Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC

eBanking aber sicher!
Lucerne University of Applied Sciences and Arts
HOCHSCHULE LUZERN
FH Zentralschweiz

iBarry

SKPPSC
Schweizerische Kriminalprävention
Prévention Suisse de la Criminalité
Prevenzione Svizzera della Criminalità

Ihre POLIZEI
Votre POLICE
La vostra POLIZIA
Kantonale und Städtische Polizeikorps
Corps de police cantonaux et municipaux
Corpi di polizia cantonali e comunali

Medienmitteilung 26. April 2021

Nationale Aktionswoche sensibilisiert für mehr Sicherheit im digitalen Raum

Meldungen zu Cybervorfällen haben in der Schweiz in den letzten Jahren deutlich zugenommen (Abb. 1). Die nationale Aktionswoche zum Thema «Sicherheit im digitalen Raum» vom 3. bis 7. Mai 2021 macht auf die Gefahren aufmerksam und zeigt auf, wie man sich schützen kann. Sie wird von namhaften Partnern der Behörden, der Wissenschaft und der Wirtschaft getragen.

Die Digitalisierung wurde durch Corona weltweit und somit auch in der Schweiz beschleunigt: Viele arbeiten von zu Hause aus, kaufen vermehrt online ein oder nutzen häufiger digitale Angebote. Das führt dazu, dass man öfter, oder auch bewusster, mit Cybervorfällen konfrontiert wird. Meldungen zu Cybervorfällen haben entsprechend sowohl bei der Polizei als auch bei der Meldestelle des Nationalen Zentrums für Cybersicherheit (NCSC) zugenommen und sich auf einem erhöhten Niveau stabilisiert. Vor allem die Phänomene Betrug und Phishing haben zugenommen (Abb. 2): Während Corona bietet sich das sogenannte Paketdienst-Phishing aufgrund der hohen E-Commerce-Aktivitäten besonders an. Im Bereich Betrug sind Fälle wie Spendenbetrug für Corona-Opfer oder falsche Gesichtsmasken-Bestellungen neu aufgetreten.

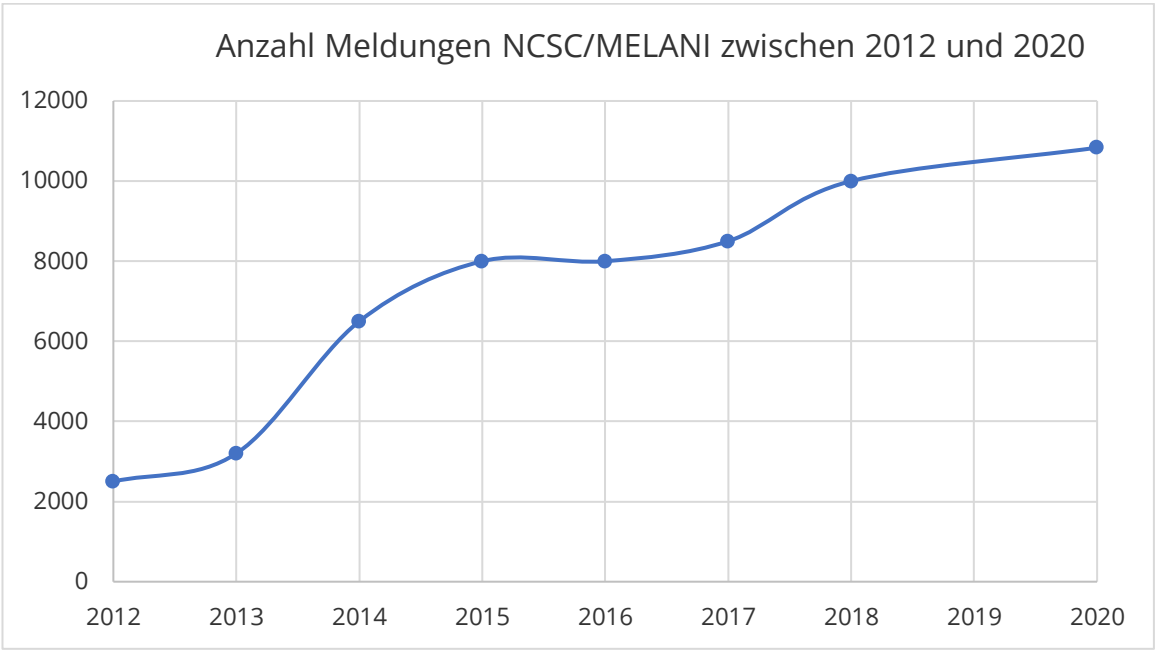

Abbildung 1: Zunahme Anzahl Meldungen Cyberangriffe beim NCSC, 2012-2020. Copyright: NCSC, 2021

