Digitale Kompetenzen

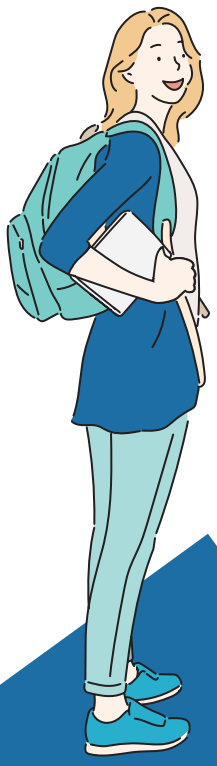
INHALT

DIGITALE KOMPETENZEN

KOMPETENZTEIL 1
Sichere Interneteinstellungen 10

KOMPETENZTEIL 2
Geräte und Software
sicher einrichten und pflegen 19

KOMPETENZTEIL 3
Sichere Logins nutzen 37



Cyberfibel –

How to / Kurzanleitung

Orientierung

Jedes Kapitel in den digitalen Lebenswelten und in den digitalen Kompetenzen ist durch ein Icon gekennzeichnet. Das Icon am rechten Seitenrand kennzeichnet, in welchem Kapitel Sie sich gerade befinden. Die Icons unterstützen zudem Ihre Orientierung bei Verweisen auf andere Kapitel der Cyberfibel. Die Legende im Umschlag der Cyberfibel führt alle Icons zu den zugehörigen Kapiteln auf.

Übungen

In den Lebenswelten der Cyberfibel können Sie mit den angebotenen Übungen das vermittelte Grundlagenwissen praktisch anwenden und erweitern. Sie befähigen dazu, Strategien und Verhaltensweisen für die sichere und souveräne Nutzung des Internets einerseits selbst zu erwerben, andererseits an andere weiterzugeben. Zur Verfügung stehen Aufgaben

- in Einzelarbeit, für das Zuhause oder das Lernen im Kurs und
- in Gruppenarbeit, die in Schulungen eingesetzt werden können.

Glossar

Am Ende der Digitalen Lebenswelten und der Digitalen Kompetenzen ist jeweils ein alphabetisches Glossar eingefügt, in dem Fachbegriffe definiert und erklärt werden. Alle im Glossar enthaltenen Begriffe sind im Text unterstrichen.

Linktipps

Die Cyberfibel bietet Ihnen anhand geprüfter Linktipps weiterführende Materialien, welche ausgewählte Artikel, Videos und Arbeitsmaterialien beinhalten. Zu den Linktipps wird stets der Herausgeber und eine Beschreibung mit angegeben. Wenn Sie den vierstelligen Webcode auf der Webseite (https://www.cyberfibel.de) eingeben, können Sie von dort aus auf die verlinkten Webseiten zugreifen, ohne dass Sie nach diesen suchen oder lange Links abtippen müssen.

Webcode: 1 1 1 1

Beispielhafter Webcode

Disclaimer: Unser Angebot enthält Links zu externen Websites Dritter, auf deren Inhalte wir keinen Einfluss haben. Deshalb können wir für diese fremden Inhalte auch keine Gewähr übernehmen. Auch können wir für mögliche Aufwände, Kosten oder sonstige nachteilige Folgen keine Haftung übernehmen, die durch die Nutzung von externen Webseiten oder aber auch im Rahmen von Übungen entstehen können. Für die Inhalte der verlinkten Seiten ist stets der jeweilige Anbieter oder Betreiber der Seiten verantwortlich und eine Benutzung der Seiten sowie die Übernahme oder Anwendung ihrer Inhalte erfolgt daher stets auf eigene Verantwortung. Bei Bekanntwerden von Rechtsverletzungen werden wir derartige Links umgehend entfernen.

Vorwort

Liebe Leser/-innen,

die zunehmende Digitalisierung trägt zu einer neuen Lebensqualität bei und fördert an vielen Stellen innovative Ideen, die zu mehr Komfort und größerer Effizienz führen. Die Corona-Krise hat uns allen vor Augen geführt, wie hilfreich digitale Technik und insbesondere digitale Kommunikationsmethoden sein können: Viele Menschen haben in dieser Zeit Videochats mit den Großeltern geführt, Online-Meetings mit den Kolleginnen und Kollegen in virtuellen Konferenzräumen abgehalten und mithilfe der Cloud gemeinsam an Dokumenten und Präsentationen gearbeitet. Erfreulich war, dass sich in dieser Zeit viele Menschen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) gewandt haben, um Handlungsempfehlungen und Tipps zur sicheren Nutzung solcher Technologien zu bekommen. Das zeigt, dass Informationssicherheit immer stärker in den Köpfen der Verbraucherinnen und Verbraucher verankert ist – nicht zuletzt auch ein Ergebnis der bereits seit vielen Jahren praktizierten Informations-, Sensibilisierungs- und Aufklärungsarbeit des BSI.

Diesen erfolgreichen Weg wollen wir mit der Cyberfibel weitergehen. Denn um die Möglichkeiten der Digitalisierung nutzen zu können, müssen Verbraucherinnen und Verbraucher über Risiken aufgeklärt und für den sicheren Umgang gerüstet sein. Die Cyberfibel richtet sich an Menschen, die beruflich oder ehrenamtlich in der Verbraucherberatung tätig sind. Diese Wissensvermittlerinnen und -vermittler tragen in Vereinen, Stiftungen, Bildungseinrichtungen oder Verbänden dazu bei, viele Menschen über die Zusammenhänge in der digitalen Welt aufzuklären. In der Cyberfibel werden grundlegende Schutzkompetenzen verständlich aufbereitet. So stellen wir Multiplikatorinnen und Multiplikatoren eine

fundierte und gleichzeitig flexibel einsetzbare Sammlung von Handlungsempfehlungen zur IT-Sicherheit zur Verfügung, die ihnen Orientierung in der Aufklärungsarbeit gibt.

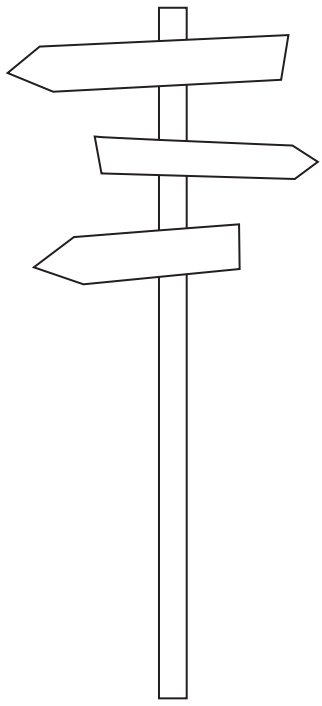
Mit dem Digitalen Verbraucherschutz wollen wir das Risikobewusstsein und die Lösungskompetenz der Menschen erhöhen, denn informierte Verbraucherinnen und Verbraucher können den Nutzen und die Sicherheit neuer Angebote und Technologien besser einschätzen, gegeneinander abwägen und somit fundiertere (Kauf-)Entscheidungen treffen. Die Cyberfibel ist dafür ein wichtiger Baustein.

Arne Schönbohm
Präsident des BSI

DIGITALE KOMPETENZEN

In diesem Teil der Cyberfibel möchten wir Ihnen die Grundlagen für Ihre digitalen Kompetenzen darlegen und Ihnen einen Überblick geben, welche Schutzmaßnahmen Sie jeweils beachten sollten. Der Teil „EXTRA: Risiken verstehen“ soll Ihnen helfen, Risiken bei der Internetnutzung besser einschätzen zu können.

IM ÜBERBLICK:



KOMPETENZTEIL 1
Sichere Interneteinstellungen

STATION 1

Sichere Internet-einstellungen für zu Hause

Wer zu Hause ins Internet möchte, nutzt meistens ein LAN-Kabel, das den Computer mit dem Router verbindet, oder das WLAN. In beiden Fällen spielt der Router eine wichtige Rolle bei der Übertragung von Daten. Darum ist er ein wesentlicher Baustein für den Basisschutz.

Den Router sicher einrichten

Der Router wacht darüber, welche Daten das Heimnetzwerk verlassen und wer von außen Zugriff auf das Netzwerk erhält. Er bildet den Knotenpunkt für die Kommunikation der internetfähigen Geräte und verbindet neben dem Computer beispielsweise auch den smarten Fernseher und teilweise auch die intelligente Haustechnik sowohl untereinander als auch mit dem Internet.

WAS SOLLTEN SIE BEIM EINRICHTEN DES ROUTERS BEACHTEN?

- **Starkes Passwort:** Das Standardpasswort kann ein einfaches Einfallstor für Cyberkriminelle sein. Wenn Sie das voreingestellte Router-Passwort ändern, dann sollte es mindestens acht Zeichen lang sein und keine gängigen Begriffe wie „admin“ oder einfache Zahlenkombinationen wie „1234“ enthalten.

- **Zweiter Faktor:** Falls der Hersteller eine Zwei-Faktor-Authentisierung anbietet, sollten Sie diese aktivieren.

- **Firewall nutzen:** Besitzt Ihr Router eine integrierte Firewall, aktivieren Sie diese. Deaktivieren Sie außerdem den Fernzugang Ihres Routers, wenn Sie ihn nicht benötigen. Falls Ihr Router das zulässt, sperren Sie alle ausgehenden Verbindungen, die Sie nicht benötigen, damit die in Ihr Netzwerk eingebundenen Geräte nicht unkontrolliert ins Internet kommunizieren können.

- **Daten verschlüsseln:** Unverschlüsselter WLAN-Datenverkehr kann auch im heimischen Netzwerk ausgelesen werden und führt zu erheblichen Sicherheitsrisiken. Wählen Sie in Ihrem Router den Verschlüsselungsstandard WPA3 oder, falls dieser noch nicht unterstützt wird, bis auf Weiteres WPA2. Zudem ist es äußerst wichtig, ein komplexes WLAN-Passwort mit mindestens 20 Zeichen zu wählen. Hierfür gelten die gleichen Regeln wie für das Router-Passwort: Keinesfalls dürfen Passwörter aus bekannten, in Wörterbüchern vorhandenen Zeichenkombinationen bestehen.

- **Updates installieren:** Prüfen Sie bereits beim Kauf des Gerätes, ob regelmäßige Aktualisierungen angeboten werden. Aktivieren Sie die automatische Update-Funktion des Routers, damit das Gerät immer auf dem aktuellen Sicherheitsstand ist.

- **Offline sein:** Einfach, aber effektiv. Wenn Sie das WLAN nicht benötigen, schalten Sie es ab.

Weiterführende Informationen

- Mehr dazu erfahren Sie in
  Lebenswelt 1, Station 2 > Wie das Internet funktioniert.

- Wie Sie das Internet nutzen können, erfahren Sie in der
  Lebenswelt 1, Station 4 > Programme und Apps kennenlernen.

Linktipp

Sichere Einrichtung von LAN und WLAN
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Erklärungen zur Funktionsweise von LAN und WLAN sowie Sicherheitstipps

Webcode: 3 1 1 1

STATION 2

Sichere Internet-einstellungen für unterwegs

Am Flughafen, im Hotel oder im Shoppingcenter: Es gibt viele Orte, an denen ein kostenloser Internetzugang über öffentliches WLAN angeboten wird. Bereits beim Verbindungsaufbau erscheint oftmals der Hinweis „ungesichertes Netzwerk“, denn die Datenübertragung kann unverschlüsselt erfolgen und Cyberkriminelle können leicht Daten abgreifen oder Schadsoftware in das Gerät einschleusen.

Mit VPN einen Tunnel bauen

Mit einer Verbindung über ein Virtual Private Network, kurz VPN, kann das Sicherheitsniveau erhöht werden. Sie überträgt sämtliche Daten via Internet grundsätzlich in verschlüsselter Form. Mögliche Ausspähversuche durch andere Teilnehmer oder Teilnehmerinnen im öffentlichen

WLAN werden somit verhindert. Diese verschlüsselten Datenleitungen heißen umgangssprachlich „Tunnelleitungen“ – die Verschlüsselung gräbt gleichsam einen abhörsicheren Tunnel durch das ungeschützte Internet. Moderne Router bieten die Möglichkeit, ein VPN einzurichten. Dann können Sie sich beispielsweise mit Ihrem Smartphone über die in Ihrem Router eingestellten Anmeldedaten registrieren und so via Internet eine gesicherte Verbindung zu Ihrem Heimnetz aufbauen.

WAS SOLLTEN SIE BEIM SURFEN IM ÖFFENTLICHEN WLAN BEACHTEN?

- **Sichere Verbindung:** Übertragen Sie sensible Daten nur über eine verschlüsselte Verbindung. Bei Webseiten erkennen Sie diese zum Beispiel daran, dass vor der Adresse ein „https://“ steht.

- **Offline sein:** Deaktivieren Sie die Funktion für die automatische Verbindung mit bekannten Netzwerken in den Systemeinstellungen Ihres Smartphones. Aktivieren Sie Drahtlosschnittstellen wie das WLAN nur, wenn Sie diese tatsächlich benötigen.

Weiterführende Informationen

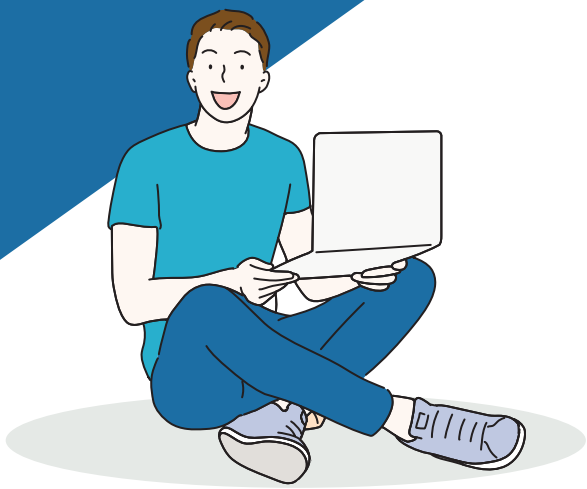
- Wie Sie das Internet unterwegs nutzen können, erfahren Sie unter **Lebenswelt 1, Station 2 > Wie das Internet funktioniert.**

Linktipps

Kleiner VPN-Leitfaden
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Informationen zur Funktionsweise von VPN, zu Einsatzmöglichkeiten und zur Einrichtung

Nutzung öffentlichen WLANs
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Erklärvideo zu Risiken und Empfehlungen bei der Nutzung öffentlichen WLANs, zur Sensibilisierung geeignet

Webcode: 3 1 1 2



STATION 3

Browser sicher einrichten

Der Browser ist wie ein Eingangstor zum Internet: Er überträgt Ihre Daten, dient als Portal für Bankgeschäfte oder ruft Ihre E-Mails für Sie auf. Gängige moderne Webbrowser unterstützen in der Regel die Möglichkeit, die Daten verschlüsselt zu übertragen. Dann steht vor der Adresse ein „https://“. Bei einer unverschlüsselten Übertragung können Angreifer/-innen Ihre Daten auf dem Transportweg mitlesen.

Hintergrund: Sicherheit von JavaScript

Mit JavaScript werden Programme in Internetseiten integriert und auf Ihrem Rechner ausgeführt, wenn Sie die Seiten ansehen. Vielfach findet dies für Werbezwecke Verwendung, aber auch für interaktive Seiten wie beispielsweise Kartendienste. JavaScript wird von Kriminellen immer wieder missbraucht, um sich Zugang zu Rechnern zu verschaffen. Das einzig zuverlässige Mittel gegen solche Angriffe ist die Deaktivierung von JavaScript. Dies hat zwar zur Folge, dass Sie gewisse Webinhalte nur noch eingeschränkt aufrufen können – es macht Ihren Computer jedoch deutlich resistenter gegen unliebsame Eindringlinge.

WAS SOLLTEN SIE BEI DER NUTZUNG DES BROWSERS BEACHTEN?

- **Verwenden Sie stets die neueste Version Ihres Browsers:** Der Browser ist eines der vielseitigsten Programme in einem Computersystem und wird häufig verwendet. Dadurch stellt er auch ein beliebtes Ziel für Attacken dar. Reduzieren Sie das Risiko, indem Sie den Browser immer aktuell halten.

- **Trennung von Browser und Passwortmanager**: In den meisten Fällen bietet der Browser Ihnen die Option, Ihre Passwörter zentral und verschlüsselt zu verwahren. Empfehlenswert sind allerdings Passwortmanager **Kompetenzteil 3, Station 2 > Einrichtung eines Passwortmanagers**, die nicht Teil eines Browsers sind, sondern als eigenständiges Programm auf dem Rechner installiert werden. Sollten Sie doch einige Passwörter in Ihrem Browser hinterlegen, sind automatische Updates umso wichtiger. Diese machen Sie am besten immer im heimischen Netzwerk.

- **Phishing- und Malware-Schutz aktivieren:** Diese integrierten Mechanismen gibt es in allen gängigen Browsern.

Linktipp

Machen Sie Ihren Browser sicher:
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Empfehlungen zum Einrichten von Browsern

Webcode: 3 1 1 3

Einstellungen von Browsern

Die ideale Browsereinstellung für alle gibt es nicht. Wenn eine Internetseite zum Beispiel nur mit Adobe Flash funktioniert, müssen Sie abwägen, ob Sie zugunsten der Sicherheit ganz auf die Nutzung der Seite verzichten oder das damit verbundene Risiko in Kauf nehmen. Hinweise und Anleitungen zu Sicherheitseinstellungen der gängigen Browser finden Sie auf den jeweiligen Hilfeseiten, eine Übersicht mit Links zu diesen Hilfeseiten und weiteren Empfehlungen zu den jeweiligen Browsern gibt es auf „BSI für Bürger“ (siehe Link-Empfehlungen).

