Willkommen zu unserer Veranstaltung

„Sicherheit im Internet“

Was bedeutet Sicherheit für mich?

5 Schritte für ihre Computersicherheit.

Erster Schritt: Daten Sichern
zum Beispiel mit: Pure Sync
https://www.heise.de/download/product/puresync-firesync-57287

Zweiter Schritt: Daten schützen
mit Windows Defender und zusätzlichen Programmen z.B.
https://www.bundespolizei-virus.de/virenschutz/

Dritter Schritt: Überwachen
z.B. mit der Windows Firewall und Win 10 Firewall Control free
http://www.computerbild.de/download/Windows-10-Firewall-Control-Free-5237059.html

Vierter Schritt: Vorbeugen
immer alle Programme aktuell halten, am besten per „automatischem update“. Geräte und Programme mit einem „sicheren“ Passwort schützen (und das Passwort merken).
Vielleicht einen Passwortmanager benutzen?
https://www.heise.de/tipps-tricks/Passwortmanager-So-verwalten-Sie-Ihre-Passwoerter-3934582.html

Fünfter Schritt: Aufpassen
sie selbst sind oft das größte Sicherheitsrisiko!
Bitte immer vorher genau lesen was sie mit „OK“ bestätigen.
z.B. eine Gewinnbenachrichtigung, wenn sie gar nicht gespielt haben…

Betrugsversuche durch angebliche Microsoft Mitarbeiter.
https://www.verbraucherzentrale.de/aktuelle-meldungen/digitale-welt/warnung-abzocke-durch-angebliche-microsoftmitarbeiter-24641

Achtung beim Installieren von Programmen.
Immer genau lesen und auf die Häkchen achten!
https://www.chip.de/downloads/PDF-XChange-Viewer_29539244.html

Remote Desktop deaktivieren.

Starts – Einstellungen - System – Remote

War WannaCry erst der Anfang? Tools gegen fiese Internet-Erpresser.

https://www.chip.de/news/War-WannaCry-erst-der-Anfang-Schutz-und-Entfernen-von-Ransomware_92035897.html

Banking

Film

https://videos.chip.de/p/1741931/sp/174193100/serveFlavor/entryId/1_hznsnwqm/v/1/flavorId/1_zj76j1p6/name/a.mp4

1. Domain-Kontrolle und Sicherheitszertifikat

Geben Sie die Internetadresse Ihrer Bank immer selbst per Hand ein und achten Sie darauf, dass Sie beim Online-Banking eine gesicherte Verbindung benutzen. Die Internetadresse beginnt dann stets mit "https://..." und erhält ein Sicherheitszertifikat.

- Bei Firefox erscheint im Adressfeld ein grüner Balken, bei dem Sie mit einem Klick auf das Schloss-Symbol die Website-Verifizierung für die Internetseite angezeigt bekommen. Diese Seite gilt dann als vertrauenswürdig, die Datenübertragung erfolgt verschlüsselt.
- Im Internet Explorer wird das Adressfeld vollständig grün hinterlegt - weitere Informationen zur Website-Identifizierung erhalten Sie am rechten Ende des Eingabefeldes (Schlüssel-Symbol). Dort finden Sie unter anderem auch das Sicherheitszertifikat für die aufgerufene Website.

2. Phishing-Schutz im Browser aktivieren

Sowohl bei Firefox wie auch beim Internet Explorer können Sie einen Phishing-Schutz aktivieren. Das bedeutet, wenn Sie beim Surfen auf eine verdächtige Seite stoßen, blockiert Ihr Browser diese automatisch. So lässt sich verhindern, dass Ihnen unbemerkt Daten geklaut werden:

- Gehen Sie in den Einstellungen bei Firefox zur Registerkarte "Datenschutz & Sicherheit". Ganz nach unten scrollen zu „Sicherheit“ und da die Häkchen setzen, um den Phishing-Schutz zu aktivieren. Standartmäßig sollte das bereits aktiviert sein.
- Der Internet Explorer nennt diese Funktionen "Smart Screen Filter" und hat sie in der Kategorie "Einstellungen – erweiterte Einstellungen" da ganz unten aufgelistet. Dort können Sie - sofern nicht bereits aktiviert - den Smart Screen-Filter einschalten.

