orell füssli

Norbert Pohlmann / Markus Linnemann

Sicher im Internet

Tipps und Tricks für das digitale Leben

Sicher im Internet
Norbert Pohlmann
Markus Linnemann
orell füssli

Ein Projekt vom Institut für Internet-Sicherheit:

securityNews: Kostenlose App für mehr Sicherheit im Netz

- Kostenlose App vom Institut für Internet-Sicherheit
- Aktuelle Sicherheitshinweise für Smartphone, Tablet, PC und Mac
- Warnung vor Sicherheitslücken in Standardsoftware, dank BSI-Schwachstellenampel
- Konkrete Anweisungen für Privatanwender und Unternehmen

» www.it-sicherheit.de

Available on the App Store

ANDROID APP ON Google play

Mit freundlicher Unterstützung

Bundesamt für Sicherheit in der Informationstechnik

Norbert Pohlmann/Markus Linnemann

Sicher im Internet
Tipps und Tricks
für das digitale Leben

Teil 3: Sicher bewegen im Internet –
Passwörter, E-Mail, Web 2.0

orell füssli Verlag AG

Sicher bewegen im Internet – So geht's

Im vorangegangenen Kapitel haben Sie bildlich gesprochen den Reifendruck Ihres Autos überprüft, die Scheinwerfer kontrolliert und den Sicherheitsgurt angelegt. Nun geht es darum, das Fahren auf der Autobahn, bei Nacht und in engen Gassen zu üben, damit Sie für alle Situationen gerüstet sind und stets sicher an Ihr Ziel gelangen. Auf das Internet übertragen heißt das, dass Sie in diesem Kapitel alles Wissenswerte zum richtigen Umgang mit den wichtigsten Internetdiensten und Sicherheitstechnologien erfahren.

Passwörter – von gestern bis morgen

Im Jahr 2008 wurde in einem britischen Unternehmen ein interessanter Versuch durchgeführt: Den Mitarbeitern wurde Schokolade im Tausch gegen ihr Zugangspasswort für das Firmennetz angeboten. Das Ergebnis: Je nach Geschlecht gingen 10 Prozent (Frauen) beziehungsweise 45 Prozent (Männer) der Befragten auf dieses Angebot ein. Die Mitarbeiter des Instituts für Internet-Sicherheit konnten das kaum glauben und beschlossen daher im Frühjahr 2009, ein ähnliches Experiment durchzuführen. Sie fragten unter einem Vorwand verschiedene Passanten in einer Fußgängerzone in Gelsenkirchen nach ihren Internetpasswörtern. Auch dieses

Ergebnis ist aus sicherheitstechnischer Sicht erschütternd: Mehr als 90 Prozent der Befragten gaben ihre persönlichen Passwörter preis, und mehr als 50 Prozent verrieten dazu sogar noch ihren (Benutzer-)Namen und die Internetdienste, für die sie ihre Passwörter verwenden. Dabei ist ein Passwort Ihr Schlüssel für die jeweilige Webseite. Und Sie würden Ihren Wohnungs- oder Autoschlüssel doch auch nicht gegen Schokolade tauschen, oder? Sicher nicht, wie das Ergebnis eines nachfolgenden Tests beweist: Bei der Frage nach dem Autoschlüssel war nämlich niemand bereit, diesen herauszugeben.

Passwörter und ihre Schlüsselfunktion

Damit ein Internetdienst, zum Beispiel ein E-Mail-Anbieter oder ein Onlineshop, feststellen kann, ob der anfragende Nutzer Zugang zu dem jeweiligen Dienst erlangen darf, muss sich dieser identifizieren und authentisieren. Die Identifikation ist die Überprüfung eines vorgelegten kennzeichnenden Merkmals, zum Beispiel des Benutzernamens oder der E-Mail-Adresse.

Der Begriff Authentikation bezeichnet einen Prozess, bei dem überprüft wird, ob jemand «echt» ist. Authentikation bedeutet also die Überprüfung der Echtheit beziehungsweise der Identität. Um eine Vergleichsmöglichkeit zu haben, muss diesem Vorgang eine Registrierung oder Anmeldung vorausgegangen sein. Das ist vergleichbar mit einer Passkontrolle. Und diese Kontrolle wird im Internet derzeit überwiegend mithilfe eines Passwortes durchgeführt. Erst wenn der Nutzer das richtige Passwort eingegeben hat, kann er den entsprechenden Internetdienst nutzen.

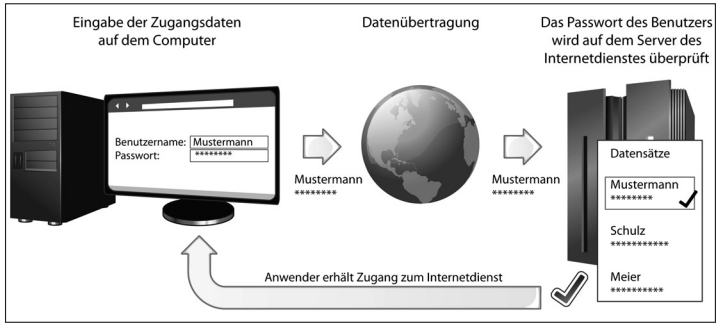

Abbildung 12: Authentikation – ein Passwort ermöglicht den Zugang zu geschützten Bereichen zum Beispiel auf einer Webseite.

In den Anfängen des Internets war noch nicht absehbar, dass irgendwann fast alle gesellschaftlichen und kommerziellen Vorgänge der realen Welt auch im Internet abgebildet sein würden. Zum Schutz personenbezogener Daten und vor dem missbräuchlichen Auslösen von Vorgängen musste daher schnell ein einfach umzusetzender Sicherheitsmechanismus gefunden werden. Und so wurde das Passwort zum Authentikationsmerkmal Nummer eins – jeder weiß, wie es funktioniert, jeder ist in der Lage, ein Passwort auszuwählen, und es bietet nahezu unendliche Variationsmöglichkeiten, solange es in der Länge nicht beschränkt ist. Aber mit ihm sind auch einige technische und gesellschaftlich begründete Schwierigkeiten verbunden, die zu Sicherheitsproblemen führen können.

Das größte Problem ist der Nutzer selbst

Traditionelle Angriffe auf Passwörter sind recht simpel: Hacker probieren alle möglichen Buchstaben- und Zahlenkombinationen aus, bis die richtige Zusammensetzung gefunden ist. Diese Art von Angriffen wird Brute-Force-Angriff

genannt und führt durch die hohe Leistungsfähigkeit heutiger Computer schnell zum Erfolg. Zusätzlich macht sich der Angreifer zunutze, dass die meisten Anwender leicht zu merkende Buchstaben- und Zahlenkombinationen verwenden, wie ihren Namen, den des Wohnorts oder ihr Geburtsdatum. Diese Möglichkeiten werden von Angreifern als Erstes unter die Lupe genommen, zum Beispiel indem alle Wörter aus dem Duden durchprobiert werden (Wörterbuchattacke).

Das Grundproblem ist also der Internetnutzer. Denn die meisten Menschen neigen dazu, einfache kurze Passwörter zu wählen. Doch gerade in Bezug auf die Sicherheit ist die Länge

Zeichenzahl eines Passwortes	Passwort bestehend aus großen und kleinen Buchstaben sowie Zahlen (68 unterschiedliche Zeichen)	Passwort bestehend aus großen und kleinen Buchstaben sowie Zahlen und Sonderzeichen (94 unterschiedliche Zeichen)
1	8,5 Mikrosekunden	11,75 Mikrosekunden
2	0,58 Millisekunden	1,10 Millisekunden
3	0,39 Sekunden	0,10 Sekunden
4	2,67 Sekunden	9,76 Sekunden
5	3,03 Minuten	15,29 Minuten
6	3,43 Stunden	23,95 Stunden
7	9,73 Tage	93,82 Tage
8	1,81 Jahre	24,14 Jahre
9	123,14 Jahre	2.260 Jahre
10	**8.370 Jahre**	**213.350 Jahre**
11	569.380 Jahre	10,05 Millionen Jahre
12	38,72 Millionen Jahre	1,89 Milliarden Jahre

Abbildung 13: Benötigte Zeit zum Knacken eines Passwortes; gilt für DualCore-Notebook (in Abhängigkeit von der Länge und den verwendeten Zeichen)

besonders wichtig, da der Rechenaufwand bei einem Brute-Force-Angriff mit jedem weiteren Zeichen, das verwendet wird, stark ansteigt. Abbildung 13 zeigt exemplarisch die Rechenzeit, die ein aktuelles, durchschnittlich ausgestattetes Notebook benötigt, um ein Passwort durch einen Brute-Force-Angriff zu knacken. Die zweite Spalte zeigt die Rechenzeit, die ein durchschnittliches aktuelles Notebook benötigt, sofern keine Sonderzeichen verwendet werden, die dritte Spalte bezieht Sonderzeichen, also Kommata, Sternchen etc. mit ein. Großrechner oder spezielle Computer in einem kriminellen Verbund benötigen nur einen Bruchteil der angegebenen Zeiten.

Das zeichnet ein gutes Passwort aus

Ein sicheres Passwort sollte aus mindestens zehn Zeichen bestehen und sowohl Klein- als auch Großbuchstaben in Kombination mit Zahlen und Sonderzeichen verwenden – am besten in einer auf den ersten Blick sinnlosen Zusammensetzung, also zum Beispiel §BhKg%80!b. Doch ein solches Passwort zu bilden, das auch noch gut zu merken ist, stellt viele vor eine schier unlösbare Aufgabe. Aber so schwer ist es gar nicht. Mit ein paar Tricks lässt sich ein gutes Passwort sogar ziemlich einfach finden und merken.

Eine gute Hilfe sind dabei Dinge aus Ihrem Alltag beziehungsweise Dinge, die Sie besonders interessieren. Das kann Ihr Lieblingsbuch sein, die Vereine, die in der Fußballbundesliga spielen oder aber ein Kinderlied, wie das folgende Beispiel zeigt:

3KDmAR8KK!
3s **K**lappert **D**ie **m**ühle **A**m **R**auschenden **8**ach **K**lipp **K**lapp**!**

Um das Passwort zu «verbessern», wurde hier für ein «E» eine «3» verwendet und für ein «B» eine «8». Auch wurden die Wörter in ihrer Groß- und Kleinschreibung verändert und zu guter Letzt wurde ein «!» als Sonderzeichen angehängt.

Auf diese Weise ist es möglich, eine Vielzahl sehr sicherer – und trotzdem einprägsamer – Passwörter zu generieren (Softlink 311).

Der richtige Umgang mit Passwörtern

Und jetzt, da Sie endlich ein sicheres Passwort haben, das Sie sich zudem gut merken können, verwenden Sie es voller Enthusiasmus bei jedem Internetdienst, den Sie nutzen … Bitte nicht! Denn damit begehen Sie den nächsten großen Fehler und spielen einem potenziellen Angreifer in die Hände.

Angenommen, jemand schafft es tatsächlich, das Passwort für Ihr E-Mail-Konto zu knacken, dann wird er die gefundene Kombination von Benutzernamen (meist die E-Mail-Adresse oder der Name) und Passwort natürlich auch bei ebay, Amazon und bei anderen Diensten ausprobieren. Mit etwas Glück kann der Angreifer nun auf Ihren Namen im Internet einkaufen oder die Zugangsdaten für kriminelle Handlungen nutzen, die auf Sie zurückfallen. Daher ist es wichtig, für jeden Internetdienst, den Sie nutzen, ein eigenes Passwort zu verwenden. Für Foren, in denen Sie über Computer, Rezepte oder Fernsehserien diskutieren, ohne sicherheitskritische Daten zu hinterlegen, können Sie auch mal ein Passwort mehrfach benutzen. Bei Inhalten mit sicherheitskritischen Daten jedoch niemals!

