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 8: Dringend nötig: die Schaffung einer Internet-Sicherheitskultur

orell füssli Verlag AG

Dringend nötig: die Schaffung einer Internet-Sicherheitskultur

Eine Internet-Sicherheitskultur ist deshalb spannend, weil sie sich auf ein globales Feld bezieht. Zur Internet-Sicherheitskultur gehört die Übertragung der gewohnten realen (Sicherheits-)Kultur auf das digitale Leben. Dazu zählt nicht nur das Verständnis für Sicherheit und Vertrauenswürdigkeit im Internet, sondern auch das Wissen darüber, wie Probleme gemeistert werden können, und die Einsicht, dass Hilfestellungen von Fachleuten auch im digitalen Leben nicht kostenlos zu haben sind.

Vom realen zum digitalen Leben – Sicherheit und Vertrauenswürdigkeit im Internet

Wie viel Sicherheit ist im Internet generell erreichbar? Wo ist wie viel Sicherheit angemessen? Wie kann Vertrauen in das Internet gestärkt werden? Dem Sicherheitsbedürfnis entsprechend besteht das Ziel darin, vor dem Surfen im Internet alle denkbaren negativen Folgen auszuschließen. Doch das Surfen ist immer mit einem Risiko verbunden, da das Internet neben vielen Vorteilen eben auch Gefahren birgt. Genau genommen gilt das aber für alle Aktivitäten im Leben. Die meisten Alltagshandlungen, zum Beispiel das Autofahren, würde niemand als besonders riskant bezeichnen, auch wenn man nie völlig

sicher sein kann, dass sie im Sinne des Handlungsziels gelingen – so sterben beispielsweise jedes Jahr mehrere Tausend Menschen im Straßenverkehr.

Analog ist das Buchen von Flügen im Internet eine sehr einfache und sinnvolle Sache. Es besteht aber die Gefahr, dass dabei Kriminelle ihre Finger mit im Spiel haben, die dafür sorgen, dass der Nutzer zwar den Flugpreis bezahlt, aber kein Ticket erhält. Wenn jemand Internetdienste nutzt, tut er das, ohne genau zu wissen, was letztlich dabei herauskommt.

Von einem Risiko spricht man, wenn etwas aufs Spiel gesetzt wird. Dabei sollte bedacht werden, welche Auswirkungen bestimmte Handlungen haben können, welche Faktoren auf ihren Ausgang Einfluss nehmen und welche möglichen Resultate erreicht werden können. Im Alltag werden diese Aspekte zumeist intuitiv beurteilt, so auch beim Autofahren: Der potenzielle Schaden beim Autofahren ist kein Risiko, das davon abhält, das Auto zu nutzen.

Wie sieht der Alltag aus?

Eine sichere Welt gibt es nicht! Aber der moderne Mensch hat gelernt, mit dieser Tatsache verantwortungsvoll umzugehen und sich mithilfe geeigneter Mittel ein Mindestmaß an Sicherheit zu schaffen. Was also ist nötig, um das auch im digitalen Leben zu erreichen?

In einer idealen Welt würden Vertrauen und Freundlichkeit regieren, wären alle Informationen frei für jeden verfügbar, würde sich niemand zulasten anderer bereichern, würden alle den gewünschten und angemessenen Preis für Waren und Dienstleistungen zahlen, wäre der Wettbewerb transparent, fair und ausgeglichen. Doch das reale Leben sieht anders aus:

Information und Wissen – und damit Macht – sind ungleich verteilt, Einbruch und Diebstahl gefährden das private Eigentum, Betrug und Verrat gehören zum Leben, Terror und Gewalt bedrohen den Alltag. Dennoch haben wir gelernt, mit diesen Gefahren zu leben und umzugehen und uns, so weit es möglich ist, zu schützen.

Welchen Schutz gibt es im realen Leben?

