibt in seinem Faltblatt »Botnetze – Computer in Gefahr« folgende Tipps:

> *Ein Hinweis auf Botnetz-Aktivitäten eines Rechners ist häufig der Versand oder der Empfang großer Datenmengen, ohne dass eine von Ihnen befugte Funktion – bspw. ein Download oder ein Update des Virenprogramms – dafür verantwortlich zu sein scheint. Ein solcher Datenversand macht sich auch dadurch bemerkbar, dass Ihr Rechner langsamer arbeitet als üblicherweise. Um den eigenen Rechner gegen die Infizierung mit einem Bot-Virus zu schützen, unternehmen Sie folgende Schritte: Schützen Sie Ihren Computer durch ein sicheres Passwort vor Missbrauch. Vorsicht bei der Verwendung fremder USB-Sticks: Hier kann Schadsoftware automatisch installiert werden! Aktualisieren Sie Ihr Betriebssystem regelmäßig und schließen Sie bekannte Sicherheitslücken durch zur Verfügung gestellte Updates. Verwenden Sie nur lizenzierte Softwareprodukte. Öffnen Sie nur vertrauenswürdige E-Mails und deren Anhänge. Klicken Sie keine Links in Spam-E-Mails an!*

Eigentlich sollte eine gute Firewall Sie warnen und Schadprogramme durch eine aktuelle Antivirensoftware identifizieren. Wenn Sie vermuten, dass Ihr Rechner bereits infiziert ist, etwa weil die Firewall eine Warnung anzeigt, sollten Sie sich eine Antivirensoftware direkt von der Seite eines Herstellers herunterladen – am besten auf einen anderen Rechner. Dann können Sie die Software auf eine CD brennen und von dort auf Ihren eigenen Computer installieren. Hilfreich ist auch

eine Prüfung, bei der der Rechner von einer Boot-CD gestartet wird. Vorsicht ist dann trotzdem noch immer geboten.

1.4 Angriffe auf Datenbanken und Webseiten und Denial-of-Service-Attacken

Schaden fügen auch diese Anwendungen zu – diesmal geht es darum, Kundendaten massenweise abzugreifen und den E-Commerce, den Handel im Internet, zu beeinträchtigen.

1.4.1 Das Ziel: die Daten von Kunden

Shops im Internet oder Zeitungen mit Content-Management-Systemen setzen Datenbanken ein, um darin Kundendaten, Artikel und Texte abzulegen. Zunehmend attackiert werden diese Datenbanken und Webanwendungen. Aber das sind kaum die riesigen Webseiten von Unternehmen wie Amazon oder Zalando, denn die sichern und überwachen ihre Systeme rund um die Uhr. Gefährdet sind hier eher kleine und mittelständische Unternehmen.

Benutzer können heutzutage auf den meisten Webseiten Kommentare, Texte oder Suchanfragen eingeben. Mittels SQL-Injection – so der Fachbegriff – versucht ein Angreifer, diese Benutzereingaben derart zu manipulieren, dass schadhafte Funktionen ausgeführt werden können.

Eine andere bösartige Attacke ist *Cross-Site Scripting (XSS)*: eine Technik, mit der Sicherheitslücken in Webanwendungen ausgenutzt werden. Diese Technik heißt Cross-Site, da dabei mehrere Webseiten zusammenspielen. Beispielsweise kann von einer nicht vertrauenswürdigen Seite spezieller Schadcode im Kontext einer anderen Webseite ausgeführt werden, um an sensible Daten des Benutzers zu gelangen.

1.4.2 Das System lahmlegen

Denial of Service (DoS) bedeutet so viel wie, etwas außer Betrieb zu setzen. Technisch passiert dies: Bei DoS-Attacken wird ein Server gezielt mit so vielen Anfragen bombardiert, dass das System die Aufgaben nicht mehr bewältigen kann und im schlimmsten Fall zusammenbricht. Auf diese Art wurden schon bekannte Webserver wie zum Beispiel Amazon, Yahoo, eBay mit bis zur vierfachen Menge des normalen Datenverkehrs massiv attackiert und für eine bestimmte Zeit für normale Anfragen außer Gefecht gesetzt.