TIPP: Grundsätzliches zu Passwörtern

- Wählen Sie ein mindestens zehnstelliges Passwort.
- Verwenden Sie Klein- und Großbuchstaben in Kombination mit Sonderzeichen und Zahlen möglichst in einer auf den ersten Blick sinnlosen Zusammensetzung.
- Nutzen Sie Gegebenheiten aus dem Alltag, um ein Passwort zu ersinnen (siehe Seite 53). Tauschen Sie dabei Buchstaben gegen ähnlich aussehende Zahlen aus, beispielsweise das B gegen eine 8 oder das E gegen eine 3.
- Verwenden Sie jedes Passwort nur für einen einzigen Dienst.
- Der beste Schlüssel bietet keinen Schutz, wenn ihn jemand kurzfristig entwenden und eine Kopie davon anfertigen kann. Das gilt auch für das Internet. Deshalb sollten Sie Ihre Passwörter nur eingeben, wenn zwischen Ihrem Browser und dem Webserver eine sichere Verbindung besteht, welche die Daten verschlüsselt (siehe Seite 36ff.).

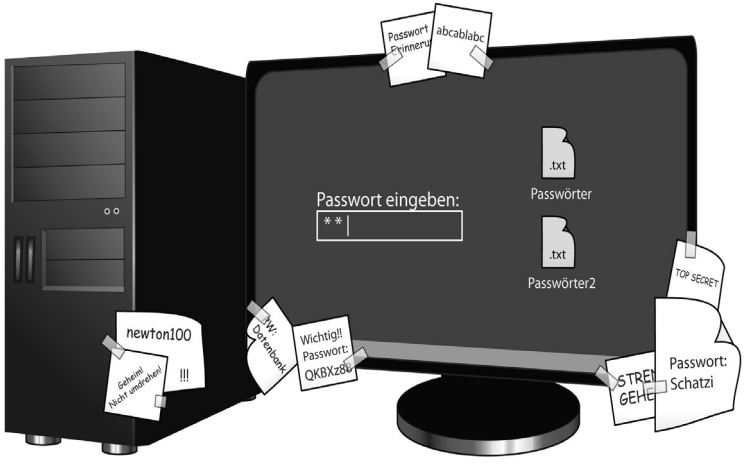

Abbildung 14: Negativ-Beispiele für die Aufbewahrung von Passwörtern

Werden sehr viele Dienste genutzt, für die Passwörter vergeben werden müssen, stoßen vielen Nutzer – was die Merkfähigkeit angeht – an ihre Grenzen, und es stellt sich die Frage: Was tun? Es gibt sehr kreative, aber leider wenig geeignete Lösungen für dieses Problem, die in der folgenden Abbildung angedeutet werden:

Denn natürlich sollten vertrauliche Daten nicht so öffentlich zur Schau gestellt werden. Eine sinnvolle Alternative sind sogenannte Passwortkarten, auf denen verschiedene Zeichenkombinationen abgebildet sind. Hier genügt es, sich lediglich bestimmte Anfangspunkte und Regeln zu merken, um ein Passwort zu hinterlegen. Beispielsweise bestimmt der Nutzer, dass ein bestimmtes Passwort bei «C/05» beginnt und ab dort zehn Stellen waagerecht verläuft, wobei jede Zeile für einen bestimmten Internetdienst steht. In Abbildung 15 wäre das Passwort «tAc8UpCpgw».

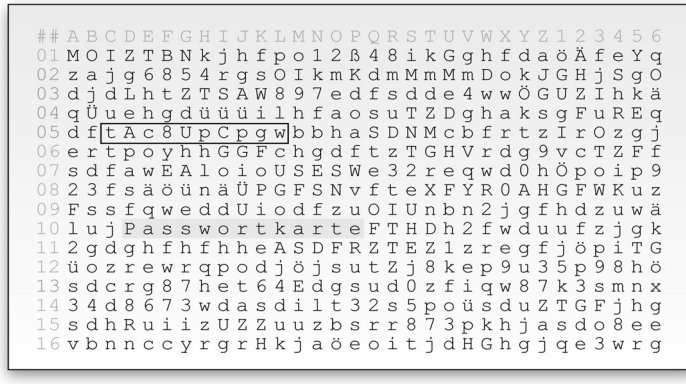

Abbildung 15: Die Passwortkarte ist eine gute Möglichkeit, um sich viele komplexe Passwörter zu merken.

Wer sehr viele Passwörter zu verwalten hat – die Autoren beispielsweise haben rund 100 Passwörter im Gebrauch –,

dem helfen Passwortspeicher. In diesen Speichern werden Passwörter verschlüsselt abgelegt, wodurch sie für niemand anderen zugänglich sind. Zusätzlich werden sie mit einem Master-Passwort geschützt. Beim Einsatz solcher Sicherheitsmechanismen muss das Master-Passwort, das den Zugang zu den gespeicherten Passwörtern schützt, den angesprochenen Sicherheitsvorgaben in besonderer Form genügen, das heißt, es sollte mindestens aus 13 Zeichen in einer kreativen, nicht nachvollziehbaren Zusammensetzung bestehen. Einige Experten empfehlen sogar ganze Sätze mit vielen Sonderzeichen. Die lassen sich meist gut merken und sind wirklich sicher.

Passwortspeicher gibt es in den unterschiedlichsten Ausführungen: als Software auf einem USB-Stick, als Programm auf dem Computer (Softlink 312) oder als Zusatzfunktion in Browsern. Letztere fragt nach einem abgeschlossenen Passwortdialog, also nachdem Sie sich mit Ihrem Benutzernamen und Passwort angemeldet haben, automatisch, ob das Passwort gespeichert werden soll (siehe Abbildung 16).

Abbildung 16: Automatische Funktion des Browsers zum Speichern von Zugangsdaten

Doch Vorsicht: Grundsätzlich kann die Passwortspeicherfunktion des Browsers nicht als ausreichend sicher betrachtet

werden. Für weniger sicherheitskritische Internetdienste, wie die Anmeldung in Foren, ist ein Einsatz möglich, beim Onlinebanking und ähnlich sensiblen Diensten sollten Sie dagegen auf diesen Service verzichten. Und vergeben Sie, falls Sie ihn verwenden, auf jeden Fall ein Master-Passwort für die Passwortspeicherung (siehe Abbildung 17). Diese Einstellung ist bei den aktuellen Browsern optional, aber absolut notwendig, um die Passwörter dem Zugriff Dritter, die denselben Computer verwenden, zu entziehen. Eingeschränkt kann ein Master-Passwort auch gegen Malware schützen, die sich auf dem Computer eingenistet hat und versucht, den Passwortspeicher auszulesen. Ist die Malware allerdings in der Lage, Tastenanschläge nachzuvollziehen oder den Hauptspeicher auszulesen, bietet auch das Master-Passwort keinen Schutz, da

Abbildung 17: Setzen Sie in den Browsereinstellungen unter dem Punkt «Sicherheit» den Haken vor «Master-Passwort verwenden», um diese Funktion zu aktivieren.

die Angreifer auf diese Weise auch an das Master-Passwort selbst gelangen.

Auch Passwortspeicher auf USB-Sticks oder die angesprochenen Programme haben unterschiedliche Sicherheitsniveaus. Am besten fragen Sie einen Fachmann oder recherchieren im Internet, ob die Lösung, die Sie nutzen wollen, für Ihre Bedürfnisse ausreichend ist. Natürlich gibt es auch in diesem Bereich frei verfügbare Tools wie beispielsweise Passwortsafe oder keepass (Workshop «keepass», siehe Softlink 312).

TIPP: Aufbewahrung von Passwörtern

- Notieren Sie Ihre Passwörter nie auf Papier, Sie machen diese sonst öffentlich zugänglich.
- Wenn Sie sich Ihre Passwörter nicht merken können, nutzen Sie kleine Helfer wie Passwortkarten oder Passwortverschlüsselungsprogramme!
- Nutzen Sie den Passwortspeicherungsservice des Browsers nur für unkritische Passwörter und nur auf Ihrem eigenen Computer. Verwenden Sie diesen aus Gewohnheit in einem Internetcafé, hat jeder Anwender, der nach Ihnen den Computer benutzt, Zugriff auf Ihre Passwörter! Verzichten Sie am besten ganz darauf.
- Besonders wichtig: Ändern Sie Ihre Passwörter regelmäßig alle drei bis sechs Monate! Tauschen Sie dabei nicht nur eine Zahl oder einen Buchstaben aus, sondern verändern Sie das Passwort stets an mehreren Stellen.

Passwort vergessen – was nun?

Es kommt natürlich vor, dass Nutzer ihr Passwort vergessen und nicht mehr auf den Internetdienst zugreifen können. Im

Normalfall gibt es für diese Situation das Helpdesk des Anbieters. Bei einem Anruf dort kann der Kundendienst im Normalfall weiterhelfen. Um diesen Vorgang zu vereinfachen und vor allem um Kosten für den Anbieter zu sparen, gibt es beim Einrichten eines personalisierten Internetdienstes häufig auch eine Möglichkeit zur Selbsthilfe für den Fall von akuter Vergesslichkeit. Wenn ein Nutzer zum Beispiel eine E-Mail-Adresse einrichtet, wird er aufgefordert, neben seinem Passwort auch Antworten auf verschiedene Fragen zu geben:

- Wie heißt Ihr Hund?
- Wie heißt Ihre beste Freundin?
- Wie lautet der Mädchenname Ihrer Mutter?

Im Verlustfall wird der Anwender dann auf eine Webseite geleitet, auf der ihm eine oder mehrere dieser Fragen gestellt werden. Beantwortet der Nutzer die Fragen richtig, wird das Passwort zurückgesetzt, und er kann ein neues wählen.

Der Grundgedanke dieser Selbsthilfemaßnahme ist nicht schlecht, aber unter Sicherheitsgesichtspunkten bedenklich. Denn bei einem Angriff dürfte es einfacher sein, diese Funktion auszuhebeln und das Passwort zurückzusetzen, als das Passwort selbst zu finden. Der Mädchenname der Mutter oder ähnliche Informationen sind meist leicht herauszufinden, besonders im Falle eines gezielten Angriffs. Die Anbieter müssen deshalb in diesem sensiblen Bereich nachbessern. Als Internetnutzer sollten Sie diese Funktion entweder meiden oder sich sicherheitstechnisch intelligente Antworten auf die Fragen überlegen. Beispielsweise könnten Sie die Namen nach einem bestimmten Schema verschlüsseln, indem Sie zwischen jeden Buchstaben eine Zahl oder ein Sonderzeichen setzen. Die Antwort auf die Frage nach dem Namen Ihres Hundes könn-

te dann zum Beispiel so aussehen: F!r1i!d1o!l1i!n1!. Stehen mehrere Fragen zur Auswahl, ist es klug, nur eine zu nutzen, denn je mehr mögliche Fragen und Antworten es gibt, desto mehr Angriffsfläche bieten Sie dem Angreifer.

Ausblick: der elektronische Personalausweis

Der Siegeszug des Passwortes scheint ungebrochen, aber der Druck, einen höheren Sicherheitslevel bei der Authentikation zu erreichen, ist enorm. Deshalb hat die Bundesrepublik mit dem neuen elektronischen Personalausweis eine Infrastruktur zur Verfügung gestellt, um den Identitätsnachweis im Internet für die Bundesbürger sicherer zu machen. Der Staat hat mit seiner Personalausweis-Infrastruktur natürlich auch optimale Voraussetzungen, dies umsetzen zu können.

Standes- und Melde- beziehungsweise Bürgerämter sichern die eindeutige und überprüfbare Identität von Personen: Das Standesamt sorgt dafür, dass wir über unseren Vor- und Nachnamen, den Geburtsort und das Geburtsdatum eindeutig identifizierbar sind. Das Melde- beziehungsweise Bürgeramt gibt die Personalausweise heraus, die es ermöglichen, diese eindeutige Identität zweifelsfrei nachzuweisen.