Die Wohnung wird abgeschlossen, sodass kein Unbefugter sie betreten und das private Eigentum stehlen kann. Verschlossene Schränke und Safes dienen zur sicheren Aufbewahrung wertvoller Güter (Geld, Sachwerte usw.). Der geschlossene Kofferraum des Autos schützt die eingekauften Waren während des Transports, sodass kein Dieb sie während eines Stopps entwenden kann. Verschlossene Briefumschläge sorgen für den vertraulichen Austausch von Informationen, die eigenhändige Unterschrift für Verbindlichkeit, zum Beispiel bei Kaufverträgen.

Reales versus digitales Leben

Ein besonders wichtiger Punkt in einer funktionierenden Gesellschaft ist die Vertrauenswürdigkeit – in der Geschäftswelt wie im alltäglichen Umgang miteinander.

Im realen Leben lernt jeder, welche Bedeutung eine Unterschrift unter einem Vertrag hat und wie er anhand äußerer Merkmale und mithilfe intuitiver Einschätzung die Vertrauenswürdigkeit seines Gegenübers im täglichen Leben bewerten kann, um mehr Sicherheit zu erlangen. Im digitalen Leben, zum Beispiel bei der indirekten Kommunikation über

das Internet, ist es jedoch nicht möglich, auf diese bewährten Mechanismen zurückzugreifen. Man kann nicht sicher sein, mit wem man tatsächlich kommuniziert und ob die Kommunikation nicht abgehört oder manipuliert wird.

Das heißt, dass die grundlegenden Sicherheitsbedürfnisse im digitalen Leben anders als im realen Leben befriedigt werden müssen.

Welche Herausforderungen stellt das digitale Leben?

In einer vernetzten Informations- und Wissensgesellschaft spielt die IT-Sicherheit und Vertrauenswürdigkeit eine immer bedeutendere Rolle. Die Werte, die als Bits und Bytes auf unseren Computern und im Internet zur Verfügung stehen, und die Abhängigkeit von den angebotenen IT-Dienstleistungen werden immer größer.

Ebenso wächst aufgrund immer leistungsfähigerer Software und immer komplexerer Zusammenhänge zwischen Protokollen, Diensten und Infrastrukturen die Angriffsfläche beständig. Daher verwundert es nicht, dass auch die Angriffe immer raffinierter, differenzierter und routinierter erfolgen; die IT-Kriminalität erfährt eine zunehmende Professionalisierung und wird damit zu einer nicht zu unterschätzenden Gefahr. Damit nimmt auch die Notwendigkeit zu, IT-Sicherheitsmaßnahmen in angemessener Weise anzuwenden. Nur so kann im digitalen Leben eine Vertrauensbasis geschaffen werden.

Eine weitere Herausforderung ist das häufig mangelnde Unrechtsbewusstsein im digitalen Leben. Wer im realen Leben Gegenstände entwenden will, der muss über Zäune klettern, Türen und Fenster aufbrechen, vielleicht sogar Tresore spren-

gen. Jedem, der so etwas tut, ist bewusst, dass er eine Straftat begeht! Im digitalen Leben sitzen die Hacker beziehungsweise Cracker mit Kaffee und Keksen vor dem Bildschirm und machen das Gleiche, aber sie haben dabei häufig nicht das Gefühl, etwas Unrechtes zu tun. Die Hemmschwelle ist niedriger, wodurch die Wahrscheinlichkeit von Angriffen im Internet steigt. Aber das muss sich durch eine Sicherheitskultur im Internet grundlegend ändern.

Ein ganz wesentlicher Unterschied zum realen Leben besteht darin, dass das Internet global ist, während die Gesetze in ihrer Wirkung derzeit meist noch national oder europaweit begrenzt sind. Das heißt, der Staat kann zurzeit keinen angemessenen rechtlichen Schutz bieten, obwohl das dringend nötig wäre.

Welcher Schutz ist im digitalen Leben angemessen?