Erweiterungen von Browsern

Es besteht die Möglichkeit, die Funktionalitäten eines Browsers über Plug-ins zu erweitern. Diese Programme können beispielsweise Webseiteninhalte anzeigen, deren Format der Webbrowser selbst nicht beherrscht, beim Download unterstützen, das Abspielen von Filmen erleichtern oder auch Passwörter verwalten. Der Einsatz von Plug-ins kann allerdings auch zu Risiken führen. Enthält ein Plug-in Programmierfehler, können Sicherheitslücken entstehen. Prüfen Sie deswegen immer genau, ob Sie das Plug-in benötigen und laden Sie es nur von vertrauenswürdigen Anbietern herunter.

Weiterführende Informationen

Wie Sie den Browser nutzen, erfahren Sie in
Lebenswelt 1, Station 3 > Im Netz surfen.

KOMPETENZTEIL 2
Geräte und Software sicher einrichten und pflegen

STATION 1

Software aktuell halten

Einer der häufigsten und effizientesten Ratschläge für die IT- und Cybersicherheit lautet: Updates installieren. Denn das bedeutet nicht nur eine Erweiterung der Funktionen einer Software – in den meisten Fällen werden damit auch Sicherheitslücken geschlossen. Wer keine Updates installiert, lässt Schlupflöcher offen, die Cyberkriminelle nutzen können. Aus diesem Grund sollten Sie sich Gedanken machen, wie Sie diese Lücken schnellstmöglich und regelmäßig schließen. Man spricht auch von einem Patch-Management.

WAS SOLLTEN SIE BEIM PATCH-MANAGEMENT BEACHTEN?

- **Überblick verschaffen:** Listen Sie auf, welche Programme auf allen Ihren Geräten im Einsatz sind. Dazu zählen Betriebssysteme, Browser, Office-Pakete oder das Virenschutzprogramm. Auch jede App auf dem Smartphone ist ein Programm.

- **Automatische Updates:** Prüfen Sie, für welche Produkte Sie automatische Update-Services erhalten können und schalten Sie diese ein. Diese machen Sie am besten immer im heimischen Netzwerk.

- **Eigenständige Updates**: Falls Sie feststellen, dass Ihnen für eines oder mehrere zentrale Programme kein automatischer Update-Service zur Verfügung steht, lohnt sich das Anlegen einer Liste. Gehen Sie diese regelmäßig durch und prüfen Sie, ob für die entsprechenden Programme Updates verfügbar sind.

- **Schwachstellen erkennen:** Informieren Sie sich regelmäßig über Sicherheitslücken, zum Beispiel mithilfe des Newsletters „Sicher informiert“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Linktipps

Leitfaden für sicheres Patch-Management
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Weiterführende Informationen zum Thema Patch-Management

Newsletter „Sicher informiert“ des BSIs
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Newsletter mit Meldungen unter anderem zu aktuellen Sicherheitsvorfällen und verfügbaren Updates, erscheint alle 14 Tage

SiBa-App
Herausgeber: Deutschland sicher im Netz e. V.
Beschreibung: Die SiBa-App informiert unter anderem über Spam-Wellen, kritische Sicherheitslücken und andere Bedrohungen in verbreiteten Programmen und Diensten.

Webcode: 3 2 1 1

Weiterführende Informationen

Wieso „Lücken“ schädlich sein können, erfahren Sie unter
EXTRA: Risiken verstehen > EXTRA 01: Schadprogramme.

STATION 2

Benutzerkonten sicher einrichten

Wenn mehr als eine Person einen PC nutzt, sollten Sie, sofern das in Ihrem Betriebssystem möglich ist, Benutzerkonten mit eigenem Berechtigungsumfang anlegen. Dies können Sie auch für bestimmte Handlungen machen – beispielsweise ein Benutzerkonto für das Onlinebanking und eines, mit dem Sie online spielen. Wichtig ist hierbei: Diese Konten sollten keine Administratorenrechte besitzen. Denn die Rechte der angemeldeten Nutzerin beziehungsweise des angemeldeten Nutzers bestimmen darüber, wie tief Schadsoftware in das System eingreifen kann, um beispielsweise Daten abzugreifen.

Anwendungsfall: Kinder und Jugendliche

Vor allem für Haushalte mit Kindern und Jugendlichen empfiehlt sich die Einrichtung von Benutzerkonten. Damit stellen Eltern sicher, dass ihr Nachwuchs nur auf freigeschaltete Anwendungen zugreifen kann. Diese Funktion ist auf nahezu allen Geräten verfügbar. So kann beispielsweise auch auf dem Smartphone der App-Download reguliert werden. Zudem kann der Einsatz von Filtersoftware sinnvoll sein, da ein solches Programm den Besuch bestimmter Webseiten verhindert. Als Startseite kann eine Kindersuchmaschine eingestellt und der Download von Programmen untersagt werden.

Weiterführende Informationen

Mehr Informationen zum Onlineshopping erhalten Sie in der
Lebenswelt 2 > Online einkaufen und bezahlen.

Mehr Informationen zum Gaming erhalten Sie in der
Lebenswelt 5, Station 2 > Im Netz spielen und Freizeit verbringen.

WIE KÖNNEN SIE BENUTZERKONTEN FÜR IHRE IT-SICHERHEIT NUTZEN?

- **Ohne Administratorenrechte surfen:** Die Administrator-Option sollten Sie nur dann nutzen, wenn Sie tatsächlich tiefgreifende Änderungen am System vornehmen oder etwa neue Programme installieren wollen.

- **Sensible Daten auf separaten Geräten bearbeiten:** Besonders sensible Vorgänge, wie etwa das Onlinebanking, sollten Sie nicht über einen Computer abwickeln, den mehrere Personen nutzen. Wenn das nicht möglich ist, achten Sie darauf, dass Sie keine Zugangsdaten und Passwörter auf dem PC speichern und dass Sie kritische Dokumente mit einem Passwortschutz versehen.

Linktipps

Surfen mit Administratorenkonto vermeiden
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Video zu Benutzerkonten und Administratorenrechte, zur Sensibilisierung geeignet

Basisschutz für Kinder
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Video zur Einrichtung von Nutzerkonten für Kinder und Jugendliche mit Schritt-für-Schritt-Anleitungen, zur Sensibilisierung geeignet

Webcode: 3 2 1 2

STATION 3

Schutzprogramme nutzen

Um einer Infektion Ihres Computers durch Schadsoftware vorzubeugen, sind Schutzprogramme eine bewährte und wichtige Maßnahme. Ein Virenschutzprogramm überprüft neue Dateien (zum Beispiel Downloads aus dem Internet oder Anhänge von E-Mails) sowie den gesamten Rechner auf Anzeichen einer Infektion. Dazu vergleicht die Software in erster Linie die Daten auf Ihrem Computer mit den Signaturen bekannter Schadprogramme. Da täglich neue Varianten von Schadprogrammen auftreten, müssen diese Signaturen immer auf dem aktuellsten Stand sein. Das bedeutet: Auch Virenschutzprogramme brauchen regelmäßige Updates.
Eine Personal Firewall (auch dezentrale Firewall oder Desktop Firewall genannt) ist eine Software, die vor Angriffen von außen schützen soll. Sie hat die Aufgabe, zu verhindern, dass bestimmte Schadprogramme (wie Spyware) Kontakt vom Rechner zum Internet aufnehmen. Aus diesem Grund kontrolliert sie alle Verbindungen in andere Netzwerke und überprüft sowohl die Anfragen ins Internet als auch die Daten, die zum Rechner gelangen.

Schutzprogramme aktivieren

In den gängigen Computer-Betriebssystemen sind ein Virenschutz und eine Firewall integriert, die bereits in der Standardkonfiguration Angriffe aus dem Internet erschweren. Aktivieren Sie diese oder verwenden Sie ein Schutzprogramm eines anderen Anbieters. Kostenfreie und kostenpflichtige Schutzprogramme unterscheiden sich in der Regel in einigen Funktionalitäten. Wägen Sie ab, welche Funktionalitäten Sie wichtig finden.

Weiterführende Informationen

Mehr zu diesem Thema erfahren Sie in der
Lebenswelt 1, Station 4 > Programme und Apps kennenlernen.

Linktipps

IT-Sicherheit: Antivirus und Firewall
Herausgeber: Stiftung Warentest – test.de
Beschreibung: Übersicht zu Tests von Schutzprogrammen

Tests von Antiviren- & Security-Software
Herausgeber: AV-Test
Beschreibung: Tests von Sicherheitsprodukten

Webcode: 3 2 1 3

WAS SOLLTEN SIE NOCH BEACHTEN?

- **Updates automatisieren:** Auch Virenschutzprogramme müssen immer auf dem aktuellsten Stand sein, um ihre Aufgabe erfüllen zu können. Aktivieren Sie automatische Updates. Falls diese Funktion nicht zur Verfügung steht, achten Sie darauf, dass gerade Schutzprogramme einen kurzen Update-Zyklus haben. Am besten machen Sie Updates immer im heimischen Netzwerk.

- **Schutzprogramme allein reichen nicht:** Bedenken Sie, dass ein Virenschutzprogramm und eine Firewall nur begleitend wirksam sein können. Beachten Sie deswegen die übrigen Tipps zur sicheren Einrichtung und Nutzung von Geräten und Software.

STATION 4

Software auswählen und sicher einrichten

Egal ob PC oder mobile Geräte wie Smartphone und Tablet: Um das Gerät Ihren Vorstellungen und Wünschen entsprechend nutzen zu können, benötigen Sie in der Regel zusätzliche Software. Beim PC wird Software üblicherweise auch als Programm bezeichnet, bei mobilen Geräten hat sich die Bezeichnung App als Abkürzung für Applikation, also Anwendung, etabliert. Bereits beim Erwerb eines Geräts ist neben einem Betriebssystem häufig ein Software-Paket vorinstalliert. Zusätzliche Software wird heutzutage meist über einen Download installiert.

WAS SOLLTEN SIE BEI DER AUSWAHL UND EINRICHTUNG VON SOFTWARE BEACHTEN?

- **Notwendigkeit prüfen:** Installieren Sie nur Software, die Sie tatsächlich benötigen. Jede Software kann Sicherheitslücken enthalten, die ein potenzielles Einfallstor für Schadsoftware darstellen. Je weniger Anwendungen Sie nutzen, desto kleiner ist die Angriffsfläche Ihres gesamten Systems. Haben Sie Zweifel an der Vertrauenswürdigkeit einer Anwendung, recherchieren Sie im Internet, ob der Anbieter seriös ist, oder wenden Sie sich beispielsweise an die Verbraucherzentralen. Im Zweifel sollte auf die Anwendung verzichtet und nach einer Alternative gesucht werden.

- **Ungenutztes löschen**: Entfernen Sie Anwendungen, die Sie nicht mehr nutzen. Denn jedes zusätzliche Programm, jede zusätzliche App ist eine mögliche Sicherheitslücke.

- **App-Berechtigungen hinterfragen:** Viele Apps räumen sich ohne erkennbaren Grund umfassende Rechte ein. Seien Sie kritisch bei einem Zugriff auf Standortdaten oder das Adressbuch. Stellen Sie sich die Frage, ob die Zugriffsrechte für die Funktionalität wirklich notwendig sind. In den meisten Fällen können Sie die Rechte unter dem Punkt „Einstellungen“ verwalten. Das bedeutet auch, dass Sie nach der Freigabe die Rechte später wieder entziehen können.

- **Berechtigungen regelmäßig kontrollieren:** Durch Updates können auch Änderungen oder Erweiterungen der Zugriffsberechtigungen erfolgen. Ist dies der Fall, wägen Sie ab, ob Sie die App unter den geänderten Bedingungen weiterhin nutzen möchten.

- **Sideloading vermeiden:** Installieren Sie Apps ausschließlich von den offiziellen App-Stores. Computerprogramme sollten direkt über den Hersteller bezogen werden, um sicherzugehen, dass wirklich die aktuellste Version installiert wird.

Linktipp

Apps auf mobilen Geräten
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Informationen zur App-Sicherheit

Webcode: 3 2 1 4

STATION 5

Cloud-Nutzung abwägen

Wer Musik bei einem Streamingdienst hört oder eine E-Mail im Internetcafé abruft, nutzt in den meisten Fällen eine digitale Dienstleistung, die auf einer Cloud-Anwendung basiert. Aber auch in anderen Bereichen werden Cloud-Dienste verwendet, zum Beispiel zum Speichern und gemeinsamen Bearbeiten von Daten oder bei vernetzten smarten Geräten: Einige Saugroboter legen Karten der Orte an, die sie reinigen, und zahlreiche Fitnesstracker geben ihre gesammelten Daten zur Auswertung in die Cloud. Ein häufiger Indikator für eine Cloud-Anbindung ist, dass die Geräte per App mittels Smartphone ausgewertet oder gesteuert werden können.

Dabei ist es wichtig, sich bewusst dafür zu entscheiden, einen bestimmten Cloud-Dienst zu nutzen. Oft sind jedoch die Dienste in gekauften Geräten (zum Beispiel im Smartphone) oder in Apps bereits fest integriert. Die Benutzung ist meist komfortabel und bietet hilfreiche Funktionen.

Sensibilisierung und Abwägung

Jeder Nutzer und jede Nutzerin sollte sich fragen, welche Cloud-Dienste wofür genutzt werden, um dann eine bewusste Entscheidung für oder gegen den Gebrauch zu treffen. Versuchen Sie, Cloud-Funktionalitäten, die Sie nicht benötigen, zu deaktivieren oder zu vermeiden. **Bei der Abwägung für konkrete Anwendungsfälle können folgende Fragen helfen:**

- Welche Daten werden in die Cloud übertragen? Ist die Übertragung der Daten eine bewusste Entscheidung?
- Welche Vorteile bietet die Nutzung des Cloud-Dienstes? Welche Nachteile haben Sie, falls Sie den Service nicht nutzen beziehungsweise deaktivieren?
- Wie sensibel sind die potenziell übermittelten Daten? Welches Risiko entsteht, falls die Daten öffentlich gemacht oder missbraucht werden?
- Ist der Cloud-Anbieter bekannt? Vertrauen Sie dem Anbieter? Worauf basiert das Vertrauen? Werden die angeforderten Daten für die jeweilige Funktionalität benötigt?
- Welche Maßnahmen ergreifen Sie auf Ihren Geräten, um die Sicherheit Ihrer Daten in der Cloud zu gewährleisten (zum Beispiel ein sicheres Passwort, Zwei-Faktor-Authentisierung oder das Einspielen von Updates)?

WAS SOLLTEN SIE BEI DER NUTZUNG DER CLOUD BEACHTEN?

- **Weitergabe von Daten:** Informieren Sie sich in den AGB: Was darf der Anbieter mit Ihren Daten machen? Werden diese an Dritte weitergegeben?

- **Rechtliche Bestimmungen**: Auch der Standort des Cloud-Anbieters beziehungsweise der Rechenzentren kann entscheidend sein. Es gelten die rechtlichen Bestimmungen des Landes oder der Länder, in dem oder denen Ihre Daten verarbeitet und gespeichert werden. Diese können sich von den Bestimmungen in Deutschland oder der EU unterscheiden.

- **Cloud-Zugang absichern:** Schützen Sie Ihren Zugang durch ein starkes Passwort und wenn möglich durch eine Zwei-Faktor-Authentisierung.

- **Daten verschlüsseln:** Verschlüsseln Sie schützenswerte Daten vor der Übertragung in die Cloud.

Weiterführende Informationen

- Einen Online-Cloud-Dienst sollten Sie unbedingt mit einem starken Login schützen. Mehr dazu erfahren Sie im
Kompetenzteil 3 > Sichere Logins nutzen.

- Wie Sie das Internet nutzen können, erfahren Sie in der
Lebenswelt 1, Station 5 > Onlinedienste sicher nutzen.

Linktipps

In die Cloud – aber sicher!
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Broschüre zu Cloud-Sicherheit mit Informationen und Empfehlungen

Cloud Computing
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Ausführliche Empfehlungen und Tipps für eine sichere Cloud-Nutzung, etwa zur Absicherung des Zugangs oder der Endgeräte, zum Umgang mit Freigaben bei Speicherdiensten oder zum Verschlüsseln von Daten

Webcode: 3 2 1 5

STATION 6

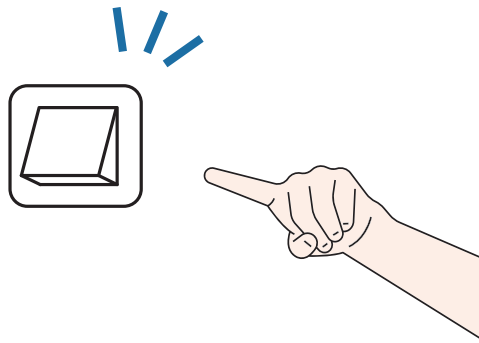
Das smarte Zuhause sicher einrichten

Der Begriff Internet der Dinge oder Internet of Things (IoT) steht für eine vernetzte Welt aus smarten Geräten. Ein smartes Gerät kann sich in der Regel mit anderen Geräten vernetzen, sich mit dem Internet verbinden und aus der Ferne gesteuert werden. Alle smarten Geräte zu Hause bilden das Smart Home. Dazu zählen beispielsweise Systeme, die automatisch Fenster, Türen und Rollläden öffnen oder schließen – sogenannte Hausautomatisierungstechnik. Darüber hinaus gibt es auch Haushaltsgeräte wie Kühlschränke, die Sie über deren Inhalt auf dem Laufenden halten, oder Unterhaltungselektronik wie Smart-TVs oder vernetzte Lautsprecherboxen mit digitalen Assistenten. Da diese Geräte in den meisten Fällen mit dem Internet verbunden sind, gelten für sie dieselben Risiken wie bei herkömmlichen internetfähigen Computern oder Smartphones.

WAS SOLLTEN SIE BEI DER NUTZUNG SMARTER GERÄTE BEACHTEN?