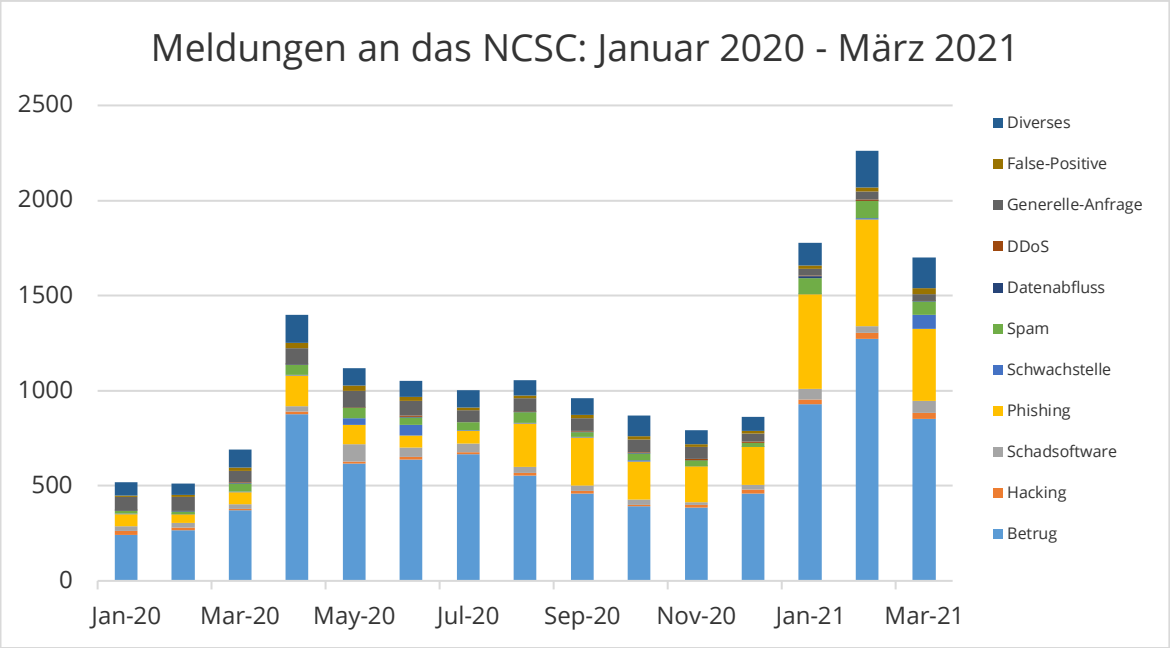

Abbildung 2: Anzahl Meldungen Cyberangriffe beim NCSC, 2020/2021. Copyright: NCSC, 2021

Nationale Aktionswoche mit namhaften Partnern

Die nationale Aktionswoche soll Aufmerksamkeit für das Thema schaffen. Gleichzeitig soll aufgezeigt werden, dass und wie Internetnutzerinnen und -nutzer mit einfachen Mitteln und geringem Aufwand viel zu ihrer individuellen Sicherheit beitragen können – etwa mit starken Passwörtern, regelmässigen Aktualisierungen der Software oder kritischem Verhalten im Cyberraum.

Die Aktionswoche wird von der Schweizerischen Kriminalprävention (SKP) in Kooperation mit dem Nationalen Zentrum für Cybersicherheit (NCSC), der Plattform «eBanking – aber sicher!» der Hochschule Luzern (HSLU), der Plattform für Internetsicherheit iBarry der Swiss Internet Security Alliance (SISA) sowie den kantonalen und städtischen Polizeicorps lanciert.

Sie dauert vom 3. bis zum 7. Mai 2021 und wird auf verschiedenen Kanälen on- und offline begleitet. In derselben Woche, am Donnerstag 6. Mai, ist auch der Welt-Passwort-Tag. Bekannte Persönlichkeiten aus Wirtschaft und Politik werden die Kampagne mit Testimonials unterstützen.