Die genannten Sicherheitsmechanismen aus dem realen Leben (siehe Seite 176) sind analog auch im digitalen Leben verfügbar:

Anti-Malware-Programme und Personal Firewalls – als Haus- und Wohnungstür – verhindern den unerlaubten Zugriff von außen auf die Daten im Computer. Datei- und Festplattenverschlüsselung sorgen als digitaler Tresor für eine sichere Aufbewahrung der elektronischen Informationen, während eine Kommunikationsverschlüsselung wie SSL/TLS die Daten während des Transports im Internet schützt. Darüber hinaus ermöglichen verschlüsselte E-Mails einen vertraulichen «Briefverkehr», und digitale Signaturen gewährleisten die Verbindlichkeit und damit eine höhere Rechtssicherheit. Wer die Vorteile des digitalen Lebens ausschöpfen will, muss,

ähnlich wie im realen Leben, das Risiko begrenzen. Das heißt, geeignete Sicherheitslösungen müssen eingesetzt und regelmäßig aktualisiert und angepasst werden.

Ein Blick in die Zukunft

Egal ob Handys, Computer, Spielzeug, Videogeräte oder Autos, das Leben wird immer digitaler. Dabei stellen die vielen Möglichkeiten, die das Internet heute schon bietet, gerade mal den Anfang der digitalen Revolution dar. Vermutlich werden schon in naher Zukunft die Tische in Cafés zu Touchscreen-Monitoren, welche die Speisekarte anzeigen, Bestellungen aufnehmen und es dem Nutzer ermöglichen, während des Essens und Trinkens im Internet zu surfen oder Fotos anzuschauen. In zehn Jahren wird es billiger sein, eine Wand als Monitor einzurichten, als eine Holzvertäfelung anfertigen zu lassen. Das «Internet der Dinge» wird Teile des Haushalts, wie zum Beispiel den Kühlschrank, die Heizung und die Jalousien, digital steuern. Wenn ein heutiger Computer die Intelligenz einer Fliege hat, dann werden die Computer in zehn Jahren die Intelligenz eines Menschen aufweisen. Intelligente Softwareagenten übernehmen Arbeiten wie das Beantworten von E-Mails, das Buchen von Reisen, das Einkaufen von Lebensmitteln und das Führen von Bankkonten.

Doch egal, was die Zukunft auch bringen wird, stets müssen das Recht auf die Privatsphäre und der Schutz des wirtschaftlichen Gutes gewährleistet sein. Dazu muss der Internetnutzer das digitale Leben als natürlichen Teil seiner Lebenswirklichkeit wahrnehmen und für die digitale und reale Welt die äquivalente Verantwortung übernehmen – eine Sicherheitskultur entwickeln und etablieren.

Hilfe zur Selbsthilfe – Probleme managen

Das Problem an den neuen Medien, Technologien und Diensten ist, dass sie sich rasend schnell entwickeln und der normale Nutzer kaum in der Lage ist, alle Funktionen der Technologie, die er nutzen könnte, zu beherrschen. Für die meisten sind der Computer und das Internet ein notwendiges Mittel zum Zweck. Sobald aber etwas nicht funktioniert, ist guter Rat teuer. Wie gilt es sich hier zu verhalten?

Im realen Leben haben sich verschiedene Mechanismen für Problemfälle etabliert. Ist etwas im Haus defekt, wird ein Handwerker gerufen oder das eigene handwerkliche Geschick unter Beweis gestellt. Bei einem Mangel am Auto wird je nach Vorfall der Pannendienst gerufen oder das Auto zur Werkstatt gefahren. Auch «Vorsorgeuntersuchungen» wie Inspektionen sind üblich, und jedem Autofahrer ist bewusst, dass dies mit Kosten verbunden ist. Im Internet und in der digitalen Welt gibt es diese Abläufe noch nicht. So gut wie niemand kommt auf die Idee, Geld für eine Computerinspektion zu bezahlen oder bei Fehlern einen Fachmann zu rufen. Dabei sollte jedem bewusst sein, dass die digitalen Dienste heute bereits so wichtig sind, dass kostenpflichtige Hilfe ab und an nötig sein wird.

