INTERNETSICHERHEIT AUF EINEN BLICK

Spam füllt das Mail-Postfach, schädliche Programme greifen den Computer an, Passwörter und Dateien in der Cloud werden ausspioniert. Das sind ernsthafte Gefahren für den Computer, das Smartphone oder das Tablet, auf denen immer mehr persönliche Daten verwaltet werden. Das Internet bringt für Nutzer viele Chancen mit sich – und einige Risiken, die manche Menschen vor dem Medium zurückschrecken lassen.

„Internetsicherheit auf einen Blick" nennt die wichtigsten Angriffspunkte und Grundregeln, um das Surfen, das Teilen und den Handel im Internet sicherer zu machen. Es wird auch erklärt, welche Einstellungen wichtig sind, um Computer und mobile Geräte vor fremden Zugriffen zu schützen.

ANGRIFFSPUNKTE

Online zu sein, ist alltäglich: Knapp 76 Prozent der Deutschen nutzen das Internet (ARD/ZDF Onlinestudie 2012). Das birgt auch Gefahren, die man kennen und vermeiden sollte, ohne auf die vielfältigen Möglichkeiten des Internets zu verzichten. Angriffspunkte bieten Browser, Mail-Programme, Apps und drahtlose Datenverbindungen wie WLAN oder UMTS.

Drahtloser Internetzugang

Lokale und mobile Funknetze sind fast allgegenwärtig, um vor allem mit mobilen Geräten wie Smartphones, Tablets und E-Readern online zu sein. Nicht nur unterwegs in Bahnhöfen, Museen, Einkaufszentren und Restaurants sind WLAN-Netze beliebt. Auch im eigenen Haushalt und Büro hat sich WLAN durchgesetzt, um Kabel zu reduzieren, Geräte flexibel zu positionieren und Gästen einen einfachen Zugang zum Internet zu gewähren.

Jedoch können Sicherheitslücken beim Surfen im öffentlichen WLAN von Hackern und Dritten ausgenutzt werden, um Daten auszuspionieren und zu manipulieren, persönliche Accounts zu übernehmen oder illegale Downloads zu tätigen. Deshalb sollten keine sensiblen Aktionen, beispielsweise Online-Banking oder -Shopping, durchgeführt werden. Das private WLAN sollte mindestens über den Verschlüsslungsstandard WPA2 verfügen und durch ein sicheres Passwort gegen unerwünschte Nutzer geschützt sein.

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.

Alternativ können Sie den Dokulink auch direkt aufrufen, indem Sie nach **mekonet.de/d/** die jeweilige Nummer des Dokulinks in die Webadresse einfügen, also z. B. **mekonet.de/d/123456**.

Quellen und weitere Informationen (I)

- „Mobil ins Netz – Smartphone & Co einfach auf den Punkt gebracht." Ausgabe 3 von Digitalkompakt LfM (Stand 2012) **Dokulink 110744**
- Studie „Vertrauen und Sicherheit im Netz" des BITKOM (Stand 2012) **Dokulink 991899**
- „Gut zu wissen! Gefahren aus dem Netz - Viren, Würmer & Co." Ein Flyer der Initiative D21 **Dokulink 880492**
- Broschüre „IMBLICKPUNKT: Internetkriminalität" (Stand 2008) **Dokulink 519310**
- Flyer „Apps to go" von handysektor.de **Dokulink 448067**
- „Gut zu wissen! Sicher surfen - sicher handeln" Eine Broschüre der Initiative D21 (Stand 2012) **Dokulink 352145**

- Einen kostenlosen Netzwerkcheck bietet „heise Security" in Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz des Landes Niedersachsen an. **Dokulink 261815**
- Die Dienstleistungsgesellschaft für Informatik GmbH stellt in Kooperation mit der EU-Initiative „klicksafe" kostenlose Lernmodule zur Verfügung, welche den Europäischen Computerführerschein ECDL ergänzen sollen. Zum Beispiel Kurs 8: IT-Sicherheit **www.ecdl-moodle.de**

Browser

Die wichtigste Schnittstelle zum Internet ist der Browser – und somit auch ein beliebtes Ziel für Angriffe. Deshalb können viele Sicherheitsoptionen im Browser eingestellt werden, die auf die persönlichen Wünsche abgestimmt werden sollten. Denn eine allgemeingültige oder richtige Lösung gibt es nicht: Strikte Einstellungen zur Sicherheit bedeuten meist, dass einige Websites nicht mehr erreicht oder bestimmte Funktionen blockiert werden, sodass ein Kompromiss zwischen Funktionalität und Sicherheit gefunden werden muss.

