Informationen zur Sicherheit im Internet

1. Zunächst einmal möchte ich auf die durchaus konkrete Gefahr hinweisen, dass der Gebrauch des Internets, besonders das Surfen, das Chatten, das Spielen (letzteres natürlich nicht nur im Internet, sondern allgemein), **süchtig** machen kann, und zwar so, dass diese Sucht der ärztlichen Behandlung bedarf. Drei Stunden pro Tag im Internet (sofern es sich nicht um Recherchen oder andere seriöse, sinnvolle Tätigkeiten handelt) werden als zulässige Grenze angesehen. Was darüber hinaus geht, gilt bereits als krankhafte Sucht.

   Man muss im Übrigen auch an körperliche Konsequenzen denken: Ständiges Sitzen vor dem Bildschirm bedeutet Bewegungsmangel und es gibt Studien, die auf vermehrtes Auftreten von Infarkten oder auch Diabetes hindeuten. Dabei steht die Zahl von 40 000 Fällen im Raum, die jährlich dadurch bedingt sein können.

   Auch soziale Folgen sind bedenklich: Soziale Kontakte über das Internet können zwar durchaus ihren Wert haben, aber auch Gefahren, weil es Erwachsene gibt, die solche Kontakte knüpfen, sich dabei ggf. als Gleichaltrige ausgeben und dabei ganz eindeutige Ziele verfolgen.

   Außerdem können Kontakte über das Internet doch nicht echte soziale Kontakte ersetzen, bei denen man sich trifft und **direkt** interagiert.

   Und was die Computerspiele betrifft, so wundere ich mich immer wieder, wenn manche Psychologen behaupten, die dabei auftretende Gewalt (Schlagen, Töten) sei nicht schädlich. Ich bin völlig davon überzeugt, dass da zumindest die Hemmschwelle herabgesetzt wird.

   Windows 8 bietet jetzt die Möglichkeit „Family Safety“ an, eine Administrationsoberfläche, die es den Eltern ermöglicht, „Onlinezeiten“ einzurichten und eine „White- bzw. Blacklist“ zu hinterlegen. Dann kann das Kind nur geeignete Inhalte anschauen und auch dies nur in einem definierten Zeitraum.

   Ich habe seinerzeit, als meine Kinder im „gefährlichen“ Alter waren, in ihren Computer einen Betriebsstundenzähler eingebaut, der mir eine Kontrolle ermöglichte.

2. Es wird ja jeder wissen, dass es mehr als fahrlässig wäre, mit einem Computer ohne entsprechende Sicherheits-Software ins Internet zu gehen. Dabei genügt

ein einfacher **Virenscanner** nicht; es muss heutzutage schon auch eine „**Firewall“** dabei sein.

Viren wurden früher in erster Linie beim Öffnen von Anhängen verbreitet (Anhänge mit der Dateiendung .exe, früher auch .bat, .com – das sind sog. ausführbare Dateien, wobei heutzutage das .exe schon von Windows ausgeblendet wird, man kann aber durch eine entspr. Anderung in den Dateioptionen in der Systemsteuerung die Endung anzeigen lassen). Wer solche Dateien öffnet, ohne genau zu wissen, dass die Mail aus einer 100%ig verlässlichen Quelle kommt, lebt mehr als gefährlich.

Leider kann man sich seit langem schon Viren auch durch den bloßen Besuch von Webseiten einhandeln, und das müssen auch keineswegs als „gefährlich“ bekannte Webseiten sein. Da hilft also nur ein ständig aktualisierter Virenscanner. Man darf sich, zumindest wenn man noch Windows XP verwendet, auch nicht auf eine dort eingebaute Firewall verlassen, sondern braucht eine eigene, verlässliche Software. Heutzutage werden Komplettpakete („Internet Security“) angeboten und man kann sich durch einfaches „Googeln“ informieren, welche in den letzten Tests als gut bewertet wurde.

Sehr wichtig ist auch die regelmäßige Aktualisierung der Computersoftware durch „Patches“, die neu entdeckte Sicherheitslücken schließen, mit denen Kriminelle in ihren Computer „eindringen“ können. Das betrifft das Betriebssystem, z.B. Windows, aber auch andere Programme wie Media Player, den Adobe Reader, Adobe Flash Player, Java Update etc.