Erste Schritte zur Selbsthilfe

Ehe allerdings der Computerfachmann aus dem Freundeskreis oder aus dem Computerladen gerufen werden muss, gibt es einige Möglichkeiten im Internet, die bei der Fehleranalyse helfen. Fast alle Fehler sind schon einmal aufgetreten, weshalb es im Allgemeinen auch für die meisten Probleme eine

Lösung gibt. Das Internet bietet den Vorteil, dass sehr viele Nutzer ihre Erfahrungen im Internet veröffentlichen und sie so jedermann zur Verfügung stellen. Wenn ein Programm eine Fehlermeldung liefert, kann diese in eine Suchmaschine eingegeben werden, und fast immer finden sich auf der ersten Seite Suchergebnisse, die beschreiben, wie das Problem gelöst werden kann. Liegt eine Fehlfunktion vor, die keine direkte Fehlermeldung auslöst, können die wichtigsten Begriffe im Zusammenhang mit dem Problem in eine Suchmaschine eingegeben werden. Auch dies führt meist zum gewünschten Erfolg.

Es gibt im Internet bereits einige interessante Webseiten, die sich diesem Thema auf humorvolle Weise nähern. GIDF.de zum Beispiel ist eine Webseite, die lediglich die Suchmaschine Google eingebettet hat und für «Google Ist Dein Freund» steht. Dies soll zeigen, dass es sich lohnt, einen Fehler erst einmal zu googeln, bevor ein Dritter zurate gezogen wird. Etliche Probleme lassen sich relativ leicht auch durch eigene Recherche lösen.

Andere Probleme sind schwer zu erklären und nicht einfach über die Eingabe in eine Suchmaschine zu formulieren oder zu finden. In diesem Fall ist es sinnvoll, in einem Forum Rat zu suchen.

Dazu muss sich der Nutzer in einem entsprechenden Forum anmelden und hat dann die Möglichkeit, dort zu bestimmten Themengebieten Fragen zu stellen. Einige Foren umfassen sehr viele Bereiche (zum Beispiel www.wer-weiss-was.de, http://forum.chip.de), weshalb sich fast alle Fragen durch die Mitgliedschaft in ein bis drei Foren klären lassen (Hilfe-Foren siehe Softlink 621). In den Foren werden die Probleme geschildert, und die Internetcommunity antwortet. Dies ist ein

hilfreicher und genialer Effekt des Internets. Es ist möglich, mit wenigen Klicks sehr viele Nutzer um Hilfe zu bitten. Natürlich sollte auch in diesen Foren ein Nickname verwendet werden.

Führen diese Möglichkeiten nicht zum Ziel, muss ein Computerexperte eingeschaltet werden, der sich des Problems annimmt und es meist rasch und professionell löst – gegen eine angemessene Bezahlung versteht sich, denn der Mechaniker in der Autowerkstatt arbeitet auch nicht umsonst …

Glossar

Access Point: Zugangspunkt zu einem WLAN
Account: Benutzerkonto, Zugang zu einem Internetdienst. Üblicherweise muss ein Nutzer sich beim Login mit Benutzername und Passwort authentisieren.
ActiveX: eine von Microsoft entwickeltes Softwarekomponenten-Modell, mit dem unter anderem kleine Programme für den Browser geschrieben werden können (vergleichbar mit JavaSkript). ActiveX funktioniert nur in der Microsoft-Welt.
Add-on: Erweiterungsmöglichkeiten für den Browser, zum Beispiel um lästige Werbung zu blocken; wird auch als Plug-in bezeichnet
AES (Advanced Encryption Standard): symmetrisches Verschlüsselungsverfahren mit einer variablen Schlüssellänge von 128, 192 oder 256 Bit. AES bietet ein sehr hohes Maß an Sicherheit (siehe Softlink 326).
AJAX (Asynchronous JavaScript and XML): ein Konzept der asynchronen Datenübertragung zwischen einem Webserver und dem Browser
Aktive Inhalte: Sammelbezeichnung für Technologien, die innerhalb eines Browsers ausführbar sind und den Nutzer in die Lage versetzen, mit einem Webserver zu interagieren
Authentifikation: Verifizierung der Echtheit des Nutzers
Back-up: Sicherungskopie von Computerdateien auf einem externen Speichermedium
Blog: Internettagebuch, Bestandteil des Web 2.0

