Überwachungsskandale, Datenlecks und großflächige Passwortdiebstähle machten überdeutlich, dass die Kommunikation via Internet teilweise nicht so sicher ist, wie es sich Nutzerinnen und Nutzer wünschen würden. Viele möchten sich und ihre Daten besser schützen, fühlen sich dieser (technischen) Herausforderung jedoch nicht gewachsen. Auch, da Sicherheit kein Produkt ist, sondern ein andauernder Prozess, bei dem laufend nachgebessert werden sollte. Dennoch können einfache Maßnahmen gesetzt werden, um die Sicherheit im Internet zu verbessern. Sicherheitsmaßnahmen müssen nämlich nicht kompliziert und unbequem sein – gut implementierte Sicherheit ist einfach und im Idealfall komfortabel.

Sicherheit

Passwörter

Passwörter dienen der Authentifizierung; mit ihnen weisen sich Userinnen und User aus. Passwörter gibt es für E-Mail-Dienste, Onlineprofile in sozialen Netzwerken und mobile Endgeräte – um nur ein paar Beispiele zu nennen. Es ist besonders wichtig, auf die eigenen Passwörter zu achten, diese sicher zu gestalten und regelmäßig zu wechseln. Auch wenn es umständlich und aufwendig erscheint – der beste Tipp für mehr Sicherheit im Internet ist, sichere Passwörter zu verwenden.

Wie können Passwörter die größtmögliche Sicherheit bieten?

- → ***Geheimhaltung:*** *Passwörter sind nur dann effektiv, wenn sie geheim sind. Sie sollten nicht aufgeschrieben und, falls doch, keinesfalls an leicht auffindbaren Orten aufbewahrt werden. Ebenso ist davon abzuraten, anderen Personen seine Passwörter mitzuteilen.*
- → ***Faustregel:*** *Passwörter sollten aus mehr als acht Zeichen bestehen. Vereinfacht gesagt: Je länger das Passwort, umso sicherer ist es.*
- → ***Die üblichen „Verdächtigen“:*** *Viele Userinnen und User wählen ihr eigenes Geburtsdatum, den eigenen Namen oder einfache Zahlenkombinationen. In der jährlichen Sicherheitsanalyse von Passwörtern war auch im Jahr 2013 das häufigste Passwort „123456“, gefolgt etwa von „password“ oder „ilove you“. Solche Passwörter sind besonders unsicher, da sie leicht zu erraten sind und leicht geknackt werden können.*
- → ***Verschiedene Passwörter:*** *Auch wenn es umständlich scheint, so sollten dennoch verschiedene Passwörter zum Beispiel für verschiedene Profile oder Onlinedienste verwendet werden. Denn wird das Passwort eines Profils oder Kontos geknackt, sind bei unterschiedlichen Passwörtern nicht gleich automatisch auch andere Konten betroffen.*
- → ***Regelmäßig das Passwort ändern:*** *Das A und O von Datensicherheit und sicheren Passwörtern ist, diese regelmäßig zu ändern. Immer wieder Passwörter gegen neue auszutauschen ist die beste Empfehlung, um sich und seine Daten zu schützen.*
- → ***Sicherheitsfragen:*** *Manche Webseiten ermöglichen es, bei einem vergessenen Passwort durch sogenannte Sicherheitsfragen (z. B. „Wie lautet der Name des Haustiers?“, „Was ist Ihre Lieblingsspeise?“) dennoch auf das*

eigene Profil zuzugreifen. Diese Sicherheitsfragen bieten Userinnen und Usern die Möglichkeit, sich trotz eines vergessenen Passworts zu authentifizieren. Es sollten jedoch Fragen gewählt werden, die lediglich von den Nutzerinnen und Nutzern selbst beantwortet werden können.

→ ***Passwort-Manager:*** *Spezielle Software, die Kennwörter verschlüsselt speichert und verwaltet. Diese Programme sind aus der Notwendigkeit entstanden, unterschiedliche Passwörter für verschiedene Konten und Onlinedienste zu verwenden, die möglichst lang und sicher sind. Hierbei gibt es ein längeres Passwort für den Passwort-Manager, mit dem alle anderen Passwörter verschlüsselt werden.*

Tipp:
Ein guter Tipp ist, die Anfangsbuchstaben eines einprägsamen Merksatzes als Passwort zu verwenden. Beispielsweise „Ich bin am 28. Februar 1980 geboren" ergäbe das Passwort „Iba28.F1980g".