Wenn man also aufgefordert wird, diese Updates zu installieren, sollte man es unbedingt tun, aber auch sicher sein, dass die Nachricht wirklich von diesem Anbieter kommt. Das zu prüfen, ist sicher nicht immer einfach, aber vielleicht kommt einem ein Logo etwas komisch vor oder aber man erkennt, dass die Nachricht gar nicht von der echten Adresse herkommt.

Wie wichtig solche Updates sind, wurde erst jetzt wieder besonders deutlich, als Benutzer von *„Fritzbox“* Routern aufgefordert wurden, unbedingt ein Update herunter zu laden, weil durch eine Sicherheitslücke bereits in der Box, also **noch vor** dem Computer, Schadcodes installiert werden können, die z.B. alle Kennworteingaben abfangen. Da nützt auch ein Virenscanner oder eine Firewall nichts, weil es ja schon außerhalb des Computers passiert. Hier ist ein Schutz also wirklich nur durch das Herunterladen des „Patch“ möglich.

Ansonsten hilft gegen das Eindringen in den Computer eben die **Firewall**, die man auch unbedingt haben sollte. So ist man z.B. gegen Trojaner, die

eingeschleust werden können und im Computer ein zerstörerisches oder sonstwie kriminelles Eigenleben entwickeln, wenigstens einigermaßen geschützt.

Es gibt da z.B. neuerdings die „**ZIP-Trojaner“,** welche als Dateianhang einer E-Mail beigefügt sind. Meist handelt es sich hier um vermeintliche Rechnungen der Telekom, Abmahnschreiben diverser Rechtsanwälte usw., die suggerieren, dass man einen höheren Rechnungsbetrag zu begleichen hätte. Näheres hierzu sei aus der Anlage „Rechnung.zip“ ersichtlich. Beim Klick installiert man sich einen Trojaner, der den Rechner sperrt und den Nutzer zur Zahlung eines Betrages nötigt. Bei Nichtzahlung ist eine PC Nutzung nicht mehr ohne Weiteres möglich. Diese Situation kann meist nur mit einem erheblichen Aufwand bereinigt werden.

Bekanntlich ist es ja sogar möglich, dass Cyber-Kriminelle Ihren Computer durch einen Angriff von außen praktisch „übernehmen“ , von diesem aus ihre kriminellen Aktivitäten verbreiten und am Ende sieht es so aus, als seien Sie selbst der Urheber der kriminellen Aktivität gewesen und es kann gegen Sie ermittelt werden!

3. Dass es immer noch Menschen gibt, die auf „**Phishing“** hereinfallen, obwohl schon seit Jahren regelmäßig davor gewarnt wird, ist ersataunlich. Der bekannteste Fall ist der, wo man durch eine E-Mail dazu aufgefordert wird, seine Zugangsdaten für das Computer-Banking einschließlich PIN sowie eine oder mehrere TANs zu senden und zwar unter dem Vorwand, dass man damit z.B. eine Sicherheitsüberprüfung ermögliche.

   Das Gemeine ist, dass die Täter es oft schaffen, ihre Mail ziemlich echt aussehen zu lassen (mit dem Logo der Bank). Aber man sollte bedenken, dass Ihre Bank meist gar nicht Ihre E-Mail Adresse hat und auf gar keinen Fall würde sie jemals von Ihnen die Bekanntgabe von PIN und TAN fordern, außer Sie sind gerade dabei, eine Überweisung vorzunehmen

   Eine neuere Erscheinung ist nun das sog. **Pharming.** Der Rechner wird hierzu im Vorfeld mit einem Schadcode infiziert und leitet den Nutzer automatisch auf eine gefälschte Bankseite, wo der Kunde dann seine Zugangsdaten und Zahlungsfreigabedaten (iTAN) eingibt. Im Hintergrund werden die Zahlungsempfängerdaten und der Betrag geändert und der Kunde gibt somit eine ganz andere Zahlung frei. Richtiger Schutz ist hier nur durch einen aktuellen Virenschutz und eine richtig eingestellte Firewall möglich.