Bluetooth: Funkverbindung über kurze Distanzen zwischen mobilen Kleingeräten sowie zwischen Computer und Peripheriegeräten

Browser: spezielles Computerprogramm zum Betrachten von Webseiten im World Wide Web (WWW) oder allgemein von Dokumenten und Daten. Webbrowser stellen die Benutzeroberfläche für Webanwendungen dar.

Brute-Force-Angriff: Angriff auf den Computer, bei dem der Angreifer alle möglichen (Zeichen-)Kombinationen durchprobiert, um zum Beispiel Passwörter zu ermitteln

ClickandBuy: ein Zahlungssystem im Internet

Cracker: Hacker, der unbefugt in fremde Computersysteme eindringt und gespeicherte Daten und Programme in böser Absicht beziehungsweise zu seinem persönlichen Vorteil manipuliert, inspiziert oder zerstört

Creative-Commons-Lizenzen: Lizenzverträge, mittels derer Autoren der Öffentlichkeit Nutzungsrechte für ihre Werke (Texte, Bilder, Musikstücke usw.) einräumen können

Cross Site Scripting (XSS): das Ausnutzen von Sicherheitslücken, um unbemerkt Angriffe in einem für den Nutzer vertrauenswürdigen Umfeld (bekannte Webseiten) zu platzieren und durchzuführen

Domain: Name einer Internetseite (Webadresse), zum Beispiel www.internet-sicherheit.de

Domain Name Service (DNS): DNS löst als Internetdienst Domainnamen in IP-Adressen auf und umgekehrt.

ebay-Käuferschutz: Absicherung für Waren, die beim Internetauktionshaus ebay gekauft und mit PayPal bezahlt wurden. Wird die Ware nicht geliefert oder weicht diese erheblich von der Artikelbeschreibung ab, wird der bezahlte Kaufpreis zurückerstattet.

E-Commerce: Unter E-Commerce wird der elektronische Handel (Internethandel, Onlinehandel) verstanden.

FinTS (Financial Transaction Services): deutscher Standard für den Betrieb von Onlinebanking. FinTS ist eine Weiterentwicklung des Onlinebanking-Standards HBCI.
Firewall: elektronischer «Wächter» im Computer (oder in einem Netzelement wie einem Router), der sich darum kümmert, dass alle Ports, die nicht gebraucht werden, geschlossen sind
Flash: proprietäre Entwicklungsumgebung zur Erstellung multimedialer Inhalte. Flash wird auch für Animationen im Internet verwendet.
Flatrate: Pauschaltarif für Telekommunikationsdienstleistungen wie Telefonie und Internetverbindung
Freeware: kostenlose Programme aus dem Internet, die lizenzfrei genutzt werden können
FTP (File Transfer Protocol): Netzwerkprotokoll zur Übertragung von Dateien in einem Netzwerk
Gateway: Vermittlungsgerät, das es Netzwerken ermöglicht, miteinander zu kommunizieren, auch wenn diese auf völlig unterschiedlichen Protokollen basieren
GNU-Lizenz: Sammelbegriff für Lizenzen des GNU-Projekts. Das GNU-Projekt wurde mit dem Ziel gegründet, ein vollständig freies Betriebssystem zu entwickeln.
Hacker: Nutzer, der sehr vielfältige Kenntnisse im Umgang mit Computern besitzt. Der Begriff wird auch häufig für Personen verwendet, die sich unbefugt Zugang zu fremden Computersystemen verschaffen.
HBCI (Homebanking Computer Interface): eine standardisierte Schnittstelle für das Homebanking und Vorgänger von FinTS. Er wurde von verschiedenen Bankengruppen in Deutschland entwickelt und vom Zentralen Kreditausschuss (ZKA) beschlossen.
Helpdesk: Informations- und Hilfsdienst eines Herstellers oder innerhalb einer Organisation, der bei Problemen mit Soft- oder Hardware Unterstützung bietet