- **Aktuelle Software und Sicherheitsupdates:** Schon vor dem Kauf sollte darauf geachtet werden, dass der Hersteller Updates über einen längeren Zeitraum bereitstellt. Diese müssen immer auf dem aktuellen Stand sein.

- **Zentrale Firewall und Router-Sicherheit:** Die Firewall in Ihrem Router schützt Ihr Heimnetzwerk vor Angriffen über das Internet. Überprüfen Sie, ob Ihr Router eine Firewall integriert hat und aktivieren Sie diese.



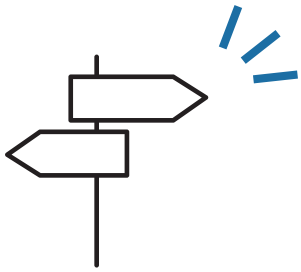
- **Keine Standardpasswörter verwenden:** Ein mögliches Einfallstor für Angreifer/-innen sind an das Internet angeschlossene Geräte, die keinen Passwortschutz besitzen oder nur mit voreingestellten Standardpasswörtern geschützt sind. Vergeben Sie sichere Passwörter und nutzen Sie – wenn möglich – die Zwei-Faktor-Authentisierung

  Kompetenzteil 3, Station 3 > Zwei-Faktor-Authentisierung.

- **Verschlüsselte Kommunikation:** Achten Sie darauf, dass Ihre IoT-Geräte sensible Daten nicht unverschlüsselt versenden. Angreifer/-innen können diese Daten sonst abfangen und auslesen. Die Verschlüsselung sollte möglichst über eine https-Verbindung erfolgen.

- **Daten in der Cloud?** Viele Hersteller speichern und verarbeiten die von IoT-Geräten generierten Daten in einer Cloud. Wägen Sie ab, ob das für die Funktionalität notwendig ist

  Kompetenzteil 2, Station 5 > Cloud-Nutzung abwägen.



Digitale Assistenten

Digitale Assistenten sind Geräte, die das Ziel haben, den Alltag von Personen zu unterstützen, beispielsweise bei der Steuerung von Smart-Home-Systemen. Immer mehr Geräte beinhalten Sprachassistenten bereits als zusätzliche Komfortfunktionalität. Dabei werden Sprachbefehle des Nutzers oder der Nutzerin verarbeitet. Die Ausführung einer Aktion wird in der Regel durch ein Aktivierungswort oder durch eine nichtsprachliche Eingabe wie die Betätigung eines Knopfes eingeleitet. Die Befehlsverarbeitung findet häufig in der Cloud statt. Dadurch können Gefährdungen für die Sicherheit von Daten entstehen. Informationen könnten gestohlen beziehungsweise unrechtmäßig kopiert, weiterverkauft, ausgewertet und beispielsweise für Betrug genutzt werden. Daher sollten Sie sich vor der Verwendung bewusstmachen, welche Daten bei der Nutzung dieser digitalen Assistenten entstehen und mit welchen Risiken dies einhergehen kann.

WAS SOLLTEN SIE BEI DER NUTZUNG VON SPRACHASSISTENTEN BEACHTEN?

- **Vermeidung von unberechtigten Zugriffen:** Deaktivieren Sie den digitalen Assistenten bei Abwesenheit oder schalten Sie ihn aus. Falls möglich, sollten Sprachprofile für verschiedene Personen zur Interaktion mit dem Gerät eingerichtet werden.

- **Geeignete Platzierung des digitalen Assistenten:** Platzieren Sie den digitalen Assistenten an einem Ort, an dem eine Nutzung nur durch Berechtigte möglich ist. Eine Position am offenen Fenster ist beispielsweise ungeeignet, wenn über den Assistenten ein smartes Türschloss gesteuert werden kann.

- **Sichern mit PIN oder Passwort:** Kritische Sprachbefehle wie Bestellungen im Internet sollten immer erst nach Eingabe eines PIN-Codes oder Passwortes ausgeführt werden dürfen.

- **Prüfung der angefallenen Daten:** Durch regelmäßige Einsicht der gespeicherten Daten kann eine missbräuchliche Verwendung des digitalen Assistenten erkannt werden. Nach Bedarf können Sie Daten löschen.

- **Datenschutzeinstellungen anpassen:** Verändern Sie die Datenschutzeinstellungen gemäß Ihrer persönlichen Bedürfnisse.

- **Nur vertrauenswürdige Erweiterungen:** Beziehen Sie Apps nur aus vertrauenswürdigen Quellen.

- **Beschränkung auf notwendige Schnittstellen:** Der digitale Assistent sollte nur mit Geräten und Accounts verbunden werden, die für das Funktionieren des Systems unabdingbar sind. Manchmal ist das Anlegen eines neuen Accounts sinnvoll, um persönliche Daten abzusichern.

Linktipps

Internet der Dinge, aber sicher!
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Tipps zur Einrichtung des smarten Zuhauses als Broschüre und im zugehörigen Erklärvideo

Digitale Assistenten
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Hintergründe und Erklärvideo zu digitalen Assistenten

Webcode: 3 2 1 6

Weiterführende Informationen

Mehr zu den Funktionsweisen des smarten Zuhauses erfahren Sie in der **Lebenswelt 5, Station 1 > Im Smart Home leben.**

KOMPETENZTEIL 3
Sichere Logins nutzen

STATION 1

Einrichtung sicherer Passwörter

Sichere Passwörter für alle Onlinekonten sind neben dem Einsatz eines zweiten Faktors zur Authentisierung der beste Schutz gegen Datenklau. Allerdings kann es zur Herausforderung werden, sich für zahlreiche Online-Accounts unterschiedliche, sichere Passwörter zu merken. Aus diesem Grund zählen „123456“, „hallo“ und „Passwort“ immer noch zu den am häufigsten genutzten Kombinationen. Diese gut zu merkenden Passwörter sind jedoch ein leichtes Spiel für Cyberkriminelle, wenn sie Zugriff auf einen Account erlangen möchten. IT-Geräte und Onlinedienste mit einem sicheren Passwort zu schützen, ist daher eine Grundvoraussetzung, um sich weniger angreifbar zu machen.

WIE SIEHT EIN SICHERES PASSWORT AUS?

- **Persönlich:** Voreingestellte beziehungsweise mitgelieferte Passwörter wie zum Beispiel bei Routern sollten bei der ersten Inbetriebnahme in ein individuelles Passwort geändert werden.

- **Unterschiedlich:** Für jeden Account sollten Sie ein anderes Passwort nutzen. Wird ein und dasselbe Passwort für mehrere Online-Accounts verwendet, haben es Cyberkriminelle leichter, nach der Erbeutung eines Passworts viele verschiedene Konten zu knacken.

- **Gut merkbar:** Bei der Wahl eines Passwortes sind Ihrer Kreativität keine Grenzen gesetzt. Wichtig ist, dass Sie es sich gut merken können.

- **Länge und Komplexität:** Diese beiden Merkmale sind entscheidend für die Sicherheit eines Passworts und sollten bei seiner Bildung immer berücksichtigt werden. Wie genau, führen wir im nächsten Absatz auf.

Länge und Komplexität – Wie kombiniere ich diese entscheidenden Merkmale?

Ein sicheres Passwort ist „kürzer und komplex“ oder „lang und weniger komplex“. Grundsätzlich gilt: **Je länger, desto besser.** Ein gutes Passwort sollte immer **mindestens acht Zeichen lang sein.** Mit kurzen, einfachen Passwörtern ist das Risiko größer, Opfer von Datendiebstahl oder einer Fremdübernahme von Diensten zu werden. Unterschiedliche Zeichenarten wie Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern erhöhen die Komplexität eines Passwortes und damit seine Sicherheit. Doch wie lang und wie komplex sollte ein Passwort mindestens sein? Folgende Beispiele geben Orientierung:

EIN PASSWORT IST SICHER, WENN ES BEISPIELSWEISE

- **20 bis 25 Zeichen lang ist und zwei Zeichenarten genutzt werden**
  (zum Beispiel eine Folge von Wörtern).
  Es ist dann lang und weniger komplex.

- **8 bis 12 Zeichen lang ist und vier Zeichenarten genutzt werden.**
  Es ist dann kürzer und komplex.

- **8 Zeichen lang ist, drei Zeichenarten genutzt werden und es zusätzlich durch eine Mehr-Faktor-Authentisierung abgesichert ist**
  (zum Beispiel durch einen Fingerabdruck, eine Bestätigung per App oder eine PIN). Dies ist generell empfehlenswert.

Linktipp

Passwörter
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Informationen zur Bildung von Passwörtern und zum Umgang mit ihnen

Webcode: 3 3 1 1

WIE MERKE ICH MIR EIN PASSWORT?

- **Merksatz:** Komplexe Passwörter behalten Sie zum Beispiel durch einen Merksatz im Kopf: Nutzen Sie jeweils den Anfangsbuchstaben der Wörter eines frei gewählten Satzes. Wichtig ist dabei, dass sowohl Groß- als auch Kleinbuchstaben, Zahlen oder Sonderzeichen darin vorkommen. Dann wird zum Beispiel aus dem Satz „Ich kaufe meiner Tante jeden Montag 4 Brötchen!“ die Kombination „IkmTjM4B!“. Alternativ können Sie auch ganze Sätze als Passwort nutzen, indem Sie beispielweise den oben genannten Satz zusammensetzen: „IchkaufemeinerTantejedenMontag4Brötchen!“ Diese Passphrasen sind oftmals besser zu merken.

- **Passwortmanager:** Wer sich viele verschiedene Passwörter nicht merken möchte, kann einen Passwortmanager

☞ **Kompetenzteil 3, Station 2 > Einrichtung eines Passwortmanagers** nutzen. Dann müssen Sie sich nur noch ein sicheres Masterpasswort merken – dieses sollte jedoch besonders stark sein.

WAS SOLLTEN SIE NOCH BEACHTEN?

- **Aktiv werden bei einem Vorfall:** Sind Sie selbst von einem Datenleak oder einem Hacking-Vorfall betroffen oder haben Sie den Verdacht, dass dies der Fall sein könnte, sollten Sie Ihre Zugangsdaten (nicht nur das Passwort des betroffenen Dienstes, sondern auch das der verwendeten E-Mail-Adresse) schnellstmöglich ändern.

- **Skeptisch sein bei Passwort-Nachrichten:** Werden Sie überraschenderweise von einem Onlinedienst aktiv aufgefordert, Ihre Login-Daten zu ändern, sollten Sie erst einmal die Echtheit dieser E-Mail überprüfen. Halten Sie Passwörter geheim – geben Sie sie niemals an Dritte weiter und verzichten Sie darauf, diese offen zugänglich zu hinterlegen.

Weiterführende Informationen

- Mehr zur Nutzung von Passwortmanagern erfahren Sie im
  Kompetenzteil 3, Station 2 > Einrichtung eines Passwortmanagers.

- Warum es sich lohnt, einen zweiten Faktor einzurichten, erfahren Sie im
  Kompetenzteil 3, Station 3 > Zwei-Faktor-Authentisierung.

- Anwendungsfelder von sicheren Logins sind unter anderem E-Mail-Postfächer und soziale Netzwerke
  Lebenswelt 3 > Online vernetzen und austauschen
  sowie Onlineshopping und Onlinebanking
  Lebenswelt 2 > Online einkaufen und bezahlen.

STATION 2

Einrichtung eines Passwortmanagers

Passwortmanager sind Programme, die Passwörter sowie Benutzernamen mittels Verschlüsselung und eines sicheren Masterpassworts in einem sicheren Container verwahren. Grundsätzlich gibt es zwei Arten von Passwortmanagern: Je nach Wahl des Programms werden die Passwörter entweder nur lokal auf einem Gerät gespeichert oder bei cloudbasierten Angeboten zwecks Synchronisierung auf verschiedenen Systemen hinterlegt – auch in der Infrastruktur des Anbieters.

Passwortmanager können eine gute Lösung sein, um sich die zahlreichen, komplexen Passwörter zu merken, die Sie für Ihre unterschiedlichen Online-Accounts benutzen. Ob sich der Einsatz eines Passwortmanagers lohnt, sollten Sie nach Abwägen der Vor- und Nachteile entscheiden. In jedem Fall ist es besser, als gängige Passwörter wiederholt zu benutzen.

Welche Vor- und Nachteile sollten Sie abwägen?

VORTEILE :

- Passwörter und Benutzernamen werden verschlüsselt verwahrt.
- Passwortmanager unterstützen bei der Passwortvergabe, zum Beispiel durch die Generierung starker Kombinationen und die Kennzeichnung schon verwendeter oder schwacher

Begriffe. Zudem warnen einige dieser Programme vor gefährdeten Webseiten und möglichen Phishing-Attacken, etwa wenn sich die URL der aufgerufenen Webseite von der gespeicherten unterscheidet.

- Wer Onlinedienste auf mehreren Geräten wie Computer und Smartphone mit unterschiedlichen Betriebssystemen nutzen möchte, kann ein Programm verwenden, das diese synchronisiert.

NACHTEILE:

- Beim Vergessen des Masterpassworts sind im ungünstigsten Fall alle Daten verloren: Das bedeutet oftmals viel Arbeit, da die einzelnen Zugänge zu den Konten individuell wiederhergestellt werden müssen. Bei einem erfolgreichen Cyberangriff auf den Passwortmanager kann es passieren, dass alle Passwörter gleichzeitig gestohlen werden.

- Bei cloudbasierten Diensten vertrauen Sie den Zugang zu Ihren gesamten sensiblen Daten in der Regel einem Unternehmen an. Hier lohnt sich ein Blick in die AGB und Datenschutzerklärungen des jeweiligen Anbieters. Die Informationen über den Standort des Cloud-Diensteanbieters und der Server geben Auskunft darüber, welchem Datenschutzrecht die Daten unterworfen sind **Kompetenzteil 2, Station 5 > Cloud-Nutzung abwägen**.

Weiterführende Informationen

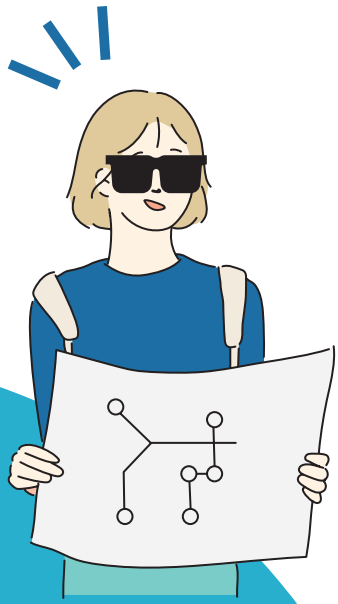
Mehr Informationen zum Thema Cloud erhalten Sie im
Kompetenzteil 2, Station 5 > Cloud-Nutzung abwägen.

Mehr Informationen zum Datenschutz gibt es in der
Lebenswelt 1, Station 3 > Im Netz surfen.

Linktipp

Wie Passwortmanager Daten schützen
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

Webcode: 3 3 1 2



STATION 3

Zwei-Faktor-Authentisierung

Mittlerweile bieten viele Online-Dienstleister Verfahren an, mit denen Sie sich zusätzlich beziehungsweise alternativ zur Passworteingabe identifizieren können, wenn Sie sich in ein Konto einloggen. Diese Zwei-Faktor-Authentisierung gibt es in zahlreichen Varianten, die vom individuellen Code per SMS bis zu einem hardwaregestützten Generator reichen können. Dann ist das Einloggen nicht allein mit Nutzername und Passwort möglich, sondern braucht eine weitere unabhängige Bestätigung (den zweiten „Faktor"). Andere Varianten kombinieren die Faktoren direkt miteinander. So gibt es erst durch die Kombination einer Bankkarte mit der PIN Geld am Automaten. Wichtig ist, dass die Faktoren dabei aus verschiedenen Kategorien stammen, also eine Kombination aus Wissen (zum Beispiel Passwort), Besitz (zum Beispiel Chipkarte) oder Biometrie (zum Beispiel Fingerabdruck) verwendet wird.

Der Vorteil der Zwei-Faktor-Authentisierung liegt auf der Hand: Sollte ein Passwort oder ein PIN einmal in falsche Hände geraten, würde es allein keinen Zugriff auf den entsprechenden Account ermöglichen. Somit verbessert sich die Sicherheit des Logins. Informieren Sie sich deswegen bei Ihren Online-Dienstleistern, ob sie dieses Verfahren anbieten.

Aber auch bei den Authentisierungsmitteln (Passwort, biometrische Merkmale, Chipkarte) besteht grundsätzlich die Gefahr, dass diese in falsche Hände gelangen können. Daher: Bewahren Sie Ihre persönlichen Gegenstände (zum Beispiel Chipkarten) sicher auf und nutzen Sie für die Eingabe von biometrischen Merkmalen und Passwörtern keine Ihnen unbekannten und öffentlich zugänglichen Rechnersysteme.

Linktipp

Zwei-Faktor-Authentisierung für höhere Sicherheit
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Informationen zur Zwei-Faktor-Authentisierung als Video und Podcast, geeignet zur Sensibilisierung

Webcode: 3 3 1 3

WAS SOLLTEN SIE NOCH BEACHTEN?

- **Gezielt anwenden:** Wenden Sie eine Zwei-Faktor-Authentisierung an, sobald ein Onlinedienst dies ermöglicht.
  Viele Dienste haben die Funktion standardmäßig deaktiviert, bieten sie aber dennoch an. Eine Überprüfung der Login-Verfahren lohnt sich.

- **Im Notfall ändern:** Gelangt Ihr Passwort oder Ihre PIN in die falschen Hände, sind Ihre sensiblen Daten dennoch gut gesichert, wenn sie durch die weitere Barriere eines zweiten Faktors vor fremdem Zugriff abgeschirmt werden. Trotzdem müssen Sie im Verdachtsfall umgehend Ihr Passwort oder Ihre PIN ändern.

