



INTERNETSICHERHEIT AUF EINEN BLICK

Immer mehr unerwünschte Werbebotschaften füllen das E-Mail-Postfach, Angriffe durch Würmer oder Trojaner gehören mittlerweile zum Alltag. Das ist teils lästig, teils eine regelrechte Gefahr für die Funktionsfähigkeit des eigenen PCs, aber auch für die eigenen Daten. Das Internet bringt ungeahnte Chancen für die Informationsgesellschaft mit sich – und gleichzeitig eine Vielzahl von Risiken.

„Internetsicherheit auf einen Blick“ erläutert die wichtigsten Begriffe und Grundregeln, um das Surfen, Tauschen und den Handel im Internet sicherer zu machen.

ANGRIFFSPUNKTE

Online zu gehen wird dank ständig sinkender Preise erschwinglicher und funktioniert durch die immer besseren Übertragungsraten auch richtig zügig. Aber der bloße Internetzugang birgt bereits gewisse Gefahrenquellen in sich. Durch die Möglichkeit, Datenverbindungen per Funk herzustellen, also zum Beispiel durch WLAN oder UMTS, steigt das Risiko noch, weil Funknetzwerke nur bedingt „einbruchssicher“ sind. Weitere Angriffspunkte bietet der Browser oder das verwendete E-Mail-Programm.

Mobile Zugänge

Lokale Funknetze (WLAN – „Wireless Local Area Network“) werden immer selbstverständlicher, insbesondere seit mobile Endgeräte mehr Verbreitung finden. Oftmals ist eine WLAN-Karte im Rechner bereits eingebaut. Darüber hinaus sind ein WLAN-Router sowie ein Netzzu-

gang notwendig. Unterwegs übernehmen diese Aufgabe sogenannte Hot-Spots, die es zum Beispiel in Flughäfen, Bahnhöfen, Parkanlagen, Universitäten, in einigen Kaffeehaus- oder Fastfoodketten oder auch in Zügen der Deutschen Bahn gibt – teilweise sogar kostenlos.

Aber Vorsicht: Sicherheitslücken beim „öffentlichen Surfen“ nutzen Hacker aus, um auf Fremdkosten online zu gehen, Daten auszuspionieren oder diese zu manipulieren („WLAN-Hack“). Daher gehört es zur persönlichen Sorgfaltspflicht, sich über die Sicherheitsgegebenheiten vor Ort und auf dem privaten (mobilen) Endgerät zu informieren. Der WPA2-Algorithmus („Wi-Fi Protected Access“) sollte immer aktiviert sein, um den Funk-Datenverkehr zu verschlüsseln. Schon beim Kauf eines WLAN-fähigen Geräts ist es wichtig, auf die Unterstützung dieses Verschlüsselungsstandards zu achten.

INTERNETSICHERHEIT AUF EINEN BLICK

mekonet Dokulinks

Mit seinem Dokulink-Service möchte **mekonet** Sie dabei unterstützen, komplexe Internetadressen leichter erreichen zu können, auf die wir in unseren Materialien hinweisen. Hinter dem Texthinweis „Dokulink“ finden Sie jeweils eine zugehörige Nummer zum Angebot. Wenn Sie dieses Angebot aufrufen möchten, tippen Sie die Nummer in das Eingabefeld auf unserer Internetseite unter www.mekonet.de/dokulink ein. Sie werden dann automatisch zum entsprechenden Angebot weitergeleitet.

Manchmal reicht auch ein Update der dazugehörigen Treibersoftware aus. Ergänzend sollte eine „Personal Firewall“ aktiviert sein. Das gilt auch für das mobile Surfen per UMTS („Universal Mobile Telecommunications System“), ebenso wie für das Surfen am heimischen Computer allgemein.