Ab November 2010 wird der elektronische Personalausweis im Scheckkartenformat, der mit einem kontaktlosen Sicherheits-Chip ausgestattet ist, den bisherigen Personalausweis ablösen. Der neue elektronische Personalausweis wird wie der alte Personalausweis für hoheitliche Kontrollen an Grenzen und im Inland verwendet.

Zusätzlich ist der elektronische Personalausweis aber mit der Funktion des elektronischen Identitätsnachweises (Authentikationsfunktion) ausgerüstet. Damit ist er auch ein Ausweis,

mit dem sich sein Besitzer im Internet sicher identifizieren und authentisieren lassen kann. Dazu muss der genutzte Computer mit einem Kartenleser und der zugehörigen Software (Bürgerclient) ausgerüstet sein. Das Besondere am Sicherheitskonzept des elektronischen Personalausweises ist, dass nur berechtigte Anbieter von Dienstleistungen in der Lage sind, die Daten des Ausweises abzufragen. Um diese Berechtigung zu erlangen, muss der jeweilige Anbieter ein entsprechendes Zertifikat beim Bundesverwaltungsamt beantragen, in dem genau definiert ist, was er kryptographisch (verschlüsselt und integritätsgesichert) auslesen darf – insbesondere im Hinblick auf den Daten- und Verbraucherschutz. Zudem behalten Sie als Ausweisinhaber stets die volle Kontrolle darüber, welche Ihrer persönlichen Daten an den Anbieter übermittelt werden. Wenn dieser mit dem Berechtigungszertifikat auf den Ausweis zugreift, werden Sie darüber informiert, was der berechtigte Anbieter auslesen darf, und können den Vorgang teilweise oder ganz untersagen.

Generell kann der elektronische Personalausweis nur ausgelesen werden, wenn der Nutzer diesen über die Eingabe einer PIN aktiviert. Diese PIN wird aber lediglich für die Aktivierung des Sicherheits-Chips auf dem Ausweis verwendet. Die eigentliche Verifikation erfolgt über sehr sichere Kryptographie-Protokolle zwischen dem Sicherheits-Chip auf dem elektronischen Personalausweis und einem Sicherheitsmodul der verifizierenden Stelle. Das Plus an Sicherheit liegt darin begründet, dass der Identifikationsnachweis nur mit dem Besitz des elektronischen Personalausweises *und* der PIN möglich ist, also mit der Kombination aus Besitz (elektronischer Personalausweis) und Wissen (Passwort). Darüber hinaus bietet der neue elektronische Personalausweis die

Möglichkeit, ein Zertifikat für die qualifizierte elektronische Signatur auf den Personalausweis zu laden. Damit sind die Besitzer dann auch in der Lage, online zu unterschreiben, zum Beispiel Verträge (Softlink 313).

TIPP: Elektronischer Personalausweis

- Geben Sie den elektronischen Personalausweis mit der passenden PIN nie weiter – auch nicht an Verwandte und Freunde!
- Legen Sie den elektronischen Personalausweis nur auf den Leser, wenn Sie sich im Internet damit anmelden wollen.
- Sorgen Sie dafür, dass der Basisschutz (siehe Seite 10ff.) stets gewährleistet ist.

E-Mail – von digitalen Postkarten und falschen Absendern

Die E-Mail ist das meistverwendete Kommunikationsmittel unserer modernen Gesellschaft. Es werden natürlich immer noch Briefe und Postkarten geschrieben, aber die meisten Informationen werden inzwischen per E-Mail versandt. Die Vorteile der E-Mail liegen auf der Hand: Sie ist meist innerhalb weniger Sekunden beim Adressaten und kann sofort bearbeitet werden.

Zusätzlich können Dateien an die E-Mail gehängt und sehr einfach und schnell ausgetauscht werden – ganz ohne Medienbruch. Auch sind E-Mails deutlich kostengünstiger als Briefe und Postkarten, was für viele, neben der Geschwindigkeit, sicher das wichtigste Argument ist. Doch wie steht es mit der Vertraulichkeit? Jeder weiß, dass man Vertrauliches nicht

auf eine Postkarte schreiben sollte, da jeder den Inhalt lesen kann. Bei einem Brief ist das anders, auch wenn es da ein paar kriminelle Tricks gibt, bei denen Wasserdampf eine Rolle spielt. Und wie sieht es bei der E-Mail aus? Um diese Frage beantworten zu können, ist es hilfreich zu verstehen, wie der E-Mail-Austausch vonstattengeht.

So funktioniert der E-Mail-Austausch im Internet

Damit eine E-Mail ihren Bestimmungsort erreicht, muss sie in einen digitalen Briefkasten geworfen werden. Diesen stellt der E-Mail-Anbieter, auch Provider genannt, zur Verfügung. Der E-Mail-Anbieter des Senders versendet die E-Mail an den Empfänger beziehungsweise an dessen E-Mail-Anbieter, was mit dem Transport von Briefen zwischen den verschiedenen Verteilerzentren vergleichbar ist. Der E-Mail-Anbieter des Empfängers liefert die E-Mail dann – genau wie ein Postbote – an das entsprechende Postfach des Empfängers. Daher heißt es E-Mail-Postfach.

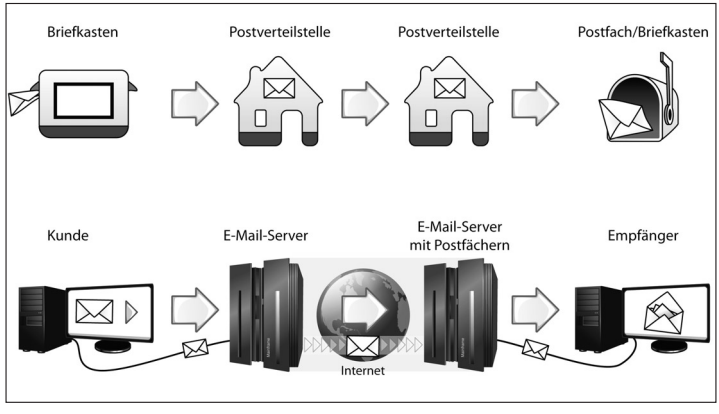

Abbildung 18: Der Postweg – real und virtuell

Die E-Mail-Adresse

Alle für die Zustellung nötigen Angaben beinhaltet die E-Mail-Adresse: Der erste Teil (vor dem @-Zeichen) gibt den konkreten Empfänger an – die E-Mail-Adresse norbert.pohlmann@sicher-im-internet.de kann beim E-Mail-Anbieter sicher-im-internet.de nur einmal vorhanden sein. Der zweite Teil (nach dem @-Zeichen) gibt die entsprechende Domain und damit meistens den Namen des E-Mail-Anbieters oder einer Firma an, also zum Beispiel gmx.de, t-online.de, yahoo.de oder siemens.de, otto.de, allianz.de. Sie ist mit der Adressangabe auf einem Brief vergleichbar.

Viele Anbieter wie GMX, WEB.DE, freenet und Google stellen Ihnen kostenlos eine E-Mail-Adresse mit Postfach zur Verfügung, wobei es eventuell überlegenswert ist, diese aufzuwerten. Meist erhalten Sie schon für ein geringes Entgelt deutlich mehr Speicherplatz für Ihr Postfach sowie zusätzliche Sicherheits- und Komfortfunktionen.

Verwalten können Sie Ihre E-Mails beziehungsweise Ihr E-Mail-Postfach auf zwei Arten: online im Internet per sogenanntem Webmailer mithilfe des Browsers oder lokal auf dem Computer über ein Programm, den sogenannten E-Mail-Client. Beispiele für E-Mail-Clients sind Mozilla Thunderbird, Microsoft Outlook oder The Bat. Natürlich können Sie auch beide Varianten parallel nutzen. Den Webmailer-Zugang stellt in der Regel der E-Mail-Anbieter zur Verfügung. Er hat den Vorteil, dass Sie von überall auf Ihr Postfach zugreifen können (über die Webseite des E-Mail-Anbieters). Allerdings müssen Sie zur Bearbeitung Ihrer E-Mails permanent online sein. Mit einem E-Mail-Client ist es dagegen möglich, auch offline zu arbeiten und nur für den Versand beziehungsweise den Empfang von E-Mails online zu gehen. Die E-Mail-

Clients bieten außerdem mehr Komfortfunktionen und ermöglichen die gleichzeitige Verwaltung mehrerer E-Mail-Adressen.

Wie Sie Ihre E-Mails verwalten, ist letztlich eine Frage des persönlichen Geschmacks. Bei permanenter Nutzung und mehreren Konten ist der E-Mail-Client aber mit Sicherheit die komfortablere Variante (Einstellungen, siehe Softlink 327).

TIPP: E-Mail-Verwaltung

Fragen Sie Ihre E-Mails nur selten oder von ständig wechselnden Computern aus ab, ist ein Webmailer-Zugang für Sie die praktischere Variante.

Wollen Sie mehrere E-Mail-Adressen komfortabel verwalten, sollten Sie sich – zusätzlich zum Webmailer-Zugang – für einen E-Mail-Client entscheiden.

Der richtige Umgang mit E-Mail-Adressen

In Telefonbüchern kann jeder seine Telefonnummern mitsamt der Anschrift angeben lassen. Seit einigen Jahren achten die Kunden jedoch immer mehr darauf, dass nur die Telefonnummer in den Telefonbüchern auftaucht, um einen Missbrauch der Daten durch Dritte zu erschweren. Inzwischen gehen viele sogar dazu über, den Telefonbucheintrag komplett zu streichen – in Zeiten von ständig zunehmender und immer aggressiver betriebener Telefonwerbung durchaus verständlich. Genau aus dem gleichen Grund sollten Sie auch Ihre E-Mail-Adresse – ebenso wie Ihre anderen persönlichen Daten – nicht leichtfertig preisgeben. Es ist sogar sinnvoll, sich mehrere E-Mail-Adressen zuzulegen und diese je nach Aktivität einzusetzen. Ihre «seriöse» Hauptadresse verwenden Sie

für Ihre Bankgeschäfte, das Buchen von Tickets, den Onlineeinkauf und die Kommunikation mit der Familie und guten Freunden. Im Geschäftsleben wählen Sie die Firmenadresse, also zum Beispiel Linnemann@internet-sicherheit.de. Und schließlich benötigen Sie eine möglichst anonyme E-Mail-Adresse wie ML04@googlemail.com Die kommt dann bei all den Gelegenheiten zum Einsatz, bei denen Sie nicht abschätzen können, wie die jeweiligen Dienste mit Ihren Daten umgehen, also in Foren, Blogs, bei Umfragen etc. Es kann nämlich leicht sein, dass Sie in der Folge mit Spam (siehe Seite 78 ff.) geradezu überschüttet werden – und es ist nicht ganz so ärgerlich, wenn das bei einem Postfach passiert, das ohnehin nicht für den regulären E-Mail-Verkehr gedacht war.

Ein weiteres Übel sind die sogenannten Harvester, die das Internet nach E-Mail-Adressen absuchen («crawlen») und diese sammeln, um anschließend Spam an sie zu versenden. Deshalb sollten Sie Ihre E-Mail-Adressen entsprechend schützen, wenn Sie sie auf privaten oder beruflichen Webseiten nennen. Das gilt auch für Dokumente, die auf einer Webseite abrufbar sind, egal ob es sich dabei um Office-Dokumente, PDFs oder PowerPoint-Präsentationen handelt. Denn gerade in solchen Dokumenten befinden sich in der Regel personenorientierte E-Mail-Adressen.

Eine einfache Gegenmaßnahme ist das «Verschleiern» der E-Mail-Adresse (Softlink 321), zum Beispiel nach folgendem Muster:

Originaladresse:
Linnemann@internet-sicherheit.de

Verschleierte Darstellung mit Leerzeichen und Umschreibungen:
Linnemann [at] internet – sicherheit [dot] de

Doch nicht nur die eigene E-Mail-Adresse muss geschützt werden, sondern auch fremde. Ein besonderer Fall ist der Versand von E-Mails an mehrere Empfänger. Hier sollten die E-Mail-Adressen der Empfänger in das Adressfeld «Bcc» eingetragen werden (siehe Seite 70). Als Empfänger in «An» wird dann meist die Absenderadresse eingetragen. So bekommen alle die E-Mail, sehen aber nur den Absender und nicht die weiteren Adressaten, welche die E-Mail ebenfalls bekommen haben.