Die Programme, die für DoS-Angriffe genutzt werden, sind mittlerweile sehr ausgefeilt, und die Angreifer sind nur schwer zu ermitteln, weil sich der Weg der Daten verschleiern lässt. Möglich sind einige der Attacken durch Bugs (das sind Softwarefehler) und Schwachstellen von Programmen, Betriebssystemen oder Fehlimplementierungen von Protokollen.

Davon konnte die Süddeutsche Zeitung (SZ) Anfang 2013 ein Lied singen: Die Webseite wurde über mehrere Stunden durch massenhafte Seitenaufrufe derart überlastet, dass sie nicht mehr erreichbar war. Dieser automatisierte Angriff heißt *Distributed-Denial-of-Service-Attacke (DDoS)*. Dabei greifen viele unterschiedliche Systeme in einer großflächig koordinierten Aktion an. Durch die hohe Anzahl der gleichzeitig angreifenden Rechner sind die Angriffe besonders wirksam.

1.5 Phishing – Passwörter angeln

Wenn Sie bisher glaubten, dass Phishing nur das Onlinebanking betrifft, dann haben Sie sich schwer getäuscht. Es betrifft auch Ihr eBay-Konto, Amazon, PayPal ... Phishing kommt als E-Mail getarnt. Und zwar täuschend echt! Phishing bedeutet: Daten von Internetnutzern werden über gefälschte Internetadressen, E-Mails oder SMS abgefangen mit dem Ziel, persönliche Daten zu missbrauchen und Inhaber von Bankkonten zu schädigen. Der Begriff Phishing ist angelehnt an das englische »fishing« in Verbindung mit dem »P« aus Passwort.

Hier können technische Schutzmaßnahmen wie Antivirensoftware und moderne Webbrowser das Problem nur mildern. Die Verbraucherzentrale Nordrhein-Westfalen zum Beispiel bietet deshalb nun eine neue Möglichkeit zur schnellen Information: das *Phishing-Radar* unter `www.vz-nrw.de/phishing`.

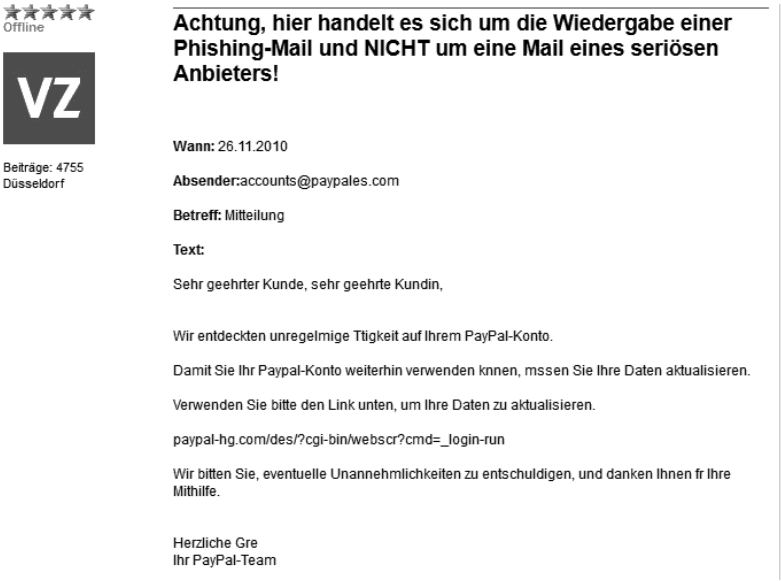


Abb. 1.6: Beispiel einer Phishing-Mail der Verbraucherzentrale NRW

Dazu schreibt die Verbraucherzentrale NRW:

> *Die als Bestellung, Rechnung oder Mahnung getarnten Trojaner-Mails tragen im Anhang schädliche Virensoftware. Wer die Dateien öffnet, der riskiert, dass sein Computer ausgespäht wird und die Daten an die Betrüger übermittelt werden. Derzeit kursieren beispielsweise zahlreiche E-Mails, wonach der Empfänger angeblich noch eine Rechnung beim Rabatt-Dienst Groupon offen habe. Mal lautet der Betreff »Groupon.de Mahnung 14.03.2013 XXX (Name)«, »XXX (Name) Groupon GmbH AG Mahnung«, mal heißt es »XXX (Name) Abrechnung Ihrer Groupon GmbH Mitgliedschaft XXX« oder auch »Rechnung Ihrer Groupon GmbH Mitgliedschaft 14. März 2013 XXX (Name)«. Auch mit Amazon als vorgeblichem Absender werden beständig Trojaner-Mails verschickt. Die Betreffzeilen lauten zum Beispiel »Bestellung bei Amazon BuyVip« oder »Bestellung bei Amazon BuyVip (Vorname) (Nachname)«. Neu sind Mails mit Betreffzeilen wie etwa »Ihre Rechnung MyDirtyHobby GmbH 10.04.2013« oder »Rechnung Seitensprung.de Portal für den Benutzer [Benutzername]«. Dabei geben sich die Betrüger als Mitarbeiter von Erotikportalen aus, um den E-Mail-Empfänger zu bewegen, den zip-Anhang zu öffnen. Der jüngste Dreh: Ahnungslose Verbraucher werden zu Tätern gemacht. Unter der realen E-Mail-Adresse eines Unbescholtenen schicken die Ganoven fingierte Rechnungen und Mahnungen an Dritte.*

1.5.1 Link auf gefälschte Internetseiten

Es kursieren massenhaft Phishing-Mails, die angeblich von Amazon, PayPal, Mastercard und Visa stammen. Über einen Betreff wie zum Beispiel »Dringend – Ihre VISA Kreditkarte wurde ausgesetzt!« wird man dazu verleitet, auf gefälschten Seiten, die denen der Firmen sehr ähnlich sehen, sensible Daten wie etwa Kontoverbindungen einzugeben.

Tipp

Das BSI gibt dazu diese Empfehlungen:

- Öffnen Sie unter keinen Umständen Anhänge oder Links solcher E-Mails! Lassen Sie sich dazu auch nicht durch persönliche Anreden oder flüssig geschriebenes Deutsch verleiten!
- Haben Sie Anhänge oder Links doch geöffnet, starten Sie Ihr Antivirenprogramm. Wenn sich die Probleme damit nicht beheben lassen, müssen Sie Ihren Rechner ggf. neu aufsetzen. Technische Hilfe und Tipps für den Fall, dass Sie schädliche Dateien bereits geöffnet und aktiviert haben, finden Sie auf den Seiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI).
- Suchen Sie regelmäßig nach Updates für Ihr Antivirenprogramm und Ihren Internetbrowser!

- Antworten Sie nicht auf diese E-Mails, auch wenn Sie sich darüber ärgern! Denn dadurch verraten Sie den Betrügern, dass diese E-Mail-Adresse regelmäßig genutzt wird.
- Sie könnten deswegen noch mehr Spam- und Phishing-Mails erhalten. Ignorieren Sie diese E-Mails und verschieben Sie die Schreiben einfach in den Spam-Ordner!
- Informieren Sie sich regelmäßig über die aktuellen Betrugsversuche in unserem Phishing-Radar! Wenn Sie genau wissen wollen, woher eine mutmaßliche Phishing-E-Mail kommt, können Sie den sogenannten Mail-Header prüfen.

Quelle: `www.bsi.de`

Die Internetseite, auf die der Link führt, sieht der Internetseite der Bank sehr ähnlich, selbst die Eingabeformulare sehen gleich aus. Die Phishing-Betrüger nutzen darüber hinaus entweder Internetadressen, die sich nur geringfügig von denen der renommierten Firmen unterscheiden. Oder aber sie fälschen die Adressleiste des Browsers mit einem JavaScript. Man glaubt also, man sei auf einer seriösen Seite, ist es aber nicht. Seriöse Banken verschlüsseln ihre Seiten immer, erkennbar am »https« in der Adresszeile des Browsers.