Mail-Programm

Beim Empfang und Versand von Mails hilft Software, die auch ein Angriffspunkt sein kann. Besonders die automatische Vorschau-Funktion für Mails ist riskant. Diese Vorschau ermöglicht es Schadprogrammen, sich im System festzusetzen. Deshalb sollte diese Funktion deaktiviert werden. Auch die Darstellung aller Mails als Rein-Text hindert Schadprogramme und HTML-Elemente, den Computer anzugreifen, jedoch muss in diesem Fall auf bequeme Funktionen wie direkte Links und automatische Bilderanzeige verzichtet werden.

Apps

Auch die praktischen Programme für Smartphones und Tablets können für Angriffe missbraucht werden. Laut einer BITKOM-Studie von Oktober 2012 haben Smartphone-Nutzer durchschnittlich 23 Apps installiert. Mit einem Klick sind die kleinen Programme auf dem Gerät gespeichert und können zum mächtigen Sicherheitsproblem werden. Die knappen Beschreibungen der Apps geben nicht immer vollständig Auskunft über Voreinstellungen, Sicherheitsoptionen und den Zugriff auf gespeicherte Daten und Funktionen oder Schnittstellen des Smartphone.

Nutzer sollten genau überlegen, ob sie den Bedingungen einer App zustimmen und ob die geforderten Zugriffe sinnvoll für die Funktionalität sind. Vor allem kostenlose Apps fordern oft unnötige Daten wie die persönlichen Kontakte oder Funktionen wie die Ortung, um diese für personalisierte Werbung und mehr zu nutzen. Eine Alternative sind WebApps, die im Browser aufgerufen werden und für die Bildschirme von mobilen Geräten optimiert sind. Im Gegensatz zu klassischen Apps können sie nicht direkt auf mobile Geräte zugreifen.

- Ein Merkblatt mit Apps zum Thema Jugendschutz und Medienerziehung hat die Arbeitsgemeinschaft Kinder- und Jugendschutz Landesstelle NRW e.V. veröffentlicht. **Dokulink 554337**

SPAM

Ein besonderer Fall ist Spam: Der Begriff steht für Mails, die Werbung, betrügerische Angebote, gefälschte Hilferufe oder andere, unverlangte Informationen enthalten. Sie sind vor allem lästig, denn täglich werden rund 300 Millionen Spam-Mails in private Postfächer zugestellt, meldete der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) im September 2012. Überdies können die Mails, enthaltene Links oder Anhänge mit Schadprogrammen infiziert sein.

Um sich gegen Spam zu schützen, sollte der im Mail-Programm integrierte Spam-Filter konfiguriert oder eine spezielle Erweiterung installiert werden. Zudem bieten Mail-Provider nicht nur kostenlose Mail-Adressen und -Postfächer an, sondern filtern auch eingehenden Spam. Meist sind diese Filterprogramme effektiver und aktueller als eigene Software. Damit keine erwünschten Mails aussortiert werden, sollten Nutzer regelmäßig den Spam-Ordner kontrollieren oder sich einen Spam-Report schicken lassen.

Folgende Verhaltensregeln schützen vor Spam:

- Die persönliche Mail-Adresse nur an bekannte Personen weitergeben, von denen Nachrichten erwünscht sind.
- Die persönliche Mail-Adresse nicht in öffentliche Mailinglisten, Newsgroups und Newsletter eintragen.
- Nicht auf Spam antworten oder enthaltene Links klicken, sonst wird dem Absender bestätigt, dass die Mail-Adresse korrekt und aktiv ist.

Für die Teilnahme an Gewinnspielen oder für öffentliche Einträge in Foren oder Blogs ist es sinnvoll, zusätzliche Mail-Adressen anzulegen, die man für keinen anderen Zweck nutzt und möglicherweise gar nicht zum Mail-Programm zufügt. Es gibt auch Wegwerfadressen, die nach ein- oder mehrmaligem Gebrauch nicht mehr aktiv sind. Leider erkennen immer mehr Internetdienste diese Mail-Adressen und verweigern eine Anmeldung.

Anbieter sind zum Beispiel:

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

SCHADPROGRAMME ABWEHREN

Selbstverständlich muss auch der gesamte Computer geschützt sein, sonst können sich schädliche Programme, die möglicherweise die Sicherheitseinstellungen im Browser, Mail-Programm oder in Apps umgangen haben, unbemerkt im System festsetzen und Schaden anrichten. Das trifft u.a. auf Trojaner, Viren, Würmer und Spyware zu.