-

3. Phishing-Mails, Hotspots und fremde Computer

- Moderne Kriminelle klingeln nicht mehr an der Haustür, sondern zocken Sie per Phishing-Email durch die Hintertür ab. Trickreich locken die Cyber-Kriminellen mit Gewinnen, lukrativen Jobs, dem Besuch von Inkassounternehmen oder sogar in Verkleidung Ihrer Hausbank in die Falle. Die Betrugsmasche ist immer gleich, denn Sie sollen entweder einen Link anklicken, den Anhang öffnen oder Daten eingeben, um scheinbar Schlimmeres zu vermeiden. Dabei greifen die Betrüger auf bekannte Unternehmen zurück: Google, Apple, Microsoft, PayPal, Ebay, Banken. Sogar die Namen von Freunden und Geschäftspartner müssen unter Umständen herhalten.
- Nutzen Sie Hotspots (öffentlich zugängliche WLAN-Netze) nur zum Surfen und nicht zum Online-Banking. Für Kriminelle ist es nicht schwer, über ein ungesichertes Netzwerk auf Ihr Smartphone, Tablet oder Laptop zuzugreifen und Ihre Kontodaten auszuspionieren.
- Auch bei fremden Geräten sollten Sie auf Online-Banking verzichten, da Sie nicht ausschließen können, dass Ihre Eingaben aufgezeichnet werden. So können Kriminelle einfach auf Ihren Namen, Kontonummer und Ihre PIN zugreifen.

Sichere TAN-Verfahren fürs Mobile Banking - diese Möglichkeiten gibt's

Wer Online-Banking betreibt, kann sich seine TANs - kurze Zahlenkombinationen zur Transaktionsbestätigung - mit dem mTAN-Verfahren als SMS senden lassen. Beim Mobile Banking raten wir Ihnen jedoch strikt davon ab: Wenn Sie Ihre TANs auf demselben

Gerät empfangen, mit dem Sie Überweisungen tätigen, haben Hacker leichtes Spiel. Die folgenden TAN-Verfahren bieten sich eher für mobile Geldgeschäfte an:

- Bei der Push-TAN lässt sich die Transaktionsbestätigungs-Nummer in einer separaten App anfordern, die Sie mit einem weiteren Passwort schützen müssen. Das ist zwar komfortabel, jedoch befinden sich hier erneut alle Daten auf dem Smartphone. Wenn sich erst einmal ein Virus auf Ihrem Gerät eingeschlichen hat, kann es sein, dass er sowohl die Banking- als auch die TAN-App ausliest.
- Die Photo-TAN bietet schon mehr Sicherheit: Hier wird vor der Überweisung ein kryptisches Bild generiert, das Sie mit einem Smartphone oder Tablet abfotografieren müssen. Eine spezielle App liest aus der Grafik dann die TAN heraus. Dieses Verfahren ist aber deutlich umständlicher - schließlich müssen Sie für Bankgeschäfte unterwegs immer zwei Geräte dabeihaben.
- Das Chip-TAN-Verfahren ist bisher die sicherste Variante fürs Mobile Banking: Mit Hilfe Ihrer Bankkarte und eines zusätzlichen Kartenlesegerätes werden für jede Transaktion einzigartige TAN-Codes erstellt. Der kleine TAN-Generator lässt sich im Grunde nicht hacken, jedoch müssen Sie sich diesen in den meisten Fällen extra kaufen.

Umgang mit Suchmaschinen (googeln)

www.google.de

Wie kann ich verhindern, dass Keiner meine Kamera im Laptop hackt?

Am leichtesten ist es einen kleinen Aufkleber oder ein Papier vor die Linse zu kleben.

Macros in Office und Acrobat abschalten mit Hilfsprogramm Protec'tor 1.0.1
Anleitung unter: https://www.heise.de/ct/ausgabe/2017-20-Mehr-Sicherheit-unter-Windows-durch-gezieltes-Deaktivieren-unnoetiger-Funktionen-3827057.html#1506636240406657_1505131375
Download des Programms unter:
Https://github.com/jamct/protector/releases/tag/1.0.1

WLAN Sicherheit

Den Router absichern!

1. Zugang zum Menü des Routers immer mit Passwort absichern.

2. Das WLAN natürlich auch immer mit Passwort sichern.

3. Dem WLAN (SSID) keinen zuordenbaren Namen geben (z.B. Familie Kleien).

4. Die Firmware des Routers immer auf den neusten Stand halten.

5. Um die Sicherheit Deines WLAN noch weiter zu erhöhen, kannst Du das Netzwerk unsichtbar machen. Es zwar da, wird aber bei einer Umkreissuche nicht mehr angezeigt. Nur die Personen, die den Namen genau kennen und ins Endgerät eingeben, werden dann mit dem WLAN verbunden**.**

6. Gerade wenn öfter Freunde von Freunden zu Besuch kommen, solltest Du auf keinen Fall Deinen Zugangsschlüssel für das WLAN einfach so herausgeben. Am besten erstellst Du ein Gastnetzwerk. Darin können Gäste sich dann einloggen und surfen, haben aber

keinen Zugriff auf Dateifreigaben oder Netzwerkfestplatten. Für das Gastnetzwerk wird ein individueller Netzwerkschlüssel vergeben.