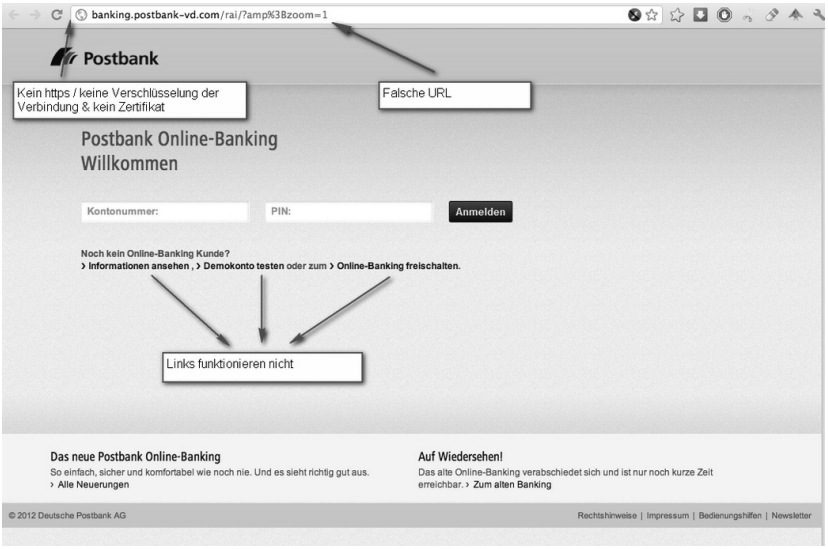


Abb. 1.7: Auf der Seite von `blog.botfrei.de` ist ein Beispiel für eine falsche Seite der Postbank –vor allem fehlt das »https«, der Hinweis auf eine verschlüsselte Seite.

1.5.2 Maßnahmen gegen Phishing

Ärger haben natürlich auch die Unternehmen, in deren Namen die Betrüger auftreten. Der Imageschaden kann riesig sein. Phishing zu bekämpfen ist schwer, da sich die gefälschten von den echten Seiten kaum unterscheiden und somit viele Nutzer sich täuschen lassen. In einigen Ländern haben sich viele Firmen bereits zur Anti-Phishing Working Group zusammengetan. Auf ihrer Internetseite kann man Phishing-Mails melden und nachlesen, welche schon bekannt sind.

Die oberste Regel: Aufpassen! Schauen Sie bei den angeklickten Internetadressen besser zweimal hin und überlegen Sie genau, wem Sie welche Daten anvertrauen.

Übrigens: Phishing ist nicht nur auf das Internet beschränkt – Datendiebe machen auch Jagd auf die Nutzer über das Telefon unter Verwendung von Internettelefonen (VoIP). Eine eigene Bezeichnung für diese neue Technik gibt es auch schon: *Vishing* (Voice Phishing).

1.6 Datenverluste

Sie kennen das: Sie haben vergessen, etwas zu speichern, und weg ist die schöne Präsentation. Wenn Sie aber ein Unternehmen haben, ist der Schaden bei Datenverlust ungleich höher. Denn sensible interne Informationen wie zum Beispiel Kundendaten gehören zu den besonders wichtigen Unternehmenswerten.

Datenverlust durch Datenklau bei dem Finanzdienstleister AWD oder SchülerVZ sind zwei Beispiele. Und trotz eines hohen technischen Sicherheitsniveaus durch Firewalls, Viren- und Spam-Kontrolle nimmt nach Einschätzung von TÜV-Rheinland-Experten der Datenklau in deutschen Unternehmen kontinuierlich zu. Längst bieten rein technische Schutzmaßnahmen keine ausreichende Sicherheit mehr vor Datendiebstahl durch Mitarbeiter oder Hackerattacken von außen.

Eine geeignete Verschlüsselung oder ein Backup – eine Datensicherung – auf anderen Geräten sind zum Beispiel vorsorgende Maßnahmen.

