Die Helfer Wiens

SELBST SCHUTZ

ZIVILSCHUTZ

www.diehelferwiens.at

INTERNET-RATGEBER

Wissen was zu tun ist

Impressum

Herausgeber, Verleger, Redaktion und Gestaltung:
Österreichischer Zivilschutzverband, Am Hof 4, 1010 Wien

Vorbereitet sein, sollte etwas passieren – vorbeugen, damit erst gar nichts passiert – unter diesem Motto bietet der Österreichische Zivilschutzverband eine Fülle von Informationen, Aktionen und Veranstaltungen. Zum persönlichen Nachlesen, aber auch durch zahlreiche Vorträge der Zivilschutzverbände vor Ort in den Bundesländern und Bezirken. Im Zentrum steht dabei der Selbstschutz. Im Fall der Fälle stehen natürlich Behörden und Einsatzorganisationen den Bürgerinnen und Bürgern zur Seite, Eigenverantwortung und das richtige persönliche Handeln bewirken aber eine Entlastung der Einsatzkräfte und Vorteile für Betroffene.

Mag. Wolfgang Sobotka, *Bundesminister für Inneres*

Der Österreichische Zivilschutzverband informiert die Bürgerinnen und Bürger seit 1961 über alle möglichen Bedrohungsszenarien. Auch wenn wir uns heute im Herzen Europas wesentlich sicherer fühlen als früher, so gibt es dennoch zahlreiche Bedrohungsszenarien, die Vorbereitungs- und Vorbeugemaßnahmen durch Behörden, Einsatzorganisationen und allen voran auch der Zivilbevölkerung erfordern. Dabei steht der Österreichische Zivilschutzverband allen Bürgerinnen und Bürgern zur Seite. In enger Zusammenarbeit mit allen sicherheitsrelevanten Organisationen und über Landes- und Bundesgrenzen hinaus.

NR Johann Rädler, *Präsident des Österreichischen Zivilschutzverbandes*

Wien ist eine der sichersten Städte der Welt und für viele Eventualitäten sehr gut vorbereitet. Im Ernstfall sind alle Behörden und Einsatzorganisationen rund um die Uhr rasch und kompetent zur Stelle. Darauf können sich die Wienerinnen und Wiener verlassen.
Sicherheit basiert in Wien aber nicht nur auf einem perfekt funktionierenden Einsatzwesen, sondern umfasst auch Bereiche wie Wohnen, Gesundheit, Umwelt und Soziales. Mit dem „K-Kreis“, dem Zusammenschluss der freiwilligen und beruflichen Wiener Hilfs- und Einsatzorganisationen, ist für jedes Anliegen rasch die richtige Stelle gefunden. Trotzdem soll jede und jeder Einzelne zur Sicherheit seiner Familie und seines alltäglichen Umfeldes beitragen. Vorbereitung auf mögliche Notfälle ist grundvernünftig. „Die Helfer Wiens“ (vormals Wiener Zivilschutzverband) sind gerne behilflich und beraten in persönlichen Gesprächen und kostenlosen Vorträgen in all diesen Bereichen. www.diehelferwiens.at

Mag.ª Renate Brauner, *Stadträtin für Finanzen, Wirtschaft und Internationales, Präsidentin „Die Helfer Wiens“*

„Vorbereitet sein – helfen können“, das ist die Mission des Teams der Helfer Wiens. So unterschiedlich die Regionen und Landschaften in Österreich sind, so unterschiedlich können auch mögliche Gefahrensituationen sein. Deshalb haben „Die Helfer Wiens“ maßgeschneiderte Schwerpunkte, Aktionen und Informationen passgenau für Wien ausgearbeitet. Die Expertinnen und Experten des K-Kreises sind in enger Zusammenarbeit mit den maßgeblichen Einrichtungen des Landes als kompetenter Partner in allen Sicherheitsfragen unterwegs. Gemeinsam wollen wir Bildungseinrichtungen, Unternehmen, vor allem aber die Privathaushalte und damit letztendlich die Gesellschaft, sicherer machen - sicherer mit Wissen, welches im Idealfall dafür sorgt, dass erst gar nichts passiert.

Für Sie da, das Team der Helfer Wiens. www.diehelferwiens.at

FÜR ALLE FÄLLE:

DER ZIVILSCHUTZ-WEBSHOP

Jeder Haushalt in Österreich sollte zumindest eine Woche ohne Einkaufen und Strom auskommen. Was dafür benötigt wird – darüber informiert der Zivilschutzverband. Vieles davon bekommt man ums Eck, bei allen anderen Produkten hilft Ihnen der Zivilschutz-Webshop.

www.selbst-sicher.com

ZIVILSCHUTZ Österreich

Denk daran: Schaff Vorrat an!

INTERNET UND INTERNETSICHERHEIT: EINE GESCHICHTE

Die Zeit nach dem zweiten Weltkrieg wird heute als Kalter Krieg bezeichnet, der erst 1989 mit dem Fall des Eisernen Vorhangs und in weiterer Folge dem Zusammenbruch der UdSSR 1991 endete. Im Kalten Krieg trafen die beiden Machtblöcke, im Westen die Nato unter der Führung der USA und im Osten der Warschauer Pakt unter der Führung der UdSSR nicht direkt aufeinander. Lediglich bei sogenannten Stellvertreterkriegen, wie dem Vietnamkrieg von 1965 bis 1975, wurden jeweils rivalisierende Parteien unterstützt. Vielmehr waren die Auseinandersetzungen vom Wettrüsten und technologischer Weiterentwicklung geprägt.

