GEFAHREN IM INTERNET

Das Internet ist zwar sehr praktisch und man kriegt viele Infos umsonst, für die man sonst teure Bücher kaufen müsste. Doch birgt das Internet leider auch viele Gefahren, denn häufig zielen vermeintliche Gratisangebote darauf ab, an irgendwelche persönliche Daten zu kommen oder dem Opfer Geld abzuknöpfen.

Von Viren und Würmern

Viren sind Teile von Programmen, die sich beim Start des Programms automatisch vermehren und weitere Dateien befallen. Dadurch werden Dateien zerstört, was zu Datenverlust führen oder sogar den ganzen Rechner lahmlegen kann. Würmer dringen aktiv durch Sicherheitslücken in den PC ein und Trojaner tarnen sich als nützliche Programme, spionieren Daten wie z.B. Passwörter oder E-Mail-Adressen aus und können sich so sogar per E-Mail an alle gespeicherten E-Mailadressen weiterverschicken.

Vorsicht geboten ist besonders bei ausführbaren Dateien und Programmen mit Endungen wie „.exe“. Da auf modernen Betriebssystemen standartmässig diese Endungen ausgeblendet werden, können solche .exe-Dateien auch als Bild oder Musikdatei getarnt auftauchen: Das schädliche Programm mit dem Namen „virus.mp3.exe“ wird also nur als „virus.mp3“ angezeigt und sieht somit wie eine harmlose Musikdatei aus.

“Schädliche Software ist häufig als nützliches Gratisprogramm getarnt“

Solche Schädlinge können in Programmen wie etwa Spielen aus dem Internet enthalten sein oder man kriegt sie als Foto getarnt per E-Mail zugeschickt (auch von Freunden, deren PC verseucht ist und selbstständig Mails verschickt) oder man lädt sie in Tauschbörsen oder anderen Downloadportalen z.B. als Mp3-Dateien getarnt herunter. Manchmal wird das Opfer auch per E-Mail aufgefordert, auf einen Link zu klicken, bei dem dann eine schädliche Software herunterlädt. Vorsicht also bei Gratis-Downloads wie Spielen, Hilfsprogrammen, Musikdateien...!

Als Schutzmassnahmen kann man Antivirenprogramme installieren (und unbedingt regelmässig updaten). Eine aktivierte Firewall schützt hingegen vor Würmern. Das automatische Ausblenden von Dateiendungen sollte man besser deaktivieren (unter Systemsteuerung: Ordneroptionen: Ansicht), gleiches gilt auch für die Autostartfunktion bei Datenträgern. Software und Betriebssysteme sollten immer up to date sein und vorinstallierte Programme wie Internet Explorer oder Outlook Express sollte man meiden, denn gerade die meistverbreitete Software ist besonders anfällig auf Schädlinge.

„Kostenlose Dienstleistungen dienen dazu, an persönliche Daten zu kommen“

Immer mehr Internetdienste sind werbefinanziert. Facebook, Google & Co aber auch Seiten mit Musikstreaming, Songtexten etc. **finanzieren sich über Werbung**. Facebook oder Google werten Benutzerdaten aus um dem Benutzer passende Werbung anzuzeigen. Wenn dieser dann das beworbene Produkt kauft, zahlt er indirekt die Benutzung des Internetdienstes. Das klingt ja eigentlich ganz praktisch.

Es gibt aber auch Internetdienste, bei denen man bei der Anmeldung ein teures Abo löst. Der Hinweis darauf steht natürlich irgendwo im Kleingedruckten versteckt. Da man bei der Anmeldung Adresse etc. angeben muss, kriegt man dann plötzlich eine happige Rechnung zugeschickt.

Die Adressendaten und E-Mailadressen die man z.B. für die Teilnahme bei Gewinnspielen angeben muss, wird meistens für Werbezwecke gebraucht. Was folgt ist eine Flut von Newslettern, Spam- und Werbemails. Wenn die Werbung an den Empfänger adressiert ist, nützt auch der Anti-Werbung-Kleber am Briefkasten nichts mehr.