1.7 Täuschen, erschrecken, nerven

Scareware (engl.: to »scare« – erschrecken) funktioniert nach einem einfachen Prinzip: Sie gaukelt dem Benutzer eine Virusinfektion seines Computers vor und bietet dabei meist an, dieses vermeintliche Virus gleich unschädlich zu machen. So weit, so gut, doch nun behauptet das Programm, dass das Entfernen des Virus nur mit der kostenpflichtigen Vollversion des Programms möglich sei. Der Nutzer wird durch den Virusalarm eingeschüchtert und kauft das Programm. Wurde die kostenpflichtige Version des vermeintlichen Antivirenprogramms gekauft, entfernt es zwar die Virenwarnung, und der Nutzer ist beruhigt. Leider ist diese Software meist vollkommen wirkungslos gegen andere Schadprogramme.

In den meisten Fällen ist es jedoch so, dass die fraglichen Webseiten derart präpariert sind, dass sie gleich beim Besuch via Drive-by-Download Malware ins System einschleusen, die Ihnen vorgaukelt, Ihr Computer sei hochgradig virenverseucht. So gibt es beispielsweise Scareware, die gezielt den Taskmanager von Windows manipuliert und dort falsche Informationen anzeigt.

1.7.1 Der Trick mit dem Callcenter

Laut dem Magazin C't gehen manche Autoren von Scareware inzwischen noch einen Schritt weiter. Die falsche Antivirensoftware bekommt sogar ein angeblich seriöses Callcenter für ihre Opfer. Als Betroffener ist man ohnehin schon völlig verunsichert. Ruft man dort an, um Hilfe bei der Installation der vermeintlichen Sicherheitssoftware zu bekommen, erhält man eine Schritt-für-Schritt-Anleitung, wie die bereits installierte (also die echte) Antivirensoftware deinstalliert werden kann, um die Scareware erfolgreich aufzuspielen.

Diese Schadprogramme sind die anfangs erwähnten Trojaner wie etwa der Bundespolizei. Auf solche Erpressungsversuche sollten sich Nutzer auf gar keinen Fall einlassen. Wichtig ist, dass die Antivirenprogramme und die Firewall auf dem neuesten Stand sind.

1.8 Spam

Spam ist nach Aussagen von BITKOM das einzige Cybercrime-Phänomen, das tendenziell abnimmt. Allerdings sind immer noch rund 90 Prozent aller E-Mails Spam. Wohl jeder, der eine E-Mail-Adresse hat, dürfte schon die berühmten »Viagra«-Spam-Mails bekommen haben. Wie eine Analyse des Sicherheitsdienstleisters Sophos zeigt, lohnt sich die Werbeflut für die Anbieter: »Pharma-Spam« soll mindestens 4.000 Dollar Umsatz pro Tag erwirtschaften. Auch wenn es nur wenige sind, die tatsächlich auf die Angebote in Spam-Mails eingehen und ein Produkt kaufen, werden doch täglich Millionen E-Mail-Postfächer mit Werbemüll überschüttet.

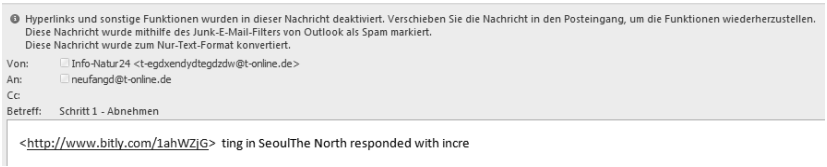


Abb. 1.8: Beispiel für eine Spam-Nachricht. Klickt man auf den Link, kann man sich Schadsoftware auf den Rechner laden.

Neu ist auch diese Masche: Eine gefälschte Dropbox-Einladung verlinkt auf eine Medikamenten-Webseite. Der Onlinespeicherdienst Dropbox hat nach Informa-

tionen des deutschen E-Mail-Sicherheitsdienstleisters Eleven Ende Mai 2013 zahlreiche Mails versendet, die eine vermeintliche Einladung zu Dropbox enthielten, am Ende landete man auf einer Seite, die Medikamente verkaufen will.