Im Zentrum der Kampagne steht die Webseite www.S-U-P-E-R.ch. Tipps und Tricks zu Datensicherung, Sicherheitsupdates, Virenschutz, Passwörtern und zum richtigen Verhalten im Web sind ebenso zu finden wie eine Übersicht über die Risiken im digitalen Raum, entsprechende präventive Massnahmen und Handlungsanweisungen. Ausserdem werden kostenlose Webinare zu verschiedenen Themen angeboten.

Fünf zentrale Themen zur Cybersicherheit – und ein Merkwort

Während der Aktionswoche wird täglich ein Thema im Zentrum stehen. Jedem Thema ist ein Buchstabe zugewiesen, der in Kombination mit den anderen das Wort S-U-P-E-R ergibt. Mit diesem Merkwort können Internetnutzerinnen und -nutzer schnell verinnerlichen, wie sie im Internet sicherer unterwegs sein können:

- **S wie Sichern** – Montag, 3. Mai 2021
  Sichern Sie Ihre Daten regelmässig auf mindestens einem zweiten Medium.

- **U wie Updaten** – Dienstag, 4. Mai 2021
  Aktualisieren Sie Ihr System, Ihre Programme und Apps regelmässig auf die neuste Version.
- **P wie Prüfen** – Mittwoch, 5. Mai 2021
  Prüfen Sie bei Ihrem Gerät, ob ein Virenschutzprogramm installiert ist und laufend aktualisiert wird.
- **E wie Einloggen** – Donnerstag, 6. Mai 2021
  Loggen Sie sich nur mit starken Passwörtern ein.
- **R wie Reduzieren** – Freitag, 7. Mai 2021
  Reduzieren Sie Betrugsrisiken im digitalen Raum mit einer gesunden Portion Misstrauen.

Prävention als wirksamstes Mittel

«Die Ermittlungen bei Cybercrime-Fällen sind schwierig und oft wenig ergiebig. Eine solche Kampagne hilft dabei, dass es gar nicht erst zu solchen Fällen kommt», ist Fabian Ilg, Spezialist für Cybercrime und Geschäftsleiter der SKP, überzeugt.

Auch wenn Cybervorfälle immer häufiger gemeldet werden, die Dunkelziffer bleibt gross. «Angriffe zu melden ist wichtig. Meldungen helfen dem NCSC, die Situation noch schneller einzuschätzen, frühzeitig neue Entwicklungen zu erkennen und Massnahmen zu ergreifen», sagt Florian Schütz, Delegierter des Bundes für Cybersicherheit und Vorsteher des NCSC. Daniel Nussbaumer, Präsident der SISA, ergänzt: «Mit dieser Aktionswoche wollen wir Bevölkerung und Medien auf das Thema aufmerksam machen, denn Prävention ist das wirksamste Mittel.»

Cyberangriffe sind vielgestaltig: Der eigene Computer oder das Smartphone wird zum Beispiel unbemerkt zu illegalen Zwecken eingesetzt, persönliche Daten, Kreditkartenangaben, Login-Daten oder ganze Identitäten werden gestohlen und missbraucht. «Cyberkriminelle sind kreativ, versiert und oft international organisiert», sagt Fabian Ilg, «es ist deshalb wichtig, die Bevölkerung jetzt auf die Risiken aufmerksam zu machen und gleichzeitig Hilfestellung und Information zu bieten. Denn es ist eigentlich einfach, sich gegen Angriffe zu schützen.»

Weitere Informationen

www.S-U-P-E-R.ch

Bildmaterial

Hier geht's zum Bildmaterial*

Organisationspartner

Schweizerische Kriminalprävention
«eBanking – aber sicher!» - eine unabhängige Plattform der Hochschule Luzern
Nationales Zentrum für Cybersicherheit NCSC
iBarry – Plattform für Internetsicherheit

Kontakt allgemeine Medienanfragen

Fabian Ilg, Geschäftsleiter, Schweizerische Kriminalprävention SKP
Haus der Kantone
Speichergasse 6
3001 Bern
E-Mail: fi@skppsc.ch
Telefon: +41 31 511 00 08

* Das Bildmaterial darf nicht verändert und nur im Kontext der Berichterstattung zur Kampagne verwendet werden.