Als Teil von vermeintlich nützlicher Software schleichen sich Trojaner ins System ein, um Computer fernzusteuern und illegale Aktionen auszuführen. Viren verbreiten sich per Mail, über Datenträger, beim Herunterladen von Dateien aus dem Internet oder auch beim Aufrufen von Websites. Diese Schadprogramme verändern, zerstören oder löschen Software und Dateien. Würmer reproduzieren und verbreiten sich per Mail und in Online-Netzwerken, die in der Regel nur beim Anklicken aktiv

Quellen und weitere Informationen (II)

- Broschüre „IM BLICKPUNKT: Social Communities“ (Stand 2009). **Dokulink 668436**
- Die Website „Surfer haben Rechte“ ist Teil des Projekts „Verbraucherrechte in der digitalen Welt“ des Verbraucherzentrale Bundesverbands und präsentiert Informationen und Nachrichten zum Thema. **www.surfer-haben-rechte.de**
- Das Portal „Verbraucher sicher online“ bietet umfassende Informationen zum sicheren Surfen im Internet und leicht verständliche Anleitungen für digitale Anwendungen wie Musik- und Videoplayer. **www.verbraucher-sicher-online.de**
- Informationen der Verbraucherzentrale Nordrhein-Westfalen zu „So funktioniert der Interneteinkauf“. **Dokulink 231960**
- Das Bürger-CERT informiert und warnt Bürger und Unternehmen schnell und kompetent vor Viren, Würmern und anderen Sicherheitslücken. Es ist ein Projekt des Bundesamtes für Sicherheit in der Informationstechnik (BSI). **www.buerger-cert.de**
- Institut für Internetsicherheit der Westfälischen Hochschule in Gelsenkirchen **www.internet-sicherheit.de**

werden. Spyware späht gespeicherte Daten und/oder das Surfverhalten aus und gibt diese Informationen unbemerkt an Dritte weiter.

- Zu Schadprogrammen gibt es auch Falschmeldungen („Hoaxes“) oder gefälschte Anleitungen zu Schutzmaßnahmen, die den Computer infizieren und schädigen. Darüber informiert der „Hoax-Info Service“ der TU Berlin **http://hoax-info.tubit.tu-berlin.de**

Wie lassen sich die verschiedenen Schadprogramme abwehren? Es gelten einige Verhaltensregeln im Internet, die beachtet werden sollten und zusammen mit technischen Hilfsmitteln wirkungsvoll schützen können.

Diese Regeln gelten:
- Keine Programme von unbekannten Servern oder Websites herunterladen
- Keine Anhänge in unbekannten Mails öffnen
- Keine Passwörter speichern
- Keine pornografischen Websites, Tauschbörsen für Musik, Filme und Software nutzen
- Sicherungskopien erstellen und Originalsoftware sowie Key-Codes aufbewahren, falls der Notfall eintritt

Technische Schutzmaßnahmen

Antiviren-Software und Firewalls sind heutzutage recht einfach zu bedienen. Dennoch haben fast 20 Prozent der Internetnutzer diese Schutzmaßnahmen nicht ergriffen, ermittelte der BITKOM im Mai 2012.
Zentral für den Schutz des Computers ist eine Antiviren-Software. Diese erkennt und entfernt Schadprogramme, welche durch das versteckte Herunterladen und Installieren von Software, durch infizierte Mails und Speichermedien wie USB-Sticks oder SD-Karten ins System geraten sind. Jedoch ist Antiviren-Software nur wirksam, wenn täglich Aktualisierungen aus dem Internet nachgeladen werden, um neue Schadprogramme zu erkennen.

- Aktuelle Tests und Links zu kostenloser Antiviren-Software bietet **www.av-test.org**

Firewalls

Die Überwachung und Steuerung des Datenverkehrs zum und vom Computer oder einem mobilen Gerät ist die Aufgabe von Firewalls. Diese „Schutzmauern“ verhindern fremde Zugriffe auf den Rechner und zeigen den aktuellen Datentransfer an. So lässt sich von Fall zu Fall entscheiden, ob der Zugriff gestattet werden soll oder nicht.

Sicherheitsupdates

Auch Sicherheitsupdates gehören zum grundlegenden Schutz des Computers. Denn immer wieder werden Lücken und Fehler im Betriebssystem und in der Software entdeckt, die von Schadprogrammen oder Dritten ausgenutzt werden können, wenn keine entsprechenden Sicherheitsupdates installiert sind. Aber Vorsicht bei Updates, die über das Beseitigen von Sicherheitsproblemen oder Fehlern hinausgehen und neue Versionen einer Software installieren. Diese sind nicht automatisch sicherer oder besser als die – möglicherweise bewährte – alte Ausgabe.