Hotspot: öffentlicher Internetzugang via WLAN

HTML (HyperText Markup Language): Auszeichnungssprache, mit der Webseiten beschrieben werden

HTTP (HyperText Transfer Protocol): Internetprotokoll, mit dem Daten zwischen Webserver und Browser ausgetauscht werden

HTTPS (HyperText Transfer Protocol Secure): Bei diesem Protokoll werden die Daten zwischen Webserver und Browser verschlüsselt und integritätsgesichert ausgetauscht.

IMAP (Internet Message Access Protocol): Anwendungsprotokoll, das den Zugriff auf und die Verwaltung von empfangenen E-Mails, die sich in einem Postfach auf einem Mailserver befinden, erlaubt

Internetauftritt: Gesamtheit der Funktionalitäten, die von einem Internetdienstanbieter in einer als zusammenhängend empfundenen Weise zur Verfügung gestellt werden, zum Beispiel ein Web- oder Chatserver

IPSec: ein Sicherheitsprotokoll, das Vertraulichkeit, Authentizität und Integrität bei der Übertragung von Datenpakten gewährleisten soll

IPv4/IPv6: Ein Internetprotokoll (IP) spezifiziert die Vorgänge, die zur Vermittlung von Datenpaketen durch das Internet notwendig sind, wie etwa die Adressierung der Computersysteme und Netzknoten. Zurzeit wird hauptsächlich die Version IPv4 eingesetzt, zukünftig soll die Version IPv6 verwendet werden.

iTAN (indizierte TAN): Onlinebanking-Verfahren, bei dem der Bankkunde seinen Auftrag nicht mehr mit einer beliebigen TAN (siehe «TAN») aus seiner Liste legitimieren kann, sondern von der Bank aufgefordert wird, eine bestimmte, durch eine Positionsnummer (Index) gekennzeichnete TAN zu verwenden.

Java-Applet: Programm, das in der Programmiersprache Java verfasst wurde und normalerweise in einem Browser ausgeführt wird

JavaScript: eine in HTML-Syntax integrierte Skriptsprache. JavaScript-fähige Browser interpretieren den in einer Webseite enthaltenen Code und führen ihn auf dem Computer aus.
JScript: Microsoft-eigene Skriptsprache für Browser
Key: Schlüssel, der für eine Verschlüsselung verwendet wird
Link (Kurzform von Hyperlink): Hyperlinks sind elektronische Verweise auf andere Webseiten, die sich überall auf der Welt befinden können. Der Nutzer folgt einem Link zum Beispiel durch Anklicken. Dieser Prozess kann unendlich oft wiederholt werden.
MAC-Adresse (Media-Access-Control-Adresse): Hardware-Adresse eines Netzwerkadapters (Computers) in einem Netz
Malware: Oberbegriff für «Schadsoftware» wie Viren, Würmer, Trojanische Pferde, Spyware usw.
mTAN (mobile TAN): Beim mTAN-Verfahren wird dem Onlinebanking-Kunden nach Übersendung der ausgefüllten Überweisung im Internet von der Bank per SMS eine nur für diesen Vorgang verwendbare TAN (siehe «TAN») auf sein Mobiltelefon gesendet. Das Verfahren wird auch als SMSTAN bezeichnet (siehe Softlink 342).
Nutzer: Person, die den Computer oder den Internetdienst für seine Zwecke nutzt
Nutzerprofil: Sammlung von Nutzerdaten eines Nutzers, zum Beispiel Cookies, Logins, Analyse von Logfiles und Bestell-/Interaktionsdaten
Onlineshop: Der Onlineshop stellt Waren und digitale Produkte im Internet zum Verkauf bereit.
Onlinestreaming/Onlinestreams: Übertragung von Realzeitanwendungen wie Radio und Fernsehen über das Internet
Patch: Aktualisierung eines Programms, um bestimmte Funktionen zu integrieren beziehungsweise zu korrigieren
PayPal: Bezahldienst mit Käuferschutz, bei dem Käufer und Verkäufer keine Kontodaten des jeweils anderen erhalten