Die USA verfügten als erste über die Atombombe, die UdSSR schoss 1957 mit Sputnik den ersten Satelliten ins Weltall und stellte somit ihre Fähigkeit zum Einsatz von Interkontinentalraketen unter Beweis. Als Reaktion auf den Vorsprung der UdSSR stellte die USA ihre vornehmlich unter militärischer Führung stehende Forschungs- und Entwicklungsarbeit vollkommen neu auf. Ein Ergebnis war die Gründung der ARPA (Advanced Research Project Agency) im Jahr 1958 (Heute: DARPA, Defense Advanced Research Projects Agency).

1969 startete der erste Vorläufer des heutigen Internets und vernetzte zu Beginn vier Forschungseinrichtungen.

Diese Agency verfügt nicht mehr über eigene Forschungseinrichtungen, sondern finanziert und koordiniert sowohl militärische als auch universitäre und private Forschungsprojekte. Zudem wurde das Einsatzgebiet der Forschungsergebnisse nicht mehr ausschließlich auf militärische Anwendungsgebiete beschränkt, auch kommerzielle Anwendungsgebiete wurden einbezogen.

Die Ergebnisse bestimmen bis heute die weltweite technologische Weiterentwicklung, rund ein Drittel aller Schlüsseltechnologien eines modernen Smartphones gehen auf DARPA-Förderungen zurück,

Im Kinofilm War Games – Kriegsspiele von 1983 spielt Matthew Broderick David Lightman, der sich Zugang zum nuklearen Verteidigungssystem der USA verschafft hatte.

Die Universität Wien erhielt 1990 den ersten Internetanschluss Österreichs

darunter auch das Internet. Der 1969 installierte Vorläufer des Internets hieß ARPANET (Advanced Research Projects Agency Network) und vernetzte zu Beginn vier Forschungseinrichtungen mittels Telefonleitungen. Erst mit der Abschaltung des ARPANET und der Freigabe zur kommerziellen Nutzung des Internets 1990 sollte die Vernetzung ihren Siegeszug antreten können. Im selben Jahr erhielt auch Österreich den ersten Internetanschluss, um die Universität Wien mit dem Forschungszentrum CERN in der Schweiz zu verbinden.

10 Jahre nach der Inbetriebnahme im Jahr 1979 verschaffte sich Kevin Mitnick erstmals unautorisierten Zugriff. Es war die Zeit der Computerpioniere, Paul Allen und Bill Gates gründeten 1975 Microsoft, Steve Wozniak und Steve Jobs 1976 Apple und erst weniger als 200 Einrichtungen waren Teil des Netzwerks. Die Einbrüche Mitnicks in gesicherte Netzwerke sowie seine Verhaftung und Bewährungsauflagen, u.a. durfte er drei Jahre keine EDV-Systeme benutzen, boten die Vorlage für zahlreiche Filmproduktionen bis heute. So wird das Thema erstmals im Film „War Games – Kriegsspiele“ im Jahr 1983 aufgegriffen, ein Teenager hatte unbeabsichtigt das Nukleare Verteidigungssystem gehackt aber es für ein Computerspiel gehalten. Auch Mitnick wurde bei seinem Prozess Jahre danach unterstellt, er könne mit Hilfe seiner Fähigkeiten einen Nuklearkrieg auslösen.

1979 verschaffte sich Kevin Mitnick erstmals unautorisierten Zugriff in ein Computernetzwerk.

Gesetze gegen Internetkriminalität gab es erst zu Beginn der 80er Jahre. Bei der Schaffung des „Internets“ war die Frage nach Vertrauen und Sicherheit kein Thema, da sich alle Akteure quasi persönlich kannten. Den ersten konkreten Schaden lösten nämlich erst im Jahr 1982 sechs Teenager aus, indem sie Rechnungen löschten. Obwohl der Gesamtschaden mit rund 1.500 $ relativ gering ausfiel, gaben die Aktivitäten der Gruppe, die sich „The 414s“, nannte den Ausschlag für eine immer ausführlichere Gesetzgebung. Ende der 80er Jahre waren bereits rund 60.000 Rechner miteinander verbunden. 1988 legte ein Computer-Wurm, ein Vorläufiger des heutigen Computer-Virus, 10 Prozent des damaligen Netzwerks lahm. Der Programmierer und Harvard-Student Robert Morris hatte mit seinem nach ihm benannten Morris-Wurm unbeabsichtigt einen Schaden von bis zu 10 Mio. $ ausgelöst. Eigentlich hätte das Programm nur die Größe des damaligen Internets feststellen sollen, indem es sich selbstständig weiterverbreitete, stattdessen brachte es innerhalb weniger Stunden rund 6.000 Rechner zum Absturz.

Bis heute bleibt die Sicherheit ein bestimmendes Thema, wenn es um die Digitalisierung geht. So ist das Datenvolumen des sogenannten Darknets und des Deep Webs heute rund 500 Mal größer als das Volumen des klassischen Internets. Deep Web bezeichnet jenen Teil des Internets, der über normale Suchmaschinen nicht

auffindbar ist. Der Name Darknet geht auf einen Artikel von vier Microsoft Mitarbeitern zurück, die 2002 direkte „Freund zu Freund“-Netzwerke (Peer-to-Peer) als wesentliches Hindernis für ein Funktionieren digitaler Rechteverwaltung bezeichneten. Bekanntestes Beispiel dafür war die Plattform Napster, die von 1999 bis zum Beginn der 2000er Jahre 80 Mio. Nutzer zählte und vornehmlich zum Tausch von Musiktiteln diente. Nutzer tauschten Musiktitel, anstatt sie zu kaufen, was zu Klagen der Rechteinhaber, allen voran der Plattenfirmen, führte.