Abb. 1.9: Diese falsche Spam-Nachricht bei Dropbox führte beim Klick auf den Link zu einer Medikamenten-Webseite. Bildquelle: Eleven Security Blog

Dank immer besserer Spam-Filter der E-Mail-Provider geht die Zahl der Spam-Nachrichten zurück. Dennoch sollte man auch in Zukunft besonders vorsichtig sein bei E-Mails mit verlockenden Angeboten, da weiterhin gefährliche Schadsoftware in Spam-Mails enthalten ist. Sie sollten keine Mails unbekannter Herkunft öffnen und auch bei Nachrichten von bekannten Onlinediensten genau hinschauen. Und das sollten Sie auch mit Ihren Kindern ausführlich besprechen.

1.9 Fantastilliarden von Datenspuren

Wie viele Daten gibt es und wie schnell vervielfachen sie sich? Indem ich dieses Buch schreibe, dann Mails versende, mit meinen Kindern über WhatsApp kommuniziere und für meine Daten auch noch einen Cloud-Dienst benötige, trage ich, wie Milliarden anderer Menschen, jede Minute zu mehr Daten bei. Das kann man (noch) in Zahlen ausdrücken. Die Menschheit verfügte zu Beginn des Jahres 2013 über ein weltweit gespeichertes Datenvolumen von über zwei Zettabyte (das ist eine 2 mit 21 Nullen oder zwei Trilliarden Byte). Doch das ist, so erklärt der Verband der deutschen Internetwirtschaft eco auf seinem Jahreskongress am 6. Mai 2013 in Köln, erst der Anfang beim Sammeln unvorstellbar großer Datenmengen. »Durch die eichhörnchenartige Sammelwut der Menschen, potenziert durch die allgegenwärtige Digitalisierung, wird sich die weltweite Datenmenge alle zwei Jahre verdoppeln und dadurch Datenberge in Fantastilliardenhöhe erzeugen«, sagt Dr. Béla Waldhauser, Leiter der Kompetenzgruppe (KG) Datacenter Infra-

struktur im eco-Verband, zum Trend »Big Data«. Um das zu veranschaulichen, stellen Sie sich den aktuellen Datenbestand der Menschheit auf iPads gespeichert und gestapelt vor, das ergäbe ein Bauwerk, das etwa genauso lang wie die Chinesische Mauer wäre, also mehr als 21.000 Kilometer!

Bei allem, was Sie online tun, hinterlassen Sie Daten. Das merken Sie recht schnell, wenn Sie zum Beispiel bei Amazon bestimmte Bücher recherchiert haben. Bei Ihrem nächsten Besuch werden Ihnen diese Bücher und weitere Vorschläge aus dem Themenbereich angezeigt – alles, ohne dass Sie bei Amazon überhaupt eingeloggt sind. Sind Sie bei Facebook und »liken« Sie bestimmte Dinge? Garantiert bekommen Sie innerhalb weniger Tage passende Werbung dazu angezeigt. Dazu erfahren Sie mehr in Kapitel 3.

Hinweis

Zum Onlineverhalten hat BITKOM 2011 eine Studie publiziert: Häufig werden Onlineprofile sowohl aus privaten als auch aus beruflichen Gründen veröffentlicht.

»Gut jeder zweite Internetnutzer macht davon Gebrauch, wobei es hier deutliche Unterschiede zwischen den Altersgruppen gibt. Mehr als drei Viertel (78 Prozent) der 14- bis 29-Jährigen stellen Angaben zu ihrer Person online. 30- bis 49-Jährige tun dies zu 53 Prozent, 50- bis 64-Jährige zu 33 Prozent und über 65-Jährige nur noch zu 23 Prozent. Mit deutlichem Abstand (48 Prozent) werden soziale Netzwerke am häufigsten für die Erstellung von Onlineprofilen genutzt. Besonders aktiv sind hier Internetnutzer zwischen 14 und 29 Jahren. Etwa drei Viertel von ihnen (74 Prozent) geben persönliche Informationen über soziale Netzwerke preis. Mit steigendem Alter sinkt die Nutzung kontinuierlich ab, bleibt aber im Vergleich zu anderen Möglichkeiten, wie Blogs oder eigenen Homepages, auf hohem Niveau. Immerhin jeder Fünfte über 65-Jährige (19 Prozent) stellt über soziale Netzwerke persönliche Angaben von sich online. Im Vergleich zwischen den Geschlechtern nutzen Frauen soziale Netzwerke etwas häufiger als Männer zur Veröffentlichung persönlicher Angaben (50 Prozent vs. 46 Prozent).«