Browser als Einfallstor

Neben dem Internetzugang ist der Browser ein wichtiges Einfallstor für Angriffe aus dem Internet, denn er ist die Haupt-Software-Schnittstelle zu den virtuellen Welten. Viele Sicherheitsoptionen sind am Browser selbst einstellbar. Dabei gibt es keine generell „richtige“ Einstellung. Ein hoher Schutzstandard bedeutet häufig, dass viele vertraute Internetseiten nicht mehr erreicht werden können, weshalb ein persönlicher Kompromiss zwischen Funktionalität und Sicherheit gefunden werden muss. Um diesen heraus zu finden, helfen Tests.

- Einen kostenlosen Selbsttest für den Rechner bietet „heise Security“ zusammen mit dem Landesbeauftragten für den Datenschutz des Landes Niedersachsen an.
Dokulink 261815
- Nicht nur junge Online-Nutzer(innen) können online lernen, sicher und kompetent mit dem Internet umzugehen. Die Dienstleistungsgesellschaft für Informatik GmbH (DLGI) in Kooperation mit der EU-Initiative klicksafe stellt als Ergänzung zum Europäischen Computerführerschein (ECDL – European Computer Driving License) Lernmodule (Kurs 7: Internet und Kommunikation) zur Internetsicherheit kostenlos zur Verfügung.
www.ecdl-moodle.de

E-Mail-Client

Das Programm zum E-Mail-Versand oder Empfang – der sogenannte E-Mail-Client – ist neben dem Internetzugang und dem Browser die dritte große Angriffsstelle auf dem Rechner.

Insbesondere Programme mit einer automatischen Vorschau-Funktion auf E-Mails (wie Outlook) bieten hier diverse Angriffsmöglichkeiten. Diese Vorschau erlaubt es schädlichen Programmen, sich sofort im System niederzulassen. Deshalb sollte diese Funktion unbedingt deaktiviert werden. In neueren Versionen wurde das bereits berücksichtigt. Die automatische Anzeige von verlinkten Bildern im Netz birgt eine weitere Gefahr.

Zudem empfiehlt sich die Benutzung eines zusätzlichen Webmail-Accounts für den E-Mail-Empfang von nicht als vertrauenswürdig bekannten Absender(inne)n – auch wenn ein eigener E-Mail-Client auf dem Rechner verfügbar ist. Die in den Mails versteckten schädlichen Programme und HTML-Elemente können dort als reiner Text angezeigt werden und so keinen Schaden auf dem heimischen Computer anrichten.

SPAM – DIE WERBEFLUT

Ein besonderer Fall ist der Umgang mit Spam: Ursprünglich ist „Spiced Ham“ – kurz Spam – eine Markenbezeichnung für Dosenfleisch. Heutzutage steht der Begriff für E-Mails, die Werbung, Pornoangebote oder andere, unverlangt zugesandte Informationen enthalten. Sie sind vor allem lästig und weniger ein Sicherheitsrisiko, es sei denn, die E-Mail oder ihr Anhang sind mit schädlichen Programmen infiziert.



Spam-Filter

Um sich gegen Spam-Mails zu wappnen, bedarf es entweder eines in das E-Mail-Programm (zum Beispiel MS Outlook, Mozilla Thunderbird, Eudora) integrierten Spam-Filters oder einer speziellen Erweiterung (engl. „Plugin“) eines Drittanbieters. Hier gibt es je nach Bedarf kostenpflichtige Anwendungen, aber auch kostenlose freie Software (engl. „Freeware“) am Markt beziehungsweise im Internet.

Sinnvoll und kostengünstiger ist es, zunächst die Funktionen des integrierten Filters des installierten E-Mail-Programms zu nutzen, und diese erst bei komplexeren Anforderungen (eventuell kostenpflichtig) zu erweitern. Zudem bieten die populären E-Mail-Provider nicht nur kostenlose E-Mail-Adressen und Postfächer an, sondern filtern auch eingehende Spam-E-Mails aus. Vorteil: Meist arbeiten die Filterprogramme der großen Provider effektiver und werden regelmäßiger aktualisiert als private Software.