Weiterführende Informationen

- Die Authentisierung mit dem zweiten Faktor findet beispielsweise Anwendung in der
  ☞ **Lebenswelt 2 > Online einkaufen und bezahlen** und in der
  ☞ **Lebenswelt 3 > Online vernetzen und austauschen**.

KOMPETENZTEIL 4
Daten schützen und sichern

STATION 1

Backup planen

Es gibt viele Möglichkeiten, wie Sie Ihre Fotos, Videos oder Dokumente verlieren können: Eine Schadsoftware verschlüsselt alle Daten, Ihr Smartphone wird gestohlen oder der Laptop beschädigt. Um sich abzusichern, sollten Sie regelmäßig Sicherungskopien anlegen, sogenannte Backups. Dazu ist es ratsam, sich vorab zu überlegen, welche Daten Sie sichern wollen und wo Sie diese speichern.

Welche Daten sichern?

Betriebssysteme und Programme müssen nicht zwingend gesichert werden, da sie relativ leicht per Download wiederherzustellen sind. Hingegen gehen Anwendungsdaten, also Texte, Bilder, Videos und Tabellen, die Sie selbst erstellt haben, im ungünstigsten Fall für immer verloren. Auf dem Smartphone haben Sie außerdem zahlreiche Kontakte. Diese sind meistens direkt in einer speziellen Datenbank abgelegt und nicht mehr auf der SIM-Karte selbst – es sei denn, vom Nutzer oder der Nutzerin wurde das explizit so eingestellt.

Welche Speichermedien sind geeignet?

Sicherungskopien von Dateien, die Sie auf dem Laptop oder dem Computer erstellt oder gespeichert haben, können auf einer externen Festplatte oder einem USB-Stick abgelegt werden. Bei Smartphones stellen die Gerätehersteller für die Sicherung der meisten Daten eine eigene Backup-Software mit entsprechenden Funktionen zur Verfügung. Oftmals können Sie über die Einstellungen des Smartphones beziehungsweise der jeweiligen App entscheiden, welche Daten gesichert werden sollen und welche nicht. In vielen Fällen landen die Daten dann in der Cloud, also einem Rechenzentrum, das von einem Dienstleister zur Verfügung gestellt wird. Es empfiehlt sich, vorab zu klären, in welchem Land die Daten liegen und ob sie verschlüsselt übertragen und abgespeichert werden.

Backup-Plan für das Smartphone

Vor allem für das Smartphone sollte ein Backup-Plan erstellt werden, weil es im Alltag ständig im Einsatz ist – was häufiger zu Verlust, Diebstahl oder Beschädigung führen kann. **Mit dem folgenden Fragenkatalog kann das eigene Vorgehen zur Sicherung der Daten auf dem Smartphone überprüft und geplant werden:**

- Welche Daten sollen gesichert werden?
- Wo sollen die Daten gespeichert werden?
  Ist der Speicherplatz ausreichend?
- Gibt es eine Software, die die Auswahl meiner Daten sichern kann?
  Benötigen einzelne Dateien eine bestimmte Software oder App zur Sicherung?
- Wann und wie regelmäßig wird das Backup angelegt?
- Sind alle gewünschten Daten im Backup abgelegt?
  Lassen sie sich öffnen und prüfen?

Weiterführende Informationen

- Schadprogramme können zum Verlust Ihrer Daten führen. Wie diese auf Ihre Geräte gelangen können, erfahren Sie im Kapitel
  EXTRA: Risiken verstehen > EXTRA 01: Schadprogramme.
- Wer sein Backup in der Cloud ablegt, sollte vorab Vor- und Nachteile abwägen. Mehr dazu im
  Kompetenzteil 2, Station 5 > Cloud-Nutzung abwägen.

Linktipp

Datensicherung und Datenverlust
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Informationen zum Anlegen von Datensicherungen

Webcode: 3 4 1 1

STATION 2

Daten verschlüsseln

Daten werden verschlüsselt, um sie davor zu schützen, von Dritten mitgelesen oder ausspioniert zu werden. Verschlüsselung kann aus verschiedenen Gründen sinnvoll sein: Auf einem gemeinsam genutzten Computer können Sie Daten für andere durch Verschlüsselung unlesbar machen. Gleiches gilt für Personen, die sich unberechtigt Zugang zu Ihrem Computer verschaffen. Informationen auf mobilen Geräten wie Notebooks und USB-Speichermedien sind bei Diebstahl und Verlust sicher, wenn die Daten darauf verschlüsselt sind.

Techniken zur Verschlüsselung ganzer Festplatten oder anderer Datenspeicher schützen die Daten jedoch nur, wenn die Geräte ausgeschaltet sind. Sobald beim Einschalten das Passwort zur Entschlüsselung eingegeben wird, ist der Zugriff auf die Daten wie bei einer unverschlüsselten Festplatte möglich – gegebenenfalls können somit auch andere im Netzwerk oder andere Benutzer/-innen des Computers mit eigenen Konten darauf zugreifen.

Verschlüsselungsverfahren bestehen aus folgenden Elementen: Schlüssel und Algorithmen. Durch Anwendung eines geheimen Schlüssels bei der zu verschlüsselnden Information gemäß eines Algorithmus entsteht die verschlüsselte Botschaft. Analog kann mithilfe des Algorithmus und dem passenden Schlüssel wieder die nicht verschlüsselte Information hergestellt werden. Bei guten Verfahren beruht die Sicherheit der Verschlüsselung auf der Geheimhaltung des Schlüssels und nicht auf der Geheimhaltung des Algorithmus.

GENERELL SOLLEN DABEI FOLGENDE MINIMALZIELE ERREICHT WERDEN:

1. Verschlüsselung und Entschlüsselung von Daten müssen (für einen entsprechend programmierten Computer) einfach sein, wenn der Schlüssel bekannt ist.

- 2. Ohne Kenntnis des Schlüssels soll für einen Angreifer oder eine Angreiferin eine Entschlüsselung von Daten auch dann nicht praktisch möglich sein, wenn sie oder er über beträchtliche Mittel verfügt und das Verfahren kennt.

Linktipp

Datenverschlüsselung
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Wissenswertes und Empfehlungen zur Verschlüsselung

Webcode: 3412

ES GIBT VERSCHIEDENE ARTEN DER VERSCHLÜSSELUNG:

- **Verschlüsselung per Software:** Zahlreiche, teilweise kostenlos verfügbare Programme ermöglichen die Verschlüsselung einzelner Dateien und Ordner oder ganzer Datenträger.

- **Hardwareunterstützte Verschlüsselung per PC:** Einige Computer, vor allem Notebook-Modelle für Geschäftskunden, sind mit einem Trusted Platform Module (TPM) ausgestattet. Dieser Chip kann als Schlüsselspeicher bei der Verschlüsselung von Daten dienen und erhöht die Sicherheit des Schlüssels.

- **Hardwareunterstützte Verschlüsselung per Festplatte:** Es gibt Festplatten, die eine eingebaute Verschlüsselungsoption anbieten.

- **Hardwareunterstützte Verschlüsselung per externem Speichermedium:** Gehäuse für externe Festplatten und USB-Speichermedien werden zum Teil mit eingebauter Verschlüsselungstechnik verkauft. Die Festplatten-Gehäuse erlauben den Zugriff auf die Daten erst, nachdem sich die Nutzerin oder der Nutzer als berechtigt ausgewiesen hat: etwa durch einen Fingerabdruck, durch Eingabe eines Codes auf der eingebauten Tastatur oder durch einen mitgelieferten Funkchip, der wie eine kontaktlose Schlüsselkarte funktioniert.

- **Hardwareunterstützte Verschlüsselung per externem Token:** Das zum Entschlüsseln eines Speichermediums notwendige Schlüsselmaterial kann auf einem externen Hardwaretoken, zum Beispiel einer Smartcard, gespeichert und das Schlüsselmaterial kann zur Nutzung beispielsweise durch die Eingabe einer PIN freigeschaltet werden.

- **Datenspeicher in lokalen Netzwerken:** Sogenannte NAS-Geräte (Network Attached Storage) können je nach Modell die auf ihnen gespeicherten Daten verschlüsseln. Bei jedem Neustart des Gerätes müssen die Daten entschlüsselt werden.

Weiterführende Informationen

- Mehr zum Thema Verschlüsseln auch im
  Kompetenzteil 5, Station 1 > Nachrichten verschlüsseln.

STATION 3

Datensparsamkeit

Soziale Netzwerke laden in den meisten Fällen ein, viel von sich preiszugeben: Fotos, Kontaktdaten, selbst Joggingrouten und Videos vom letzten Geburtstag. Und auch wenn Sie sich bei anderen Onlinediensten wie Shops oder Foren anmelden, hinterlassen Sie dort persönliche Daten, die zwar durch den Anbieter geschützt werden, aber unter Umständen durch ein Datenleak oder einen Hack im Internet verfügbar sein können. Tragen Kriminelle solche Informationen zusammen, können sie das in manchen Fällen zu ihrem Vorteil nutzen, beispielsweise beim Identitätsdiebstahl. Generell sollten Sie deswegen nur so viel über sich preisgeben, wie für die Nutzung des jeweiligen Dienstes benötigt wird.

WAS SOLLTEN SIE BEACHTEN?

- **Eingeschränkte Sichtbarkeit:** Sie sollten die verfügbaren Optionen des sozialen Netzwerkes nutzen, mit denen die von Ihnen eingestellten Informationen und Bilder nur eingeschränkt sichtbar sind: Sollen nur bekannte Kontakte Zugriff darauf haben oder auch deren Kontakte oder gar alle Nutzerinnen und Nutzer dieses Dienstes?

- **Kontaktanfragen prüfen:** Nehmen Sie möglichst nur Freundschaftsanfragen von Ihnen bekannten Personen an. Kontakte, die Sie nicht kennen, sollten Sie kritisch prüfen. Der oder die Unbekannte könnte auch unangemessene Absichten haben, beispielsweise ausspionieren, wann Sie im Urlaub sind und folglich Ihre Wohnung nicht nutzen.

- **Accounts schützen:** In vielen Accounts hinterlegen Sie persönliche Daten und Informationen. Schützen Sie Ihre Accounts vor fremden Zugriff durch sichere Passwörter und Zwei-Faktor-Authentisierung ☞ **Kompetenzteil 3 > Sichere Logins nutzen**. Wird ein Account nicht mehr genutzt, sollten Sie ihn ganz löschen.

- **Recht am Bild sichern:** In einigen Fällen geben Sie mit Ihrem Einverständnis in die AGB die Rechte an Ihren Bildern ab. Dann können diese von den Betreibern weiterverkauft werden. Prüfen Sie vorab, ob das gewährte Nutzungsrecht womöglich bestehen bleibt, wenn Sie Ihr Profil löschen.

Weiterführende Informationen

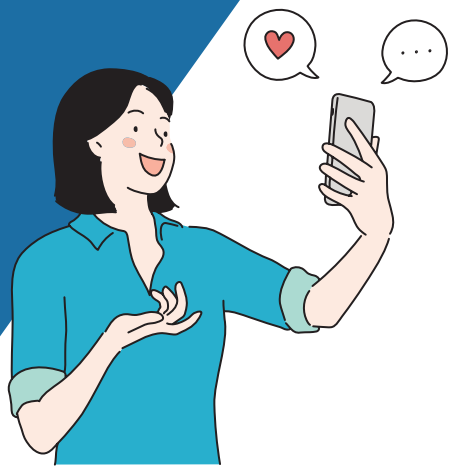
- Datensparsamkeit ist hilfreich, um sich beispielsweise gegen Social Engineering ☞ **EXTRA 02: Onlinebetrug** und Doxing ☞ **EXTRA 03: Missbrauch von sensiblen Daten** zu schützen.

- Mehr zu den sozialen Netzwerken erfahren Sie in der ☞ **Lebenswelt 3, Station 3 > In sozialen Netzwerken austauschen.**

Linktipp

Datenschutz in sozialen Netzwerken – Meine Daten gehören mir
Herausgeber: Klicksafe (EU-Initiative)
Beschreibung: Informationen zum Umgang mit Datenschutz in sozialen Netzwerken

Webcode: 3 4 1 3



KOMPETENZTEIL 5
Sicher digital kommunizieren

STATION 1

Nachrichten verschlüsseln

Täglich werden weltweit Millionen E-Mails und Chatnachrichten über die unterschiedlichsten Programme verschickt. Was viele dabei nicht wissen: Während die Nachricht im (nicht generell verschlüsselten) Internet unterwegs ist, kann sie potenziell mitgelesen werden. Wer sensible Daten versenden möchte, kann eine Verschlüsselung nutzen, um das Risiko des Mitlesens auszuschließen.

ES GIBT ZWEI ARTEN DER VER-SCHLÜSSELUNG VON NACHRICHTEN:

- Bei der **Transportverschlüsselung** werden einzelne Abschnitte im Versandkanal verschlüsselt. Die Technik wird auch als Punkt-zu-Punkt-Verschlüsselung bezeichnet, da die Nachricht an Knotenpunkten wie zum Beispiel dem Server eines E-Mail-Dienstanbieters kurzzeitig unverschlüsselt vorliegt. Die Nachricht selbst wird dabei nicht verschlüsselt, sondern lediglich der Transportweg ist durch Verschlüsselung gesichert. Da mehrere E-Mail-Server bei der Zustellung involviert sein können, kann ein Absender nicht kontrollieren, ob alle Transportstrecken auch wirklich verschlüsselt sind. Durch die Transportverschlüsselung wird das Mitlesen durch Unbefugte zwar erschwert, aber zumindest die beteiligten E-Mail-Service-Provider könnten sich potenziell Zugriff auf den Klartext der Nachricht verschaffen.

- Bei der **Ende-zu-Ende-Verschlüsselung** hingegen wird jede einzelne E-Mail oder Chatnachricht selbst verschlüsselt. Nur Sender/-in und Empfänger/-in können die Nachricht im Klartext lesen, wenn sie über die notwendigen Schlüssel verfügen. **Allein die Ende-zu-Ende-Verschlüsselung erfüllt durchgehend die drei Ziele der Verschlüsselung:**

  - **Schutz der Vertraulichkeit:** Die Nachrichten oder Daten sind nur für denjenigen im Klartext zu lesen oder deutlich zu hören, für den sie bestimmt sind.

- **Schutz der Authentizität:** Die Echtheit des Absenders oder der Absenderin wird verifiziert. Es handelt sich dabei wirklich um die Person, die als Absender/-in angegeben ist.

- **Schutz der Integrität:** Die Nachricht kann auf dem Weg zwischen Absender/-in und Empfänger/-in nicht unbemerkt durch Dritte verändert werden.

WAS SOLLTEN SIE BEI DER VERSCHLÜSSELUNG BEACHTEN?

- **Verschlüsselung nutzen:** Damit gewährleisten Sie die Vertraulichkeit, Authentizität und Integrität der E-Mail. E-Mail-Programme und E-Mail-Dienstanbieter unterstützen bei der Einrichtung der Verschlüsselung.

- **Digitale Unterschrift einsetzen:** Um die Integrität und Authentizität einer Nachricht zu sichern, kann auch eine sogenannte digitale Signatur an die Nachricht angefügt werden.

Linktipps

E-Mail-Verschlüsselung
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Themen-Dossier mit Erklärvideo zur E-Mail-Verschlüsselung

E-Mail-Verschlüsselung rückt in den Fokus
Herausgeber: Bundesdruckerei
Beschreibung: Tipps der Bundesdruckerei zur E-Mail Verschlüsselung

Webcode: 3 5 1 1

Weiterführende Informationen

- Mehr Informationen zum Umgang mit digitalen Nachrichten erhalten Sie in der
  Lebenswelt 3 > Online vernetzen und austauschen.
- Neben Nachrichten können Sie auch Dateien verschlüsseln. Mehr dazu im
  Kompetenzteil 4, Station 2 > Daten verschlüsseln.

STATION 2

Kommunizieren über E-Mail

E-Mails gehören zu unserem Alltag und stehen damit auch im Fokus von Cyberkriminellen. Diese versuchen, an sensible Daten zu kommen und Schadprogramme wie Viren, Würmer und trojanische Pferde (Trojaner) zu verbreiten.

Mit einem Drei-Punkte-Sicherheits-Check können die Risiken bereits gemindert werden. Absenderadresse, Betreff und Anhang sind hierbei drei kritische Punkte, die vor dem Öffnen jeder E-Mail bedacht werden sollten: Ist die Absenderin beziehungsweise der Absender bekannt? Ist der Betreff sinnvoll? Wird ein Anhang oder ein Link erwartet? In Kombination liefern diese Fragen einen guten Anhaltspunkt, um zu entscheiden, ob die E-Mail als vertrauenswürdig einzustufen ist. Es sollte dabei auch bedacht werden, dass Absenderadressen gefälscht werden können.

WAS SOLLTEN SIE NOCH BEACHTEN?

- **Virenschutzprogramm aktivieren:** Diese Software überprüft neue Dateien (zum Beispiel Anhänge von E-Mails) und den gesamten Computer auf Anzeichen von Schadprogrammen.

- **Text-Format nutzen:** Bei vielen E-Mail-Diensten ist das HTML-Format eingestellt, weil die Nachrichten oftmals farbig sowie mit verschiedenen Schriften und Grafiken gestaltet sind. Doch im sogenannten Quellcode einer HTML-formatierten E-Mail kann auch ein schädlicher Code versteckt sein, der bereits beim Öffnen der Nachricht auf Ihrem Computer ausgeführt wird. Dafür müssen Sie nicht einmal einen Anhang anklicken.