Allerdings kann es manchmal auch gewünscht sein, dass alle sehen, wer sonst noch im Verteiler steht, zum Beispiel bei einer Geburtstagsüberraschungsparty.

Übrigens: Wenn eine E-Mail an sehr viele Adressaten (weit über 100) im An- oder Cc-Feld verschickt wird, können entsprechende Kontrollinstanzen im Internet das erkennen und den Absender als Spammer einstufen. Das hat zur Folge, dass dessen E-Mails nicht mehr zugestellt werden.

TIPP: Umgang mit E-Mail-Adressen

- Gehen Sie grundsätzlich vorsichtig mit Ihren privaten Daten wie E-Mail-Adresse, Name, Alter und Anschrift um. Viele Firmen verkaufen Datensätze, die dann für Werbezwecke verwendet werden.
- Geben Sie Ihre E-Mail-Adresse nur an Personen, die Sie kennen und/oder denen Sie vertrauen!
- Nutzen Sie je nach Aktivität verschiedene E-Mail-Adressen.
- Verschleiern Sie Ihre E-Mail-Adresse auf Dokumenten und Webseiten im Internet, um E-Mail-Harvestern zu entgehen.
- Nutzen Sie das Bcc-Feld, wenn Sie E-Mails an eine große Gruppe von Adressaten versenden, um nicht sämtliche E-Mail-Adressen für alle sichtbar zu machen.

Die wichtigsten Verhaltensregeln beim E-Mail-Austausch

Die Kommunikation via E-Mail ist im privaten und beruflichen Leben für viele bereits selbstverständlich geworden. Die Vorteile des schnellen und kostengünstigen Austauschs von Informationen und Dateien sind enorm, und man möchte sie nicht mehr missen.

Der richtige Umgang mit der E-Mail-Anwendung ist jedoch noch nicht optimal etabliert. Aus diesem Grund werden einige Verhaltensregeln beschrieben, die für alle Beteiligten bei der richtigen Umsetzung hilfreich sind. Diese Regeln helfen auch, die Vertrauenswürdigkeit von E-Mails besser einschätzen zu können.

Inhalt und Form

Jeder, der eine E-Mail schreibt, sollte sich genau überlegen, was er dem oder den anderen eigentlich mitteilen möchte. Die Tatsache, dass eine E-Mail schnell verfasst ist und kein Porto kostet, ist kein Grund, andere mit Belanglosigkeiten zu bombardieren. Auch ist die Unkompliziertheit des Mediums kein Freibrief für formale Nachlässigkeit. Ein freundlicher Umgangston, korrekte Rechtschreibung, Anrede und Schlussformel sowie eine übersichtliche Struktur sollten in einer E-Mail ebenso selbstverständlich sein wie in einem «normalen» Brief. Dazu gehört auch, dass die Betreffzeile immer einen aussagekräftigen Hinweis auf den Inhalt der E-Mail enthält.

Der oder die Empfänger

In einer E-Mail können verschiedene Kategorien von Empfängern definiert werden:

- Das Feld «An» (To) gibt die E-Mail-Adresse von primären Empfängern an. Hier sollten Sie nur Empfänger eintragen, von denen Sie eine Reaktion erwarten.
- Das Feld «Cc» (Carbon Copy = Durchschlag) gibt die E-Mail-Adressen der sekundären Empfänger an, die den Inhalt der E-Mail lediglich zur Kenntnis nehmen sollen. Bei der Zustellung wird zwischen primären und sekundären Empfängern nicht unterschieden.
- Das Feld «Bcc» (Blind Carbon Copy) hat die gleiche Bedeutung wie das Feld «Cc» – mit dem Unterschied, dass die Zeile «Bcc» in den Kopien, die an die verschiedenen Empfänger gesendet werden, nicht sichtbar ist. Das ermöglicht Ihnen, eine E-Mail an eine Gruppe von Empfängern zu schicken, ohne dass jeder die E-Mail-Adressen der anderen sieht (siehe Seite 68).

Die Antwort

Die E-Mail wird sehr schnell an den Empfänger ausgeliefert, der sich bemühen sollte, diese auch zügig zu beantworten. Im Geschäftsleben erwartet der Absender heute eine Antwort innerhalb eines Werktages. Wenn Sie also wissen, dass Sie nicht so schnell reagieren können, sollten Sie eine automatische Abwesenheitsnotiz versenden, die den Sender darüber informiert, dass Sie nicht da sind und ab wann er Sie wieder erreichen kann. Die entsprechende Autoresponder-Funktion bietet inzwischen fast jeder E-Mail-Anbieter an (Softlink 322).

Nutzen Sie zudem die Antworten-Funktion, damit der ursprüngliche Text wieder mit zurückgeschickt wird. So weiß der Empfänger auf einen Blick, worauf Sie sich beziehen. Dabei sollte der alte Text immer unten stehen und Ihre Antwort oben. Geht eine E-Mail mehrfach hin und her, sollten Sie sie

zwischendurch neu anlegen, damit sie nicht unendlich lang wird.

Die Signatur

Die Signatur ist ein Text, der an das Ende einer E-Mail angehängt wird und Informationen über den Absender enthält. Sie erleichtert die Kontaktaufnahme, zum Beispiel im Falle einer telefonischen Rückfrage, zeigt die rechtliche Stellung des Absenders (bei Unternehmen gesetzlich vorgeschrieben) und hilft bei der Einschätzung der Vertrauenswürdigkeit des Absenders. Die Signatur kann automatisch durch den E-Mail-Client oder Webmailer eingefügt werden.

TIPP: Vertrauenswürdigkeit einer E-Mail

Bei der Einschätzung, ob eine E-Mail vertrauenswürdig ist oder nicht, können neben der Signatur auch folgende Aspekte hilfreich sein:

- Sind Aufbau und Inhalt der E-Mail für Sie klar nachvollziehbar?
- Ist Ihnen der Absender oder die Organisation, von der die E-Mail kommt, persönlich bekannt oder haben Sie zumindest eine Vorstellung, warum Sie diese E-Mail bekommen?
- Wird Ihnen in der E-Mail ein Angebot gemacht, das unrealistisch ist (Geschenke)?
- Haben Sie die E-Mail erwartet?

E-Mails – Angriffe und Gefahren

Folgendes Szenario kann so oder so ähnlich überall passieren: Eine Angestellte versendet von ihrem Arbeitsplatz eine E-Mail an ihre Freundin im Büro nebenan, mit vielen intimen Einzelheiten zu ihrer heimlichen Beziehung mit dem Chef. Kurz

darauf erhalten alle Mitarbeiter des Unternehmens diese E-Mail von einem unbekannten Absender. Die E-Mail wurde «abgefangen» und veröffentlicht. Eine höchst unangenehme Situation für die Angestellte und natürlich auch für den Chef. Was ist passiert?

Eine E-Mail zu verschicken ist nichts anderes als eine Postkarte zu versenden, sprich: Jeder, der die E-Mail «in die Finger bekommt», kann sie auch lesen. Das ist den meisten Nutzern nur nicht bewusst. So kann zum Beispiel der E-Mail-Anbieter sämtliche E-Mails lesen, die über ihn verschickt werden (ob er es darf, ist eine andere Frage), aber auch jeder, der Zugriff auf das Netzwerk hat, in dem Sie sich befinden – sowohl am Arbeitsplatz als auch im Internetcafé. Deshalb sollten Sie sensible Daten niemals per E-Mail versenden, ohne entsprechende Vorsichtsmaßnahmen zu treffen (siehe Seite 82 f.). Und es lauern noch weitere Gefahren …

Vermeintlich vertrauenswürdige E-Mails

In Ihrem E-Mail-Postfach befindet sich eine E-Mail mit dem Absender eines guten Freundes. Laut Betreff bietet er Ihnen darin günstig Viagra-Tabletten an, oder er verweist per Link auf eine tolle Seite im Internet. Da Ihnen das seltsam vorkommt, fragen Sie nach. Das Ergebnis: Er versichert Ihnen glaubhaft, dass diese E-Mail nicht von ihm stammt. Wie aber kann das sein?

Der Absender kann bei E-Mails frei benannt werden – genau wie bei einer Postkarte. Dort können Sie als Absender auch den Namen des Bürgermeisters verwenden (wobei wir hierbei davon ausgehen, dass Sie nicht der Bürgermeister sind). Der Absender ist also kein Indiz für die Vertrauenswürdigkeit der E-Mail.

Das ist aus Betrügersicht natürlich eine hervorragende Grundlage für einen Angriff, nämlich mit E-Mails, die von einem vermeintlich vertrauenswürdigen Absender stammen und einen auf den ersten Blick interessanten Link beinhalten. Klicken Sie deshalb niemals auf Links, wenn Sie nicht genau wissen, worum es sich dabei handelt. Der Link könnte beispielsweise auf eine infizierte Webseite leiten, wodurch Malware auf den Computer geladen wird, die Ihre Daten ausspioniert und/oder die Kontrolle über Ihren Computer übernimmt. Auch der Link ist letztlich nur ein Text, der frei eingegeben werden kann. Ohne eine Kontrolle können Sie sich deshalb nie sicher sein, ob er Sie tatsächlich zu der angekündigten Webseite führt.

Bedeutet das jetzt, dass Sie nie wieder einen Link anklicken dürfen? Grundsätzlich natürlich nicht. Es gibt verschiedene Anhaltspunkte, anhand derer Sie drohende Gefahren erkennen können und die sich sehr schnell überprüfen lassen. Das Wichtigste ist wiederum, dass Sie bei der Bearbeitung Ihrer E-Mails gesunden Menschenverstand walten lassen. Warum sollten Sie einer E-Mail Beachtung schenken, die eine seltsame Information enthält oder in einer Sprache geschrieben ist, die der Absender normalerweise nicht verwendet? Bei Unsicherheit hilft es, den Freund oder Geschäftspartner einfach anzurufen, der die E-Mail geschickt hat, und nachzufragen, was es damit auf sich hat. Die meisten Angriffsversuche lassen sich so bereits abwehren. Zudem ist es immer ratsam, das Ziel eines Links durch Darüberfahren mit der Maus zu überprüfen (siehe Abbildung 19 sowie Seite 29 f.).

Grundsätzlich gibt es zwei Möglichkeiten, um auf eine solche E-Mail, wie sie Abbildung 19 zeigt, nicht hereinzufallen. Bei dieser E-Mail handelt es sich um eine HTML-Mail.