- Die Webseite verbraucher-gegen-spam.de ist Teil des Projekts „Spamkampagne“ und klärt Privatpersonen über das Thema Spam auf. Das Projekt „Spamkampagne“ setzt die Ziele des auf Initiative des Bundesverbraucherministeriums geschlossenen Aktionsbündnisses zur Bekämpfung von Spam um.
www.verbraucher-gegen-spam.de

E-Mail im Netz

Für die Teilnahme an Gewinnspielaktionen oder für öffentliche Einträge zum Beispiel in Foren oder Chatrooms lohnt es sich, zusätzliche E-Mail-Adressen anzulegen, die

nach ein- oder mehrmaligem Gebrauch nicht mehr benutzt werden (sogenannte Wegwerfadressen).

Anbieter hierfür sind zum Beispiel:

- Spamgourmet www.spamgourmet.com
- trash-mail www.trash-mail.com
- Spambog www.spambog.com

Leider erkennen viele Anbieter mittlerweile die sogenannten Wegwerfadressen und erlauben keine Anmeldung mehr über sie, weshalb diese Strategie nicht immer funktioniert.

Verhaltensregeln

Aber auch die Einhaltung bestimmter Verhaltensregeln schützt eine E-Mail-Adresse vor Spam:

- Die persönliche E-Mail-Adresse nur Freund(inn)en und Geschäftspartner(inne)n mitteilen.
- Die persönliche E-Mail-Adresse nicht unbedacht in öffentliche Adresslisten, Newsgroups und Newsletter eintragen.
- Nie auf Spam-Mails antworten oder auf darin enthaltene Links klicken, ansonsten erhält der Versender eine Bestätigung, dass die angeschriebene Adresse in Gebrauch ist.

Weitergehende Informationen finden sich auch

- im Anti-Spam Leitfaden des Verbandes der deutschen Internetwirtschaft e.V. (eco).
Dokulink 362172
- in der Broschüre „IM BLICKPUNKT: Identitäten im Netz“.
Dokulink 986622

INTERNETSICHERHEIT AUF EINEN BLICK

Quellen

- Die Broschüre „IM BLICKPUNKT: Internetkriminalität“, beschreibt Erscheinungsformen und Aufkommen der Internetkriminalität wie zum Beispiel „WLAN-Hacking“, nennt Verhaltensregeln, Anlaufstellen, Informationsmöglichkeiten und Reaktionsmaßnahmen.
Dokulink 519310

- Die Broschüre „IM BLICKPUNKT: Social Communities“ erklärt, wie soziale Gemeinschaften im Netz funktionieren, welche Möglichkeiten sie bieten, aber auch, welche Risiken mit ihrer Nutzung verbunden sind und zeigt Wege auf, um sich und seine Daten zu schützen.
Dokulink 668436

- Die Internetpräsenz „Surfer haben Rechte“ ist Teil des Projekts „Verbraucherrechte in der digitalen Welt“ des Verbraucherzentrale Bundesverbands und bietet umfangreiche Informationen und Nachrichten zum Thema.
www.surfer-haben-rechte.de

- Das Portal „Verbraucher sicher online“ bietet sowohl umfassende Informationen zum sicheren Surfen im Netz als auch leicht verständliche Anleitungen für digitale Anwendungen wie beispielsweise Musik- und Videoplayer.
www.verbraucher-sicher-online.de

- Das Bürger-CERT ist ein Projekt des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Das Bürger-CERT informiert und warnt Bürger(innen) und kleine Unternehmen schnell und kompetent vor Viren, Würmern und anderen Sicherheitslücken – kostenfrei und absolut neutral.
www.buerger-cert.de

GEFAHREN & ABWEHR

Für die meisten Nutzer(innen) gehört Sicherheitssoftware immer noch nicht zum Standard, so die Ergebnisse einer Studie im Auftrag des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) vom Juni 2008. Fraglich ist, ob die Risiken unbekannt sind oder einfach nur unterschätzt werden.