4. Wichtig (gerade bei Kindern) ist, dass bei beliebten Internet-Angeboten wie z.B. Klingeltönen (ohnehin sehr fragwürdig), Spielen oder Ähnlichem vor dem Herunterladen das **Kleingedruckte** genau gelesen wird. Mir ist es selbst vor

Jahren einmal passiert, dass ich das versäumt und für eine eigentlich kostenlose Software einen abzockerischen „Download-Dienst“ genommen habe, der mir dann sofort 70 Euro in Rechnung gestellt hat. Nach der heutigen Rechtsprechung sind Anbieter aber auch verpflichtet, **deutlich** auf entstehende Kosten hinzuweisen; ein Hinweis im Kleingedruckten genügt nicht.

Es gibt auch Dienste, die überhaupt nicht auf entstehende Kosten hinweisen, was natürlich illegal ist. Wenn man dann zum Bezahlen aufgefordert wird, ist man allerdings geschützt; man braucht also nicht zu bezahlen, auch wenn noch so wüste Drohungen von „Geldeintreibern“ kommen. Man kann da auch die Hilfe von Verbraucherzentralen in Anspruch nehmen.

Übrigens führt auch manchmal das Anschauens eines legalen Videostreams zu Zahlungsaufforderungen seitens bestimmter Anwaltsbüros (es gibt etliche, die auf so etwas regelrecht spezialisiert und ständig auf der Suche nach angeblichen Missetätern sind). Das ist unberechtigt, denn erst das weitere Verbreiten wäre ungesetzlich.

Überhaupt ist es oft gut, sich bei allen möglichen Anbietern, z.B. beim Einkauf von Waren per Internet, sich von der Seriosität der Firmen zu überzeugen, z.B. auf den Foren, die man leicht durch Eingabe des Namens bei Google o.ä findet. Oft wird vor Vorauszahlungen gewarnt. Ich habe das in der Vergangenheit schon des öfteren gemacht, mich aber vorher über den guten Ruf der Firma informiert und es war dann auch alles in Ordnung.

5. Da ich selbst Mitglied bei Facebook bin, wundere ich mich manchmal, wie sorglos Beiträge gepostet werden, die dem guten Ruf des Betreffenden nicht gerade dienlich sind, z.B. die Organisation eines „Saufgelages“ o.Ä. Einmal habe ich einen Abiturienten eindringlich gewarnt, der sich durch so etwas in ein wirklich schlechtes Licht gerückt hatte (z.B. bei potenziellen Arbeitgebern, die ja auch angeblich regelmäßig Facebook u.Ä. durchforsten). Die Antwort war dann: „Das ist mir wurscht!“

6. Besonders ist auch vor sorglosem Umgang mit Fotos zu warnen, was naturgemäß vor allem Mädchen betrifft. Immer wieder liest man, dass Fotos in allzu leichter Bekleidung ins Netz gestellt werden. Manche finden das „cool“, andere lassen sich z.B. durch ihren Freund erpressen . Wenn man bedenkt, wie leicht man heutzutage ziemlich perfekte Fotomontagen machen kann, indem man den Kopf einer/eines X-beliebigen auf einen nackten Körper setzt, dann ist das Posten von Fotos schon problematisch und es wird z.B. empfohlen, dass man eine niedrige Auflösung wählt, bei der eine evtl. Fotomontage eine so schlechte Qualität erhielte, dass sie uninteressant wäre.

7. <u>Urheberrecht</u>

Es gab – auch in jüngster Vergangenheit - immer wieder Schlagzeilen über angebliche wie auch wirkliche Verletzungen von Urheberrechten, die zu erheblichen finanziellen Forderungen durch Anwaltsbüros führten. Der Laie ist vielleicht nicht immer in der Lage, eventuelle urheberrechtliche Konsequenzen beim Herunterladen von Bildern, Filmen, Musik, Spiele-Software oder beim Kopieren von CDs oder DVDs einzuschätzen. Andererseits gab es schon Gerichtsurteile, in denen der Richter dem Beklagten vorwarf, er hätte erkennen müssen, dass ein Angebot, sich aus dem Internet etwas herunterzuladen (z. B. bei den beliebten TAUSCHBÖRSEN) gegen das Urheberrecht verstieß.