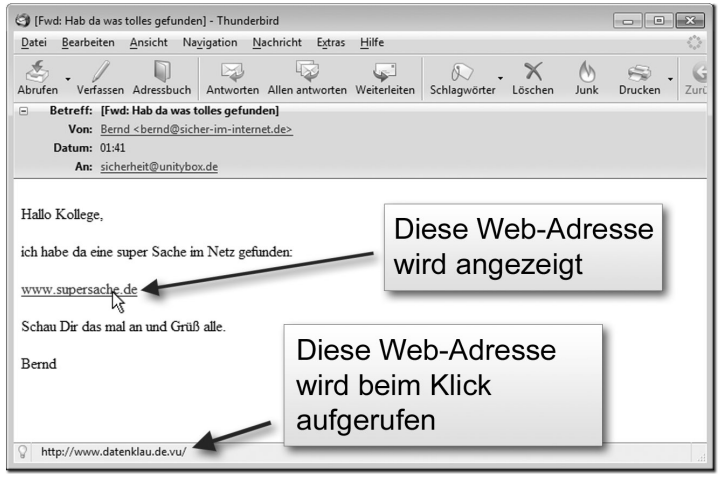

Abbildung 19: Gefälschte HTML-Mail im E-Mail-Client

Das bedeutet, dass sie wie eine Webseite aufgebaut ist und im Hintergrund mehr steht, als vordergründig zu sehen ist. Jedes

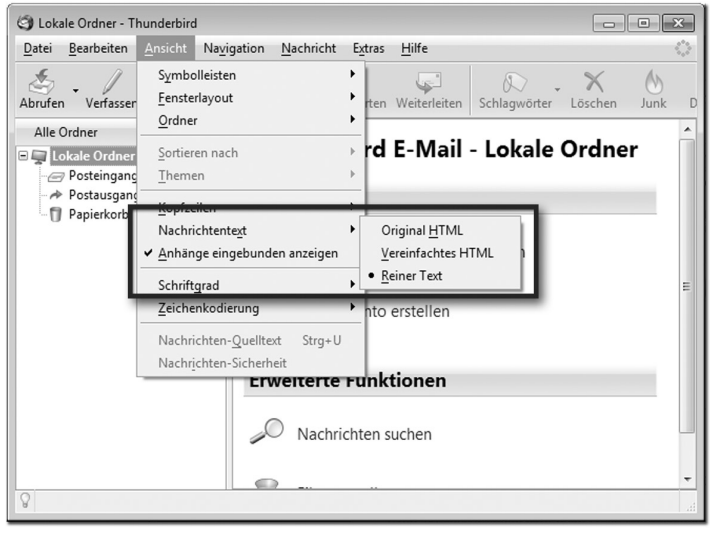

Abbildung 20: Umstellen der E-Mail-Ansicht von HTML zu reinem Text

E-Mail-Programm bietet aber die Möglichkeit, E-Mails in reiner Textform anzuzeigen (siehe Abbildung 20). Dann ist auf den ersten Blick zu erkennen, wohin ein Link führt, und es werden keine versteckten Befehle ausgeführt (siehe Abbildung 22).

Selbstverständlich können HTML-Mails nach der Überprüfung im «Nur-Text-Modus» wieder auf HTML umgestellt werden. Auch dabei ist allerdings Vorsicht geboten, da in HTML-Mails aktive Inhalte (siehe Seite 31 ff.) eingebettet sein können.

Dieselbe Problematik besteht beim Webmailer (siehe Abbildung 21), wobei manche E-Mail-Anbieter heute bereits darauf hinweisen, wenn die E-Mail HTML-Inhalte enthält. Dementsprechend gilt es auch hier, erst den Link zu kontrollieren, bevor ein Klick ausgeführt wird. Zwar sind inzwischen sowohl die Onlineangebote über Webmailer als auch die E-Mail-Clients auf den Computern mit Vorkehrungen verse-

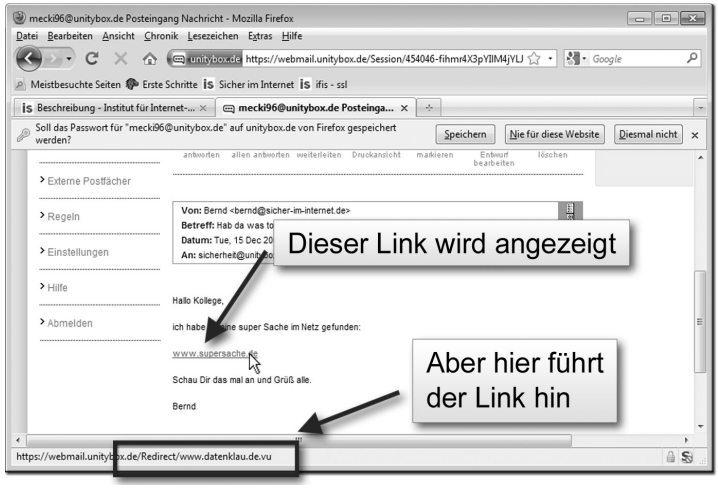

Abbildung 21: Gefälschte HTML-Mail bei einem Webmailer

hen, welche die gängigsten «bösen» Links erkennen, aber allein darauf sollten Sie sich nicht verlassen. Sie wissen ja: Vorsicht ist besser als Nachsicht.

Die zweite Möglichkeit, den Betrug zu durchschauen, ist die Kontrolle der sogenannten Headerdaten. Sowohl der E-Mail-Client als auch der Webmailer enthüllt in einer entsprechenden Einstellung «konkretere» Daten zum Absender, sodass Sie diese mit der im Feld «Von» angezeigten Adresse abgleichen können (siehe Abbildung 22). Die dazu notwendigen Kopf- oder Headerdaten rufen Sie auf, indem Sie im E-Mail-Client über den Menüpunkt «Ansicht» auf den Punkt «Kopfzeilen anzeigen» klicken. Je nach Webmailer können die einzelnen Benennungen ein wenig variieren. Suchen Sie in diesem Fall nach einer ähnlichen Webmailer-Einstellung. Die Daten, die im Header einer Mail angezeigt werden, sind für den Laien allerdings schwer zu lesen. Manchmal offenbart sich hier direkt die echte Absenderadresse, aber das muss nicht so sein (siehe Abbildung 22).

Mit geübtem Auge kann man in Abbildung 22 sehen, von welchem Mail-Server die E-Mail gekommen ist, was durchaus aufschlussreich sein kann. Zugegeben, hier sind einige Fachkenntnisse vonnöten, aber es zeigt, dass betrügerische E-Mails sehr wohl entlarvt werden können. Allerdings ist auch diese Methode kein 100-prozentiger Schutz, da Absender-E-Mail-Adressen so gefälscht werden können, dass es selbst im Header nicht zu erkennen ist. Es ist sogar möglich, E-Mails von sich selbst zu erhalten, die man nie losgeschickt hat.

Übrigens: In der reinen Textansicht wäre der Link, der sich in der HTML-Mail hinter «www.superSache.de» verbirgt, ebenfalls sichtbar – nämlich «www.datenklau.de». Generell sollten Sie Links in E-Mails niemals anklicken, wenn die

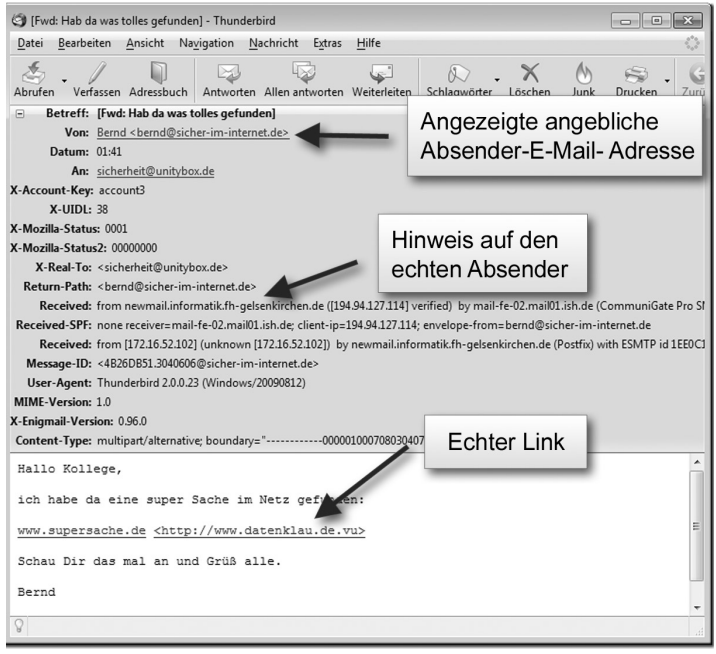

Abbildung 22: Hier wird die E-Mail als reiner Text mit vollständigem Header (Quelltext des E-Mail-Headers) angezeigt.

E-Mail nicht vertrauenswürdig ist. Suchen Sie ein in der E-Mail angegebenes Thema lieber «per Hand» im Internet oder geben Sie bei bekannten Links das Ziel auch per Hand in den Browser ein.

TIPP: Abwehr von E-Mail-Angriffen

- Versenden Sie sensible Daten niemals per E-Mail, ohne entsprechende Vorsichtsmaßnahmen zu treffen (siehe Seite 82 f.).
- E-Mails, die Ihnen seltsam vorkommen, sollten Sie umgehend löschen. Sind Sie sich nicht sicher, kontaktieren Sie den Absender, um nachzufragen – aber natürlich nicht über die Antwort-Funktion!

- Fahren Sie mit der Maus über jeden Link und überprüfen Sie in der Statusleiste dessen Zieladresse, bevor Sie ihn anklicken. Ist die E-Mail nicht absolut vertrauenswürdig, verzichten Sie darauf. Suchen Sie das in der E-Mail angegebene Thema dann lieber «per Hand». Auch Ihnen bereits bekannte Adressen sollten Sie besser manuell in den Browser eingeben, anstatt sie per Link anzusteuern.
- Empfangen Sie E-Mails möglichst in reiner Textform und bearbeiten Sie sie nicht als HTML-Mail.
- Kontrollieren Sie – sofern Sie bereits über einige Computerkenntnisse verfügen – beim geringsten Verdacht den Quelltext des E-Mail-Headers und vertrauen Sie nicht blind auf die Absenderadresse.

Spam

SPAM war ursprünglich ein Markenname für Dosenfleisch. Die Übernahme des Begriffs als Bezeichnung für unerwünschte Nachrichten lässt sich unter anderem auf einen Sketch aus der englischen Comedyshow «Monty Python's Flying Circus» zurückführen. Doch leider ist das Thema Spam im Internet weniger amüsant. Spam-E-Mails, in einigen E-Mail-Programmen auch als Junk bezeichnet, sind unerwünschte, wert-, nutz- und sinnlose Nachrichten. Sie stellen derzeit vermutlich das größte Problem im Internet dar, denn rund 95 Prozent des gesamten E-Mail-Verkehrs sind Spam, also E-Mails, die keiner haben möchte.

Die Gefahren, die von ihnen ausgehen, sind vielschichtig. Die reine Werbemail möchte Sie meist nur dazu verleiten, ein bestimmtes Produkt zu kaufen. Es kann sich dahinter aber auch ein Angriff auf Ihre persönlichen Daten verbergen. Entsprechende Links können Sie, wie bereits auf Seite 31 ff.

beschrieben, auf Seiten führen, die direkt Trojanische Pferde auf Ihren Computer laden. Die Folge ist der Kontrollverlust über den Computer und die Dateien. Phishing-Mails haben es auf Ihre Bankdaten abgesehen und werden im Abschnitt «Onlinebanking» genauer erläutert (siehe Seite 98 ff.). Darüber hinaus gibt es eine bestimmte Sorte von Spam-Mails, Jamaika-E-Mails genannt, in denen Ihnen eine Provision versprochen wird, wenn Sie eine bestimmte Summe Geld entgegennehmen und weiterüberweisen. Auf dieses Angebot sollten Sie keinesfalls eingehen und die E-Mail sofort löschen, denn hier wird Geldwäsche betrieben oder aber ein Versuch gestartet, Ihnen Geld aus der Tasche zu ziehen. Leider fallen immer wieder Menschen auf diesen Trick herein und verlieren dadurch viel Geld.

Denken Sie daran: Auch im Internet wird kein Geld verschenkt!

Oftmals enthalten Spam-Mails auch Viren, Würmer und andere Malware, die Sie jedoch mit einem entsprechenden Sicherheitsprogramm entschärfen können (siehe Seite 11 ff.). Die meisten Security Suiten enthalten zudem einen Spam-Filter, der Ihnen hilft, das Problem Spam in den Griff zu bekommen (Softlink 323).