Sicherheitslücken minimieren

Um Sicherheitsrisiken zu vermeiden, empfiehlt es sich in erster Linie, bekannte Sicherheitslücken zu schließen. Die erste Empfehlung in diesem Zusammenhang ist, die vom Hersteller empfohlenen Software-Updates regelmäßig durchzuführen. Software-Updates enthalten kleine Systemverbesserungen: Sie reparieren Fehler oder schließen eventuelle Sicherheitslücken. Die Herstellerinnen und Hersteller haben, sobald sie Kenntnis über ein (Sicherheits-)Problem bei einem ihrer Produkte erlangen, großes Interesse daran, umgehend zu reagieren, und versuchen, schnell eine Lösung des Problems zu erarbeiten. Beispielsweise kann beim Browser oder anderen Programmen vorgesehen werden, dass sie regelmäßig auf Software-Aktualisierungen hin überprüft oder dass diese automatisch durchgeführt werden.

In einem nächsten Schritt können potenzielle Sicherheitslücken, wie unnötige Plug-ins, entfernt werden. Userinnen und User sollten generell – am besten vor Installation – genau prüfen, ob das ***PLUG-IN*** tatsächlich benötigt wird.

Ebenso prinzipiell vorsichtig sollten Userinnen und User beim Einsatz von Browser-Plug-ins wie Java oder Flash sein. Beides sind Anwendungen, die die Darstellung von multimedialen und interaktiven Inhalten ermöglichen (z. B. Videoclips, Werbebannern, Programmen oder Spielen, die über den Webbrowser laufen). Sind Flash und Java trotzdem im Einsatz, sollten Userinnen und User regelmäßig auf die aktuellste Softwareversion umstellen.

Patch:
(Engl. für flicken, auch Nachbesserung.) Software-Update, das Korrekturen enthält, Fehler behebt oder Sicherheitslücken schließt.

Plug-in:
(Engl. für einstecken, konkret auch Erweiterungsmodul.) Softwaremodul, das zur Erweiterung der Funktionalität einer bestehenden Software eingesetzt werden kann.

Auch gibt es die Möglichkeit, Java und Flash auf den manuellen Einsatz zu beschränken – hierbei fragen Webseiten, die diese Plug-ins benötigen, nach, ob diese verwendet werden sollen.

Ein weiteres Risiko stellen offene WLAN-***HOTSPOTS*** dar. Der eigene mobile Datentarif kann bei intensiver Nutzung und Überstrapazierung teuer werden, gleichzeitig gibt es immer wieder Funklöcher, in denen es weniger guten oder auch keinen Empfang gibt. Hotspots sind hier eine attraktive Alternative, vor allem im Ausland. Viele Userinnen und User verbinden ihre Geräte achtlos mit offenen WLAN-Hotspots und nutzen sie wie gewohnt. Jedoch können hier – vor allem bei unverschlüsselten Verbindungen – Passwörter und Zugangsdaten ausgelesen werden. Oft ist jedoch gar nicht erkennbar, ob die Daten verschlüsselt übertragen werden oder nicht. Um dieses Sicherheitsrisiko ohne großen Aufwand zu verringern, sollten offene WLAN-Hotspots gemieden oder die Nutzung dieser auf ein Minimum reduziert werden, beispielsweise darauf, Online-Artikel zu lesen. Für Onlineshopping sind solche Verbindungen eher nicht geeignet.

Hotspot:
(Engl. für Brennpunkt.) Öffentlicher drahtloser Internetzugriffspunkt.