Bei **Filmen, Musik und Software** ist sicher besondere Vorsicht geboten, weil die Film- und Medienindustrie ein berechtigtes Interesse hat, gegen Diebstahl ihres Eigentums vorzugehen. Und als solcher ist ein illegales Herunterladen aus dem Internet anzusehen.

Andererseits gibt es auch jede Menge seriöser Firmen, die etwas kostenlos zum Herunterladen anbieten, so z.B. Computerzeitschriften, über deren Website man sich kostenlos Programme installieren kann. Finanziert wird das oft durch Werbung oder auch (leider!) dadurch, dass der Anbieter Ihre E-Mail-Adresse an einschlägige Firmen verkauft. Hinsichtlich des Kopierens von eigentlich urheberrechtlich geschützten CDs, DVDs usw. ist zu bemerken, dass das nicht grundsätzlich verboten ist. So ermöglichen die Paragrafen 53 und 54 des Urheberrechtsgesetzes Kopien zum privaten Gebrauch oder „sonstigen eigenen Gebrauch“, was auch die Weitergabe an Verwandte oder gute Freunde einschließt. Aber wohlgemerkt, es sind nur „einzelne“ Kopien erlaubt, wobei „einzeln“ nach einem Urteil des Bundesgerichtshofs von vor etwa vierzig Jahren „nicht mehr als sieben“ bedeutet. In jedem Fall ist aber ein Kopieren unter Umgehung des Kopierschutzes verboten, weswegen die gängigen Kopierprogramme das auch nicht gestatten, sondern den Kopiervorgang abbrechen. Zwar gibt es dann Software, die den Kopierschutz „knacken“, aber das ist auf jeden Fall illegal!

Es gab einen Fall, in welchem die minderjährige Tochter 7000 Lieder auf einer Tauschbörse heruntergeladen hat. Problematisch war in erster Linie hier nicht der eigentliche Download, sondern eher die Tatsache, dass die Tochter nicht wusste, dass sie im Falle eines Downloads diese Daten auch automatisch wieder anderen Nutzern zur Verfügung stellt und somit aktiv verbreitet. Dies ist im Übrigen der Sinn und Zweck von Tauschbörsen. Hat man z.B.10% eines Liedes auf einer Tauschbörse geladen, ermöglicht man automatisch anderen Nutzern sofort, genau diese 10% von zu laden. Der Streitwert wurde in diesem Fall auf 700.000 Euro festgelegt (1000 Euro pro Titel) und die Abmahnanwälte haben ein Vergleichangebot i.H.v. 7000 Euro unterbreitet, auf welches die Eltern eingegangen sind, da die Anwaltskosten bei dem angegebenen Streitwert wohl

höher gewesen wären. Dies zeigt deutlich, dass auch im Internet eine „Dummheit“ der Kinder oftmals auch schwerwiegende Konsequenzen für die Erziehungsberechtigten bedeuten kann.

8. Passwörter:

In der letzten Zeit wurde die Bedeutung der Passwörter besonders deutlich, nachdem 16 Millionen E-Mail Konten mit Passwort gehackt worden waren. Dadurch bestand die Gefahr, dass die Hacker auch auf andere Konten (z.B. Ebay, Amazon) Zugriff erhielten und Einkäufe tätigen konnten, zumal viele ein und dasselbe Passwort für mehrere Konten verwenden.

Man soll also verschiedene Passwörter nehmen, und zwar mindestens acht Zeichen, darunter Klein- und Großbuchstaben, Zahlen und Sonderzeichen.

Gestern kam im Fernsehen ein ganz guter Tipp für die Erstellung eines Passworts, das man sich auch merken kann – man nimmt einen Spruch, in dem auch Zahlen und Satzzeichen vorkommen und verwendet die Anfangsbuchstaben. Hier das Beispiel:

„Alles hat ein Ende, nur die Wurst hat zwei.“ Das ergibt also:

Ah1E,ndWh2.

Pegnitz, Februar 2014 Werner Dunst