TIPP: Schutz vor Spam-Mails

- Nutzen Sie Spam-Filter, um Ihr Postfach möglichst Spam-frei zu halten. Diese werden auch von vielen E-Mail-Providern angeboten.
- Ignorieren Sie E-Mails, mit denen Sie nichts anfangen können, einfach und löschen Sie sie ungeöffnet.
- Öffnen Sie keine E-Mails, die Ihnen seltsam vorkommen. Wenn jemand, den Sie nicht kennen, wirklich etwas von Ihnen

möchte, wird er sich – wenn es wichtig ist – auch telefonisch melden oder eine E-Mail so verfassen, dass Sie sie von Spam unterscheiden können.
- Folgen Sie niemals irgendwelchen dubiosen Aufforderungen wie Geldüberweisungen für Erbschaften oder Ähnlichem.
- Kaufen Sie keine Ware oder Dienstleistung, die mittels Spam-Mail beworben wird. Wenn niemand mehr auf diese Angebote eingeht, wird Spam als Marketinginstrument uninteressant.

Hoax – falsche E-Mails

Hoax-E-Mails warnen klassischerweise vor angeblichen Viren oder anderen Gefährdungen: «Ein sehr gefährlicher Virus verbreitet sich aktuell sehr schnell. Sie erkennen ihn an dem Betreff , …'. Löschen Sie E-Mails mit diesem Betreff sofort und leiten Sie diese Warnung auch an andere weiter, damit der Virus sich nicht weiter verbreitet.»

Die Botschaft klingt im ersten Moment sehr hilfsbereit, ist aber nur eine Täuschung. Diese, als Hoax bezeichneten Nachrichten, sind nämlich völlig haltlos. Sie spielen mit der Angst des Anwenders, beinhalten selbst einen Virus oder dienen dem Sammeln von E-Mail-Adressen für Spam-Zwecke. Sie können sie also getrost löschen, selbst wenn Sie mittlerweile sogar mit dem Tod bedroht werden, falls Sie sie nicht weitersenden. Häufig enthalten diese E-Mails auch Verweise auf bekannte Organisationen wie Microsoft und verfügen über einen Absender, der auf den ersten Blick über jeden Zweifel erhaben ist (Polizei, Krankenhaus usw.). Doch lassen Sie sich davon nicht täuschen! Eine Liste bekannter Hoax-Mails finden Sie unter Softlink 324.

E-Mail-Anhänge

Auf zwei Arten können E-Mails direkt, also ohne erst auf einen Link zu klicken, für den Computer gefährlich werden. Erstens, indem sie HTML-Code beziehungsweise JavaScript enthalten. Das können Sie mithilfe entsprechender Einstellungen ausschließen (siehe Seite 74ff.). Die zweite Möglichkeit ist, dass sich die Schadsoftware im Anhang befindet. Das ist zugleich die einfachste Form eines Angriffs. Ein solcher Virus, Wurm oder ein solches Trojanisches Pferd wird aber nur gefährlich, wenn Sie den Anhang auch öffnen.

Besonders problematisch sind selbstausführende Dateien – vermeintlich schnell erkennbar an der Endung «.exe» –, deren Ausführung die direkte Installation einer Schadsoftware auf Ihrem Computer zur Folge haben kann. Aber die Angreifer sind schlauer geworden und verbergen die Exe-Dateien in anderen Dateiformaten (zum Beispiel pdf, doc oder avi) oder nutzen Sicherheitslücken in Office- und Multimediaprogrammen. Doch solange Sie eine einfache Regel beherzigen, ist auch diese Gefahr relativ leicht zu bannen: Öffnen Sie E-Mail-Anhänge nur, wenn Sie diese für vertrauenswürdig halten. Haben Sie Zweifel, kann eine kurze Nachfrage beim Absender der E-Mail Klarheit schaffen.

TIPP: E-Mail-Anhänge

- Öffnen Sie keine E-Mail-Anhänge, die Ihnen nicht vertrauenswürdig erscheinen – und erst recht keine Exe-Dateien.
- Bedenken Sie, dass Angreifer ihre Malware in so ziemlich allen Formaten (insbesondere auch pdf oder doc) verstecken können.
- Nehmen Sie im Zweifelsfall Rücksprache mit dem Absender, bevor Sie etwas öffnen.

Verschlüsselung – von der Postkarte zum Brief

Dass eine E-Mail von Dritten genauso leicht gelesen werden kann wie eine Postkarte, wurde bereits erwähnt. Aber auch das lässt sich mit ein wenig Mehraufwand ändern, indem Sie Ihre E-Mails verschlüsseln und sie so für alle außer einem spezifischen Empfänger unleserlich machen. Dazu benötigen sowohl Sie als auch der Empfänger einen Schlüssel, mit dessen Hilfe Sie die Daten ver- beziehungsweise entschlüsseln können. Die drei am häufigsten genutzten Technologien zur Verschlüsselung von E-Mails sind:

- PGP (Pretty Good Privacy)
- S/MIME (Secure/Multipurpose Internet E-Mail Extensions)
- passwortverschlüsselte Anhänge

Der Vollständigkeit halber sei erwähnt, dass S/MIME auch zusammen mit PGP verwendet werden kann.

Die Verfahren unterscheiden sich vor allem durch die Art des Schlüssels. PGP benötigt einen entsprechenden PGP-Schlüssel, während S/MIME typischerweise ein sogenanntes X.509v3-Zertifikat zur Verschlüsselung erfordert. S/MIME wird von den meisten E-Mail-Clients standardmäßig unterstützt, für PGP ist dagegen häufig eine Erweiterung notwendig. Beide sind auch kostenlos einsetzbar, wobei es für S/MIME nur sehr wenige kostenlose und sinnvoll nutzbare Zertifikate gibt. Einen PGP-Schlüssel können Sie mithilfe verschiedener Programme erzeugen, die den OpenPGP-Standard umsetzen. Das kann zum Beispiel über das freie PGP-Programm des Projekts GnuPG geschehen oder auch über kommerzielle Angebote (Workshop «PGP», siehe Softlink 325).

Durch den Einsatz dieser Technologien können E-Mails nicht nur verschlüsselt und somit für Fremde unleserlich gemacht werden, sondern auch digital signiert, also unterschrieben werden. Damit kann der Empfänger sicher sein, dass der Absender tatsächlich der ist, für den er sich ausgibt. So wird gleichzeitig das Problem des gefälschten Absenders gelöst.

Für den privaten Gebrauch ist es am einfachsten, PGP einzusetzen. Dabei ist wichtig zu wissen, dass der Kommunikationspartner natürlich über die gleiche Verschlüsselungsmethode verfügen muss. Bei PGP benötigen die Partner jeweils die öffentlichen Schlüssel voneinander. Ist die Verschlüsselung jedoch erst einmal eingerichtet, genügt ein Mausklick, um eine E-Mail zu verschlüsseln. Wie Sie eine solche PGP-Verschlüsselung installieren und verwenden, zeigt der Onlineworkshop (Softlink 325). Wollen Sie mehr zum Thema Verschlüsselung wissen, sei Ihnen der Onlineartikel «Kryptographie» empfohlen, den Sie unter Softlink 326 finden.

TIPP: E-Mail-Verschlüsselung

- Wenn Sie sicherheitskritische Daten per E-Mail versenden, sollten Sie die Daten unbedingt verschlüsseln.
- Wenn Sie eine Verschlüsselung verwenden, können Sie auch signieren. So können Sie den Absender eindeutig identifizieren und sicher sein, dass die E-Mail nicht manipuliert worden ist.

Ausblick: DE-Mail

Unter dem Namen DE-Mail wird von der Bundesrepublik und einigen privatwirtschaftlichen Unternehmen ein E-Mail-Dienst ins Leben gerufen, der den sicheren Austausch rechts-

gültiger Mails (Dokumente) zwischen Bürgern, Behörden und Unternehmen über das Internet möglich machen soll.

Um eine flächendeckende und sichere E-Mail-Kommunikation zu ermöglichen, sollen bei dem neuen DE-Mail-Dienst die Anbieter im Rahmen eines staatlich definierten Akkreditierungsverfahrens nachweisen, dass sie die geforderten Funktionalitäten erfüllen, die IT-Sicherheit gewährleisten und den Datenschutz einhalten. Dieser Zustand wird dann regelmäßig überprüft, und die Sicherheitsanforderungen werden der aktuellen Entwicklung angepasst. Anbieter des DE-Mail-Dienstes sollen die heutigen Webmail-Anbieter sein, die sich für den Dienst akkreditieren lassen. Als besondere Sicherheitsmechanismen werden die folgenden Maßnahmen umgesetzt:

- Sichere Anmeldeverfahren werden verwendet, zum Beispiel mithilfe des neuen elektronischen Personalausweises.
- Die Kommunikationsverbindung vom Computer des Nutzers zum DE-Mail-Anbieter erfolgt unter der Nutzung einer SSL/TLS-Verschlüsselung (siehe Seite 36 ff.).
- Die E-Mails werden zwischen den DE-Mail-Anbietern nur in verschlüsselter und integritätsgesicherter Form übertragen und gespeichert.
- Der Absender kann zusätzlich eine qualifizierte signierte (Kryptographie, siehe Softlink 326) Bestätigung anfordern, wann er die E-Mail verschickt hat und wann die E-Mail in das Postfach des Empfängers eingestellt wurde (DE-Mail-Einschreiben), die der heutigen Zustellung eines Einschreibens durch den Briefträger entspricht.

Dadurch, dass nur eindeutig identifizierbare Teilnehmer den DE-Mail-Dienst nutzen, wird sich auch die Spam-Rate voraussichtlich auf einem sehr niedrigen Niveau bewegen.

Die E-Mail-Adressen sollen folgendermaßen aufgebaut sein: ‹Vorname›.‹Nachnahme›@‹DE-Mail-Anbieter›.de-mail.de.

DE-Mail stellt mit den beschriebenen Verfahren aber keine durchgehende Verschlüsselung der E-Mails sicher, sondern nur des Transports. Dementsprechend wird bei sensiblen Daten auch weiterhin eine zusätzliche Verschlüsselung (PGP, S/MIME) notwendig sein.

Web 2.0 – das Mitmach-Web

Stellen Sie sich vor, Sie sitzen mit ein paar Freunden zusammen und reden über die wirklich wichtigen Dinge des Lebens: Welche aktuellen Musikalben gibt es? Wo kann man gut essen gehen? Wie war die Premiere des neuen Theaterstücks? Was macht der Nachbar wieder Verrücktes? Dieser Austausch von Informationen und Meinungen hilft uns, auf dem neusten Stand zu bleiben. Allerdings ist das informationstechnische Potenzial eines solchen «Kaffeekränzchens» doch sehr beschränkt, weil nur eine begrenzte Anzahl von Personen daran teilnehmen kann. Wäre es da nicht genial, wenn Sie sich aussuchen könnten, wer alles zum Kaffeeklatsch kommt und zudem das Thema selbst bestimmen? Herzlich willkommen im Web 2.0!

Der Begriff Web 2.0 ist durchaus umstritten, hat sich aber für die aktuelle Entwicklung im Internet etabliert und steht mittlerweile für die interaktive Zusammenarbeit vieler Nutzer, die gleichzeitig Anbieter und Konsumenten von Informationen sind. War das World Wide Web ursprünglich eine riesige Sammlung von verknüpften Dokumenten, die mithilfe

eines Browsers gefunden werden können, stellt ein Anbieter heute lediglich eine Web-2.0-Anwendung zur Verfügung, und die Nutzer sorgen für die Inhalte selbst.