Vorsicht geboten ist immer dann, wenn man sich für die Nutzung eines Angebotes registrieren und persönliche Daten angeben muss. Am besten **liest man hier immer die AGBs** genau durch und nimmt den Hacken bei „Newsletter abonnieren" raus. Das Konsumentenmagazin K-Tipp bietet eine ganze Warnliste mit Links zu Abo-Fallen, welche man meiden sollte. Darunter sind auch einige Songtext-Seiten.

„Damit wir Ihnen den Gewinn auszahlen können, benötigen wir Ihre Kreditkartennummer"

Immer häufiger kriegt man per Post oder E-Mail die Nachricht, dass man etwas gewonnen hätte. Um den Gewinn abzuholen muss man irgendetwas vorauszahlen, persönliche Daten wie Kreditkartennummer angeben oder an einen Ort reisen, an dem einem teurer Mist aufgeschwatzt wird (Werbefahrt). Auf einer Internetseite mit Songtexten meldet dem User z.B. ein Pop-Up, dass er als 999'999. Besucher eine Kreuzfahrt gewonnen habe und sofort auf die eingeblendete (vermutlich sogar teure) Rufnummer anrufen soll. Am Telefon wird ihm dann erklärt, dass er für den Weg zum Hafen ein Auto mieten müsse und dass sie nun deshalb als Sicherheit seine Kreditkartennummer benötigten. Doch wer sagt ihm, wer am anderen Ende dieses Telefons sitzt und was dieser in Wirklichkeit mit seiner Kreditkartennummer vor hat? Ausserdem taucht das gleiche Pop-Up beim nächsten Besuch dieser Seite auf wieder auf.

Vorsicht also bei Gewinnen, bei denen man etwas vorauszahlen, irgendwo hinfahren, heikle Daten angeben oder eine teure Rufnummer (z.B. 0900er Nummer mit 4Fr. pro Minute) anrufen muss.

„Wer einmal persönliche Daten ins Internet stellt, kriegt sie da so schnell nicht mehr heraus"

Viele Internetdienste sammeln Daten von uns. Gerade in sozialen Netzwerken landen viele persönliche Infos wie Alter, Interessen, Fotos, Adressen, persönliche Meinungen… Doch was ist daran gefährlich?

Mobbing: Fotos oder peinliche Informationen können für Cyber-Mobbing missbraucht werden. Plötzlich taucht das Portrait aus dem Facebook-Profil einer glücklich verheirateten Frau in einer gefälschten Kontaktanzeige auf. Was wohl der Ehemann dazu meint?

Schlechter Eindruck bei der Bewerbung: Immer mehr Arbeitgeber suchen im Internet nach Infos zu ihren Bewerbern. Peinlich, wenn da Bilder eines betrunkenen Bewerbers von seiner letzten Party auftauchen. Sind Bilder mal im Internet, kriegt man sie manchmal gar nicht mehr so leicht wieder

raus. Bei Suchmaschinen bleiben nämlich auch alte Suchergebnisse lange gespeichert.

Spam-Mails: Adressen und E-Mail-Adressen können für Spam- und Pishing-Attacken missbraucht werden. Plötzlich bekommt fragt einen die Bank per E-Mail nach Kontodaten und Kennwörtern. Das Mail stammt natürlich nicht von der Bank sondern von Betrügern, welche die Mailadresse kennen und wissen, bei welcher Bank das Opfer Kunde ist. Sehr häufig werden E-Mailadressen für Werbung gebraucht.

Kontoplünderung: Passwörter und Kreditkartendaten können dazu verwendet werden, Konten zu plündern, Benutzerkonten nach weiteren Daten auszuspionieren oder im Namen der Opfer Unsinn zu treiben.

Ortsangaben und Feriengrüsse: Wenn ein Einbrecher z.B. auf Facebook sieht, dass der Bewohner von Mustergasse 77 in Musterhausen momentan in den Ferien weilt, weiss er genau, wo er als nächstes einbrechen kann. Und die hübsche Dame im 2. Stock des Hauses ist alleine zuhause, gehen wir die doch mal besuchen.