E-COMMERCE / ONLINE-BANKING

Das größte Sicherheitsrisiko beim E-Commerce und Online-Banking sind Transaktionen per Internet, die sensible Zahlungsdaten erfordern. Wenn Konto- oder Kreditkartendaten übermittelt werden, sollte auf eine gesicherte Internetverbindung geachtet werden, die am vorangestellten „https://" oder einem Schlosssymbol in der Eingabe- oder Fußzeile des Browser zu erkennen ist. Dann werden die Daten verschlüsselt ausgetauscht. Andernfalls können die Zahlungsdaten abgefangen oder Bestellungen manipuliert werden.

Zahlungsarten

Sicher ist die Zahlung per Rechnung oder Einzugsermächtigung, weil man erst zahlen muss, wenn die bestellten Artikel geliefert und in Ordnung sind. Einer Einzugsermächtigung kann einfach widersprochen werden, dann bucht die Bank den gezahlten Betrag zurück. Die Vorkasse ist insofern riskant, dass man nicht sicher sein kann, ob eine Bestellung tatsächlich verschickt wird und die Ware in Ordnung ist. Das Geld zurück zu erhalten, ist bei Betrug oder Schäden mit recht viel Aufwand für den Kunden verbunden. Sehr verbreitet, aber besonders heikel ist die Kreditkartenzahlung, die auch eine Art Vorkasse ist. Zudem ist Missbrauch leicht möglich, weil abgefangene oder kopierte Kreditkartendaten von Dritten genutzt werden können.

- Gütesiegel von Onlineshops und deren Qualitätskriterien hat die Initiative D21 zusammengestellt. **www.internet-guetesiegel.de**

Phishing und Pharming

Wird im Internet nach der Geheimzahl für eine Bank- oder Kreditkarte gefragt, ist Phishing oder Pharming sehr wahrscheinlich. Phishing bezeichnet alle Verfahren, bei denen versucht wird, mit Hilfe gefälschter Mails vertrauliche Zugangs- und Identifikationsdaten auszuspähen. Diese Daten werden – unter der Identität des Inhabers – im E-Commerce eingesetzt, um Waren zu bestellen oder illegale Transaktionen zu tätigen.

Noch perfider ist Pharming, das ohne Mitwirkung des Opfers geschieht: Man wird auf eine gefälschte Website umgeleitet, die der offiziellen Banken-Website absolut ähnelt. Die eingegebenen Zugangs- und Bankdaten geraten in die Hände von Dritten, die das betreffende Konto im schlimmsten Fall leeren. Um Pharming vorzubeugen, sollte man die Internetadresse immer händisch in den Browser eingeben und auf ungewöhnliche Veränderungen der Banken-Website achten. Gibt es verdächtige Hinweise oder unklare Transaktionen auf dem Konto, muss die Bank sofort informiert werden. Hinsichtlich der Sicherheit von sensiblen Daten ist auch das mobile Banking oder das Bezahlen mit mobilen Geräten mit einiger Vorsicht zu betrachten.

SICHERES SMARTPHONE

Mobiltelefone mit Zugang zum Internet und Apps als Software sind für viele Menschen zum ständigen Begleiter geworden. Nach der ARD/ZDF-Onlinestudie 2012 besitzen 21 Prozent der Deutschen ein Smartphone, unter den Jugendlichen zwischen 12 und 19 Jahren ist der Anteil mit 47 Prozent schon mehr als doppelt so hoch (JIM-Studie 2012). Für die meisten Smartphone-Nutzer ist der Internetzugang mindestens so wichtig wie die klassischen Telefon- und SMS-Funktion. Dennoch möchten fast alle den Zugriff von Dritten auf persönliche Daten kontrollieren.

Das erfordert einige Sicherheitsmaßnahmen durch die Besitzer: Das Smartphone sollte immer durch ein Passwort geschützt sein, jedoch ist zu beachten, das bei einem verlorenen oder gestohlenen Gerät die SIM-Karte ausgetauscht werden kann, um so Zugriff auf die gespeicherten Daten und Apps zu erhalten. Deshalb ist es wichtig, sich auch innerhalb der einzelnen Apps abzumelden. Zusätzlich gibt es Programme, die den Fernzugriff auf das eigene Smartphone erlauben, um es zu orten oder die gespeichtern Daten zu löschen. Weil die Mobiltelefone eigentlich kleine Computer sind, sollten sie auch durch Antiviren-Software, Firewalls und Sicherheitsupdates geschützt werden.