Quelle: Datenschutz im Internet – Eine repräsentative Untersuchung zum Thema Daten im Internet aus Nutzersicht, BITKOM, 2011

Jeder Website-Betreiber hat ein Interesse daran herauszufinden, wie viele Besucher sich auf seinen Seiten bewegen. Anhand der IP-Adresse kann er zum Beispiel sehen, wie lange die Seite und welche Inhalte konkret besucht wurden. Dieselben Informationen haben zum Beispiel Onlinezeitungen oder Diensteanbieter wie Facebook oder auch Suchmaschinen und E-Mail-Dienste wie Google.

Abb. 1.10: Ein Video des Verbraucherministeriums zum Thema Datenspuren informiert Jugendliche zum bewussteren Umgang mit ihren Daten.

Tipp

Jedes Unternehmen und jede Behörde muss Ihnen auf Ihre Anfrage hin sämtliche Daten, die über Sie gespeichert sind, schriftlich nennen. Das regelt § 34 des Bundesdatenschutzgesetzes. Mehr dazu finden Sie in Kapitel 11.

1.9.1 Quantify yourself – gezählt, gewogen, gemessen

Noch so ein neuer englischsprachiger Begriff: *Quantified-Self-Dienste*. Solche Dienste erfassen und werten persönliche gesundheitsbezogene Daten aus. Meist in Form von Apps auf dem Smartphone helfen sie, die körperliche Fitness zu steigern, oder beim Abnehmen – und gerade hier sind gesundheitsbewusste Jugendliche angesprochen, die mit dem coolen Smartphone alles steuern lassen.

Ein einfaches Beispiel: Nike bietet eine einfach und gut gemachte kostenlose App an, die das Laufverhalten dokumentiert. Man speichert das Programm auf dem

Smartphone und aktiviert GPS und läuft los – die gesamte Strecke wird aufgezeichnet, und man weiß genau, wie viele Kilometer man in welcher Zeit gelaufen ist. Das wird perfekt grafisch aufbereitet und macht zugegebenermaßen Spaß. Ich gebe ein paar persönliche Daten wie mein Gewicht ein, und schon misst die App gleich meinen Kalorienverbrauch beim Laufen. Wäre ich jetzt 14 Jahre alt, hätte ich das dringende Bedürfnis, meine tollen Joggingrunden mit anderen zu teilen.

Abb. 1.11: Die Running-App von Nike

Wenn ich meine Daten bei `Nikeplus.de` speichern will, richtet Nike mir sogar ein Konto ein. In den Datenschutzbestimmungen, die unter den Einstellungen der App zu finden sind, steht übrigens, dass Nike meine »persönlichen Informationen, die ich aktiv an die Nike EU-Website oder andere Nike-Websites übermittelt habe, in der zentralen Nike-Datenbank in den USA speichern« wird.

Es gibt andere Quantified-Self-Apps, die entweder per GPS oder durch kleine mit Bewegungssensoren versehene Geräte – Armbänder, Brust- oder Pulsgurte – versendet werden. Jede Aktivität oder auch das Nichtstun werden gespeichert und analysiert. Diese Daten können auf dem eigenen Computer gespeichert werden. So entstehen Trainingsprogramme. Als Nutzer kann man sich zu den Themen dann in Foren und Blogs mit anderen Usern austauschen, Fotos und Rezepte posten und Tipps geben.