Die Begriffserklärungen vermitteln das Basiswissen über die bedeutsamsten Gefahren und die wichtigsten Abwehrmaßnahmen.

Gefahren

Wenn die Rechnerleistung des PCs plötzlich rapide abnimmt oder Dateien auf einmal verschlüsselt sind, steckt meistens ein Befall durch schadhafte Programme dahinter: Trojaner „schleichen“ sich, als Teil eines vermeintlich nützlichen Programms getarnt, ein und ermöglichen die Kontrolle eines Computers von außen. Teilweise werden die befallenen Rechner auch zu sogenannten Botnetzen verknüpft und für bestimmte Aktionen ferngesteuert (zum Beispiel „Denial of Service“-Attacken oder massenhafter Versand von Spam-E-Mails). Viren verbreiten sich per E-Mail, beim Tausch von Datenträgern, beim Herunterladen von Dateien aus dem Internet oder auch nur beim bloßen Ansurfen einer Webseite und verändern oder löschen Programme und Dateien beziehungsweise machen diese unbrauchbar. Teils passiert aber auch gar nichts, würde der Virus mit nachhaltigen Schäden doch seinen „Wirt“ gefährden oder auf sich aufmerksam machen. Würmer reproduzieren sich selbst und verbreiten sich dann per E-Mail im Anhang weiter, etwa nach der

Anmeldung in einem befallenen Online-Netzwerk. Sie werden in der Regel nur durch Anklicken aktiv.

Spyware „spioniert“ private Daten – gespeicherte Informationen und/oder das Surfverhalten – mit Hilfe unerkannt eingeschleuster kleiner Programme aus und gibt diese unbemerkt an Dritte weiter.

Verhaltensregeln

Welche Abwehrmaßnahmen sind zu ergreifen? Es gibt ein paar Verhaltensregeln beim Surfen, die zusammen mit den passenden technischen Vorkehrungen bereits wirkungsvoll schützen. Wer ausschließlich auf vertrauenswürdigen Seiten surft, also etwa pornografische Angebote oder Websites mit illegaler Software meidet, senkt die Gefahr, sich schadhafte Software einzufangen. Die „Erfolge“ der Hacker beruhen nicht zuletzt auf Gutgläubigkeit, Neugierde und Bequemlichkeit der Internetnutzer(innen).

Folgende Regeln gilt es zu beachten:

- Keine Programme von unbekanntem Servern oder Seiten herunterladen.
- Keine Dateianhänge in unbekanntem E-Mails öffnen.
- Keine Passwörter auf dem Rechner speichern.
- Für den Notfall Sicherungskopien erstellen und Originalsoftware sowie Key-Codes aufbewahren.
- Auch wer über eine „Flatrate“ verfügt, sollte die Internetverbindung beenden, wenn nicht mehr am Rechner gearbeitet wird – auch aus Energiespargründen.

INTERNETSICHERHEIT AUF EINEN BLICK

Antiviren-Software

Schadhafte Programme gelangen entweder durch das unabsichtliche Herunterladen, beim Installieren von unbekannter Software, beim Öffnen verseuchter E-Mail-Dateianhänge oder aber über infizierte Speichermedien, wie zum Beispiel USB-Sticks, auf den PC. Eine zentrale Sicherheitsmaßnahme zum Schutz des Computers ist daher der Einsatz von Antiviren-Software. Sie identifiziert und löscht schadhafte Programme und gehört in vielen Fällen bereits zur Rechnergrundausstattung.

- Unter www.av-test.org finden sich aktuelle Tests und Links zu kostenlosen Antiviren-Programmen und Virenscoannern. Diese helfen aber nur, wenn die Virendatenbanken regelmäßig per Internet aktualisiert werden.