Mit der zunehmenden Verbreitung des Internets – heute nutzt es rund drei Viertel aller Österreicher regelmäßig, nahmen auch die Angriffe auf bzw. Schäden für Privatpersonen zu. Seit Mitte der 90er Jahre gingen die ersten Sozialen Netzwerke (Social Networks) online, vornehmlich als Plattform für kleine überschaubare Gruppen, Klassen- oder Schulgemeinschaften. Auch das bekannteste Soziale Netzwerk Facebook, mit fast 4 Mio. heimischen Nutzern, startete 2004 als gemeinsame Plattform für Harvard-Studenten. Bei Sozialen Netzwerken werden Daten nicht mehr auf privaten Rechnern gespeichert, sondern auf Servern. Selbiges gilt für sogenannte Clouddienste. Werden solche Server angegriffen und Daten gestohlen, sind somit eine Vielzahl von Nutzern betroffen. Der größte derartige Schadensfall trat 2014 ein, als die Mailadressen, Telefonnummern und Geburtstage samt Passwörtern von 500 Mio. Menschen der Internetfirma Yahoo gehackt wurden. Aber auch Angriffe auf private Rechner können immense, vor allem auch psychologische Schäden, anrichten. Ein gehackter Webcam-Zugriff wird für wenige Dollar im Internet bzw. Darknet gehandelt. In den Jahren 2012 und 2014 sorgte vor allem die Veröffentlichung von Nacktfotos von prominenten SchauspielerInnen für öffentliche Aufmerksamkeit, die Opfer von Hackern wurden.

Bereits 1988 legte ein Computer-Wurm, ein Vorläufiger des heutigen Computer-Virus, 10 Prozent des damaligen Netzwerks lahm.

Internetpioniere deren Startups zu den wertvollsten Unternehmen der Welt wurden: Ende 1970er Jahre gründet Bill Gates Microsoft und Steve Jobs Apple, 2004 gründet Mark Zuckerberg Facebook.

JEDER ZEHNTE GEHT MIT SEINER UHR INS INTERNET

Klar ist, dass das Internet aus unserem Leben nicht mehr wegzudenken ist. Es hat unsere Gesellschaft in den letzten Jahrzehnten grundlegend verändert, wie die Dampfmaschine im 19. Jahrhundert, das Automobil im 20. Jahrhundert oder parallel zum Internet das Mobiltelefon – kein Wunder, dass Mobiltelefon und Internet miteinander verschmolzen sind.

Wie schnell das Internet unsere Gesellschaft verändert, zeigt sich an einem berühmten Zitat, 2014 vom finnischen Regierungschef Alexander Stubb getätigt: „Das iPhone hat Nokia gekillt und das iPad unsere Papierindustrie". Stubb gab den Innovationen des heute wertvollsten Unternehmens der Welt die Schuld an der schlechter werdenden wirtschaftlichen Lage seines Landes. Was Stubb nicht dazu sagte: Nokia hatte den Mobilfunk- und Smartphone-Boom selbst ausgelöst, als es gegen Ende der 80er Jahre begann die ersten wirklich tragbaren Mobiltelefone herzustellen. Auch die ersten Vorläufer heutiger Tablets stammen von Nokia, man hatte lediglich 2007 mit der Präsentation des ersten iPhones von Apple den technologischen Vorsprung und 2011 die Marktführerschaft verloren.

Der Niedergang des ehemaligen Weltmarktführers Nokia ist bis heute maßgeblich für das Verhalten der gesamten Internet- und Technologiebranche. Kein großes Unternehmen auf diesem Sektor, weder Google, Microsoft oder Samsung können und wollen einen technologischen Vorsprung bei ihren Konkurrenten dauerhaft zulassen – entsprechend schnell werden Innovationen und neue Produkte präsentiert bzw. kopiert und entsprechend schnell ändert sich dadurch die Art und Weise, wie wir das Internet nutzen. Daten werden immer schneller weitergeleitet und auch immer umfangreicher gesammelt. Heute nutzen drei von vier Österreichern regelmäßig das Internet. Und: Heute nutzen mehr Menschen mobiles Internet mittels Smartphones oder Tablets als auf klassischen PCs (Personal Computer). Jeder dritte Internetnutzer greift mittlerweile mit seinem Fernseher auf das World Wide Web zu und besitzt damit einen Smart-TV, jeder zehnte mit seiner Uhr und besitzt damit eine Smart-Watch. Und in Zukunft sollen immer mehr Gegenstände des täglichen Lebens „smart", also mit dem Internet verbunden, werden. So wie alle Innovationen und tiefgreifenden Änderungen unseres Zusammenlebens, sind auch durch das Internet immer präzisere Regeln und Verhaltensregeln notwendig. Bereits Mitte der 1880er Jahre prägten Automobile das Stadtbild, erste Gesetze zur Straßenverkehrsordnung wurden erst zu Beginn des 20. Jahrhunderts erlassen und werden bis heute laufend angepasst. Auch das Internet birgt, wie das Automobil, nicht nur Vorteile, sondern auch Gefahren und die rechtlichen Rahmenbedingungen werden mehr und mehr geregelt und Regelverstöße werden zunehmend geahndet.

Heute nutzen mehr Menschen mobiles Internet mittels Smartphones oder Tablets als auf klassischen PCs

Moderne Schadsoftware schleicht sich getarnt in Systeme ein

WAS SCHADSOFTWARE ANRICHTEN KANN

Ransomware, also Schadprogramme, die Daten blockieren oder verschlüsseln und für die Herausgabe des Schlüssels Lösegeld verlangen, meist in Form von BITCOINs, werden zunehmend festgestellt. Allein von 2015 auf 2016 verzehnfachten sich entsprechende Fälle in Österreich.

1989 wurde der erste Vorläufer, ein Trojaner genannt „AIDS“ entwickelt und sollte augenscheinlich infizierte Computer lediglich auf die Gefahren der Erkrankung AIDS aufmerksam machen. Erst nach ca. 90 Neustarts wurden die Daten verschlüsselt und Lösegeld gefordert. Seit 2015 wurde für alle Betriebssysteme, auch für Smartphones, Ransomware ausfindig gemacht.