Personal Firewall: Sicherheitsprogramm, das den ein- und ausgehenden Datenverkehr auf dem zu schützenden Computer filtert und reglementiert; erweitert die Firewallfunktionen um die Kontrolle von Anwendungen

Personensuchmaschine: Suchmaschine, die speziell nach personalisierten Einträgen im Internet sucht

Phishing: der Versuch, durch Vortäuschen einer fremden Identität mittels gefälschter E-Mails und Webseiten vertrauliche Passwörter zu ergaunern

PIN (persönliche Identifikationsnummer): eine nur einer oder wenigen Personen bekannte Zahl, mit der diese sich gegenüber einem Dienst authentisieren können (Anwendung bei Webseiten, ec-Karten, beim elektronischen Personalausweis ...).

POP3 (Post Office Protocol Version 3): Übertragungsprotokoll, über das ein Client E-Mails von einem E-Mail-Server abholen kann

Port: Ports sind interne und externe Schnittstellen eines Computers (Servers). Sie werden zum Beispiel von dem jeweiligen Transportprotokoll benutzt, um Anwendungen auf einem Server zu adressieren (beispielsweise über Port 80 einen Webserver und über Port 25 einen E-Mail-Server).

Pre-Shared Key: ein vorab vereinbarter beziehungsweise verteilter Schlüssel, zum Beispiel für die WLAN-Verschlüsselung

Programmcode: ein in einer Programmiersprache geschriebener Text eines Computerprogramms

Provider: Dieser Begriff bezeichnet einen Anbieter oder Dienstleister (zum Beispiel Telekommunikationsanbieter, Mobilfunkanbieter, Internetdienstanbieter).

Repeater: elektrischer Signalverstärker, der dazu dient, Netze zu erweitern, deren räumliche Ausdehnung aus physikalischen Gründen (Signaldämpfung und Signalverformung) begrenzt ist

Router: Netzwerkkomponente, die verschiedene Teilnetze koppelt beziehungsweise trennt

Server: Der Begriff Server bezeichnet eine Soft- und Hardware im Rahmen des Client-Server-Modells. Das Client-Server-Modell beschreibt eine Möglichkeit, Aufgaben und Dienstleistungen innerhalb eines Netzwerks, zum Beispiel dem Internet, zu verteilen. Der Client kann auf Wunsch eine Aufgabe vom Server anfordern. Der Server beantwortet die Anforderung.

Smartphone: modernes Mobiltelefon (Handy), das mit einem erweiterbaren Betriebssystem arbeitet, gut vernetzt ist (GSM, UMTS, WLAN, Bluetooth usw.) und die Nutzung von zusätzlicher Software (E-Mail-Client, Browser etc.) gestattet

SMTP-Server: Ein E-Mail-Anbieter stellt mindestens einen sogenannten SMTP- oder E-Mail-Server zur Verfügung. Das SMTP-Protokoll ist das Kommunikationsprotokoll, das für den Transfer der E-Mail vom Mail-Client zum Mail-Server und zwischen den Mail-Servern über das Internet sorgt.

Social Network/soziales Netzwerk: Webdienst, bei dem die Nutzer gemeinsam eigene Inhalte erstellen

SSL (Secure Socket Layer): vorherrschendes Protokoll für die Verschlüsselung der Datenübertragung im Web

Suchmaschine: Programm zur Recherche von Dokumenten, die in einem Computer oder im Internet gespeichert sind. Nach Eingabe eines Suchbegriffs liefert eine Suchmaschine eine Liste von Verweisen auf möglicherweise relevante Dokumente Die bekanntesten Suchmaschinen im Internet sind Google, bing und Yahoo.