Bettelbriefe: Hat ein Betrüger erstmal Zugriff auf den E-Mail-Account seines Opfers, findet er dort viele interessante Informationen zur Person, Adressen von Bekannten und Passwörtern. Er kann im Namen seines Opfers E-Mails verschicken. Z.B. ein solches: Hallo Franz, mein bester Freund, ich habe ein kleines Problem. Mir ist da in den Ferien das Geld geklaut worden. Könntest du nicht schnell 1000.- auf Konto xxxx überweisen, muss eben das Ticket für die Rückfahrt noch bezahlen, denn das wurde auch geklaut. Man sieht sich, deine liebe Lissi.

Wer Bettelbriefe von Verwandten oder Freunden bekommt ruft diese besser persönlich an, um sicherzustellen, dass der Brief auch wirklich von ihnen stammt. Auch hinter Bettelbriefen von irgendwelchen armen Leuten aus Osteuropa stecken häufig ganze Mafia-Banden.

„Kein gesetzliches Widerrufsrecht bei Internetkäufen in der Schweiz“

Dass man Überraschungen erleben kann, wenn man im Versandhandel Dinge bestellt, ohne sie vorher in den Händen gehalten zu haben, das dürfte mittlerweile jedem klar sein. Es gibt eben Dinge, die man vorher ausprobieren muss, bevor man sie kauft. Deshalb dürfen Produkte oft auch wieder zurückgeschickt werden. Aber längst nicht alle! Entsiegelte Datenträger, Zeitschriften, Frischwaren und Sonderanfertigungen werden normalerweise nicht zurückgenommen. Es bleibt auch die Frage, wer die Versandkosten bei einer Rücksendung bezahlt. Das gleiche gilt auch für das Einschicken zur Reparatur bei einem Garantiefall.

Es ist auf jeden Fall ratsam, vor der Bestellung die **allgemeinen Geschäftsbedingungen**, Liefer- und Garantiebedingungen sowie die Beschreibung des Artikels genau anzuschauen. Ein gesetzliches Widerrufsrecht bei Internetkaufverträgen besteht in der Schweiz (im Gegensatz zu Deutschland) nämlich nicht.

Aufgepasst werden muss auch bei der Bezahlung – besonders ins Ausland. Bei Zahlungen müssen die Bankangaben stimmen, am besten benutzt man die internationale Bankkontonummer IBAN. Ansonsten können Gebühren entstehen, welche die Bank dem Betrag einfach abzieht. Schlimmstenfalls kommt die Zahlung beim Empfänger gar nicht an oder wird dort nicht gefunden. So verschwinden auch gerne mal Vorauszahlungen irgendwo im grossen WWW.

Beim Eingeben der Zahlungsdaten sollte immer auf **verschlüsselte Übertragung** geachtet werden: in der Adresszeile des Browsers steht am Anfang dann https://. Weiter sollte man **sichere Passwörter** wählen. Ein solches besteht aus mindestens acht

Zeichen, Zahlen, Buchstaben und Sonderzeichen und sollte in keinem Wörterbuch vorkommen.

Um die **Seriosität eines Anbieters** zu überprüfen, achtet man am besten auf die Transparenz: Sind Identität des Anbieters und Geschäftsbedingungen gut ersichtlich?

Bei Bestellungen aus dem Ausland muss – je nach Betrag – mit Zollgebühren gerechnet werden. Der Sender muss die Mehrwertsteuer abziehen und das Paket wenn nötig richtig beschriften (z.B. Büchersendung) und eventuell einen Lieferschein mit dem Warenwert für den Zoll beilegen.

Links zum Thema:

http://de.wikipedia.org/wiki/Malware über verschiedene Schadsoftware und wie man sich davor schützt.

http://www.ktipp.ch/service/Warnlisten/InternetAbofallen.php Warnliste mit Abofallen des Konsumentenmagazins K-Tipp

http://www.kaufenmitverstand.de – Tipps zum sicheren Einkaufen im Internet (gilt für Deutschland)

www.e-commerce-guide.admin.ch – Infos des Bundes zum Thema Online Shopping (gilt für die Schweiz)