Zur Prävention wird eine Reihe von Maßnahmen empfohlen. **Die neusten Patches für das Betriebssystem und für den Virenschutz sollten immer eingespielt werden,** Daten sollten regelmäßig extern gesichert werden und besonders mit Admin Accounts, also mit Profilen, die auf Computern oder in Computersystemen erweiterte Rechte haben, sollte besonders vorsichtig umgegangen werden.

Generell wird zu einem bewussten Umgang mit Inhalten im Internet geraten. Im Jahr 2011 zählte zum Beispiel die mittlerweile auch in Österreich gesperrte Internetseite Kino.to zu den 50 meistbesuchten Webseiten im deutschsprachigen Raum. Raubkopien oder illegale Aufnahmen von Kinofilmen konnten dort auf den ersten Blick unentgeltlich konsumiert werden. Finanziert wurde diese Webseite über massive Werbung, die nicht zuletzt zu Schadsoftware und pornografischen Inhalten oder in Abo-Fallen führte.

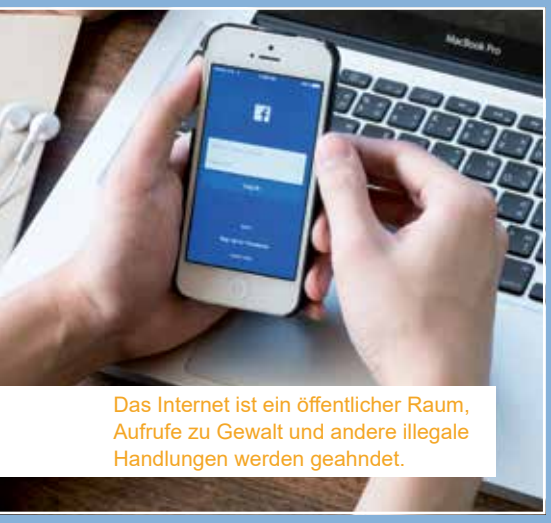
Zu Schadsoftware zählen u.a. Viren und Würmer, die Daten zerstören, Speicherplatz verbrauchen oder die Leistung drosseln. Trojaner, die getarnt als nützliche Software – wie das sprichwörtliche Trojanische Pferd – in Wahrheit Schaden anrichten. Backdoor-Software wiederum verschafft einem Angreifer verdeckt Zugang auf ein Computersystem und somit auf Daten oder Funktionen, wie die Webcam. Ähnliches gilt für Spyware, Programme, die ungefragt Daten sammeln, wie Surf- und Suchverhalten (tracking), und an Dritte weiterverkaufen.

Gerade die (Aus)Nutzung von Daten wird heute und wohl auch in Zukunft ausgiebig diskutiert werden. Zumal Daten von verschiedensten Firmen nicht nur gesammelt, sondern auch verkauft und oftmals sogar gestohlen werden. **2015 wurde die zweitgrößte Krankenversicherung der USA Opfer einer Cyberattacke, die Krankenakten von 80 Millionen Kunden wurden gestohlen.** 2013 wurde einer der größten Einzelhändler der USA gehackt, dabei wurden 40 Millionen Kreditkartennummern gestohlen.

MEHR SENSIBILITÄT IM INTERNET: HASS-POSTINGS, SHITSTORMS UND IN-GAME-KÄUFE

Im Februar 2015 titelt die renommierte „New York Times“: How One Stupid Tweet Blew Up Justine Sacco's Life (Wie ein blöder Eintrag auf Twitter das Leben von Justine Sacco zerstörte). Fast zwei Jahre nach dem eigentlichen Vorfall wurde die Geschichte der PR-Frau Justin Sacco zu einem Synonym für einen falschen Umgang in und mit Sozialen Netzwerken – und ist es bis heute.

Was war geschehen: Justine Sacco war PR-Beraterin des Internet- und Medienunternehmens IAC. Die damals 30-jährige hatte den ganzen Tag über mehr oder weniger witzige Kurznachrichten auf Twitter veröffentlicht und auch ein wenig getrunken. Kurz vor ihrem Abflug nach Afrika twittert sie folgenschwer: „Fliege nach Afrika. Hoffentlich bekomme ich kein Aids. Mache nur Spaß. Bin weiß.“ Erst nach dem mehrstündigen Flug schaltete sie ihr Smartphone wieder ein und erlitt den Schock ihres Lebens. Ihre Nachricht wurde millionenfach geteilt, zu einem weltweiten Twitter-Trend und löste einen gewaltigen Shitstorm (lawinenartige Verbreitung negativer Meldungen im Internet, vornehmlich auf Sozialen Netzwerken) aus. Trotz Entschuldigungen und Klarstellungen verlor Sacco ihren Job, ihren Partner und einen Großteil ihrer Freunde. „Ich kann mich mit niemanden verabreden. Heutzutage googelt man doch die Leute, mit denen man sich trifft“, schreibt Sacco in einem später veröffentlichten Buch. Sie sei keine Rassistin und habe einfach einen ganz schlechten Scherz machen wollen, wie sie später ebenfalls sagt.



Das Internet ist ein öffentlicher Raum, Aufrufe zu Gewalt und andere illegale Handlungen werden geahndet.

Die Geschichte der PR-Frau Justine Sacco wurde zu einem Synonym für einen falschen Umgang in und mit Sozialen Netzwerken.