Die Webseite »Surfer haben Rechte« (`www.surfer-haben-Rechte.de`) kritisiert diese Dienste im Hinblick auf den Datenschutz, da diese nur funktionieren, wenn man persönliche, teilweise höchst sensible Daten eingibt. Diese Daten verbleiben nämlich nicht auf Ihrem Rechner, wenn Sie Auswertungen brauchen oder Ihre Erkenntnisse teilen. Sie werden auf den Servern der Anbieter oder in einer Cloud gespeichert – vermutlich unverschlüsselt.

Diese Daten können in die falschen Hände geraten, wenn sie Hackerangriffen zum Opfer fallen. Der Verbraucherzentrale Bundesverband e. V. (vzbv) hat Quantified-Self-Dienste stichprobenartig untersucht. Die Anbieter räumen sich »in ihren Allgemeinen Geschäftsbedingungen und Datenschutzbestimmungen umfassende Rechte hinsichtlich der Nutzerdaten« ein, etwa die Nutzung für Werbezwecke.

> *Aus körper- und gesundheitsbezogenen Daten in Kombination mit bestimmten Verhaltensmustern lassen sich sehr genaue Rückschlüsse auf die jeweilige Person ziehen. Dass der 35-jährige Hans Müller aus Hamburg, der mit seinem Samsung-Handy mit der Gerätekennung 12341a5b6c7890 und dem Betriebssystem Android 4.2 über das Mobilfunknetz der Telekom telefoniert und im Internet surft und jeden Morgen bei einem Pulsschlag von 130 seine 10 Kilometer an der Alster entlangjoggt, um weitere 5 Kilogramm an Gewicht zu verlieren und seinen Body-Mass-Index von 30 weiter zu reduzieren, ist nicht nur für den eigenen Diensteanbieter von Interesse, sondern weckt unter Umständen auch Begehrlichkeiten Dritter, wie Werbeunternehmen, Krankenkassen oder Versicherungen.*
>
> *Quelle: www.surfer-haben-rechte.de*

Sie sollten sich dazu einmal die Checkliste auf der oben genannten Webseite ansehen.

Vorsicht

Und dann auch noch PRISM!

PRISM ist ein seit 2007 bestehendes, als streng geheim eingestuftes und von der amerikanischen National Security Agency (NSA) geführtes Programm zur Überwachung und Auswertung von elektronischen Medien und elektronisch gespeicherten Daten. Laut einer zuerst von der Washington Post und dem britischen Guardian im Juni 2013 veröffentlichten Präsentation sind an dem Programm neun der größten Internetkonzerne und Dienste der USA beteiligt: Microsoft (u.a. mit Skype), Google (u.a. mit YouTube), Facebook, Yahoo!, Apple, AOL und Paltalk. Die Diskussionen dazu sind in vollem Gange. Unter `www.prism-break.org` finden Sie Hinweise, welche Software und Onlinedienste Sie nutzen können, wenn Sie sich nicht ausspionieren lassen wollen.

1.10 Zusammenfassung

Dieses erste Kapitel hat Ihnen einen groben Überblick über die wichtigsten Gefahren im Netz gegeben. Von Spam, Viren und Trojanern haben Sie wahrscheinlich schon gehört, andere, neue Gefahren werden nicht zuletzt dank des Internets schnell bekannt gemacht.

Wie anfällig ein Smartphone für Attacken aus dem Netz ist, wissen vor allem die Kinder nicht, die ohne ihr Handy kaum leben können. Ihren Rechner – das sehen Sie im nächsten Kapitel, können Sie für Ihre Kinder sicher machen, beim Handy wird es schwieriger, weil Sie kaum Zugriff darauf haben. Zu den Sicherheitseinstellungen der Smartphones kommen wir in Kapitel 8.

Wichtig für Sie als Erziehungsberechtigte ist, sich der aktuellen und potenziellen Gefahren bewusst zu sein. Noch wichtiger ist, dass Sie sich mit Ihren Kindern zusammensetzen und über die Gefahren sprechen.