- Tipps für die mobile Internetnutzung liefert die Broschüre „Mobile Sicherheit – Ortung – Datenschutz" des Bundesministeriums für Wirtschaft und Technologie. **Dokulink 498743**

SOZIALE NETZWERKE

Sicherheitsfragen sind auch in sozialen Netzwerken relevant. Durch Phishing- oder Pharming-Methoden werden Benutzerdaten übernommen, so dass es zum Identitätsdiebstahl kommen kann. Eine zunehmende Form der Internetkriminalität, denn im Jahr 2011 wurden fast 6500 Fälle beim Bundeskriminalamt angezeigt.

Als größtes soziales Netzwerk wird Facebook oft zur Verbreitung von Schadprogrammen missbraucht, indem vermeintlich interessante oder lustige Links und Anleitungen platziert werden, die mit Schadprogrammen infiziert sind oder automatisch in den Profilen von Freunden erscheinen, um Vertrauenswürdigkeit zu suggerieren.

ONLINESPEICHER

Immer mehr Menschen nutzen das Internet als Speichermedium, indem sie Daten wie Dateien, Fotos und Musik in passwortgeschützten Bereichen des Internet – der „Cloud" (englisch für Wolke) – ablegen, statt auf dem eigenen Computer. Solche „Datenwolken" sind bereits in die Betriebssysteme von Apple und Microsoft integriert oder werden von Mail-Providern und

Internetfirmen wie Google, Amazon und Dropbox angeboten. Vorteile der Cloud sind, dass Dateien immer in der letzten, aktuellen Version auf jedem internetfähigen Gerät verfügbar sind. Zudem können die Dateien mit anderen Menschen geteilt oder gemeinsam bearbeitet werden. Durch das Speichern im Internet sind die Daten auch besser vor Verlust oder Zerstörung geschützt als auf privaten Computern und Datenträgern.

Dennoch sind die Onlinespeicher nicht unbedingt sicher, weil die privaten Daten nicht ausreichend vor dem Zugriff durch Dritte geschützt sind. Die meisten Server, welche die Dateien speichern, befinden sich in den USA und dort haben Behörden aufgrund der Terrorbekämpfung leichten Zugang zu allen Daten. Wer diesen Zugriff vermeiden möchte, sollte bei der Auswahl eines Cloud-Dienstes beachten, dass sich die Server und auch der Hauptsitz der Firma in Deutschland oder der EU befinden. Hier gelten strengere Datenschutzrichtlinien, so dass richterliche Beschlüsse nötig sind, wenn Behörden auf die Daten zugreifen möchten.

Cloud-Dienste sind auch ein beliebtes Ziel von Hackern, weil sie massenhaft potenziell interessante Daten speichern. Diese werden gewöhnlich verschlüsselt im Onlinespeicher abgelegt, trotzdem ist eine Cloud zu empfehlen, welche die Daten schon beim Hochladen verschlüsselt. In diesem Fall kennt nur der Kunde das Passwort zu seinen Dateien – und nicht der Cloud-Dienst.

- Das Portal „iRIGHTS CLOUD“ informiert zu rechtlichen, technischen und kulturellen Aspekten der Cloud und ist Anlaufstelle bei Fragen zu diesem Thema. **http://cloud.irights.info**

NOCH FRAGEN?

Spannende Projekte, interessante Studien und vertiefende Literatur finden Sie im „Grundbaukasten Medienkompetenz“ unter **www.mekonet.de**. Auch die Broschürenreihe 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 Grimme-Institut
Gesellschaft für Medien, Bildung und Kultur mbH
Eduard-Weitsch-Weg 25
D-45768 Marl

Tel.: +49 (0) 2365 / 9189-61
Fax: +49 (0) 2365 / 9189-89

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

Facebook: facebook.com/mekonetnrw
Twitter: twitter.com/mekonet
Youtube: youtube.com/mekonetnrw

Ministerin für Bundesangelegenheiten, Europa und Medien des Landes Nordrhein-Westfalen

Landesanstalt für Medien Nordrhein-Westfalen (LfM)

Grimme Institut

ClimatePartner° klimaneutral
Druck | ID: 10956-1304-1002

mekonet, das Medienkompetenz-Netzwerk, wird gefördert von der Ministerin für Bundesangelegenheiten, Europa und Medien des Landes Nordrhein-Westfalen und der Landesanstalt für Medien Nordrhein-Westfalen. Das Grimme-Institut ist mit der Projektleitung von ***mekonet*** betraut.

Stand: April 2013 – Fotos: Amy Walters/Fotolia.com