Die Geschichte der Justine Sacco sollte sich bis heute mehrfach wiederholen. Immer wieder werden Hasspostings und Shitstorms thematisiert. Ein bekanntes Beispiel aus Österreich ist jenes eines Lehrlings, der auf Facebook den Einsatz von Flammenwerfern gegen ein junges Flüchtlingsmädchen forderte. Das Foto, zu dem der junge Mann gepostet hatte, zeigt ein Flüchtlingsmädchen wie es ein Wasserbad nahm und wurde im Zuge einer Sommeraktion einer freiwilligen Feuerwehr aufgenommen. Auch der Lehrling entschuldigte sich, verlor aber dennoch seinen Job. Das Internet ist ein öffentlicher Raum, Aufrufe zu Gewalt und andere illegale Handlungen werden geahndet. Aber auch abseits von Diskriminierung, Wiederbetätigung oder anderen strafbaren Handlungen geht es im Internet und Sozialen Netzwerken um richtiges Verhalten. Der Europäische Gerichtshof für Menschenrechte hat 2016 die Entlassung eines Ingenieurs gebilligt, der während seiner Dienstzeit Facebook nutzte. Aber nicht nur die Entlassung, auch die Tatsache, dass der Arbeitgeber die Internetaktivitäten überwache, sei zulässig.

Aber auch Leichtsinn und Leichtgläubigkeit spielen eine Rolle. Rund 9 von 10 E-Mails sind Spam-Mails (unerwünschte Nachrichten, die unverlangt zugestellt werden) und zielen oftmals auf Betrug

Für das beliebte und eigentlich gratis vertriebene Smartphone-Spiel „Pokémon Go“ gab im Herbst 2016 jeder fünfte Nutzer Geld aus, um sich im Spiel Vorteile zu sichern

oder die Verbreitung von Schadsoftware ab. Nichts desto trotz werden ein Drittel bis die Hälfte aller Spam-Mails geöffnet. Zudem kommen Internettrends, die oftmals offensichtlich dumm und gefährlich sind und dennoch bereitwillig mitgemacht werden. So folgte 2014 auf die eher harmlose „Ice Bucket Challenge“, bei der man sich für einen guten Zweck Eiswasser über den Kopf leert, immer extremere Videos, bis ein 15-jähriger die „Fire Challenge“ startete. Dabei leerte er sich Alkohol über den Oberkörper, um sich danach anzuzünden. Der junge „Initiator“ überlebte schwer verletzt, ein „Imitator“ kam dabei zu Tode. Seit vielen Jahren weit verbreitet ist das sogenannte Sexting, bei dem sich gegenseitig anstößige Nachrichten und auch Nacktfotos geschickt werden, die später aber zum Leid vieler Betroffener veröffentlicht werden und zu Mobbing führen. 2015 gaben bei einer Studie rund ein Drittel aller österreichischen Jugendlichen an, mit diesem „Trend“ bereits in Berührung gekommen zu sein, jeder Sechste gab an solche Fotos von sich gemacht bzw. verschickt zu haben.

Ebenfalls viel zu leichtfertig wird mit Apps, also Programmen für Smartphones, und mit Browser-Addons, Erweiterungen für Internetbrowser, umgegangen. Zum einen bekommen Apps und Addons oftmals unnötige Berechtigungen, sie haben Zugriff auf Kontakt- oder Standortdaten, Fotos, Videos und den gesamten Benutzer-Account. Auch das bekannteste und beliebteste Smartphone-Spiel des Jahres 2016 „Pokémon Go“, das zu Spitzenzeiten rund 50 Mio. Spieler gleichzeitig verzeichnete, hatte durch einen Softwarefehler kurzzeitig Zugriff auf die gesamten Account-Daten. Der Fehler wurde erst später korrigiert. Bei Browser-Addons sind mehrere Fälle bekannt, bei denen die Herstellerfirma den Besitzer wechselte und plötzlich ungefragt aufdringliche Werbung einspielen oder noch viel tiefgreifender: Passwörter oder anderer sensible Daten zum Hersteller übermittelt („nach Hause telefoniert“). In-App oder In-Game-Käufe zählen neben Roaminggebühren, die beim Telefonieren bzw. beim Internetsurfen im Ausland anfallen, zu den größten und gängigsten Kostenfallen im Internet bzw. bei der Smartphone-Nutzung. Dabei werden Spiele oder Programme oftmals gratis angeboten, gewisse Funktionen sind allerdings nur gegen zusätzliche Kosten zu benutzen. Für das oben genannte eigentlich gratis vertriebene Smartphone-Spiel „Pokémon Go“ gab im Herbst 2016 jeder fünfte Nutzer Geld aus, um sich im Spiel Vorteile zu sichern – was (vermutlich) dem Geschäftsmodell entspricht. Davon wiederum jeder Zehnte mehr als 100 Euro. Gerade Kinder halten In-App oder In-Game-Käufe oftmals für normale Programm- bzw. Spielfunktionen und geben dadurch unbeabsichtigt wesentlich höhere Beträge aus. In den letzten Jahren wurden die Bestimmungen verschärft, Hinweise hinzugefügt, Passwort oder Fingerabdruckeingaben werden bei Käufen verlangt.

Vor allem bei Jugendlichen weit verbreitet: Sexting, dabei werden sich gegenseitig anstößige Nachrichten und auch Nacktfotos geschickt.


Gerade Kinder halten In-App oder In-Game-Käufe oftmals für normale Programm- bzw. Spielfunktionen und geben dadurch unbeabsichtigt Geld aus.

WIE INTERNETKRIMINELLE IN ÖSTERREICH ZUSCHLAGEN

Die Sicherheitseinrichtungen Österreichs, allen voran das Innen- und Verteidigungsministerium, führen regelmäßig Risiko- und Gefahrenanalysen durch. Ganz oben, wenn es um Bedrohungspotenziale geht, steht die Internetkriminalität, auch Cybercrime genannt. 10.000 Anzeigen, darunter Hacker-Angriffe auf zentrale Infrastruktur, wie Telekommunikation und den Flugverkehr, wurden verzeichnet.