Ihre Kontakte (alphabetisch)

Folgende Personen stehen für Rückfragen und Interviews zu den aufgeführten Themen im Kontext der Berichterstattung zu der Aktionswoche zur Verfügung.

Marcus Beyer
Security Awareness Officer Swisscom (Schweiz) AG
- IT-Sicherheit
- Cyber Security Awareness
- Cyber Resilienz in Unternehmen

E-Mail: marcus.beyer@swisscom.com
Telefon: +41 58 221 12 18 / +41 79 307 81 33

Andreas Hölzli
Leiter Kompetenzzentrum Cyber Risk Schweizerische Mobiliar Versicherungsgesellschaft AG
- Cyberversicherung für Privatpersonen, KMU und Unternehmen
- Cyberangriffe gegen KMU

Kontakt: Jürg Thalmann, Mediensprecher
E-Mail: media@mobiliar.ch
Abwesenheit: 30.04-07.05.2021

Chantal Billaud
Stv. Geschäftsleiterin Schweizerische Kriminalprävention SKP
- Kriminologie und Psychologie
- Mechanismen bei Cyber-Betrug

E-Mail: cb@skppsc.ch
Telefon: +41 31 511 00 09

Fabian Ilg
Geschäftsleiter Schweizerische Kriminalprävention SKP
- Prävention Cybersicherheit
- Cybercrimephänomene

E-Mail: fi@skppsc.ch
Telefon: +41 31 511 00 08

Ivan Bütler
Gründer und Verwaltungsratspräsident Compass Security
- Ethical Hacking inklusive Praxisbeispiele aus der Schweiz/bei Schweizer Unternehmen
- Cyber-Risiken sind auf dem Vormarsch

E-Mail: ivan.buetler@compass-security.com
Telefon: +41 79 250 06 28

Nationales Zentrum für Cybersicherheit NCSC
- Zahlen & Fakten der Nationalen Anlaufstelle beim NCSC
- Malware-Angriffe
- Was tun bei einem Angriff / Verdacht
- Blick in die Zukunft: Was wird uns künftig erwarten?

E-Mail: ncsc-media@gs-efd.admin.ch

André Duvillard (Deutsch und Französisch sprechend)
Delegierter für den Sicherheitsverbund Schweiz
- Schweizer Sicherheitspolitik
- Zusammenspiel Schweizer Sicherheitsakteure
- Strafverfolgung und Kriminologie

E-Mail: andre.duvillard@gs-vbs.admin.ch
Telefon: +41 58 464 21 13

Dr. iur. Daniel Nussbaumer
Leiter Cyber Security T-Systems und Präsident der Swiss Internet Security Alliance
- Cybercrime und Prävention
- Risiken und Chancen der Digitalisierung

E-Mail: daniel@swiss-internet-security-alliance.ch
Telefon: +41 79 672 32 05

Lt Serdar Günal Rütsche
Chef Abteilung Cybercrime Kantonspolizei Zürich und Leiter NEDIK (Netzwerk Ermittlungsunterstützung digitale Kriminalitäts-bekämpfung)
- Digitalisierte Kriminalität und Cybercrime

E-Mail: gus@kapo.zh.ch
Telefon: +41 44 247 22 00, Abwesenheit: 19.-23.04.2021

lic. iur. Stephan Walder
Stv. Leitender Staatsanwalt, Staatsanwaltschaft II des Kantons Zürich, Cybercrime
- Strafverfolgung und juristische Situation

E-Mail: stephan.walder@ji.zh.ch
Telefon: +41 44 247 31 40

Oliver Hirschi
Dozent Informationssicherheit und Leiter der Plattform «eBanking – aber sicher!», Hochschule Luzern HSLU
- Brute-Force-Angriff inklusive Live-Demo
- Expertise zu Passwörtern, E-Banking und ID-Diebstahl
- ID-Diebstahl

E-Mail: oliver.hirschi@hslu.ch
Telefon: +41 41 757 68 58

Anonym
- Opfer eines Kleinanzeigenbetrugs

E-Mail: medien@skppsc.ch
Telefon: +41 52 269 16 64 (Frau Honegger)
Abwesenheit: 5.-15.05.2021

Kurzinterviews und Aussagen zur Verfügung

Diese Interviews dürfen nur im Kontext einer Berichterstattung über die Aktionswoche verwendet werden. Bei Verwendung in anderem Kontext oder Abänderung der Aussagen müssen die betreffenden Personen kontaktiert werden.