Schadprogramme (Malware)

Etwa zur Jahrtausendwende brachen die ersten großen Virenepidemien über das Internet herein. „MyDoom", „Sobig" und „Slammer" waren in aller Munde – und in vielen Computern. Mittlerweile ist es um Viren etwas ruhiger geworden, die großen und medienwirksamen Epidemien wurden aber lediglich durch chronische Gefahren ersetzt. Die Schadprogramme sind heute auch nicht mehr zwingend das Produkt von Hackerinnen und Hackern, sondern von organisierten Cyberkriminellen.

Die früheren Generationen von Viren löschten einfach die Festplatte oder gewisse Dateien auf dem verseuchten Rechner und waren fähig, sich eigenständig weiterzuverbreiten. Die neue Generation der ***COMPUTERVIREN, TROJANER, SPYWARE*** oder ***RANSOMWARE,*** tarnt sich als harmloses, nützliches Programm, um so seine Opfer zu täuschen. Im Hintergrund werden jedoch ganz andere Operationen vollzogen, von denen die Nutzerinnen und Nutzer nichts mitbekommen. Anfällig sind Nutzerinnen und Nutzer, die Geräte mit veralteter und somit unsicherer Software verwenden. Regelmäßige Software-Updates sind notwendig, da in diesen oftmals Patches für Sicherheitslücken enthalten sind. Das gilt für Betriebssysteme (z. B. Windows) genauso wie für Internetbrowser (z. B. Firefox, Safari) und Softwareprogramme (z. B. Adobe). Werden sie nicht regelmäßig durchgeführt, setzen sich Nutze-

Malware:
(Engl. für Schadsoftware.) Bösartige Programme, die den Rechner oder das Betriebssystem angreifen, Daten stehlen oder diese an Dritte übertragen.

Trojaner:
Software, die sich als harmloses, nützliches Programm tarnt und dabei im Hintergrund ohne das Wissen von Nutzerinnen und Nutzern andere Operationen vollzieht.

Spyware:
(„Spy“, Engl. für Spion.) Software, die ohne das Wissen oder die Zustimmung von Nutzerinnen und Nutzern Daten ausspäht und diese an Dritte übermittelt.

Computervirus:
Software, die sich eigenständig vermehren und verbreiten und dabei Hardware, Software oder Betriebssysteme angreifen und verändern kann.

Ransomware:
(„Ransom“, Engl. für Lösegeld.) Software, mit der der Zugriff oder die Nutzung von Daten oder Computern verhindert oder verschlüsselt wird; für die Freigabe oder Entschlüsselung wird Lösegeld gefordert.

Clickjacking:
(Engl. für Klickeintreibung.) Mit Täuschungsabsicht gestaltete Internetseiten oder Klickflächen, die echte Webseiten oder Klickflächen überlagern, um Nutzerinnen und Nutzer in die Irre zu führen.

rinnen und Nutzer einem unnötigen Sicherheitsrisiko aus, da ihre Geräte (eher) für Schadsoftware angreifbar sind.

Nutzerinnen und Nutzer können sich vor diesen ungeliebten Schadprogrammen schützen, indem sie beispielsweise keine Mail-Anhänge von fragwürdigen Quellen öffnen, Programme nur von vertrauenswürdigen Quellen downloaden oder ihre Smartphone-Apps von den offiziellen App-Stores beziehen (Google Playstore für Android, App Store für iOS oder Windows Store für Windows Phone). Insbesondere sollten Nutzerinnen und Nutzer bei fragwürdigen Download- und Streaming-Webseiten aufpassen, denn hier tummelt sich oft Malware, die z. B. als Software (z. B. ein Videoplayer oder Donwload-Manager) getarnt ist. Obwohl es keinen hundertprozentigen Schutz vor Schadsoftware geben kann, ist die Reduktion von Gefahren und Risiken der erste Schritt zu mehr Sicherheit.

Malware und andere Sicherheitsrisiken verbreiten sich auch immer mehr über soziale Netzwerke, beispielsweise über Facebook. Nutzerinnen und Nutzer, die auf Links von „schockierenden“ Videos klicken, einschlägige Webseiten besuchen oder Facebook-Add-ons herunterladen, die versprechen, die Farbe der Chronik zu ändern oder diese überhaupt vollständig zu entfernen, sind leider der traurige Klassiker von Malware. Durch die Klicks oder Downloads kann schlimmstenfalls das Konto von fremder Seite übernommen werden, und ohne das Zutun der Userinnen und User wird in ihrem Namen gespammt, gepostet und verlinkt – mit dem Ziel, die Freundinnen und Freunde in die gleiche Falle zu locken. Besonders gefälschte Spiele und Seiten machen sich dieses System zunutze.