- **Inhalte verschlüsseln:** Bisher wird die Ende-zu-Ende-Verschlüsselung bei E-Mails nur sehr selten eingesetzt. Das ist unter anderem darauf zurückzuführen, dass viele Diensteanbieter diese Verschlüsselungstechnik nicht bereits automatisch integriert zur Verfügung stellen. Sie müssen sich selbst darum bemühen, Ihr Mail-Programm mit entsprechenden Plug-ins zu erweitern. Mit dem E-Mail-Verschlüsselungsverfahren EasyGPG hat das BSI den Vorgang des öffentlichen Schlüsseltausches vereinfacht und eine Möglichkeit geschaffen, den Schlüssel direkt über den E-Mail-Anbieter automatisiert versenden zu lassen.

- **Digitale Unterschrift einsetzen:** Um die Integrität und Authentizität einer Nachricht zu sichern, kann auch eine sogenannte digitale Signatur an die Nachricht angefügt werden.

Linktipps

Drei Sekunden für mehr E-Mail-Sicherheit
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Erklärvideo zum Check von E-Mails

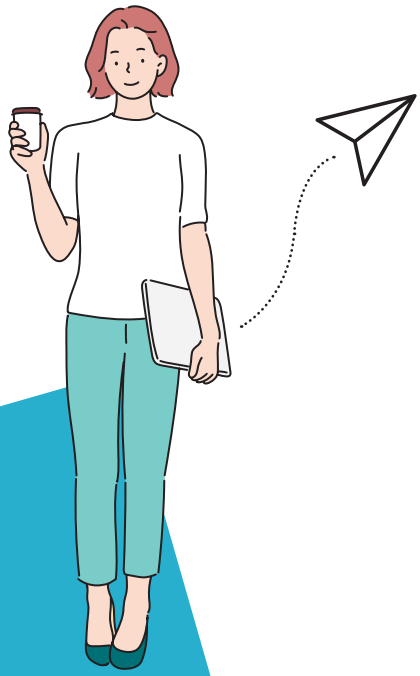
Schlüsseltausch einfach gemacht
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Informationen zur E-Mail-Verschlüsselung mit EasyGPG

Webcode: 3 5 1 2

Weiterführende Informationen

- Die Schadsoftware Emotet sorgt für den Versand authentisch aussehender E-Mails, die besonders schwer zu erkennen sind. Mehr Informationen dazu und zu betrügerischen E-Mails erhalten Sie im Kapitel
  EXTRA: Risiken verstehen > EXTRA 02: Onlinebetrug.

- Wie Sie die E-Mail im Alltag nutzen können, erfahren Sie in der
  Lebenswelt 3, Station 1 > Mit E-Mails beruflich und privat sicher kommunizieren.



STATION 3

Kommunizieren über Messenger

Messenger haben Dienste wie SMS und MMS bei Mobilgeräten weitestgehend verdrängt. Sie bieten die Vorteile, unkompliziert Videos oder Bilder versenden sowie in Gruppen und auch per Videochat kommunizieren zu können. Durch Cyberangriffe oder einfach durch Unachtsamkeit der Nutzerinnen und Nutzer können private Daten jedoch in die Hände unbefugter Dritter geraten.

Wie Sie digitale Spuren hinterlassen

Nachrichten, die über Messenger verschickt werden, bestehen aus dem Text der Nachricht und möglichen Dateianhängen wie einem Foto, aber auch aus Metadaten. Dazu zählen die Kennung der Absenderin oder des Absenders, häufig in der Form der Telefonnummer, die Kennung der Adressatin beziehungsweise des Adressaten, das Datum und die Uhrzeit. Auch weitere Angaben sind möglich. Solche Daten dienen nicht nur der korrekten Zustellung der Nachricht, sondern können auch zur Analyse von Gewohnheiten und von Freundschaftsbeziehungen verwendet werden. Auf diese Weise lassen sich Profile erstellen.

WAS SOLLTEN SIE NOCH BEACHTEN?

- **Zugriffsrechte prüfen:** Wählen Sie Ihren Messenger auch danach aus, welche Zugriffsrechte er auf persönliche Daten wie das Adressbuch einfordert.

- **AGB lesen:** Die AGB von Messenger-Diensten unterscheiden sich deutlich. Achten Sie zudem in der Datenschutzerklärung darauf, ob und wie Ihre Daten weiterverarbeitet werden dürfen und welche Maßnahmen zum Schutz Ihrer Daten getroffen werden.

- **Verschlüsselung nutzen:** Auch Chatnachrichten lassen sich verschlüsseln. Viele Messenger bieten mittlerweile eine Ende-zu-Ende-Verschlüsselung an, bei der Nachrichten nur auf den Geräten der Personen, die gerade kommunizieren, im Klartext vorliegen. Die Datenübertragung erfolgt durchgehend verschlüsselt. Bei manchen Messenger-Diensten müssen Sie die Verschlüsselung selbstständig aktivieren. Vergleichen Sie dazu die Stufen und Arten der Verschlüsselung der verschiedenen Diensteanbieter. Trotz Verschlüsselung sollten Sie keine vertraulichen Daten, wie zum Beispiel Kontoinformationen, über Messenger versenden.

Weiterführende Informationen

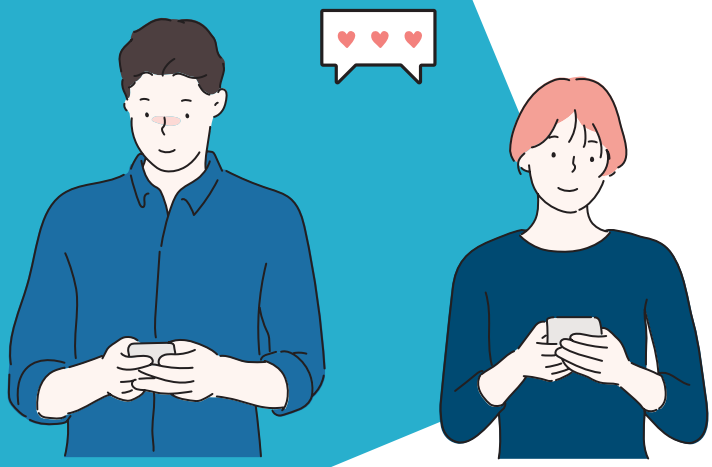
- Mehr zu den Vorteilen von Nachrichten-Anbietern und was Sie bei der Nutzung beachten sollten, erfahren Sie in der **Lebenswelt 3, Station 2 > Mit Instant Messengern schnell und direkt Kontakte pflegen.**

Linktipps

WhatsApp-Alternativen: Messenger im Überblick
Herausgeber: Verbraucherzentrale NRW
Beschreibung: Überblick zum Umgang mit Daten bei unterschiedlichen Messengern

Verschlüsselte Messenger
Herausgeber: Mobilsicher.de
Beschreibung: Vergleich von verschlüsselten Messengern

Webcode: 3 5 1 3



STATION 4

Kommunizieren über soziale Netzwerke

Soziale Netzwerke vereinfachen die Kommunikation mit Menschen, die wir kennen oder kennenlernen wollen. Diese Dienste können jedoch von Kriminellen ausgenutzt werden, um Identitätsdiebstahl, Phishing oder Datendiebstahl zu begehen. Minimieren Sie das Risiko, indem Sie ein paar wenige, aber grundlegende Maßnahmen ergreifen. Allen voran sollten Sie immer skeptisch bei Nachrichten sein, die einen Link enthalten. Manche Cyberkriminelle verschicken betrügerische Nachrichten, die auf manipulierte Webseiten und Schadsoftware weiterleiten. Andere sammeln Kontakte, um Personen auszuspionieren.

Darüber hinaus sind auch Zusatzanwendungen bei sozialen Netzwerken wie Mini-Spiele problematisch, weil sie von Drittanbietern stammen, deren Sicherheitsstandards nicht zwangsläufig denen der sozialen Netzwerke entsprechen. Auf diese Weise können – ob beabsichtigt oder ungewollt – ebenfalls Schadprogramme verbreitet werden.

WAS SOLLTEN SIE NOCH BEACHTEN?

- **Datensparsamkeit:** Wägen Sie gründlich ab, welche Informationen Sie preisgeben. E-Mail-Adressen, Telefonnummern, Hobbys und Vorlieben können sehr aufschlussreich sein.

- **Einstellungen prüfen:** Die Voreinstellungen zum Schutz der Privatsphäre bei der Eröffnung eines Accounts sind oft nicht ausreichend. Viele Daten sind dann automatisch für alle Nutzerinnen und Nutzer des sozialen Netzwerks sichtbar. Auszüge der Profile können teilweise sogar über Suchmaschinen gefunden werden und sind dadurch allen Internetnutzern und -nutzerinnen weltweit zugänglich. Passen Sie deswegen die Einstellungen entsprechend an.

- **Sichere Passwörter:** Unzureichende oder leicht zu erratende Passwörter gefährden die Sicherheit Ihres Accounts. Ein gutes Passwort sollte möglichst lang und für Kriminelle nicht zu erraten sein **Kompetenzteil 3 > Sichere Logins nutzen**.

- **Zweiter Faktor:** Eine sogenannte Zwei-Faktor-Authentisierung kann Ihren Account sogar dann schützen, wenn Ihr Passwort erraten wurde oder auf anderen Wegen abhandengekommen ist. Prüfen Sie, welche Optionen hinsichtlich einer Zwei-Faktor-Authentisierung vom Anbieter des sozialen Netzwerkes unterstützt werden **Kompetenzteil 3, Station 3 > Zwei-Faktor-Authentisierung**.

Linktipps

Tips zum sicheren Umgang mit sozialen Netzwerken
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Zehn wichtige und leicht umsetzbare Sicherheitstipps für das soziale Leben im Internet

Allein unterwegs? Kinder und Jugendliche in den Sozialen Medien
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Podcast mit Empfehlungen zum Umgang mit sozialen Netzwerken für Eltern

Soziale Netzwerke
Herausgeber: Klicksafe (EU-Initiative)
Beschreibung: Umfangreiche Informationen zu populären sozialen Netzwerken

Webcode: 3514

Weiterführende Informationen

Die Risiken in sozialen Netzwerken sind sehr vielfältig und reichen von Schadprogrammen über Onlinebetrug und Missbrauch von Daten bis hin zu Beleidigung und Belästigung. Wie Sie sich im Einzelnen davor schützen können, erfahren Sie im Kapitel
EXTRA: Risiken verstehen.

KOMPETENZTEIL 6
Sichere Transaktionen

STATION 1

Onlinebanking

Bankgeschäfte über das Internet abzuwickeln, ist heutzutage eine Selbstverständlichkeit für viele Menschen. Sie nutzen entweder die Onlineportale der Geldhäuser, über die sie den Kontostand abfragen, Überweisungen durchführen oder Daueraufträge anlegen können, oder speziell für diese Zwecke zur Verfügung gestellte Apps. Da es beim Onlinebanking um Geld geht, ist dieser Bereich für Kriminelle besonders verlockend – sie wollen Konto- und Kreditkartendaten ausspähen und versuchen Wege zu finden, an Ihr Geld zu kommen.

WAS SOLLTEN SIE BEIM ONLINEBANKING BEACHTEN?

- **Basisschutz umsetzen:** Die Geräte, mit denen Sie Onlinebanking betreiben, sollten auf Grundlage des Basisschutzes gesichert sein. Dazu zählt etwa das Installieren von Updates.

Kompetenzteil 2 > Geräte und Software sicher einrichten und pflegen

- **Echtheit der Bank-Webseite und der Verschlüsselung prüfen:** Achten Sie grundsätzlich darauf, dass Sie tatsächlich auf der Webseite Ihrer Bank sind, da immer wieder gefälschte Webseiten kursieren. Geben Sie dafür am besten bei jedem Aufruf die Internetadresse Ihrer Bank erneut über die Tastatur ein oder setzen Sie sich ein Lesezeichen nach einer manuellen Adresseingabe. Rufen Sie die Webseite nicht über eine Suchmaschine auf. Onlinebanking sollte immer über das geschützte https-Protokoll erfolgen.

- **Zwei-Faktor-Authentisierung nutzen:** Zwei-Faktor-Authentisierung ist inzwischen ein Standard beim Onlinebanking. Dort werden in der Regel als zweiter Faktor nach einem Passwort beispielsweise TAN-Generatoren (Hardware) eingesetzt. Diese generieren zeit- oder ereignisbasierte Einmalkennwörter. Außerdem müssen bei der Erzeugung der TAN auch Daten aus der Transaktion (zum Beispiel Kontonummer und Betrag) einbezogen werden.

- **Phishing (er)kennen:** Insbesondere mittels Phishing versuchen Kriminelle, an Ihre Daten zu kommen. Ihre Bank oder Ihr Kreditkartenanbieter wird Sie niemals per E-Mail auffordern, Ihre Daten offenzulegen oder zu ändern.

- **Regelmäßig prüfen:** Informieren Sie sich regelmäßig über Ihre Kontobewegungen und melden Sie Ihrer Bank, wenn Ihnen etwas nicht richtig erscheint.

Linktipps

Onlinebanking
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Tipps und Wissenswertes zum Onlinebanking

Onlinebanking: Wie sicher ist welches TAN-Verfahren?
Herausgeber: Verbraucherzentrale.de
Beschreibung: Vergleich und Bewertung der verschiedenen TAN-Verfahren

Webcode: 3 6 1 1

Weiterführende Informationen

- Mehr zu den Vorteilen des Onlinebankings und weiterer Möglichkeiten, online Geld zu transferieren, erfahren Sie auch in der
  Lebenswelt 2, Station 2 > Einfach und sicher im Netz bezahlen.

STATION 2

Online Geld bezahlen

Konto- oder Kreditkartendaten direkt bei mehreren Onlineshops zu hinterlegen, kann nicht nur lästig, sondern auch riskant sein. Eine Alternative hierzu bieten sogenannte Bezahlsysteme. In der Regel legen Sie dann bei einem Anbieter ein Konto an, in dem Sie Ihre persönlichen Daten angeben, darunter auch Ihre Bankverbindung oder die Kreditkartendaten. Unterstützt ein Onlineshop ein solches Bezahlsystem, werden Sie an der Kasse auf die jeweilige Webseite geleitet, melden sich dort an und bestätigen die Transaktion. Daraufhin kommuniziert der Bezahlsystemanbieter mit dem Shop und zieht schließlich den Betrag von Ihrem Bankkonto oder Ihrer Kreditkarte ein – in vielen Fällen nach Versand der Ware.

WAS SOLLTEN SIE BEI BEZAHLSYSTEMEN BEACHTEN?

- **Konto absichern:** Ebenso wie beim Onlinebanking gilt bei der Nutzung von Bezahlsystemen, dass Sie den Zugang zu Ihrem Nutzerkonto gut absichern sollten – mit einem starken Passwort und möglichst auch mit einer Zwei-Faktor-Authentisierung **Kompetenzteil 3 > Sichere Logins nutzen**.

- **Anbieter vergleichen:** Es gibt verschiedene Anbieter, deren Bezahlsysteme und Leistungen sich unterscheiden. Einige bieten beispielsweise Prepaid-Möglichkeiten, also ein

Guthaben-System. Zudem ist bei einigen Bezahlsystem-anbietern kein Nutzerkonto nötig. Außerdem stehen nicht immer alle Anbieter in den einzelnen Shops zur Auswahl.

Sicherheit im Blick behalten: Auch Bezahlsystemanbieter können Ihnen keine absolute Sicherheit garantieren. Überprüfen Sie regelmäßig die Vorgänge auf Ihrem Konto und seien Sie aufmerksam bei möglichen Betrüger-E-Mails.

Linktipp

Bezahlen im Internet:
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Informationen zu unterschiedlichen Bezahlverfahren im Internet

Webcode: 3 6 1 2

Weiterführende Informationen

Mehr Informationen zu Bezahlsystemen und weiteren Möglichkeiten, online Geld zu transferieren, erhalten Sie in der
Lebenswelt 2, Station 2 > Einfach und sicher im Netz bezahlen.

STATION 3

Kontaktloses Bezahlen

Viele Geschäfte bieten inzwischen das kontaktlose Bezahlen an. Dies kann mit einer entsprechenden Bankkarte oder mit mobilen Geräten wie Smartphones oder Smartwatches samt installierter App geschehen. Dabei wird beispielsweise ein Handy oder eine Karte an ein Zahlterminal gehalten. In vielen Fällen funktioniert das über die NFC-Technik (Near Field Communication).

Auf diese Weise laufen Transaktionen schneller ab. Außerdem lassen sich alle einzelnen Positionen nachvollziehen, sodass die Geldbewegungen insgesamt besser überprüfbar sind. Der Gelegenheitsdiebstahl und die Verbreitung von Falschgeld sind zwar dadurch schwieriger, jedoch eröffnen sich neue Möglichkeiten für Kriminelle.

WAS SOLLTEN SIE BEIM KONTAKTLOSEN BEZAHLEN MIT DEM SMARTPHONE BEACHTEN?

Voraussetzung für das mobile Bezahlen mit dem Smartphone ist ein NFC-Chip, mit dem aktuelle Geräte in der Regel ausgestattet sind.

- **Bezahl-App herunterladen:** Installieren Sie die entsprechende Software nur von vertrauenswürdigen Quellen, etwa Ihrem bekannten App-Store.

- **Updates installieren:** Verwenden Sie immer nur die neueste Version der App und des Betriebssystems Ihres mobilen Geräts. Installieren Sie Software-Updates, sobald sie verfügbar sind. Am besten installieren Sie Updates immer im heimischen Netzwerk.

- **Sperre einrichten:** Verwenden Sie die Bildschirmsperre Ihres Geräts mit PIN, Passwort, Fingerabdruck oder Gesichtserkennung. Sofern es möglich ist, richten Sie eine automatische Sperre ein, die bei wiederholter Falscheingabe des Anmeldepassworts oder einer PIN den Zugriff verweigert.