Situation allgemein: «Cybersicherheit gewinnt an Bedeutung.»

Florian Schütz, Delegierter des Bundes für Cybersicherheit, Vorsteher NCSC

Was sind die Gründe dafür, dass die Meldungen während Corona zugenommen haben?
Das NCSC konnte einen deutlichen Anstieg an Meldungen feststellen. Die Zahl der tatsächlichen Cyberangriffe stieg jedoch nur leicht. Wir führen die gestiegene Zahl von Meldungen auf die höhere Sensibilität von Unternehmen und Privatpersonen zurück. Was wir hingegen feststellen konnten, war, dass sich die Angriffe vermehrt auf die Pandemie beziehen.

Was sind die im Moment häufigsten Bedrohungen?
Wir verfolgen sehr genau, welche Arten von Bedrohungen sich jeweils häufen – das kann sich rasch entwickeln. Es gibt ganz verschiedene Bedrohungsarten, Phishing ist eine der bekanntesten und gewissermassen ein Dauerbrenner. Bei Phishing versuchen Kriminelle mit gefälschten E-Mails oder SMS die Opfer dazu zu bringen, dass sie persönliche Informationen angeben, zum Beispiel Passwörter oder Kreditkarteninformationen. Solche E-Mails oder SMS können sehr professionell wirken und sind oft nicht auf den ersten Blick zu erkennen.

Was sollte man tun, wenn man Opfer eines Angriffs wurde oder einen Verdacht hat?
Das kommt ganz auf den Angriff an – grundsätzlich sollte aber rasch gehandelt werden, um weitere Schäden zu vermeiden. Das heisst zum Beispiel Kreditkarten sperren oder Personen informieren, die ebenfalls betroffen sein könnten. Ausserdem sollte der Vorfall beim Nationalen Zentrum für Cybersicherheit (NCSC) gemeldet werden. Hat das Opfer finanziellen Schaden erlitten, sollte es bei der zuständigen Polizeibehörde Anzeige erstatten.

Welche Rolle spielt die Cybersicherheit in der Schweiz?
Durch die zunehmende Digitalisierung gewinnt auch die Cybersicherheit an Bedeutung. Auf Bundesebene spielt sie in der Aussen- und Sicherheitspolitik eine zentrale Rolle. Auch für den Wirtschaftsstandort und die Schweizer Bevölkerung wird das Thema zunehmend wichtig werden.

Thema Prävention: «Je besser wir informiert sind, desto geringer sind die Chancen der Cyberkriminellen.»

Daniel Nussbaumer, Präsident der Swiss Internet Security Alliance SISA mit der Präventions-Plattform iBarry.ch

Wieso setzen Behörden und Wirtschaft im Cyberbereich so stark auf Prävention?
Die Strafverfolgung hat im Cyberbereich stark zugelegt. Es gelingt immer öfter und immer besser, Täter auch zur Verantwortung zu ziehen. Weil die Täter beim digitalisierten Verbrechen aus der ganzen Welt kommen und die internationale Strafverfolgung komplex und aufgrund fehlender Abkommen nicht immer möglich ist, ist es wichtig, die Bevölkerung über die Gefahren aufzuklären.

Hinkt Prävention den Tätern nicht immer hinterher?
Es gibt alle Arten von Tätern. Solche, die weniger erfinderisch sind und solche, die sich immer wieder neue Tricks und Herangehensweisen ausdenken. Letztere machen es für die Prävention tatsächlich schwieriger. Darum setzt Prävention ebenfalls auf verschiedene Techniken. Wir beschreiben einerseits die verschiedenen Maschen der Betrüger von falschen Support-Anrufen über Liebesbetrug bis zu Phishing-Mails. Andererseits zeigen wir auf, dass die Geschichten der Kriminellen zwar ändern, die Techniken, mit denen sie uns zu erwischen versuchen, aber ähnlich bleiben. Denn sie wissen, wo wir verwundbar sind.