Die Täter sitzen im Ausland genauso wie im Inland, sind Einzeltäter, aber auch in Netzwerken wie dem bekannten Anonymus-Kollektiv organisiert, sogar in staatlichen Geheimdiensten. Auch Terroristen nützen Soziale Medien oder kommunizieren über Chatfunktionen von harmlosen Computerspielen. Trotz dieser Vielfalt lag die Aufklärungsquote 2015 bei 40 Prozent. **Der Schaden ist jedenfalls enorm und wird von Experten für Österreich auf rund 1 Mrd. Euro pro Jahr geschätzt.** Internetkriminelle greifen in der USA in den Wahlkampf ein, indem sie geheime Dokumente stehlen und veröffentlichen, aber genauso sind auch heimische Betriebe und Privatpersonen betroffen.

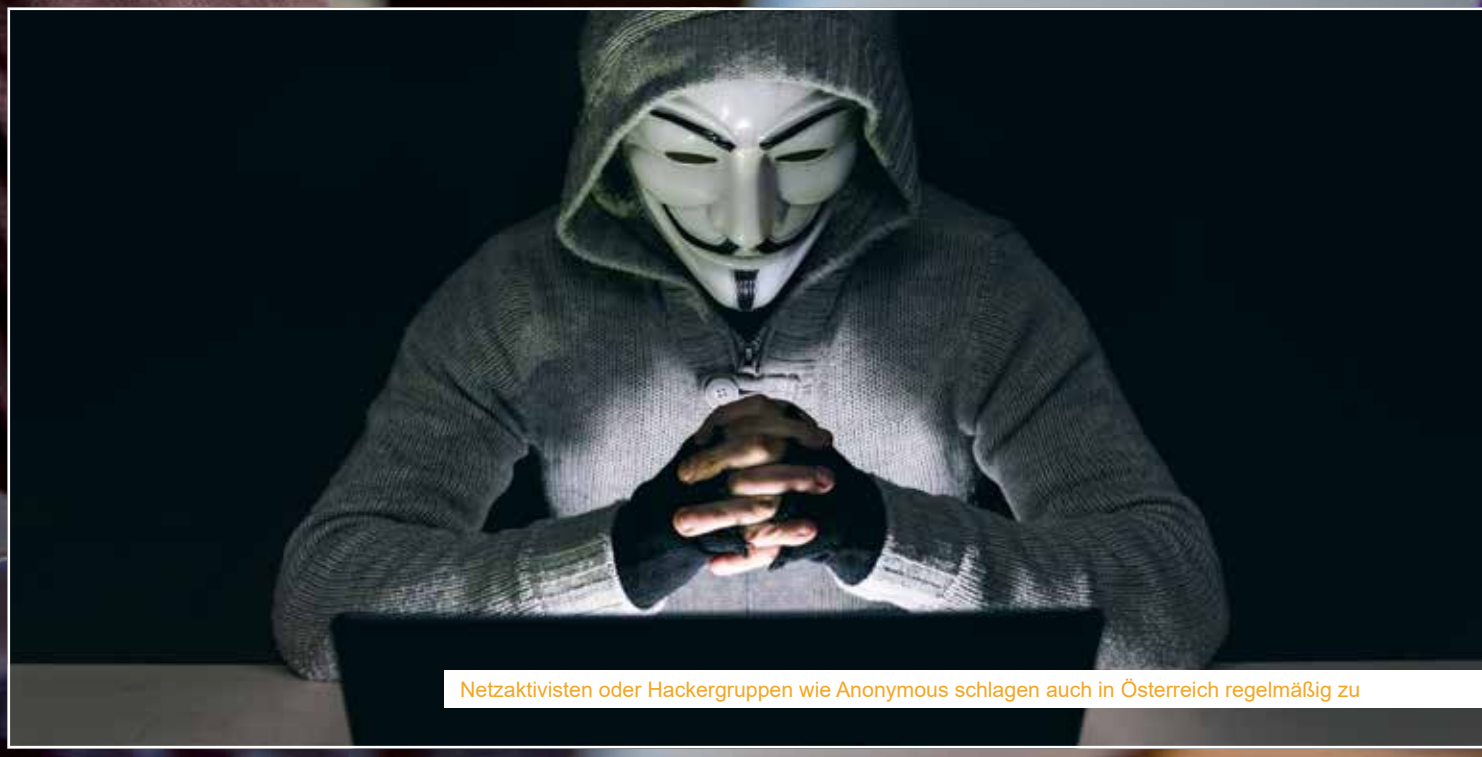
Zwei von drei Österreichern haben bereits negative Erfahrungen mit Schadsoftware, wie Viren oder Spams gemacht, einer von drei wurde Opfer von Internetbetrug. Häufig werden Waren im Internet nur gegen Vorauszahlung geliefert, das Produkt kommt aber nie an. Angeblich liebesbereite Internetbekanntschaften bitten um Geld für das Flugticket und kommen nie an. In plötzlich aufpoppenden Browserfenstern kommen die Nutzer der Aufforderung Kreditkartennummern oder Kontaktdaten einzugeben viel zu oft nach und werden somit zu sogenannten Phishing-Opfern. Abmahnschreiben werden mittels Spam-Mails oder auch per Post verschickt, für Produkte, die man nie gekauft hat. 2013 wurde ein besonders pikanter Fall in Deutschland publik. Bis zu 30.000 Internetnutzer bekamen ein anwaltliches Schreiben wegen illegalen Streamings bzw. Downloads von

Pornofilmen. Die Betroffenen dürften wirklich die Seite besucht haben, die Abmahnungen kamen tatsächlich von einem Anwalt - nur war lange Zeit unklar, ob die Abmahnungen rechtens waren oder nicht. In der Folge kam es auch in Österreich zu ähnlichen Betrugsdelikten. Jedenfalls wird geraten nicht einzuzahlen, zumal die Rechtslage in Österreich solche großflächigen Abmahnungen verunmöglicht.