- **Funktionen deaktivieren:** Aktivieren Sie Bluetooth, NFC oder WLAN nur bei Gebrauch. Auf diese Weise erschweren Sie Angreiferinnen oder Angreifern, eine Verbindung mit dem mobilen Gerät herzustellen.

- **Datensparsamkeit:** Überlegen Sie sich genau, welche Daten Sie in welcher App preisgeben. Denn das Risiko, aussagekräftige Nutzerprofile zu erstellen, entsteht durch die mögliche Verknüpfung von Zahlungs- und Einkaufs- mit Nutzungs- und Standortdaten.

- **Regelmäßig prüfen:** Informieren Sie sich regelmäßig über Ihre Kontobewegungen und melden Sie Ihrer Bank, wenn Ihnen etwas nicht richtig erscheint.

Linktipps

NFC – (fast) kontaktlos bezahlen mit Girocard, Smartphone und Co.
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Informationen und Tipps zum kontaktlosen Bezahlen

Mobiles Bezahlen deaktivieren – so geht es
Herausgeber: Verbraucherzentrale.de
Beschreibung: Schutzmaßnahmen beim mobilen Bezahlen

Webcode: 3 6 1 3

WAS SOLLTEN SIE IM NOTFALL TUN?

1. **Unverzüglich Bankkonto sperren:** Banken haben in der Regel eine eigene Notfallnummer für solche Fälle eingerichtet, bei der Sie anrufen können, oder entsprechende Anleitungen zum Sperren eines Kontos auf ihren Webseiten. Alternativ können Sie die Anmeldemaske zum Onlinebanking aufrufen und dreimal hintereinander die falsche PIN eingeben. Oder rufen Sie den zentralen Sperr-Notruf 116 116 an (aus dem Ausland +49 116 116).

2. **Danach Kontakt mit Bank aufnehmen:** Gegebenenfalls besteht die Möglichkeit, Kontobewegungen rückgängig zu machen.

3. **Ursache klären:** Sollten Sie Opfer eines Phishing-Angriffs mittels eines Trojaners geworden sein, müssen Sie Ihren PC oder Ihr Smartphone fachgerecht von der Schadsoftware befreien.

Weiterführende Informationen

Welche Möglichkeiten es gibt, im Internet zu bezahlen, erfahren Sie in der

Lebenswelt 2, Station 2 > Einfach und sicher im Netz bezahlen.

EXTRA:
Risiken verstehen

EXTRA 01:

Schadprogramme

Schadprogramme, auch Malware genannt, gelangen meist unbemerkt auf ein System und lösen dort schädliche Aktionen aus. Sie dienen Cyberkriminellen als Werkzeug für Delikte wie Datendiebstahl, Betrug und Erpressung. Aktuell sind über 900 Millionen Schadprogrammvarianten im Umlauf und täglich kommen rund 390.000 hinzu. Sie gefährden nicht nur Computer, sondern auch Smartphones, Tablets und andere internetfähige Geräte.

WIE INFIZIEREN SIE SICH MIT SCHADPROGRAMMEN?

- **E-Mail-Anhänge:** Verseuchte E-Mail-Anhänge sind nach wie vor ein häufiger Weg, Schadsoftware auf Computer einzuschleusen. Deshalb gilt stets erhöhte Aufmerksamkeit vor dem Doppelklick auf den Anhang. Anhänge in Dateiformaten wie .exe oder .scr können Schadsoftware direkt auf Ihr Gerät laden. Schadprogramme, die üblicherweise als Wurm bezeichnet werden, verbreiten sich selbstständig ohne Nutzerinteraktion. Sie verstecken sich beispielsweise im Anhang einer E-Mail und nutzen häufig nicht geschlossene Sicherheitslücken aus.

- **Software:** Trojaner bezeichnen eine versteckte Schadkomponente von Software. Eine solche Komponenten enthaltende Software wird von Nutzerinnen und Nutzern meist eigenständig installiert, zum Beispiel unbemerkt beim Download von kostenlosen Software-Angeboten.

- **Webseite:** Auch der Aufruf einer mit Malware präparierten Webseite im Browser beispielsweise über einen Link in einer Nachricht kann den Rechner infizieren. Man spricht in solchen Fällen von einer Drive-by-Infektion, weil sie gleich-

sam im „Vorbeifahren“ erfolgt. Das Gefährliche daran: Selbst seriöse Webseiten können mit einem Drive-by-Code verseucht sein – etwa durch manipulierte Werbebanner, die von einem externen Server geladen werden. Für Drive-by-Infektionen werden ebenfalls oft nicht geschlossene Sicherheitslücken ausgenutzt.

Was verursachen Schadprogramme?

Es gibt unterschiedliche Arten von Schadprogrammen. Die meisten werden für breit gestreute, ungezielte Cyberangriffe eingesetzt. Es geht darum, möglichst viele Geräte zu infizieren. In den meisten Fällen steht also nicht eine bestimmte Person im Fokus eines Angriffs. Über das eingeschleuste Schadprogramm können Computer, Tablet oder Smartphone beispielsweise ausgeschaltet, beschädigt oder Nutzerdaten gestohlen werden. **Zu den häufigsten Auswirkungen einer Infektion zählen:**

- **Fernsteuerung:** Schadprogramme mit einer Funktionalität zur Fernsteuerung des infizierten Systems – üblicherweise

ohne dass der Nutzer oder die Nutzerin dies bemerken – können von Cyberkriminellen zum Aufbau eines sogenannten Botnetzes verwendet werden. Ein Botnetz kann beispielsweise zum Lahmlegen von Internetseiten oder zum Versand von Spam genutzt werden.

- **Erpressung:** Ransomware bezeichnet Arten von Schadprogrammen, die den Zugriff auf die Daten oder das System einschränken beziehungsweise komplett unterbinden. Entweder sperrt sie den Systemzugriff, sodass sich beispielsweise Programme auf einem PC nicht mehr aufrufen lassen, oder sie verschlüsselt bestimmte Daten. Für die Freigabe wird dann ein Lösegeld (englisch: ransom) verlangt. Da nicht sicher ist, ob die Daten nach Zahlung des Lösegelds tatsächlich wieder entschlüsselt werden, empfiehlt die Polizei, nicht auf die Forderungen einzugehen und weder Geld noch Onlinewährungen wie Bitcoins zu transferieren. Neuerdings werden auch Daten von Computern gestohlen und es wird ein Lösegeld gefordert, damit sie nicht veröffentlicht werden.

- **Ausspionieren von Daten:** Spyware spioniert Daten aus, die zum Beispiel während einer Software-Registrierung eingegeben werden, und lässt mit jedem Seitenaufruf im Web ein immer genaueres Profil der Nutzerinnen und Nutzer entstehen.

- **Anzeige von Werbung:** Darüber hinaus gibt es auch Adware, eine Schadsoftware zur Anzeige von Werbung.

WIE KÖNNEN SIE SICH VOR SCHADPROGRAMMEN SCHÜTZEN?

- **Führen Sie Updates durch** – von Ihrem Betriebssystem und Programmen auf allen Geräten, um Sicherheitslücken zu schließen.

- **Installieren Sie ein Virenschutzprogramm und eine Firewall**, um Schadprogramme bereits beim ungewollten Download zu erkennen.

- **Verwenden Sie Benutzerkonten mit reduzierten Rechten,** damit Schadprogramme keine Administratorrechte haben.

- **Seien Sie vorsichtig beim Öffnen von E-Mails** – insbesondere, wenn Sie Links und Anhänge anklicken und wenn es sich um die unerwartete Nachricht eines unbekannten Absenders handelt.

- **Nutzen Sie nur vertrauenswürdige Quellen,** um Daten herunterzuladen.

- **Legen Sie Backups wichtiger Daten an,** um sich vor deren Verschlüsselung zu schützen und verlorene Daten selbst wiederherstellen zu können.

Sonderfall: Emotet

Die Schadsoftware Emotet gilt derzeit als eine große Gefahr im Internet und verursacht auch in Deutschland hohe Schäden. Sie funktioniert so: Der Empfänger oder die Empfängerin erhalten E-Mails mit authentischen Inhalten, zum Beispiel Kommunikationsverläufe, die von einem bereits infizierten System übernommen wurden. Es entsteht der Eindruck, die Nachricht sei von einem Absender oder einer Absenderin, mit dem Sie tatsächlich in Kontakt standen. Aufgrund der korrekten Angabe der Namen und Mailadressen in Betreff, Anrede und Signatur wirken diese Nachrichten auf viele authentisch. Deswegen verleiten sie zum unbedachten Öffnen des schädlichen Dateianhangs oder der in der Nachricht enthaltenen URL. Über neu infizierte Systeme werden wiederum solche E-Mails versendet.

Den eigentlichen Schaden richten die Täter/-innen mit nachgeladener Schadsoftware an. Dies ist meist zunächst ein Banking-Trojaner, der ihnen Komplettzugriff auf das Netzwerk verschafft, bevor dann manuell beispielsweise ein Verschlüsselungstrojaner (Ransomware) eingesetzt wird.

Was haben Botnetze mit Ihnen zu tun?

Zu den Schadprogrammen zählen auch Bots, die sich unauffällig auf Ihren PC oder andere internetfähige Geräte schleichen. Beim Bot handelt es sich um ein Programm, das ferngesteuert auf Ihrem PC arbeitet. Von Botnetzen spricht man dann, wenn sehr viele internetfähige Geräte – meist mehrere Tausend – per Fernsteuerung zusammengeschlossen und zu bestimmten Aktionen missbraucht werden. Jeder Computer, jedes Tablet oder jedes Smartphone, aber auch smarte TV-Geräte oder der Router können Teil eines Botnetzes sein.

Alles beginnt mit dem Infizieren mit einem Schadprogramm. Das kann beispielsweise beim Öffnen eines E-Mail-Anhangs geschehen. In den meisten Fällen nutzen Cyberkriminelle Schwachstellen aus, die zum Beispiel durch fehlende Updates entstanden sind. Viele Bots verhalten sich zunächst ziemlich unauffällig, sodass Betroffene davon nichts bemerken. Dennoch sind sie im Hintergrund eventuell aktiv: Die Schadprogramme können per Knopfdruck aktiviert werden. Jedes einzelne Gerät bekommt entsprechende Befehle und führt diese ohne Ihre Kontrolle aus – wird

sozusagen vom Opfer zum Täter. Die einzige Voraussetzung dafür: Die infizierten Geräte müssen online sein – was in vielen Haushalten fast durchgehend der Fall ist.

WELCHEN SCHADEN KÖNNEN BOTNETZE VERURSACHEN?

Botnetze werden von Cyberkriminellen zu bestimmten Aktionen missbraucht:

- **DDoS-Angriffe (Distributed Denial of Service)** haben das Ziel, beispielsweise eine Webseite unzugänglich zu machen oder außer Betrieb zu setzen. Ein Server wird gezielt mit so vielen Anfragen bombardiert, dass das System die Aufgaben nicht mehr bewältigen kann und im schlimmsten Fall zusammenbricht. Auf diese Art können beispielsweise bekannte Unternehmensseiten dermaßen überfordert werden, dass sie für eine bestimmte Zeit für normale Anfragen außer Gefecht gesetzt sind.

- **Massen-E-Mails**: Botnetze können automatisiert massenhaft und unerkannt Spam versenden.

- **Informationsdiebstahl** ist ein weiterer Hauptanwendungszweck. Die Schadprogramme können beispielsweise Kontodaten und Passwörter ausspähen.

Linktipps

Botnetze
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Informationen zu Botnetzen und wie man sich schützen kann inklusive Erklärvideo zum Thema

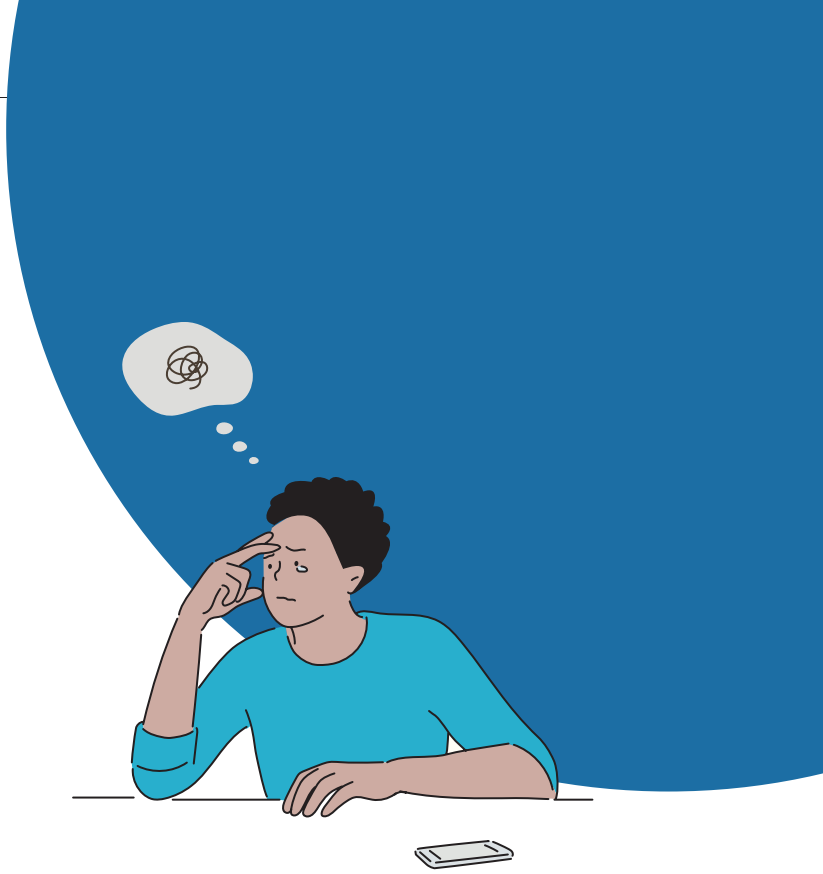
No more ransom
Herausgeber: Initiative von der National High Tech Crime Unit der niederländischen Polizei, Europols europäischem Cybercrime Center, Kaspersky und McAfee
Beschreibung: Informationen zu Ransomware und zu Entschlüsselungswerkzeugen

Webcode: 4 1 1 1

Weiterführende Informationen

- Auch Geräte des smarten Zuhauses können sich mit Schadprogrammen infizieren. Wie Sie sich davor schützen, erfahren Sie im
  Kompetenzteil 2, Station 6 > Das smarte Zuhause sicher einrichten.

- Mehr Infos rund um das Smart Home erhalten Sie auch in der
  Lebenswelt 5, Station 1 > Im Smart Home leben.



EXTRA 02:

Onlinebetrug

Onlinebetrug hat viele Facetten. Einerseits werden immer wieder betrügerische Nachrichten versandt, andererseits werden Webseiten gefälscht. In den meisten Fällen geht es darum, Passwörter, PINs oder andere sensible Daten abzugreifen, Schadprogramme zu verbreiten oder sich schlussendlich finanziell zu bereichern.

Was ist Spam?

Wer einen E-Mail-Account besitzt, hat sicherlich schon einmal eine unerwünschte Nachricht erhalten. Der Begriff Spam-Nachrichten wird als Sammelbegriff für alle Formen von massenhaft versandten, unerwünschten E-Mails beziehungsweise elektronischen Kettenbriefen oder Werbeposts in sozialen Netzwerken genutzt. Mitunter wird Spam auch als Junk bezeichnet – was im Englischen so viel wie Plunder oder Ramsch bedeutet. Häufig enthält Spam jedoch auch Schadprogramme im Anhang oder Links zu verseuchten Webseiten.

BEISPIELE FÜR SPAM SIND:

- **Scam:** Wird auch Vorschussbetrug genannt. Solche Mails versprechen meist den schnellen Weg zum großen Geld. Nur müssen Sie zuvor einen vergleichsweise kleinen Betrag, zum Beispiel für angebliche Anwaltsgebühren, bezahlen.

- **Hoax:** Ein Hoax ist eine Falschmeldung oder ein schlechter Scherz – zumeist mit der Aufforderung verbunden, die Mail an andere Empfänger weiterzuleiten.

- **Phishing:** Mit dieser Spam-Variante versuchen Internet-kriminelle, Ihnen persönliche Informationen zu entlocken – etwa die Zugangsdaten zu Ihrem Bankkonto.

Was ist Phishing?

„Phishing" setzt sich aus den englischen Wörtern „password" und „fishing" zusammen, was frei übersetzt so viel bedeutet wie „nach Passwörtern angeln". Das Prinzip dieses Online-Betrugsversuchs: Cyberkriminelle schreiben (gefälschte) Nachrichten und verlinken auf gefälschte Web-seiten, um Nutzer/-innen vertrauliche Informationen wie Passwörter, Zugangsdaten oder Kreditkartennummern zu entlocken. Allzu oft wirken diese Mails und Seiten überzeugend echt, da das Logo, die Farbgebung und Schriftarten gezielt an eine bekannte Firma oder Organisation erin-nern und teils sogar korrekte Anreden in den E-Mails verwendet werden.

WIE KÖNNEN SIE PHISHING ERKENNEN UND ABWEHREN?

- **Absender gefälscht?** Ob eine Adresse gefälscht ist, kann man oftmals im Header, also der Kopfzeile einer Mail, erkennen. Lassen Sie sich nicht nur den Namen, sondern die ganze E-Mail-Adresse anzeigen. Schauen Sie genau hin, denn manchmal weist nur ein fehlender Buchstabe oder Zahlendreher darauf hin, dass die Nachricht gar nicht von einem bekannten Unternehmen oder Kontakt kommt.

- **Unpersönliche Anrede?** Steht da Ihr Name oder ist die Anrede unpersönlich gehalten („Lieber Kunde der x-Bank!“)? Letzteres ist ein Indiz für eine Sammel- oder gar Phishing-Mail.