7. Wenn du alle deine Geräte am Router angemeldet hast, gibt es bei den meisten Routern die Möglichkeit das Netz auf die bekannten Geräte zu beschränken. Dann kann sich kein neues (fremdes) Gerät mehr mit dem Router verbinden.

Sicherer Zugang im öffentlichen WLAN

Kostenloses WLAN in Hotels, Restaurants, an Bahnhöfen oder Flughäfen nutzen Anwender gerne, um das eigene Datenvolumen zu schonen. Den wenigsten ist dabei allerdings bewusst, dass alle anderen Nutzer in einem offenen Netzwerk auch ihr Gerät sehen und damit auch belauschen können: Alle unverschlüsselten Daten sind ohne große Mühe direkt rekonstruierbar. Telefongespräche – sofern nicht verschlüsselt – lassen sich leicht belauschen. Dies können Sie jedoch einfach verhindern, wenn Sie Ihren Zugang mittels VPN (Virtual Private Network) absichern. Damit bauen Sie einen direkten Tunnel zwischen sich und dem VPN-Anbieter auf, und Ihr Zugang zum Internet wird dabei verschlüsselt.
Der kostenlose Tor-Browser ist dafür das richtige Instrument.

http://www.computerbild.de/download/Tor-Browser-Paket-5270217.html

Mittlerweile bieten auch viele Antivirenprogramme einen VPN Zugang an, der muss aber oft extra bezahlt werden.

Sicherheit mit Android Smartphone und Tablets

1. **NFC, Bluetooth und unbekannte Quellen ausschalten (**Installation von anderen Quelle als Play Store erlauben**).**

2. **Antivirenschutz**
   https://www.av-test.org/de/antivirus/mobilgeraete/
3. **Passwort einrichten**
4. **Sicherheitsrichtlinien automatisieren**
5. **Diebstalschutz**
   https://www.vodafone.de/featured/digital-life/smartphone-sicherheit-diebstahlschutz-via-app/

Anonym und sicher im Netz -
per Tor-Client und dem Security-Browser Orfox

http://www.computerbild.de/download/Tor-Browser-Paket-5270217.html

Sicherheit mit dem IPhone

https://www.kaspersky.de/blog/iphone-sicherheitstipps/4094/

https://www.schau-hin.info/informieren/medien/surfen/sicherheit-fuer-mobile-geraete/sicherheit-ios.html

Sind meine biometrischen Daten sicher?

https://www.tagesschau.de/wirtschaft/biometrische-daten-105.html

Sicher einkaufen bei Ebay mit PayPal.

Ebay ist eine Handelsplattform auf der Jedermann seine Ware anbieten kann. Ebay selbst ist es egal wer da verkauft, da Ebay ja von der zu bezahlenden Provision lebt. Ebay kontrolliert nicht die Seriosität der Anbieter. Es gibt viele gute Anbieter, auch reale Geschäfte die über diese Plattform verkaufen, aber auch einige die sich einfach nur bereichern wollen.
Als Käufer sollten sie sich die Bewertungen des Verkäufers genau

ansehen, nicht nur wie viele positive es sind, sondern auch was geschrieben wurde. Bei Bezahlung per Banküberweisung gibt es keinen Käuferschutz. Das heißt, wenn sie defekte oder falsche Ware zugesendet bekommen haben sie kein Rückgaberecht, Ebay lässt sie dann alleine. Käuferschutz gibt es nur, wenn sie über PayPal bezahlen!

Mit PayPal können Sie sicher und einfach auf zahlreichen Plattformen und Online-Shops wie Ebay bezahlen. Die Überweisungen sind zudem kostenlos. Sollten Sie Geld auf Ihr PayPal-Konto erhalten, wird eine Gebühr erhoben.