Obwohl die Anzeigen ansteigen und Medien-Berichte zunehmen, ist die Achtsamkeit heimischer Internetnutzer nicht besonders hoch, nur ein Drittel der Österreicher verfügt über Virenscanner oder Passwortschutz. **Ein Trend der Internetkriminalität in Österreich: Ransomware, auch Erpressungstrojaner oder Cryptolocker genannt.** Dabei verhindert eine Schadsoftware dem Besitzer eines Computers oder eines Computersystems die Benutzung. Erst gegen die Bezahlung von „Lösegeld“ wird den Opfern die Wiedererlangung der Kontrolle über ihre Systeme versprochen, was in den meisten Fällen trotz Bezahlung aber nicht geschieht. **Von Ransomware und damit verbundenen Lösegeldaufforderungen bzw. Erpressungen sind große und kleine Unternehmen aber auch Privatpersonen betroffen.** Ein Hotelier, dessen Buchungssystem lahmgelegt wurde oder eine Studentin, die gerade ihre Abschlussarbeit schreibt. In der Regel betragen die Forderungen zwischen 500 und 1.000 Euro und werden in der digitalen Währung BITCOIN verlangt. Bitcoin ist ein weltweit verwendbares Zahlungssystem, eine Währung, die keinem Land zugerechnet wird und dennoch in einem Wechselkurs gehandelt werden kann. Ende 2015 waren rund 15 Mio. Bitcoins im Umlauf mit einem Gesamtwert von rund 6 Mrd. $.

Ein weiterer Trend: DoS-Angriffe. DoS bedeutet Denial of Service, zu Deutsch Dienstblockade. Wird dies durch Überlastung des Systems durch unzählige gleichzeitige verteilte (distributed) Zugriffe versucht, wird von Distributed Denial of Service (DDoS) gesprochen. Dabei werden künstlich unzählige Anfragen an ein System, zum Beispiel eine Webseite, gestellt, wodurch dieses derart beschäftigt wird, dass reguläre Anfragen nicht mehr bearbeitet bzw. beantwortet werden können – vereinfacht gesagt: Es wird eine Überlastung herbeigeführt. **2016 wurden zum Beispiel die Webseiten des Flughafen Wien Schwechat oder der Österreichischen Nationalbank auf diese Weise angegriffen** und damit, wenn auch nur für kurze Zeit, deren Internetauftritt lahmgelegt.

Ein zukünftiger Trend: Das Internet der Dinge (Internet of Things) bietet durch die gigantische Steigerung von vernetzten Computern im Internet (geschätzte 50 Milliarden im Jahr 2020) ein erhebliches Potenzial für Cyberkrimininelle. Diese Computer agieren vom Besitzer selbständig (der Kühlschrank bestellt, das Auto sendet permanent an den Hersteller, die Versicherung oder der Herzschrittmacher an den Arzt oder Hersteller) und werden meist nur mit sehr schwachen Sicherheitsfunktionen ausgestattet. Welches Potenzial sich daraus lukrieren lässt, war vor kurzem anhand des Angriffs auf ein entsprechendes Netzwerk zu sehen, der massive Folgen u.a. für Netflix, Amazon und PayPal hatte.



Netzaktivisten oder Hackergruppen wie Anonymous schlagen auch in Österreich regelmäßig zu

Im Besonderen sollte man sich um die Internetsicherheit von Kindern kümmern.

SCHÜTZEN SIE SICH JETZT! UND BESONDERS IHRE KINDER!

Es ist kaum zu glauben, aber Selbstschutz im Internet ist wesentlich einfacher als man denkt. Zunächst einmal verfügen eine Vielzahl von Geräten, auch nicht elektronische wie zum Beispiel ein Fahrradschloss oder ein Tresor, über Passwörter, die von vorne herein eingestellt sind, in der Regel 1234 oder 1111 usw.

Jedes Produkt, das über eine Passwortfunktion verfügt, sollte man auch mit einem eigenen Passwort sichern. Ein sicheres Passwort besteht aus Zahlen, Buchstaben und Sonderzeichen. Es verwendet sowohl groß als auch klein geschriebene Buchstaben und hat mindestens 10 Zeichen, wobei gilt: Umso mehr Zeichen, umso besser. In regelmäßigen Abständen sollten Passwörter auch geändert werden. Zudem sollten die Passwörter für unterschiedliche Dienste und Produkte variieren, man sollte also nicht ein und das selbe Passwort für unterschiedliche Produkte nutzen. Einem gehackten Mail-Passwort kann in diesem Fall zum Beispiel auch der Facebook-Account zum Opfer fallen. Unglaublich aber wahr: **Im Jahr 2014 waren die beliebtesten Passwörter „123456“, „password“ und „12345“, im Jahr darauf „123456“, „password“ und „12345678“.** Immer wieder gern genommen werden Namen oder Geburtsdaten. Trotz ständiger Medienberichte über Hacker und Internetkriminalität bleiben die Internetnutzer unvorsichtig und leichtsinnig. Für Smartphones sollten zudem die Funktionen zum Finden und Löschen gestohlener oder verlorener Geräte aktiviert werden.