Sicherheits-Updates

Absoluter Schutz ist nicht zu erreichen. Das Schutzniveau erhöhen aber – neben der regelmäßigen Aktualisierung der Antiviren-Software – Sicherheitsupdates des Betriebssystems sowie des Browsers.

Aber Achtung bei Updates, die über das Beseitigen von Sicherheitsmängeln und Fehlern hinausgehen (Upgrades oder Versionssprünge): Neue Versionen einer Software sind nicht automatisch besser als die vorherigen. Teilweise entstehen sogar neue Probleme, weil einzelne Anwendungen plötzlich blockiert werden oder nicht mehr wie bisher funktionieren. Günstig ist in diesem Fall, sich Erfahrungsberichte anderer Benutzer aus entsprechenden Foren zu beschaffen, bevor die Installation vorgenommen wird. Und unbedingt die Informationen des Softwareherstellers beachten!

Firewalls

Die Überwachung und Steuerung des Datenflusses in den und aus dem Computer ist die Aufgabe von Firewalls (dt. „Brandschutzmauern“). Externe Zugriffe auf den Rechner werden verhindert, Datentransfers nach außen (zum Beispiel ins Internet) mit Hilfe eines Programmfensters angezeigt. So kann man von Fall zu Fall entscheiden, ob der Zugriff gestattet werden soll oder nicht.

E-COMMERCE UND SOZIALE NETZWERKE

Die größten Sicherheitsrisiken beim E-Commerce liegen im Zahlungsvorgang von Waren und Dienstleistungen. Hier sollte auf eine gesicherte Verbindung zwischen dem eigenen Rechner und dem Anbieter geachtet werden, also auf den verschlüsselten Austausch sensibler Daten, erkennbar am Wechsel des verwendeten Internetprotokoll: Aus <http://> in der Adresszeile wird <https://>. Teils wird dieser im Browserfenster auch durch ein Schloss-Symbol angezeigt. Es erscheint un-

ten links beim MS-Internet Explorer oder unten rechts beim Mozilla Firefox, bei dem zusätzlich die Adressleiste farbig unterlegt wird.

Zahlungsarten

Risikoarm ist die Zahlung per Rechnung oder Einzugsermächtigung. Im Falle der Rechnung wird nur dann gezahlt, wenn die Ware bei Erhalt in Ordnung ist. Im Falle der Einzugsermächtigung kann dem Bankeinzug widersprochen werden, wenn die Ware zu beanstanden ist, und das Kreditinstitut bucht den Betrag dann zurück. Bei Nachnahmesendungen ist das nicht möglich. Vertragspartner sind daher sorgfältig auszuwählen und bei Zweifeln Adressangaben und Telefonnummern zu prüfen.

Die Kreditkartenzahlung ist risikoreicher, weil die Zahlung dem Warenerhalt voraus geht. Wenn die Ware bei Erhalt zu beanstanden ist, muss die bereits erfolgte Zahlung vom Anbieter zurückgefordert werden. Und das kann sehr mühselig sein, auch wenn die Rechtslage klar ist. Siehe hierzu ausführlicher die Informationen der Verbraucherzentrale Nordrhein-Westfalen.

Dokulink 231960

Phishing oder Pharming

Sollte bei EC- oder Kreditkartenzahlungen nach der Geheimzahl (PIN-Nummer) gefragt werden, ist der Zahlungsvorgang sofort abzubrechen – Phishing oder Pharming droht. Phishing bezeichnet alle Verfahren, bei denen versucht wird, etwa mit Hilfe gefälschter E-Mails, vertrauliche Zugangs- und Identifikationsdaten argloser Dritter auszuspähen. Mit diesen Daten wird dann – unter der Identität des Inhabers – im Online-Verkehr gehandelt. Waren werden angeboten und abkassiert oder illegale Transaktionen durchgeführt.