Social Networking – ein Trend erobert das Web

Eine immer beliebter werdende Form von öffentlichen Web-2.0-Anwendungen ist das sogenannte Social Networking. Beispiele dafür sind Webseiten wie Facebook, StudiVZ, SchuelerVZ, MySpace, YouTube, XING, LinkedIn, Twitter & Co, wo sich Nutzer aus verschiedenen Gesellschaftsgruppen

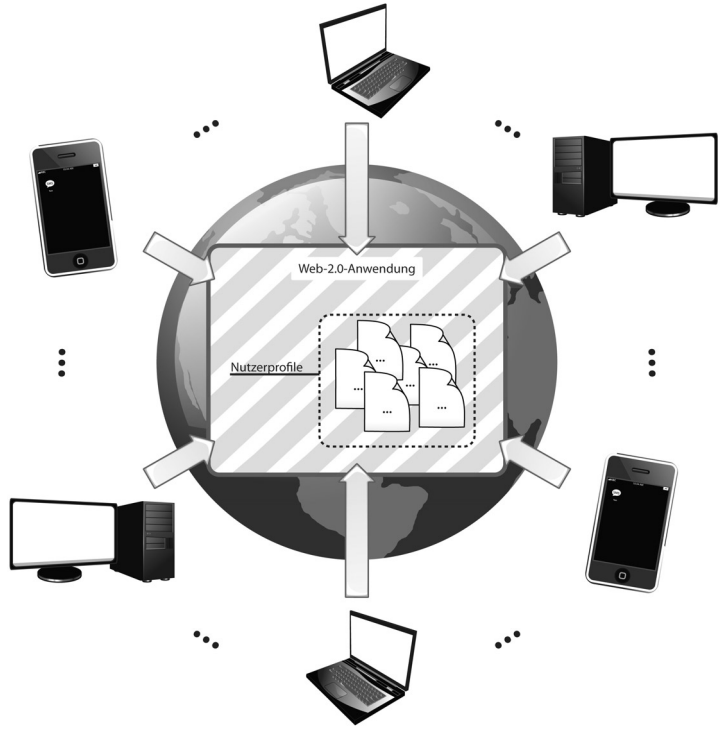

Abbildung 23: Social Networking als Web-2.0-Anwendung

auf verschiedene Arten kennenlernen und miteinander vernetzen können. Es gibt aber auch viele Web-2.0-Anwendungen, die speziell für bestimmte Städte und Regionen, bestimmte Berufsgruppen wie Lehrer und Anwälte oder einzelne Interessensgruppen wie SAP-Anwender aufgebaut wurden.

Neben den Social-Networking-Portalen, in denen die Nutzer Profilseiten mit persönlichen Informationen wie Werdegang, Freunde und Hobbys anlegen können, zählen auch Blogs, Wikis und Tauschseiten für Bilder oder Videos zu den Web-2.0-Anwendungen. Ebenfalls spannend sind Angebote wie Radio-Webseiten, bei denen anhand des Musikverhaltens der Nutzer aus Hunderten von Radiosendern ein entsprechendes Musik-Programm zusammengestellt wird.

Bei einem Blog oder Weblog handelt es sich um ein öffentlich einsehbares Tagebuch oder Journal. Autoren schreiben über bestimmte Aspekte des eigenen Lebens sowie ihre Meinungen zu spezifischen Themen – und die Leser kommentieren das Ganze. Ein Wiki ist eine Artikelsammlung im Internet, die nicht nur von jedem gelesen, sondern auch von jedem verändert werden kann. Das bekannteste Wiki ist Wikipedia, eine Wissens-Enzyklopädie, bei der die Idee der kollektiven Intelligenz umgesetzt wird, indem jeder Nutzer an den Inhalten aktiv mitarbeiten kann. Dadurch entsteht ein selbstregulierender Mechanismus, denn im Prinzip kann jeder Nutzer den Inhalt auf Korrektheit überprüfen und die vorhandenen Artikel korrigieren.

All diese neuen Anwendungen sind nur möglich, weil das Internet inzwischen eine breite Akzeptanz gefunden hat. Die Hemmschwelle, neue Anwendungen im Internet auszuprobieren, ist gesunken, sodass viele Nutzer den neuen Web-2.0-

Angeboten offen gegenüberstehen. Diese positive Entwicklung hat aber natürlich auch ihre Kehrseite. Gerade junge Menschen erzählen arglos über ihr Privatleben, ihre Arbeit, ihre Hobbys und ihre Interessen. Scheinbar hat diese Generation ein hohes Maß an Grundvertrauen, was den Umgang mit ihren persönlichen Daten angeht. Sie fühlen sich aufgrund der Anonymität in der Masse sicher und geben sehr viel von sich preis. Und diese Informationen sind im Prinzip für jeden einsehbar. Nicht nur Freunde oder Bekannte, sondern beispielsweise auch Personalchefs können sie lesen. Internetnutzer müssen deshalb – als Individuum und als Gesellschaft – lernen, mit den neuen Herausforderungen des digitalen Lebens umzugehen. Dazu gehört in erster Linie ein waches Bewusstsein dafür, was mit den eingestellten Informationen geschehen kann.

Ein weiterer interessanter Aspekt ist die rechtliche Situation hinsichtlich der von den Nutzern generierten und veröffentlichten Inhalte. Wem gehören die Kommentare in Blogs, die hochgeladenen Videos oder zur Schau gestellten Bilder? Wie verdienen die Anbieter von Web-2.0-Anwendungen das Geld, das nötig ist, um diese zu betreiben? Denn das kann je nach Größe schnell 100.000 bis mehrere Millionen Euro pro Jahr kosten.

Wikipedia zum Beispiel finanziert sich durch freiwillige Spenden, während bei einigen beruflich genutzten Web-2.0-Anwendungen die Nutzer monatliche Beiträge bezahlen müssen. Und manche finanzieren sich eben durch den Verkauf von Informationen, welche die Nutzer in die Web-2.0-Anwendung einstellen, oder durch generelle sowie individualisierte Werbung, die aus den vorhandenen Nutzerinformationen (Alter, Geschlecht, Hobbys, Beruf usw.) erstellt wird.

Social Networking mit Blick auf Datenschutz und Datensicherheit

Durch die Selbstbeschreibung in Social-Network-Anwendungen können Nutzer leicht alte Freunde wiederfinden, neue Freundschaften knüpfen oder virtuell Gruppen beitreten, welche die gleichen Interessen teilen. All das geschieht freiwillig und in einem ziemlich großen Umfang. Denn je mehr jeder Einzelne von sich preisgibt, und je aktiver er sich in der digitalen Szene bewegt, desto stärker wird er wahrgenommen.

Doch gerade dieser Aspekt des Social Networking wirft die Frage auf, wie es bei diesen Anwendungen um die informationelle Selbstbestimmung bestellt ist. Werden persönliche Daten analysiert oder gar an Dritte weitergegeben? Nicht selten basiert das Geschäftsmodell eines Web-2.0-Anbieters auf der Weitergabe von anonymisierten oder auch nicht anonymisierten Informationen, die Profile oder Statistiken über die Nutzung von spezifischen Seiten enthalten. Die jeweilige Handhabung des Datenschutzes wird explizit in den jeweiligen Allgemeinen Geschäftsbedingungen (AGB) erläutert. Es gibt zum Beispiel Anbieter, die penibel darauf achten, dass die Datenschutzgesetze eingehalten und personenbezogene Daten geschützt werden. Und es gibt natürlich Web-2.0-Anbieter, welche die Weitergabe von Informationen ausdrücklich erwähnen, um dadurch die gesetzlichen Bestimmungen zu erfüllen, die Nutzungsbedingungen durchzusetzen und ihre Interessen zu schützen, damit sie mit den Informationen der Nutzer Geld verdienen können.

Neben den scheinbar anonymen Bewegungsprofilen besteht auch die Gefahr, dass aus einer Kombination der per-

sönlichen Nutzerinformationen und den Verlinkungen innerhalb eines Netzwerks regelrechte Soziogramme erstellt werden. Die Web-2.0-Anbieter können diese für eine individualisierte Werbung nutzen. Ebenso ist die Möglichkeit, indirekt und relativ anonym neue Kontakte zu knüpfen, ein weiterer Gefahren-Aspekt des Social Networking. Zum Beispiel können Sexualstraftäter die Netzwerke nutzen, um Minderjährige anzusprechen. Vorfälle dieser Art nehmen Behörden immer öfter zum Anlass, die Profildatenbanken der betroffenen Web-2.0-Anbieter mit Informationen zu Sexual- oder anderen Straftätern abzugleichen. Dieses eigentlich positive Vorgehen wirft einmal mehr die Frage auf, ob und inwieweit der Datenschutz beim Social Networking tatsächlich gegeben ist und ob die Anwender nicht zu gläsernen Menschen werden, wenn eigentlich voneinander unabhängige Datenbestände miteinander verknüpft werden.

Weiß ein Internetnutzer nicht, mit wem er Kontakt hat, besteht noch eine weitere Gefahr. Große Web-2.0-Anwendungen sind genau wie Internetauktionshäuser und ähnliche Anwendungen attraktive Ziele für das Ausspähen von Nutzerdaten, etwa durch Phishing-Attacken (siehe auch Seite 100 ff.). Die so erlangten Zugangsdaten werden beispielsweise benutzt, um das Profil des Betroffenen zu manipulieren. Das hat meist einen großen sozialen Schaden für die betreffende Person zur Folge, zum Beispiel durch falsche Informationen über politische oder sonstige Einstellungen des Nutzers (Stichwort Cyber-Bullying, also virtuelles Mobbing). Auch ist die Wahrscheinlichkeit leider groß, dass der Geschädigte das gleiche Passwort für weitere Internetdienste benutzt, was zu Folgeschäden führen kann – zum sogenannten «Identitätskollaps».

Um sich dagegen zu schützen, bieten die meisten Web-2.0-Anwendungen Ihnen die Möglichkeit festzulegen, welche Informationen von wem gelesen werden dürfen. Sie können sich also überlegen, ob Sie Ihr Profil – oder Teile davon – auch außerhalb der eigentlichen Anwendung, also zum Beispiel für Suchmaschinen, freigeben möchten oder nicht. Genauso ist es in der Regel möglich, innerhalb der Web-2.0-Anwendungen zu entscheiden, ob alle Nutzer oder nur eine definierte Auswahl (Freunde, Nachbarn, Sportkameraden, Geschäftspartner …) auf Ihr Profil zugreifen dürfen. So können Sie unter anderem verhindern, dass unerwünschte Personen, wie der bereits angesprochene Personalchef, diese Inhalte zu sehen bekommen.

Soziale Beziehungen sind eine elementare Voraussetzung für ein erfülltes Leben. Wir lernen schon sehr früh, soziale Beziehungen einzugehen und integrieren uns – zumindest tun das die meisten von uns – in Gemeinschaften, denen wir uns zugehörig fühlen, zum Beispiel in die Familie, den Freundes- oder den Kollegenkreis. Innerhalb dieser Gemeinschaften positionieren wir uns entsprechend unserer Rolle. So hat beispielsweise jeder eine klare Vorstellung davon, wie er sich in seinem Freundeskreis verhalten soll, beziehungsweise was dort von ihm erwartet wird. Diese genauen Vorstellungen sollten wir auch in Bezug auf das digitale Leben entwickeln und uns überlegen, wie unsere Darstellung im Web 2.0 aussehen soll. Das heißt, jeder sollte bewusst entscheiden, welche Fotos er seinen Verwandten, seinen Freunden, seinen Kollegen oder seinen Sportkameraden präsentieren will. Und schon allein bei diesem Aspekt wird deutlich, dass wir uns in den verschiedenen Web-2.0-Angeboten wahrscheinlich auch unterschiedlich präsentieren wollen. Ebenfalls wichtig ist, zu entscheiden, wie groß die Gruppe sein soll und wer Mitglied

werden darf, beziehungsweise wer nicht hinein soll. Wenn jeder von uns diese Möglichkeiten aktiv gestaltet, dann können Social Networks eine echte Bereicherung für unser digitales Leben sein.