Eine weitere beliebte, ähnliche Betrugsmethode ist ***CLICKJACKING***. Hierbei werden Schalt- und Klickflächen mit einer Täuschungsabsicht gestaltet; nichts ahnende Nutzerinnen und Nutzer klicken auf einen scheinbar harmlosen Link und bewerten plötzlich zum Beispiel unwissentlich eine dubiose Fanseite mit „Gefällt mir“.

Achtung:
Malware kann man sich nicht nur im Internet holen. Ein Sicherheitsrisiko sind infizierte Endgeräte, die das eigene „anstecken“ (beispielsweise über USB-Verbindungen), oder ***USB***-Sticks. Über eine USB-Schnittstelle können verschiedene Geräte an einen Computer angeschlossen werden (z. B. Maus, Tastatur, USB-Sticks). Die Malware liegt dabei in den kontaminierten Geräten verborgen. Wird etwa ein infizierter USB-Stick an den Computer an-

geschlossen (z. B. BadUSB), kann die Schadsoftware ohne Zutun übertragen werden; es kommt zu Datenverlust, technischen Störungen, „Nach-Hause-Telefonieren“ (Übertragung von Daten an Dritte) bis hin zum Kontrollverlust über das Gerät. Daher ist es ratsam, keine unbekannten (z. B. gefundenen) USB-Sticks an den eigenen Computer anzustecken.

Virenschutz

Eine ***VIRENSCHUTZ***-Software ist ein Programm, das Daten auf Viren, Würmer, Spyware und Trojaner, also generell auf Malware prüft und diese blockiert. Prinzipiell wird zwischen drei Arten von Virenscannern unterschieden: Echtzeitscanner, manuellem Scanner und Online-Virenscanner.

Ein Echtzeitscanner ist eine installierte Software, die im Hintergrund aktiv ist und Dateien und Programme auf Malware scannt und beim Finden einer solchen die Userin oder den User darauf aufmerksam macht; der Echtzeitscanner eignet sich besonders zum präventiven Schutz eines Systems.

Manuelle Scanner müssen – wie ihr Name verrät – manuell von den Nutzerinnen und Nutzern gestartet werden, beispielsweise, wenn ein Mail-Attachment downgeloadet und geöffnet werden soll.

Bei einem Online-Virenscanner braucht der Rechner eine Internetverbindung, die Virenmuster werden online abgeglichen. Ist das Gerät jedoch tatsächlich von Viren befallen, ist gerade die Internetverbindung nicht ohne Risiko, da hier das Gerät ferngesteuert werden kann, um beispielsweise Spam zu verschicken oder andere Rechner anzugreifen. Es empfiehlt sich daher, ein potenziell infiziertes Gerät offline zu nehmen und mit einem Offline-Virenscanner zu untersuchen.

Achtung:
Nutzerinnen und Nutzer müssen sich bewusst sein, dass ein Virenscanner nur gegen bereits bekannte Schadsoftware oder Schadlogiken etwas ausrichten kann; somit kann kein absoluter Schutz garantiert werden. Virenscanner sind dennoch eine sehr gute Ergänzung zu sonstigen Sicherheitsmaßnahmen.

Sensible Daten

Der wichtigste Tipp in diesem Zusammenhang ist, die eigenen schutzwür-

USB bzw. Universal Serial Bus:

Ein Bus ist ein System zur Datenübertragung zwischen mehreren Teilnehmerinnen oder Teilnehmern über einen gemeinsamen Übertragungsweg (= Schnittstelle). Mit USB ausgestattete Medien können bei laufendem Betrieb miteinander verbunden werden, die angeschlossenen Geräte werden automatisch erkannt.