- **Dringender Handlungsbedarf?** Sätze wie „Wenn Sie nicht sofort Ihre Daten aktualisieren, gehen diese verloren.“ sind in den meisten Fällen unplausibel.

- **Drohungen?** „Wenn Sie das nicht tun, müssen wir Ihr Konto leider sperren.“ – Solche Aussagen sollen Sie zu schnellen, unüberlegten Handlungen verführen.

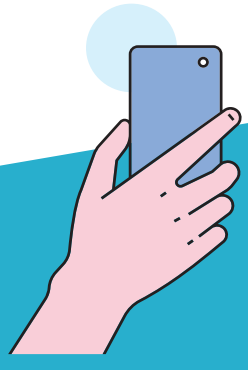
- **Abfrage vertraulicher Daten?** Vertrauliche Daten (wie etwa PINs und TANs) werden von keinem Dienstleister per E-Mail abgefragt.

Gefälschter Link? Seien Sie skeptisch bei eingefügten Links. Wenn Sie mit der Maus über die Adresse fahren – ohne zu klicken –, können Sie in den meisten Fällen sehen, welche Zieladresse angegeben wird. Diese Links können zum Download von Schadprogrammen führen oder auf gefälschte Webseiten weiterleiten. Entspricht der Link der echten Webadresse der genannten Organisation? Wenn Sie sich nicht sicher sind, versuchen Sie die im E-Mail-Text genannte Seite über die Startseite der betreffenden Organisation zu erreichen – also ohne den angegebenen Link anzuklicken, sondern indem Sie die Adresse der Organisation in die Adresszeile des Browsers eintippen.

Was ist Social Engineering?

Beim Social Engineering werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autoritäten ausgenutzt, um Personen geschickt zu manipulieren. Der Angreifer oder die Angreiferin verleitet das Opfer auf diese Weise beispielsweise dazu, vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln, Überweisungen zu tätigen oder Schadsoftware auf dem privaten Gerät oder einem Computer im Firmennetzwerk zu installieren. Dies kann sowohl per Telefon als auch per E-Mail geschehen.

Privat und beruflich ausgerichtete soziale Netzwerke bieten Täter/-innen eine einfache Möglichkeit, im Vorfeld des Angriffs eine Vielzahl von Hintergrundinformationen über Personen zu sammeln und gegebenenfalls zu verknüpfen. Ähnlich wie gestohlene Kommunikationsverläufe können diese Informationen genutzt werden, um Angriffe gezielter auszurichten.



Für Täter oder Täterinnen wird es beispielsweise leichter, eine vertrauliche Beziehung zum Opfer aufzubauen – etwa durch den Verweis auf Hobbys, Freund/-innen oder Kolleg/-innen. Diese kann in der Folge dann zu unzulässigen Handlungen verleiten.

WIE KÖNNEN SIE DAS RISIKO VON SOCIAL ENGINEERING MINIMIEREN?

- **Datensparsamkeit:** Gehen Sie verantwortungsvoll mit sozialen Netzwerken um. Überlegen Sie genau, welche persönlichen und beruflichen Informationen Sie dort offenlegen, da diese von Kriminellen gesammelt und für Täuschungsversuche missbraucht werden können.

- **Vertrauliche Daten zurückhalten:** Teilen Sie Passwörter, Zugangsdaten oder Kontoinformationen niemals per Telefon oder E-Mail mit. Banken und seriöse Firmen fordern ihre Kunden nie per E-Mail oder per Telefon zur Preisgabe von vertraulichen Informationen auf.

- **Im Zweifel anrufen:** Sollte eine Reaktion zwingend erforderlich sein, vergewissern Sie sich durch einen Anruf beim Absender oder bei der Absenderin, dass es sich um eine legitime E-Mail handelt.

WIE KÖNNEN SIE GENERELL SCHÄDLICHE NACHRICHTEN ABWEHREN?

- **Löschen:** Wenn eine E-Mail eines Unbekannten mit einem oder mehreren der oben genannten Merkmale eintrifft, sollte diese sofort gelöscht werden. Sollte es sich doch um eine „echte“ E-Mail halten, wird sich derjenige oder diejenige erneut bei Ihnen melden.

- **Telefonisch nachfragen:** Wenn Sie die Mail eines bekannten Kontakts bekommen haben, diese aber nicht plausibel erscheint, fragen Sie telefonisch bei ihm nach. Nutzen Sie hierfür jedoch nicht die Telefonnummer aus der Signatur der E-Mail.

- **Nicht klicken:** Klicken Sie keinesfalls auf Links oder Anhänge.

- **Generell:** Nutzen Sie Spamfilter und Virenschutzprogramme und halten Sie Ihr Betriebssystem und Ihre Programme aktuell.

Linktipps

NoPhish-Konzept: Awareness-/ Schulungs-/ Trainingskonzept zum Thema Phishing und andere betrügerische Nachrichten
Herausgeber: Forschungsgruppe Security – Usability – Society (SECUSO)
Beschreibung: Unterschiedliche Maßnahmen und Materialien zum Umgang mit Phishing

Phishing-Radar: Aktuelle Warnungen
Herausgeber: Verbraucherzentrale.de
Beschreibung: Aktuelle Beispiele von gemeldeten Phishing-Mails

Wie erkenne ich Phishing-E-Mails?
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Erklärvideo zu Phishing und zum Erkennen gefälschter E-Mails

Social Engineering – der Mensch als Schwachstelle
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Informationen und Statement-Video zum Thema Social Engineering

Webcode: 4 2 1 1

Weiterführende Informationen

- Was Sie darüber hinaus noch beachten können, um sicher zu kommunizieren, erfahren Sie im
  Kompetenzteil 5 > Sicher digital kommunizieren.
- Mehr Informationen über E-Mails, Chats oder die sozialen Netzwerke erhalten Sie auch in der
  Lebenswelt 3 > Online vernetzen und austauschen.

Was sind Fake-Shops?

Fake-Shops bezeichnen gefälschte Internet-Shops, hinter denen sich Betrüger beziehungsweise Betrügerinnen verbergen. Wer dort bestellt, bekommt nach geleisteter Zahlung entweder ein fehlerhaftes Produkt oder keine Lieferung. In vielen Fällen sehen Fake-Shops aus wie echte Onlineshops und sind nur schwer zu erkennen. Ein Indikator ist oftmals ein auffallend niedriger Preis.

WIE KÖNNEN SIE FAKE-SHOPS ERKENNEN?

- **Internetadresse überprüfen:** Es handelt sich häufig um identisch wirkende Kopien bekannter Onlineshops unter leicht veränderter Adresse. Achten Sie deswegen auf die korrekte Schreibweise der URL.

- **Erst Ware, dann Geld:** Vor allem wenn Sie sich unsicher sind, sollten Sie darauf achten, erst nach Erhalt der Ware den Rechnungsbetrag zu zahlen. Mitunter bieten Fake-Shops zahlreiche Bezahlarten an, die jedoch kurz vor Kaufabschluss aufgrund „technischer Probleme“ nicht zur Verfügung stehen.

- **Skeptisch bleiben:** Gütesiegel, Impressum, AGB oder Kundenbewertungen vermitteln ein Gefühl der Sicherheit, können aber gefälscht sein. Das Trusted-Shop-Siegel ist beispielsweise nur dann echt, wenn es mit der Zertifizierungsseite verlinkt ist. Darüber hinaus kann im Zweifel im Impressum der Verweis auf das Handelsregister mit entsprechender Nummer geprüft werden.

Linktipps

Abzocke online: Wie erkenne ich Fake-Shops im Internet?
Herausgeber: Verbraucherzentrale.de
Beschreibung: Übersicht zu Erkennungszeichen von Fake-Shops

Liste betrügerischer Online-Shops
Herausgeber: Watchlist Internet
Beschreibung: Liste von gemeldeten Onlineshops, die als eindeutig unseriös qualifiziert werden

Checklist: So erkennen Sie gefälschte Online-Shops
Herausgeber: Trusted Shops
Beschreibung: Zehn Hinweise auf gefälschte Onlineshops

Webcode: 4 2 1 2

Weiterführende Informationen

Mehr zum Onlineshoppen erfahren Sie in der
Lebenswelt 2 > Online einkaufen und bezahlen.

EXTRA 03

Missbrauch von sensiblen Daten

Wenn viele persönliche Daten einer Person im Internet kursieren, kann das Folgen haben. Kommen diese einmal in die Hände von Unbefugten, können sie damit unter falschem Namen Onlinebestellungen tätigen oder Verträge und Abonnements abschließen. In solchen Fällen spricht man von Identitätsdiebstahl. Immer wieder kommt es auch zu Erpressungsfällen oder Bloßstellungen Betroffener. An die Daten gelangen die Cyberkriminellen beispielsweise durch Datenleaks oder Doxing.

Was ist ein Datenleak?

Bei einem Datenleak werden zumeist zahlreiche sensible Daten veröffentlicht. Es kann sich dabei zum Beispiel um E-Mail-Adressen und Passwörter von Privatpersonen handeln. Die Cyberkriminellen können einerseits über eine kompromittierte Webseite an diese Daten kommen oder über eine Panne, bei der das betroffene Unternehmen die sensiblen Daten ungeschützt aufbewahrt. Gegen solch ein Leak (auf Deutsch „undichte Stelle“) können Sie sich in den meisten Fällen nicht vorbeugend schützen. Aus diesem Grund sollten Diensteanbieter nach Seriosität und angebotenen Sicherheitseigenschaften ausgewählt und wichtige Passwörter nicht wiederverwendet werden.

Was ist Doxing?

Beim sogenannten Doxing sammeln Täter/-innen personenbezogene Daten, die sie bündeln und öffentlich verfügbar machen. Die beste Vorbeugung gegen einen Doxing-Fall ist der sparsame Umgang mit den eigenen Daten im Internet.

- **Nutzen Sie starke und unterschiedliche Passwörter,** vor allem für Zugänge zu Kunden-Accounts bei Banken, Onlineshops, sozialen Netzwerken und für E-Mail-Postfächer.

- **Aktivieren Sie eine Zwei-Faktor-Authentisierung,** wenn diese verfügbar ist.
- **Passwortmanager** können eine hilfreiche Unterstützung sein, wenn Sie viele unterschiedliche Accounts nutzen.
- **Seien Sie sparsam mit den Daten,** die Sie im Internet über sich preisgeben.

WAS SOLLTEN SIE TUN, WENN SIE BETROFFEN SIND?

Personen, deren sensible Daten öffentlich gemacht oder für andere Zwecke missbraucht wurden, müssen umgehend reagieren:

- Überprüfen Sie, von welchen Konten Ihre Daten abgegriffen wurden.
- Setzen Sie die Konten zurück und wählen Sie starke Passwörter, beginnend mit den Accounts, die für das Zurücksetzen von Passwörtern in anderen Anwendungen notwendig sind (zum Beispiel E-Mail-Konten). In einem zweiten Schritt setzen Sie Onlineprofile zurück, mit denen Sie sich auch bei anderen Diensten anmelden können, beispielsweise von sozialen Netzwerken.
- Erstatten Sie in jedem Fall Anzeige. Existierendes Datenmaterial – wie E-Mails, Chatverläufe in Messenger-Diensten, digitale Fotos oder Videos – sind wichtige Beweismittel, die Sie bis zum ersten Kontakt mit der Polizei bestenfalls komplett unverändert lassen.

Linktipp

Unsere Tipps für den Schutz Ihrer digitalen Identität
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Schutzmaßnahmen vor Identitätsdiebstahl

Webcode: 4 3 1 1

Weiterführende Informationen

- Um sich vor dem Missbrauch Ihrer Daten zu schützen, achten Sie auf einen sicheren Zugang zu Ihren Online-Accounts
  Kompetenz 3 > Sichere Logins nutzen.
- Zudem sollten Sie Daten nur sparsam angeben
  Kompetenz 4, Station 3 > Datensparsamkeit.
- Daten können aber auch durch Schadprogramme
  EXTRA 01: Schadprogramme
  oder betrügerische E-Mails
  EXTRA 02: Online-Betrug abgegriffen werden.

EXTRA 04

Belästigung und Beleidigung

Es gibt zahlreiche Möglichkeiten, sich im Internet auszutauschen – per Nachricht, über Kommentare oder eigene Postings. Sie können persönliche Informationen sowohl mit bekannten Kontakten teilen, aber sich auch mit neu kennengelernten Personen austauschen. Diese vielfältigen Möglichkeiten bergen jedoch auch die Gefahr missbraucht zu werden, um Personen zu belästigen, zu beleidigen oder öffentlich zu diffamieren.

Was ist Cybermobbing?

Der Begriff Cybermobbing steht für verschiedene Formen der Diffamierung, Belästigung, Bedrängung und Nötigung anderer Menschen oder Organisationen über das Internet, zum Beispiel über E-Mail, Messaging oder soziale Netzwerke. Laut JIM-Studie 2018 ist ein Drittel der befragten Jugendlichen bereits mit Cybermobbing in Berührung gekommen und hat mitbekommen, wie jemand online gedemütigt wurde.

Cybermobbing kann auch durch Diebstahl und Missbrauch persönlicher Daten erfolgen. Dabei werden beispielsweise in einem sozialen Netzwerk im Namen des vermeintlichen Kontoinhabers beziehungsweise der vermeintlichen Kontoinhaberin Hassnachrichten geschrieben, angebliche sexuelle Vorlieben geäußert oder unangenehme Fotos hochgeladen. Für dieses Phänomen besteht insbesondere in der sozialen Kinder- und Jugendarbeit sowie an Schulen ein hoher Grad an Sensibilität und Interventionskompetenz. Aber auch Erwachsene können betroffen sein.

WIE KÖNNEN SIE SICH DAVOR SCHÜTZEN?

- **So wenig private Daten wie möglich veröffentlichen:** Auch ganz harmlose Fotos oder Videos können beispielsweise so manipuliert werden, dass sie jemanden in Verlegenheit bringen. Deswegen sollten Sie so wenig Fotos und persönliche Informationen wie möglich online stellen.

- **Mobbing melden:** Beleidigungen, Hass-Postings und unangemessene Bilder können in vielen Fällen direkt bei den Diensten gemeldet werden, in denen sie auftauchen.

- **Privatsphäre-Einstellungen:** Private Informationen und Fotos in sozialen Netzwerken oder Apps sollten nicht für alle sichtbar sein. Gehen Sie die Privatsphäre-Einstellungen durch und nehmen Sie keine Freundschaftsanfragen von Fremden an.

WAS KÖNNEN BETROFFENE TUN?

- **Aktionen stoppen:** Blockieren Sie die Person, sodass diese Ihnen keine Nachrichten mehr zuschicken kann und antworten Sie nicht auf bereits zugestellte Nachrichten.

- **Anbieter informieren:** Informieren Sie den Anbieter des Dienstes, der zum Mobbing gegen Sie verwendet wird, und fordern Sie diesen auf, das Konto des Täters oder der Täterin zu sperren.

- **Beweise sichern:** Machen Sie zum Beispiel Bildschirmfotos.
- **Anzeige erstatten:** Gehen Sie zur Polizei. Cybermobbing ist strafbar.

Was ist Cybergrooming?

Cybergrooming ist das englische Wort für „Internet-Anbahnung". Gemeint ist damit das gezielte Ansprechen von Personen im Internet mit dem Ziel der Anbahnung sexueller Kontakte. Insbesondere Kinder sind gefährdet, da die Täter/-innen meist gezielt in Kommunikationsdiensten, auf Videoportalen oder in Onlinespielen nach Kontakten suchen, um ein Vertrauensverhältnis aufzubauen.

Was ist Cyberstalking?

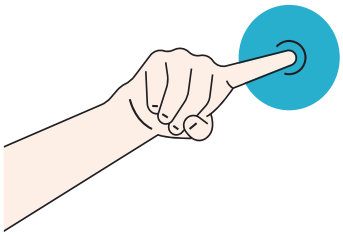
Cyberstalking (auch Digital Stalking oder Onlinestalking) bezeichnet das Nachstellen, Verfolgen und Überwachen einer Person mit digitalen Hilfsmitteln. Dies geschieht insbesondere in Beziehungen, beispielsweise überwacht jemand seinen aktuellen Partner oder seine Ex-Partnerin. Hierzu werden nicht nur Informationen des Opfers verwendet, die es in sozialen Netzwerken veröffentlicht, sondern auch sogenannte Stalkerware, also Programme auf dem Smartphone des Opfers, mit denen Informationen gesammelt werden können. Ähnlich der Spyware können solche Apps dafür verwendet werden, Chatnachrichten, SMS oder den Standort der Person auf den Computer des Täters oder der Täterin zu übermitteln.

WIE KÖNNEN SIE SICH DAVOR SCHÜTZEN?

- **Datensparsamkeit und Privatsphäre-Einstellungen:** Wie auch beim Cybermobbing sollten Sie so wenig persönliche Informationen wie möglich online stellen und anpassen, wer Ihre Inhalte in sozialen Netzwerken sehen darf.

- **Zugriff schützen:** Schützen Sie Ihr Smartphone vor dem Zugriff durch Dritte. Achten Sie darauf, dass die SIM/USIM-PIN und die Bildschirmsperre Ihres Telefons stets aktiviert sind. Nutzen Sie eine PIN, ein Kennwort oder den Fingerabdruck. Geben Sie diese Informationen auch nicht an nahestehende Personen weiter.

- **Drittanbieter-Apps blockieren:** Stellen Sie ein, dass Apps nur über die offiziellen Stores installiert werden können.



WAS KÖNNEN BETROFFENE TUN?

- **Hilfe suchen:** Wenn Sie den Verdacht haben, dass Ihr Smartphone ausspioniert wird und Sie Hilfe suchen, nutzen Sie dafür ein anderes Gerät. So erfährt der Täter beziehungsweise die Täterin nicht davon.