Können Sie das genauer beschreiben?
Zuerst wecken sie das Interesse ihrer Opfer. Das kann von einer Freundschaftsanfrage in den Sozialen Medien über ein E-Mail, eine Nachricht, ein Inserat oder einen Telefonanruf bis zu einem angeblichen Auftrag an ein Unternehmen reichen. Haben sie dieses Interesse geweckt, versuchen sie potenzielle Opfer daran zu hindern, mit Distanz über alles nachzudenken und den Fall zu überprüfen. Meist tun sie dies, indem sie hohen Druck aufbauen. Zum Beispiel mit Mails, Nachrichten und Anrufen oder knapper Zeit – oder sie liefern angebliche Beweise gleich selbst, um Nachforschungen zu verhindern.

Hat Prävention denn Erfolg?
Den Erfolg von Prävention nachzuweisen ist immer schwierig. Wirtschaft und Behörden haben aber schon viel in die Aufklärung investiert und wir können sehen, dass die Bewohnerinnen und Bewohner in der Schweiz immer besser über die Risiken im Internet Bescheid wissen. Wir müssen sie aber noch mehr für sicheres Verhalten im Internet sensibilisieren. Darum haben wir auch die S-U-P-E-R.ch-Kampagne lanciert.

Thema Sichern: «Denken Sie an Ihr Smartphone.»

Fabian Ilg, Geschäftsleiter Schweizerische Kriminalprävention SKP

Dass man seine Daten auf zusätzlichen Speichern sichern soll, wissen wohl die meisten – oder?
Das mag sein – doch das Tun ist eine andere Sache. Wir gehen davon aus, dass ca. ein Drittel der Schweizer Bevölkerung die Daten nicht zusätzlich sichert.

Ist Datenverlust wirklich ein häufiges Problem?
Denken Sie an Ihr Smartphone – das kann rasch verloren gehen, gestohlen werden oder kaputt gehen. Dann sind die Daten weg, wenn sie nicht anderweitig gespeichert wurden. Viele sind sich dessen erst bewusst, wenn es soweit ist. Und gerade bei diesen Daten schmerzt der Verlust sehr.

Was genau sollte man machen?
Entweder man speichert seine Daten regelmässig auf einer externen Festplatte oder in der Cloud. Ersteres kann aber etwas zeitintensiv und damit abschreckend sein. Darum gibt es bei den gängigsten Betriebssystemen Sicherungsprogramme – diese sind sehr einfach zu bedienen. Wir haben die wichtigsten Infos auf www.S-U-P-E-R.ch zusammengestellt.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC

eBanking aber sicher!
Lucerne University of Applied Sciences and Arts
HOCHSCHULE LUZERN
FH Zentralschweiz

iBarry

SKPPSC
Schweizerische Kriminalprävention
Prévention Suisse de la Criminalité
Prevenzione Svizzera della Criminalità

Ihre POLIZEI
Votre POLICE
La vostra POLIZIA
Kantonale und Städtische Polizeikorps
Corps de police cantonaux et municipaux
Corpi di polizia cantonali e comunali

Thema Updates: «Software ist nicht perfekt.»

Ivan Bütler, Gründer Compass Security

Warum sind Updates so wichtig?
Software ist nicht perfekt und hat immer auch Schwachstellen. Mit Updates werden solche Schwachstellen behoben. Wer Updates also nicht macht, riskiert, dass diese Schwachstellen bleiben und von Hackern ausgenutzt werden können – diese halten aktiv Ausschau danach und können dann sehr einfach in Systeme eindringen und Schaden anrichten.

Inwiefern ist Hacking durch veraltete Software für Privatpersonen ein Problem?
Seitens Hacking ist die grösste Bedrohung für Privatpersonen die Erpressung: Es wird von aussen auf die Daten zugegriffen und diese werden verschlüsselt, sodass man selbst nicht mehr darauf zugreifen kann. Um die Daten zurückzuerhalten wird Lösegeld verlangt. Oft geschieht nach Bezahlung des Lösegelds natürlich nichts und sowohl das Geld als auch die Daten sind verloren.

Thema Prüfen: «Es ist wie zu Hause: Schliessen Sie die Türe ab.»

André Duvillard, Delegierter für den Sicherheitsverbund Schweiz

Schutzprogramme sind doch mittlerweile selbstverständlich – oder nicht?
Leider nicht: Wir haben eher den Eindruck, dass die Anzahl der Internetnutzerinnen und -nutzer, die einen Virenschutz installiert haben, abnimmt oder dieser zumindest vernachlässigt wird.