Virenschutz:

(Auch Virenscanner oder Antivirenprogramm genannt.) Software, die Computerviren und andere Schadprogramme aufspürt, blockiert und beseitigt.

digen Zugangsdaten nicht weiterzugeben (z. B. Zugangsdaten für Finanzonline.at). Möchten Nutzerinnen und Nutzer sie dennoch weitergeben, beispielsweise an die Partnerin oder den Partner, sollte dies persönlich geschehen. Besteht ein triftiger Grund dafür, sie schriftlich zu übermitteln, sollten Log-in-Daten getrennt voneinander übermittelt werden (z. B. Username per E-Mail und Passwort telefonisch).

Um sensible Daten, die per E-Mail versandt werden sollen, zu schützen, können sie als passwortgeschützte PDFs im Anhang übermittelt werden. Dies ist bei der Erstellung von PDFs auf Basis eines Word-Dokuments unter Datei > Vorbereiten > Dokument verschlüsseln möglich.

Werden sensible oder private Daten auf einem USB-Stick oder anderen Wechseldatenträgern (z. B. auf einer externen Festplatte) weitergegeben, sollten sie unbedingt verschlüsselt werden, um beispielsweise Datenmissbrauch bei Verlust des Geräts zu verhindern; ein kleiner USB-Stick kann schnell einmal verloren gehen. Für Windows-Systeme kann zum Beispiel die Verschlüsselungssoftware BitLocker to go empfohlen werden.

Kryptografie

Kryptografie:
(„Kryptós", Altgr. für geheim, und „gráphein", Altgr. für schreiben.) Verschlüsselung von Informationen; ist Teil der Kryptologie, der Wissenschaft von der Informationssicherheit.

Verschlüsselung und kryptografische Verfahren gewinnen als eine Möglichkeit des Daten- und Privatsphärenschutzes mehr und mehr an Gewicht. Userinnen und User sollten sich nicht von diesen Begriffen einschüchtern lassen, denn es gibt einfache Sicherheitsmaßnahmen, die nicht unbedingt großes technisches Vorwissen voraussetzen. Viele Dienste bieten einfache Lösungen für technisch durchschnittlich kompetente Userinnen und User an.

Es gibt verschiedene Wege, die eigene E-Mail-Kommunikation zu sichern. Eine Option, um den eigenen Mail-Account zu schützen, ist es, diesen auf Verschlüsselung umzustellen. Der Sicherheitsmodus heißt je nach Anbieterin oder Anbieter unterschiedlich, beispielsweise „SSL" oder „verschlüsselte Verbindung". Diese Einstellungen können bei den erweiterten Kontoeinstellungen vorgenommen werden, doch nicht alle E-Mail-Dienste bieten eine Möglichkeit durchgängiger Verschlüsselung an.

Eine weitere Option ist, auf Mail-Dienste umzusteigen, die verschlüsselte Kommunikation unterstützen (z. B. ProtonMail). Einige von diesen Diensten bieten auch die Möglichkeit an, dass nicht nur die Nachrichten selbst verschlüsselt werden, sondern es auch eine Signatur gibt, die die Authentizität

der Absenderin oder des Absenders belegt.
Möchten Nutzerinnen und Nutzer auf keinen neuen Mail-Dienst umsteigen, können sie entsprechende Software einsetzen. Zur Sicherung der eigenen E-Mail-Kommunikation, aber auch zur Verschlüsselung der eigenen Daten empfiehlt sich beispielsweise die freie Software Gpg4win (für Windows). Das Herzstück, Gnu Privacy Guard, erledigt die kryptografischen Operationen, also das Ver- und Entschlüsseln von Nachrichten, wie auch das Erzeugen und Überprüfen von elektronischen Signaturen. Für Mac OS X empfiehlt sich GPGTools.

Achtung:
Obwohl es mittlerweile einige verhältnismäßig einfache Lösungen gibt, wird für die Implementierung von Verschlüsselungssoftware oder dergleichen ein technisches Grundverständnis notwendig sein. Es empfiehlt sich daher, dass sich weniger versierte Nutzerinnen und Nutzer Unterstützung holen oder sich (zusätzlich) über die verschiedenen Verschlüsselungsarten informieren.