TIPP: Social Networks

- Gehen Sie stets sparsam mit Ihren persönlichen Daten um und geben Sie in Ihren Profilen nur die notwendigsten Informationen an.
- Wenn Sie sich bei einem Angebot nicht sicher sind, nutzen Sie ein Pseudonym statt Ihres echten Namens und ein eigenständiges Passwort.
- Verwenden Sie ein sicheres Passwort (siehe Seite 53 f.), damit niemand Ihre persönlichen Daten unbefugt ändern kann (Stichwort «Identitätsdiebstahl»).
- Geben Sie Ihr Passwort nicht leichtsinnig weiter.
- Definieren Sie für sich, welche Informationen Sie in welchem Social Network angeben wollen, um sich im Web 2.0 darzustellen.
- Legen Sie nach dem Beitritt zu einem Social Network sofort fest, wer auf Ihr Profil zugreifen darf (von außen und von innen), und nutzen Sie die Profileinstellungen zum Datenschutz.
- Sie sollten nur Informationen preisgeben (Fotos, Hobbys etc.), die Ihnen auch später einmal nicht peinlich sind oder schaden können.
- Zum Schutz Ihrer personenbezogenen Daten sollten Sie die AGBs des Web-2.0-Anbieters vor dem Erstellen eines Profils genau prüfen. Beachten Sie dabei, ob Informationen an Dritte weitergegeben werden und besonders in welchem Ausmaß.
- Seien Sie gegenüber anderen Teilnehmern im Web 2.0 zunächst einmal grundsätzlich misstrauisch. Das schützt Sie unter

Umständen vor fatalen Fehlentscheidungen. Bedingt durch die Anonymität des Internets ist nämlich nicht jeder der, für den er sich ausgibt.

User generated Content – die rechtliche Situation

Im Web 2.0, dem Mitmach-Web, ist jeder angehalten, eigene Texte zu veröffentlichen oder fremde zu kommentieren sowie Informationen zu sammeln und zu tauschen. Diese vom Nutzer eingestellten Inhalte werden auch User generated Content genannt. Da es dabei im Prinzip keine konkrete Unterscheidung zwischen dem Nutzer und dem Autor gibt, stellt sich die Frage, wem die Inhalte gehören. Hierzu gibt es einige Regelungen, wie zum Beispiel die Creative-Commons-Lizenzen (Softlink 331), deren Abstufungsgrade vom fast vollständigen Vorbehalt der Rechte bis hin zum völligen Verzicht auf Urheberrechte (Gemeinfreiheit) reichen. Wichtig sind in diesem Zusammenhang drei Punkte: Soll die Nennung des Urhebers vorgeschrieben sein? Ist die kommerzielle Nutzung der Inhalte erlaubt? Sind Veränderungen erlaubt? Mit diesen Lizenzen können Sie beispielsweise für Ihr Internettagebuch (Blog) festlegen, was genau mit den veröffentlichten Inhalten passieren darf.

Eine nicht so ohne Weiteres zu beantwortende Frage ist die, wem die zahlreichen Kommentare in den Blogs gehören. Aber auch hier können die Creative-Commons-Lizenzen Klarheit schaffen, indem man mit ihrer Hilfe in den AGBs festlegt, dass sämtliche Inhalte des Blogs, also alle Blogeinträge sowie die Kommentare der Besucher, nicht kommerziell verwendet oder verändert werden dürfen – wohl aber mit Nennung des Urhebers zitiert oder anderweitig publiziert werden

können. Ist ein Kommentator mit dieser Regelung nicht einverstanden, muss er sich entscheiden, ob er seinen Kommentar trotzdem an dieser Stelle abgibt oder in einem anderen Blog (mit passender rechtlicher Grundlage) und dann darauf verweist.

Ein anderer Bereich, in dem die rechtliche Situation bezüglich der Inhalte von großer Bedeutung ist, sind Dokumente, die der Allgemeinheit über Wikis zugänglich gemacht werden. Das im Internet sehr bekannte Beispiel Wikipedia zeigt, dass eine Gruppe interessierter Menschen sogar eine ganze Enzyklopädie auf die Beine stellen kann. Hierbei kommt für die Texte eine GNU-Lizenz zum Tragen, nämlich die GNU-Lizenz für freie Dokumentation – GNU-FDL (Softlink 332) –, zusammen mit der Creative-Commons-Attribution-ShareAlike-Lizenz 3.0 (CC-BY-SA). Dies sind Lizenzen für «freie Inhalte», die besagen, dass der Autor, also der Urheber der Information, keine Vergütung erhält und die Verbreitung ausdrücklich wünscht. Der Autor stellt den Inhalt damit jedem im Internet kostenlos zur Verfügung, macht ihn also gemeinfrei. Das gilt allerdings nur dann, wenn ein Dritter mit der Benutzung, Vervielfältigung, Verbreitung oder Veränderung des Inhalts auf gleiche Weise verfährt.

TIPP: Eigene Inhalte im Internet

- Überlegen Sie sich – bevor Sie den Inhalt einstellen – genau, was damit im Internet möglich sein soll und was nicht.
- Überprüfen Sie, ob die von der Web-2.0-Anwendung festgelegten Lizenzen und Rechte mit Ihren Vorstellungen übereinstimmen.
- Beachten Sie die entsprechenden gesetzlichen Bestimmungen (siehe Seite 162 ff.).

Inhaltsspeicherung und -austausch

Das Speichern und Tauschen von Bildern und Videos ist ein weiterer großer Bereich, in dem es viele Web-2.0-Anwendungen gibt. Die Nutzer können ihre Dokumente auf den Web-2.0-Server des Anbieters laden und so jederzeit und von jedem Ort darauf zugreifen. Außerdem sehen einige Nutzer diesen Dienst auch als eine Art Back-up ihrer lokalen Daten. Und natürlich wird auch hier über Inhalte, die der Allgemeinheit zugänglich gemacht wurden, diskutiert und sich ausgetauscht. Besonders Videoplattformen wie YouTube oder sogenannte Video-Podcasts erfreuen sich derzeit großer Beliebtheit. Mittels Videobotschaften bieten Autoren individuelle Videos, beispielsweise ihr Tagebuch, allen Interessierten im Internet zum Download an.

Spannend ist hierbei die Betrachtung der vom Anbieter beanspruchten Rechte und Lizenzen, wobei zwischen der Inhaltsspeicherung und dem Inhaltsaustausch unterschieden werden muss. Es gibt Anbieter, die sich komplett vom übertragenen Inhalt distanzieren und keinerlei Haftung übernehmen, während andere weitgehende Rechte und Lizenzen für Veränderung, Verkauf, Vervielfältigung oder Verbreitung der Inhalte für sich beanspruchen. Beide haben zwei Dinge gemeinsam: Sie setzen voraus, dass der Nutzer des Dienstes die Rechte für den eingestellten Inhalt besitzt und dass dieser nicht gegen geltendes Recht verstößt.

Nutzt nun jemand ein solches Angebot als Onlinefestplatte oder als Back-up-Möglichkeit, hat er keine Garantie dafür, dass die Daten unverändert und vor allem verfügbar bleiben. In den Nutzungsbedingungen und AGBs wird meist nur vage auf diese Punkte eingegangen. Schwammige Formulierungen

wie: «Wir fahren öfter Back-ups, als Sie die Dateien ändern können», geben dem Nutzer keine Sicherheit, da auf die Punkte Integrität und Verfügbarkeit nur indirekt eingegangen wird. Auch andere harte Fakten wie Verschlüsselung und Übertragungssicherheit werden weder konkret angesprochen noch garantiert.

Wie Sie bereits an diesen kurzen Ausführungen sehen, sind die Möglichkeiten des Web 2.0 sowie die entsprechende Rechtslage noch ziemlich undurchsichtig. Gehen Sie deshalb stets mit der gebotenen Vorsicht zu Werke. Sie sollten bei Ihren Ausflügen in die digitale Welt zudem im Hinterkopf behalten, dass das Internet nichts vergisst. Das bedeutet, dass alle Informationen sehr lange im Internet gespeichert werden und im Regelfall für alle Interessierten jederzeit verfügbar sind. Ein Beispiel dafür ist das gemeinnützige Projekt www.archive.org. Ein Internetarchiv, das 1996 gegründet wurde und sich die Langzeitarchivierung digitaler Daten in frei zugänglicher Form zur Aufgabe gemacht hat. Es speichert Momentaufnahmen von allen Webseiten sowie weitere Informationen.

TIPP: Inhaltsspeicherung und -austausch

Überprüfen Sie, ob die von der Web-2.0-Anwendung festgelegten Lizenzen und Rechte mit Ihren Vorstellungen übereinstimmen. Auch sind Plattformen wie YouTube oder Flickr keine adäquate Back-up-Möglichkeit.

Vertrauliche Unternehmensdaten im Web 2.0

Das Web 2.0 ist auch für Unternehmen interessant. Deren Mitarbeiter können sich über Web-2.0-Anwendungen sehr schnell neues Wissen aneignen und Informationen beschaffen,

was die Innovationsgeschwindigkeit im Unternehmen steigern kann. Dazu tragen natürlich auch Diskussionen unter den Mitarbeitern über neue Ideen bei. Doch wer sich an Diskussionen in den Web-2.0-Anwendungen beteiligt, sollte immer bedenken, dass er der Konkurrenz damit unter Umständen wertvolle Informationen in die Hände spielt. Daher gilt: Vertrauliche Unternehmensinformationen sollten generell nicht im Internet besprochen werden.

Exkurs: das Phänomen Twitter

Barack Obama tut es, Britney Spears tut es und Paulo Coelho ebenfalls: twittern. Mithilfe des Internetdienstes Twitter lassen immer mehr Menschen – ob prominent oder nicht – die Welt daran teilhaben, was sie gerade tun, denken oder planen. Dabei handelt es sich um ein öffentlich einsehbares Tagebuch (Mikroblog), in dem sich der Nutzer mittels kurzer Nachrichten (maximal 140 Zeichen) entsprechend darstellen kann. Die Nachrichten sind in der Regel aus der Ich-Perspektive verfasst und stellen für den Verfasser und die Leser ein einfach zu handhabendes Echtzeit-Kommunikationsmedium dar, wobei die Leser bei Twitter als Follower bezeichnet werden. Der Verfasser kann entscheiden, ob er seine Nachrichten allen Interessierten oder nur einer definierten Gruppe zugänglich machen will.

Ein Problem bei Twitter ist, dass viele Nutzer ein Passwort auswählen, das sich leicht knacken lässt (siehe Seite 51 ff.). Die Folge: Fremde können unter einer falschen Identität Nachrichten versenden. Das Problem dabei ist, dass die Unbekannten den Betroffenen so Dinge in den Mund legen können, die nicht der Wahrheit entsprechen und diese in ein schlechtes Licht rücken.

Ein weiteres Problem ist, dass Nutzer sich unter einem falschen Namen anmelden können. Eine Überprüfung des sich registrierenden Nutzers wird nicht zwingend durchgeführt. Das vermutlich beste Beispiel für einen solchen Fall ist Rob Vegas, der einige Monate lang als Harald Schmidt «zwitscherte». Zwar hat Twitter hier einen ersten Schritt unternommen, um Abhilfe zu schaffen, und sogenannte Verified Accounts eingeführt (bei denen eine Verifikation des Nutzers vorgenommen wird), die an einem blauen Siegel zu erkennen sind. Doch aufgrund des hohen manuellen Aufwands erhalten dieses Siegel derzeit nur sehr wenige Accounts.

Und schließlich gilt auch bei der Twitter-Nutzung, dass sich der «Twitternde» genau überlegen sollte, was er der Öffentlichkeit preisgibt. Die Information über den momentanen Aufenthaltsort zum Beispiel kann auch für Einbrecher durchaus interessant sein …

TIPP: Vorsichtsmaßnahmen beim Twittern

- Wollen Sie über Twitter Nachrichten verbreiten, überlegen Sie sich im Vorfeld genau, wer die Nachrichten lesen soll und welche Art von Information darin enthalten sein soll.
- Nutzen Sie Twitter als Follower, sollten Sie aufpassen, dass die Nachrichten auch wirklich von demjenigen stammen, den Sie hinter dem Profil vermuten.

Freuen Sie sich auf Teil 4:
Sicher bewegen im Internet – Onlinebanking, E-Commerce, Auktionshäuser im Internet

Ab 28.01.2013 zum kostenlosen Download auf
www.internet-sicherheit.de