Wie genau kommen Malware und Viren auf ein System?
Das Eintrittstor ist der Mensch: Über Links oder Downloads kann man sich Malware und Viren auf das System holen – wenn man es nicht schützt. Diese können ganz verschiedene Auswirkungen haben: Das System kann zum Beispiel extrem langsam werden oder komplett blockieren. Daten können gestohlen werden oder Kriminelle übernehmen die Kontrolle über den Computer oder das Smartphone.

Was kann man konkret tun?
Es ist wie zu Hause: Schliessen Sie die Türe ab, damit niemand hereinkommt. Das tut man beim Computer mit Schutzsoftware, also zum Beispiel einem Antivirus-Programm. Ausserdem sollte man regelmässig den «Schädlingsbefall» mit einer Systemprüfung kontrollieren. Für Schutzsoftware auf verschiedenen Betriebssystemen gibt es auf der Webseite www.S-U-P-E-R.ch eine gute Übersicht. Auch Smartphones kann und sollte man schützen.

Thema Einloggen: «Das ständige Wechseln des Passworts ist nicht nötig.»

Oliver Hirschi, Dozent und Leiter der Plattform «eBanking – aber sicher!» der Hochschule Luzern

Was macht ein gutes Passwort aus?
Eigentlich geht es darum, es einem Angreifer möglichst schwierig zu machen, das Passwort durch Probieren oder Erraten zu knacken. Je länger und komplexer also das Passwort, desto geringer die Chance, dass sie das Passwort herausfinden.

Wie macht man das?
Dazu sollte man erstens ein starkes Passwort wählen, dazu haben wir die wichtigsten Regeln auf www.S-U-P-E-R.ch zusammengestellt. Zweitens sollte man für jeden Login ein anderes Passwort verwenden. Wenn man so vorgeht, ist das ständige Wechseln des Passworts, wie oft behauptet, gar nicht nötig. Ausserdem kann auf sogenannte Passwortmanager zurückgegriffen werden, einige stellen wir auf der Webseite ebenfalls vor.

Was sind die Risiken bei schwachen Passwörtern?
Das kann sehr unangenehm werden, wenn zum Beispiel das Passwort für Dienste geknackt wurde, wo Zahlungsmittel hinterlegt sind – solche Informationen können abgegriffen und missbraucht werden. Oder falls der Zugriff auf Geräte gelingt, können Daten gestohlen oder Malware installiert werden.

Thema Reduzieren: «Jeder kann zum Opfer werden.»

Chantal Billaud, Stv. Geschäftsleiterin Schweizerische Kriminalprävention SKP

Kann jede und jeder Opfer eines Cyber-Betrugsfalls werden?
Ja – auch wenn die meisten Menschen der Überzeugung sind, dass sie nicht darauf hereinfallen würden. Bei uns melden sich täglich Betrugsopfer, und das sind keine besonders naiven oder dummen Menschen. Sie kommen aus unterschiedlichsten sozialen Schichten.

Wie laufen diese Betrugsfälle ab?
Alle Menschen haben schwache Momente, in denen sie verwundbar und bedürftig sind. Bedürftig nach Anerkennung, Zuwendung, Intimität oder ganz einfach auch Geld. Betrugsmaschen zielen immer auf eine dieser Schwächen ab. Wenn Betrugsversuche massenweise über das Internet gestreut werden, ist die Chance gross, dass sie auf einen Menschen treffen, der für genau diese Verlockung empfänglich ist. Wenn dann noch Zeitdruck aufgebaut wird und das Angebot beschränkt scheint, kann die Falle bei den meisten von uns zuschnappen.

Was hilft dagegen?
Manchmal hilft es schon, dass man informiert ist: Wenn man weiss, dass im Netz jede Information gefälscht werden kann und auch oft zu Betrugszwecken gefälscht wird, glaubt man vielleicht nicht mehr so schnell alles. Zum Beispiel, dass ein amerikanischer Berufssoldat, der in Afghanistan stationiert ist, ausgerechnet Sie heiraten will. Dann schaut man ein Profil oder Angebot generell kritischer an. Medienkompetenz und Information hilft also, sich vor Betrug zu schützen.