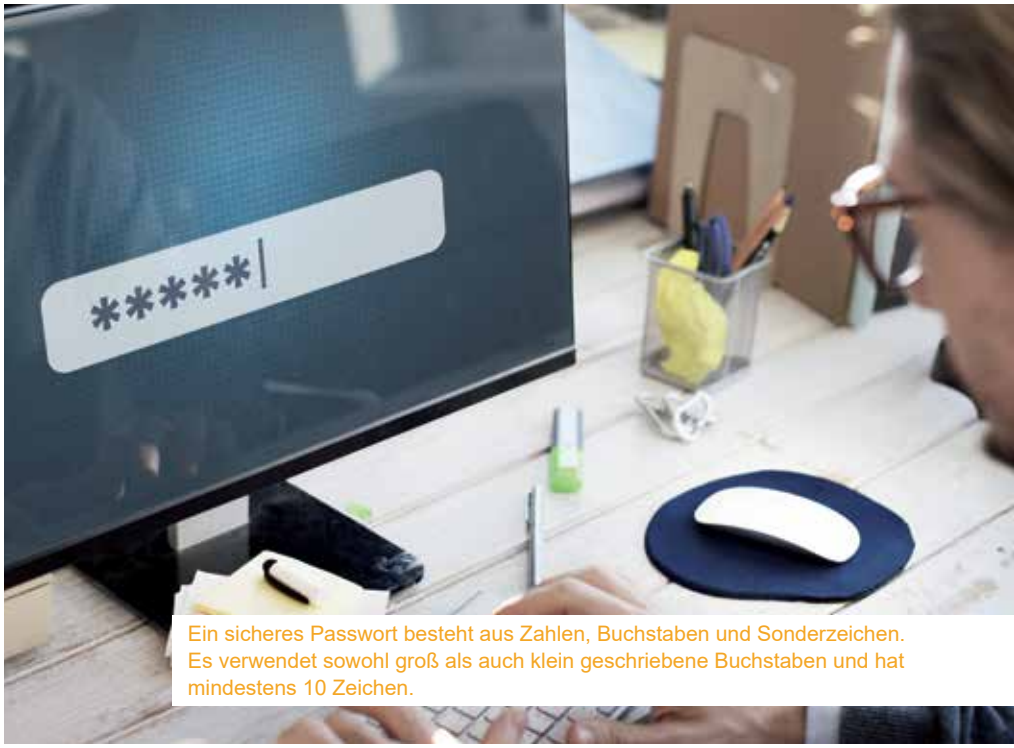
Eines der größten Risiken birgt das Öffnen von gefährlichen E-Mails, vor allem Anhänge oder weiterführender Links. In der Regel gilt: **Keine Anhänge oder Links von unbekannten Quellen öffnen und überprüfen Sie, ob eine verdächtige E-Mail überhaupt mit Ihnen in Verbindung stehen kann.** Denn selbst eine

Prüfung der Absender-E-Mailadresse birgt keine garantierte Sicherheit, diese kann sehr leicht gefälscht werden. Es gibt im Internet sogar Plattformen, mit denen E-Mails von beliebigen E-Mailadressen verschickt werden können. Einen relativen Schutz bieten Filter und Virenschutzprogramme, die oftmals gleich mehrere Schutzmöglichkeiten, zum Beispiel Firewall oder Linksscanner, anbieten. Nichts desto trotz sind mit dem Erwerb einer Sicherheitssoftware regelmäßige Updates verbunden, sie muss immer auf dem neuesten Stand gehalten werden, so wie das komplette Betriebssystem und der Internetbrowser.

Eigene Daten, vor allem jene mit sensiblen Inhalt, sollten zusätzlich verschlüsselt werden, vor allem, wenn sie in einer Cloud gespeichert werden. Unternehmen wird zudem empfohlen sensible Daten vor Exporten, als Kopien z.B. auf einem USB-Stick, zu schützen. USB-Sticks aus unseriösen oder unbekannten Quellen bergen noch ein zusätzliches Problem: Sie sind oftmals mit Schadsoftware infiziert. **USB-Sticks sind die zweithäufigste Verbreitungsform von Viren, Würmern und Co.** Indem z.B. infizierte Sticks gezielt verteilt werden.

Im Besonderen sollte man sich aber um die Internetsicherheit von Kindern kümmern. Filter gegen Inhalte wie Extremismus, Gewalt, Pornografie, Abo-Fallen oder illegale Downloads. Im deutschsprachigen Raum wird die Seite http://www.kinderserver-info.de/ empfohlen, dort werden Programme und Apps für alle Betriebssysteme angeboten, um kindergerechtes Internetsurfen sowie Computer- und Smartphone-Nutzung zu ermöglichen. Auch die Berechtigungen sollten auf allen Geräten so eingestellt werden, dass keine ungewünschten Installationen möglich sind. **Dabei kann auf manchen Geräten von vorne herein eine Kindersicherung aktiviert werden, um zum Beispiel App-Käufe oder In-App Käufe zu verhindern.** Solche Einstellungen finden sich auch auf TV-Geräten oder bei Onlineanbietern wie Netflix oder Amazon, damit können nicht nur die Inhalte an das Alter der Kinder angepasst werden, auch die Dauer für geregelte Fernsehzeiten lässt sich festlegen.

Gemeinsam mit den Kindern sollten auch regelmäßig die Privatsphären-Einstellungen auf Sozialen Netzwerken eingestellt bzw. geprüft werden, da häufig anbieterseitig Änderungen vorgenommen werden. Updates und neue Versionen setzen diese Einstellungen oft zurück. Der wohl wichtigste Punkt ist aber, dass Kinder alles, womit sie sich im Internet nicht wohl fühlen, jemandem erzählen. Optimalerweise den Eltern. Dazu ist es aber unabdingbar, dass sie wissen, dass sie keine Strafe zu erwarten haben.



Ein sicheres Passwort besteht aus Zahlen, Buchstaben und Sonderzeichen. Es verwendet sowohl groß als auch klein geschriebene Buchstaben und hat mindestens 10 Zeichen.

Cyber-Crime Meldestelle des Bundesministeriums für Inneres

Wenn Sie einen Verdacht auf Internetbetrug haben und über die weitere Vorgangsweise Informationen benötigen, wenden Sie sich bitte an

against-cybercrime@bmi.gv.at

www.diehelferwiens.at