Surfen: das Bewegen im Web beziehungsweise das Durchstöbern des Webs

TAN (Transaktionsnummer): Einmalpasswort, das üblicherweise aus sechs Dezimalziffern besteht und vorwiegend im Onlinebanking verwendet wird

TKIP (Temporal Key Integrity Protocol): Verschlüsselungsprotokoll für WLANs. TKIP wird in dem Standard WPA verwendet.

UMTS (Universal Mobile Telecommunications System): Mobilfunkstandard der dritten Generation (3G), mit dem deutlich höhere Datenübertragungsraten als mit dem Mobilfunkstandard der zweiten Generation (2G) und dem GSM-Standard möglich sind

URL (Uniform Resource Locator): URLs identifizieren und lokalisieren eine Ressource über das verwendete Netzwerkprotokoll (beispielsweise HTTP oder FTP) und den Ort der Ressource im Netzwerk.

USB-Stick: kompaktes Speichermedium mit hoher Kapazität und Zugriffsgeschwindigkeit mit integriertem USB-Stecker

Verschlüsselung: mathematische Transformation von Daten, die es einem Angreifer unmöglich machen soll, die Originaldaten zu rekonstruieren (Softlink 326).

Virensignatur: eindeutiges Erkennungsmerkmal von Viren, das von Anti-Virus-Programmen zu deren Identifizierung genutzt wird

Web 2.0: interaktives Internet, das es dem Nutzer ermöglicht, zum Beispiel Kommentare zu hinterlassen oder Spiele im Netz zu spielen

Webadresse: Adresse, mit der eine Webseite adressiert werden kann, zum Beispiel www.sicher-im-internet.de

Webbrowser: siehe «Browser»

Webserver: ein Server, der Webseiten anbietet

Zertifikat: Dieser Begriff bezeichnet eine Datenstruktur, die eine Identifikation des Besitzers, seinen öffentlichen Schlüssel, ein Ablaufdatum und die digitale Signatur einer Zertifizierungsstelle enthält und so die Integrität und Authentizität garantiert.

Zugangsdaten: Daten, die zur Überprüfung der Berechtigung verwendet werden (Nutzerkennung und Passwort)

Weitere Glossareinträge finden Sie unter Softlink 710.

Danksagung

In erster Linie möchten wir Ihnen, den Leserinnen und Lesern, danken, dass Sie dieses Buch gekauft haben. Ein Buch zu schreiben ist eine sehr spannende Aufgabe und der Beweis dafür, dass der Weg von einer Idee bis zu ihrer Umsetzung doch ein recht weiter ist. Die Idee war, das Internet und damit das digitale Leben ein bisschen sicherer zu machen, indem wir für jeden verständliche Tipps und Informationen in diesem Buch zusammentragen. Wir hoffen, dass uns dies gelungen ist. Der Weg war lang, aber er wäre viel länger gewesen, wenn uns nicht so viele wunderbare Menschen unterstützt hätten. Wir möchten hiermit all unseren tatkräftigen Weggefährten danken: den Mitarbeitern des Orell Füssli Verlags und von Ariadne-Buch, den fleißigen Probelesern Gertrud, Marian, Josef, Luisa, Alexander, Björn, Dirk, Boris, Gerda, Sven und Julia sowie Andrej und den if(is)-Mitarbeitern, insbesondere den «Live-Hacking-Team-Mitgliedern» Marian und Niklas. Ein besonderer Dank gilt unseren Partnerinnen Bettina und Britta für ihre Kritik, die unermüdliche Unterstützung und die aufmunternden Worte.

Das gesamte Buch „Sicher im Internet“ ist ab dem 04.03.2013 als PDF und E-Book kostenlos verfügbar.

www.internet-sicherheit.de