Das Pharming kommt ohne bewusste Mitwirkung der Opfer aus und stellt eine Weiterentwicklung des Phishing dar. Hierbei wird der oder die ahnungslose Nutzer(in) auf eine Seite umgeleitet, die der bekannten Bankwebseite täuschend ähnelt. Er oder sie gibt seine/ihre private PIN/ TAN-Kombination ein – damit in die Hände krimineller Dritter – und es kommt zu Abbuchungen. Fallen diese auf, sollte umgehend das Kreditunternehmen informiert werden, um Gegenmaßnahmen einzuleiten.

Gütesiegel

Vertrauenswürdige Onlineshops sind an Gütesiegeln zu erkennen. Welchen man vertrauen kann und warum, erklärt die Initiative D21 unter www.internet-guetesiegel.de. Getestete und für gut befundene Gütesiegel und Empfehlungen finden sich ebenso bei www.label-online.de, einem Portal der Verbraucher Initiative e.V.

INTERNETSICHERHEIT AUF EINEN BLICK

Soziale Netzwerke

Sicherheitsfragen stellen sich zunehmend auch hinsichtlich der sozialen Netzwerke. Ähnlich dem klassischen Spam-Versand per E-Mail können auch über gekaperte Benutzerkonten – per Phishing oder Pharming – oder die Ausnutzung von Schwachstellen in Webanwendungen gefälschte oder mit Schadsoftware infizierte Nachrichten etwa in Twitter oder Facebook versandt werden. Teils wird auch über falsche Identitäten zu finanziellen Transaktionen aufgefordert – alle hier beschriebenen Bedrohungen finden ebenfalls innerhalb dieser populären Sphäre Opfer.

NOCH FRAGEN?

Spannende Projekte, interessante Studien und vertiefende Literatur finden Sie unter www.mekonet.de im „Grundbaukasten Medienkompetenz“. Auch die Handreichungen *mekonet* kompakt und die Dokumentationen der Fachtagungen bieten weiterführende Informationen. Oder wenden Sie sich direkt an das *mekonet* Projektbüro.

KONTAKT

mekonet – Medienkompetenz-Netzwerk NRW
Medienbildung für Multiplikatoren

Projektbüro *mekonet*
c/o ecmc
Europäisches Zentrum
für Medienkompetenz GmbH
Bergstr. 8
45770 Marl

Tel: +49 (0) 2365 9404-48
Fax: +49 (0) 2365 9404-29

E-Mail: info@mekonet.de
Internet: www.mekonet.de

Der Ministerpräsident
des Landes Nordrhein-Westfalen



>lfm:
Landesanstalt für Medien
Nordrhein-Westfalen (LFM)



Die Staatskanzlei des Landes Nordrhein-Westfalen und die Landesanstalt für Medien Nordrhein-Westfalen haben *mekonet*, das Medienkompetenz-Netzwerk, initiiert und beauftragt. Die ecmc Europäisches Zentrum für Medienkompetenz GmbH ist mit der Projektleitung von *mekonet* betraut. Das Werk einschließlich seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung der ecmc Europäisches Zentrum für Medienkompetenz GmbH, der Staatskanzlei des Landes Nordrhein-Westfalen und der Landesanstalt für Medien Nordrhein-Westfalen unzulässig und strafbar.

Haftungsansprüche gegen die ecmc Europäisches Zentrum für Medienkompetenz GmbH, die Staatskanzlei des Landes Nordrhein-Westfalen und die Landesanstalt für Medien Nordrhein-Westfalen, die sich auf Schäden materieller oder ideeller Art beziehen, welche durch die Nutzung oder Nichtnutzung der dargebotenen Informationen oder durch fehlerhafte und unvollständige Informationen verursacht wurden, sind vollumfänglich ausgeschlossen, sofern seitens der ecmc Europäisches Zentrum für Medienkompetenz GmbH, der Staatskanzlei des Landes Nordrhein-Westfalen und der Landesanstalt für Medien Nordrhein-Westfalen kein nachweisliches vorsätzliches oder grob fahrlässiges Verschulden vorliegt.