- **Auf Werkseinstellungen zurücksetzen:** Setzen Sie Ihr Smartphone auf die Werkseinstellungen zurück. Installieren Sie alle Apps neu und vergeben Sie neue, individuelle Passwörter für Ihre wichtigen Accounts, zum Beispiel E-Mail, soziale Netzwerke oder Cloud-Dienste.

- **Anzeige erstatten:** Stalking ist strafbar. Sie können sich an die Polizei wenden und Anzeige erstatten.

Weiterführende Informationen

- Seien Sie sparsam mit der Veröffentlichung von Daten
  Kompetenz 4, Station 3 > Datensparsamkeit
  und schützen Sie Ihre Online-Accounts
  Kompetenz 3 > Sichere Logins nutzen.

- Mehr zu den Möglichkeiten in den sozialen Netzwerken erfahren Sie in der
  Lebenswelt 3, Station 3 > In sozialen Netzwerken austauschen.

Linktipps

Cybermobbing und Cyberstalking
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Informationen, Schutzmaßnahmen und Hinweise zur Reaktion im Ernstfall zu Cybermobbing und Cyberstalking

Ratgeber Cyber-Mobbing
Herausgeber: Klicksafe.de (EU-Initiative)
Beschreibung: Informationen für Eltern, Pädagogen, Betroffene und andere Interessierte

Cybermobbing ist digitale Gewalt
Herausgeber: Polizeiliche Kriminalprävention der Länder und des Bundes
Beschreibung: Informationen zu den Folgen von Cybermobbing

#StopCybermobbing: Behaupte dich gegen Cybermobbing
Herausgeber: handysektor.de
Beschreibung: Erklärvideos und Tipps zum Schutz vor Cybermobbing

Was tun bei (Cyber)Mobbing?
Herausgeber: Klicksafe.de (EU-Initiative)
Beschreibung: Handbuch, das pädagogischen Fachkräften systemische Interventions- und Präventionsmethoden an die Hand gibt sowie Praxisbeispiele zur Bearbeitung des Themas mit Kindern und Jugendlichen

Cybermobbing: Was kann ich dagegen tun?
Herausgeber: Bundesministerium für Familie, Senioren, Frauen und Jugend
Beschreibung: Informationen für Betroffene, Eltern und pädagogische Fachkräfte

Cyber-Grooming
Herausgeber: Klicksafe.de (EU-Initiative)
Beschreibung: Informationen zu Cybergrooming und entsprechenden Schutzmaßnahmen

Cybergrooming: So schützen Eltern ihre Kinder
Herausgeber: Schau hin
Beschreibung: Tipps für die Sicherheit von Kindern im Internet

Webcode: 4 4 1 1

Glossar

BEGRIFF	ERKLÄRUNG
Add-on	Kleine Erweiterung zum Browserprogramm, um bestimmte Funktionalitäten hinzuzufügen.
Account	Ein Account ist ein Benutzerkonto bei einem Dienste-anbieter, das eine Zugangsberechtigung erfordert.
Algorithmus	Definierte Handlungsvorschrift zur Lösung eines Problems oder einer bestimmten Art von Problemen. In der Infor-matik: Verarbeitungsvorschrift, die so eindeutig formuliert ist, dass sie durch ein maschinell ausführbares Programm wiedergegeben werden kann.
Antiviren-programm	Siehe Virenschutzprogramm.
App	Eine Applikation, kurz App, ist eine Anwendungssoftware. Der Begriff App wird oft im Zusammenhang mit Anwendun-gen für Smartphones oder Tablets verwendet.
Authentifizierung	Bei der Authentifizierung wird der bei der Authentisierung vorgelegte Identitätsnachweis einer Person überprüft. Erst nach erfolgreicher Authentifizierung erfolgt dann eine Autorisierung.
Authentisierung	Bei der Authentisierung legt eine Person einen Nachweis über ihre Identität vor, um ihn von einem System über-prüfen zu lassen. Dies kann u. a. durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen, die Authentisierung von Daten z. B. durch kryptographische Signaturen.

BEGRIFF	ERKLÄRUNG
Autorisierung	Bei der Autorisierung werden für eine bereits erfolgreich authentifizierte Person die ihr auf einem System eingeräumten Rechte freigeschaltet.
Avatar	„Virtueller Stellvertreter“, Grafik oder Animation, die im Internet – beispielsweise in Chatrooms – zur Darstellung einer Person genutzt wird.
Backup	Ein Backup ist eine Sicherung der Daten zum Schutz vor Datenverlust. Es werden dabei Kopien von vorhandenen Datenbeständen erstellt.
Bluetooth	Bluetooth ist ein Industriestandard für die Datenübertragung zwischen Geräten über kurze Distanz per Funktechnik.
Browser	Der Browser ist ein spezielles Programm, um im Internet zu surfen. Das englische Wort „to browse“ bedeutet so viel wie „blättern“ oder „durchstöbern“.
Botnetz	Als Botnetz wird ein Verbund von Systemen bezeichnet, die von einem fernsteuerbaren Schadprogramm (Bot) befallen sind.
Cache	Pufferspeicher, der Daten schneller zur Bearbeitung bereitstellt. Zum Beispiel: Lokales Verzeichnis für beim Surfen im Internet besuchte Seiten, die so nicht neuerlich geladen werden müssen.
Chat	Über bestimmte Programme oder auf bestimmten Internetseiten ist mit dem Chat eine schnelle, direkte Kommunikation in Echtzeit möglich.
Cloud	Cloud Computing kann als „Rechenleistung aus der Wolke“ verstanden werden. Die Wolke ist dabei ein bildlicher Ausdruck für Rechenzentren, die mit dem Internet verbunden sind. Dabei wird nicht mehr auf die Rechenleistung oder den Speicher der eigenen Geräte zurückgegriffen, sondern die Rechenleistung eines Cloud-Anbieters genutzt.

BEGRIFF	ERKLÄRUNG
Cookie	Zeichenfolge, die mit einer Web-Seite vom Server geladen werden kann und bei einer erneuten Anfrage an den Server mitgesendet wird. Sinn ist, unter anderem Besucher wiederzuerkennen, so dass es beispielsweise nicht erforderlich ist, Nutzerdaten neu einzugeben.
Cybergrooming	Cybergrooming bezeichnet die Kontaktaufnahme von Erwachsenen zu Kindern und Jugendlichen über das Internet mit dem Ziel, sexuelle Handlungen oder Kontakte anzubahnen.
Cybermobbing	Cybermobbing steht für verschiedene Formen der Diffamierung, Belästigung, Bedrängung und Nötigung anderer Menschen oder Firmen über das Internet. Das Opfer wird durch aggressive oder beleidigende Texte, kompromittierende Fotos oder Videos angegriffen oder der Lächerlichkeit ausgesetzt.
Cyberstalking	Cyberstalking (auch Digital Stalking oder Onlinestalking) bezeichnet das Nachstellen, Verfolgen und auch Überwachen einer Person mit digitalen Hilfsmitteln. Dies geschieht insbesondere in Beziehungen, beispielsweise überwacht ein Partner seinen aktuellen Partner oder Ex-Partner.
Datenleak	Bei einem Datenleak geraten Daten in falsche Hände. Cyberkriminelle können über eine kompromittierte Webseite an diese Daten kommen oder über eine Panne, bei der ein Unternehmen die sensiblen Daten ungeschützt aufbewahrt. Teilweise werden die sensiblen Daten dann auch veröffentlicht. Leak heißt auf Deutsch „undichte Stelle“.
Datensicherung	Siehe Backup.

BEGRIFF	ERKLÄRUNG
DoS-/DDoS-Angriffe	Denial-of-Service-Angriffe, kurz DoS, richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten DoS- oder DDoS-Angriff (DDoS = Distributed Denial of Service). DDoS-Angriffe erfolgen häufig durch eine sehr große Anzahl von Computern oder Servern.
Download	Übertragung von Daten von einem fremden Rechner auf den eigenen Rechner, zum Beispiel die aktuelle Version des eigenen Browsers aus dem Internet.
Doxing	Beim so genannten Doxing sammeln Täter/-innen personenbezogene Daten, die sie bündeln und öffentlich verfügbar machen.
Echokammer-Effekt	Siehe Filterblase.
E-Mail	Elektronische Post.
Fake News	Fake News sind Falschmeldungen, die teils irrtümlich, teils bewusst im Internet verbreitet werden, insbesondere in den sozialen Medien.
Fake-Shops	Fake-Shops bezeichnen gefälschte Internet-Shops, hinter denen sich Betrüger bzw. Betrügerinnen verbergen. Nach Erhalt der Bezahlung wird keine Ware ausgeliefert.
Filterblase	Filterblase beschreibt einen Effekt aus den Medienwissenschaften: Weil Webseiten oder soziale Netzwerke versuchen, algorithmisch vorauszusagen, welche Informationen der Benutzer oder die Benutzerin auffinden möchte, werden vermehrt Inhalte gezeigt, die der eigenen Meinung entsprechen. Das führt dazu, dass Leser nicht mehr mit Informationen konfrontiert werden, die den bisherigen Ansichten widersprechen. Auf diese Weise können die eigenen Auffassungen auch nicht mehr überprüft und eventuell relativiert werden.

BEGRIFF	ERKLÄRUNG
Firewall	Die Firewall besteht aus Hard- und Software, die den Datenfluss zwischen dem internen Netzwerk und dem externen Netzwerk kontrolliert. Alle Daten, die das Netz verlassen, können ebenso überprüft werden, wie die, die hinein wollen.
GPS	GPS steht für „Global Positioning System“. Es handelt sich um ein globales Navigationssatellitensystem zur Positionsbestimmung.
Hoax	Der Begriff Hoax bezeichnet eine Falschmeldung (Gerücht oder Scherz), die über E-Mail, Messenger-Programme, SMS oder MMS verbreitet wird.
http	Die Abkürzung steht für Hypertext Transfer Protocol und bezeichnet ein Übertragungsprotokoll für Webseiten.
https	Die Abkürzung steht für Hypertext Transfer Protocol over SSL und bezeichnet ein Protokoll zur verschlüsselten Übertragung von Webseiten.
Instant Messenger	Siehe Messenger.
Internet der Dinge	Im Gegensatz zu „klassischen“ IT-Systemen umfasst das Internet der Dinge „intelligente“ Gegenstände, die zusätzliche „smarte“ Funktionen enthalten. Diese Geräte werden in der Regel an Datennetze angeschlossen, in vielen Fällen drahtlos, und können sogar oft auf das Internet zugreifen und darüber erreicht werden.
Internet of Things (IoT)	Siehe Internet der Dinge.
IP-Adresse	Eine Adresse, unter der ein Rechner innerhalb eines Netzwerks nach dem Internetprotokoll erreichbar ist. Eine IP-Adresse besteht aus vier Byte, die durch Punkte getrennt sind: z. B. 194.95.179.205.

BEGRIFF	ERKLÄRUNG
Junk/Junk-Mail	Bedeutet übersetzt „Abfall-Mail“. Als Junk-Mails bezeichnet man Massenmails, die einem Empfänger ungewollt zugestellt werden und meistens Werbeangebote enthalten.
LAN	LAN steht für Local Area Network und bezeichnet ein lokales Netz. So wird beispielsweise das hausinterne Netz eines Unternehmens genannt.
Leak	Siehe Datenleak.
Login	Anmeldevorgang für die Nutzung eines PC, von einzelnen auf dem PC installierten Programmen oder von Online-diensten.
Malware	Siehe Schadprogramm.
Messenger	Instant-Messaging bedeutet „sofortige Nachrichtenüber-mittlung“. Ein Messenger ist ein Service für Online-Chats und das Versenden kurzer Nachrichten. Dabei ist vorab keine Verabredung nötig – die Anwesenheit von Gesprächs-partnern/-innen wird automatisch signalisiert.
NFC	NFC steht für Near Field Communication und ermöglicht unter anderem das kontaktlose Zahlen. Durch die NFC ist es möglich, auf sehr kurze Distanz kleine Datenmengen zu übertragen. Dazu zählen Zugangs-, Bezahldaten oder Daten-pakete, die beispielsweise Passwörter oder andere Codes enthalten.
Onlinebanking	Bankgeschäfte (z. B. Überweisungen oder Aktienhandel) über das Internet.
Passwortmanager	Programm, beispielsweise als Bestandteil eines Internet-browsers, das bei der Verwaltung von Passwörtern hilft und diese archiviert. Es unterstützt dabei, für jeden Dienst ein seperates Passwort zu nutzen.

BEGRIFF	ERKLÄRUNG
Patch	Ein Patch („Flicken“) ist ein Softwarepaket, mit dem Softwarehersteller Sicherheitslücken in ihren Programmen schließen oder andere Verbesserungen integrieren.
Patch-Management	Als Patch-Management bezeichnet man Prozesse und Verfahren, die helfen, verfügbare Patches für die IT-Umgebung möglichst rasch erhalten, verwalten und einspielen zu können.
Phishing	Das Wort setzt sich aus „Password“ und „Fishing“ zusammen, zu Deutsch „nach Passwörtern angeln“. Beim Phishing wird z. B. mittels gefälschter E-Mails und/oder Webseiten versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen.
PIN-/TAN-Verfahren	Verfahren zur Authentisierung, besonders beim Onlinebanking. Hierbei sind für den Zugang zum Konto neben der Konto- oder Kundennummer die geheime PIN (Personal Identification Number) und für Transaktionen (z. B. Überweisungen) zusätzlich eine TAN (Transaktionsnummer) anzugeben.
Plug-in	Ein Plug-in ist eine Zusatzsoftware oder ein Softwaremodul, das in ein Computerprogramm eingebunden werden kann, um dessen Funktionalität zu erweitern.
Ransomware	Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch „ransom“) wieder freigeben.
Router	Der Router verbindet das Heimnetzwerk und das Internet. Er bildet den Knotenpunkt für die Kommunikation der internetfähigen Geräte und verbindet neben dem Computer auch den smarten Fernseher und teilweise die intelligente Haustechnik mit dem Internet.

BEGRIFF	ERKLÄRUNG
Schadprogramme	Die Begriffe Schadfunktion, Schadprogramm, Schadsoftware und Malware werden häufig synonym benutzt. Sie bezeichnen Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen.
Server	Typischerweise bezeichnet ein Server einen Rechner, der seine Hardware- und Software-Ressourcen in einem Netz anderen Rechnern zugänglich macht. Beispiele sind Applikations-, Daten-, Web- oder E-Mail-Server.
Signatur	Eine digitale Signatur (=Unterschrift) besteht aus Daten in elektronischer Form. Die Signatur wird an andere elektronische Daten angehängt, um den Verfasser bzw. die Verfasserin von Informationen klar zu identifizieren und zu belegen, dass die Daten nach dem Signieren nicht mehr verändert wurden. Dokumente, Programme usw. können signiert werden.
Social Engineering	Bei Cyber-Angriffen durch Social Engineering versuchen Kriminelle ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren.
Software	Sammelbegriff für Betriebssysteme, Anwendungs- und Dienstprogramme.
Spam	Unter Spam versteht man unerwünschte Nachrichten, die massenhaft und ungezielt per E-Mail oder über andere Kommunikationsdienste versendet werden.
Streaming	Streaming (englisch „strömen“) bezeichnet das Abspielen von Video- und Audioinformationen, ohne sie dauerhaft auf dem Gerät zu speichern. Das Streaming wird durch eine spezielle Software (Plug-ins oder Wiedergabeprogramme) ermöglicht, die in der Regel kostenlos angeboten werden. Durch Streaming gelangen Videobilder und -töne live auf den Bildschirm des Computers.

BEGRIFF	ERKLÄRUNG
Suchmaschine	Eine Suchmaschine ermöglicht die Recherche von Inhalten, die im Internet oder in einem Computer gespeichert sind.
TAN	Siehe PIN-/TAN-Verfahren.
Update	Neue Version bzw. Ergänzung einer Software, die Programmmängel korrigiert oder Programmverbesserungen enthält. Updates werden in der Regel in elektronischer Form zum Herunterladen aus dem Internet zur Verfügung gestellt.
URL	Eine URL gibt eine Adresse im Internet an. Sie besteht aus dem Protokoll (z. B. http://), dem Rechnernamen (z. B. www.bund.de) und ggf. auch aus der Angabe des Ports (z. B. :80) und der Pfadangabe (z. B. /startseite.html).
USB-Stick	Mobiles Speichermedium, das an den USB-Port angeschlossen wird.
Virenschutzprogramm	Ein Virenschutzprogramm überprüft neue Dateien (zum Beispiel Anhänge von E-Mails) und den gesamten Computer auf Schadsoftware. Dazu vergleicht es in erster Linie die Daten auf dem Rechner mit den „Fingerabdrücken“ bekannter Schadprogramme.
VPN	VPN steht für Virtual Private Network. Es verschlüsselt die Datenkommunikation zwischen zwei Endpunkten – zum Beispiel zwischen einem Endgerät und einem VPN-Server. Auf diese Weise kann die Kommunikation nicht ohne weiteres mitgelesen oder verändert werden.
Webbrowser	Siehe Browser.
WLAN (Wireless Local Area Network)	WLAN steht für Wireless Local Area Network und bezeichnet drahtlose Funknetzwerke, die kabelfreie Kommunikation zwischen mehreren lokalen Computern ermöglichen. Es wird häufig genutzt, um unterwegs mit dem Computer oder Smartphone ins Internet zu gehen.

BEGRIFF	ERKLÄRUNG
Zwei-Faktor-Authentisierung	Die Zwei-Faktor-Authentisierung bezeichnet die Kombination von zwei Faktoren aus den drei Bereichen Wissen (zum Beispiel Passwort), Besitz (zum Beispiel Chipkarte) und Biometrie (zum Beispiel Fingerabdruck).