- Datenschutz: Der große Vorteil von PayPal ist, dass Ihre sensiblen Daten bei dem Dienst verschlossen bleiben. Der Verkäufer kennt lediglich Ihre E-Mail-Adresse von PayPal, mehr nicht. Daten wie Ihre Kontonummer erfährt dieser nicht. Lediglich PayPal besitzt die Daten und regelt den Bazahlvorgang intern ab.
- PayPal Käuferschutz: Sind Sie beim Online-Shopping auf Betrüger hereingefallen, können Sie dies bei PayPal melden. PayPal überweist Ihnen dann nach Kontaktaufnahme sofort Ihr Geld zurück aufs Konto und regelt die Angelegenheit alleine. So müssen Sie nicht Tage oder Wochen um Ihr Geld bangen.
- Verschlüsselung: Die Website von PayPal läuft nicht nur über die bekannte https-Verschlüsselung, sondern auch intern werden Ihre Daten verschlüsselt und geheim gehalten. Zudem prüft PayPal bei einer Benutzerkonto-Eröffnung, ob Sie der rechtmäßige Inhaber des Bankkontos sind, und stellt weitere optionale Sicherheitseinstellungen zur Verfügung. Der TÜV-Saarland hat PayPal geprüft und als sicheres Online-Zahlungsmittel deklariert.
- Probleme: Der Dienst macht leider nicht nur gute Schlagzeilen. Des Öfteren kommt es zur ungerechtfertigten Einfrierung von PayPal-Konten. Dies geschieht, wenn Käufer oder Verkäufer sich bei PayPal beschweren, falls der Handel nicht richtig abgelaufen ist. Leider werden aber nicht nur in richtigen Fällen Konten eingefroren, so kommt es nicht selten zu Missverständnissen,

die zur ungerechtfertigten Einfrierung führen. Rechtlich umstritten ist diese Willkür des Dienstes allemal.
- Fazit: Möchten Sie nicht Gefahr laufen, dass Ihre Finanzen eingefroren werden, sollten Sie den Dienst nicht als Kontoersatz, sondern nur als Treuhänder für Ihre Online-Überweisungen nutzen.

Gütesiegel für Online-Shops

Zwar gibt es kein einheitliches Gütesiegel für Internethändler. Unter www.internet-guetesiegel.de finden Sie aber empfehlenswerte Gütesiegel, deren Prüfkriterien von der "Initiative D21" festgelegt werden, einem gemeinsamen Projekt von Wirtschaft, Politik und Verbraucherschützern.

- **Trusted Shops**

  Trusted Shops zertifiziert Online-Shops nach sorgfältig ausgewählten Qualitätskriterien bevor das Europäische Gütesiegel verliehen wird. Mit der Kombination aus Geld-zurück-Garantie und Händlerbewertungs-System von Trusted Shops kaufen Verbraucher im Internet sicher ein.

- 

  Internet privacy Standards

  Die Datenschutz Cert GmbH bietet Konformitätsbewertungen auf dem Gebiet des Datenschutzes und der Informationssicherheit an. Diese umfassen Prüfaktivitäten sowie Zertifizierungstätigkeiten. Im Fokus stehen dabei IT-Systeme, -Produkte, Verfahren und Prozesse.

- 

  EHI Geprüfter Online-Shop

  Für den sicheren und verbraucherfreundlichen Einkauf bietet das Siegel Geprüfter Online-Shop insbesondere Test-bestellungen, die Überprüfung der telefonischen Erreichbarkeit, alle gesetzlichen Informationspflichten und vieles mehr.

- 

S@fer Shopping

Zum Erhalt des TÜV SÜD Prüfsiegel ist ein dreistufiges Prüfverfahren vorgesehen, das aus einer Online-Prüfung, einem Security-Check und einem Audit vor Ort besteht. Dadurch wird den Kunden beim Online-Einkauf eine angemessen hohe Qualität und Sicherheit geboten.

Welche Angriffs Instrumente gibt es?

Eine kleine Abhandlung über Trojaner, Würmer, Viren und ….

Trojaner verdanken ihren Namen dem Heldenepos über den Kampf um Troja: Mit einem Geschenk, dem Trojanischen Pferd, schleusten die Griechen ihre darin versteckten Soldaten nach Troja ein. Trojaner arbeiten genauso: Eine als nützlich angepriesene Software verbirgt in sich ein tückisches Schadprogramm. Dabei ist es egal, ob die Software die versprochenen „guten“ Funktionen hat oder nicht: Einmal gestartet, installiert sie den Schädling, etwa ein Spionage-Programm, und sorgt dafür, dass dieser auch unabhängig vom Trojaner auf dem Computer läuft.

Daher nützt es meist wenig, wenn Sie den Trojaner wieder löschen. Da der nur das Transportmittel für das eigentliche Schadprogramm ist, bleibt dieses nach der Entfernung auf dem Computer. Man unterscheidet zwischen solchen Trojanern, die den Schädling schon an Bord haben, und solchen, die das Schadprogramm nachträglich aus dem Internet laden („Download-Trojaner“).

Würmer nutzen die Netzwerkverbindungen des Computers, um sich selbst auf andere PCs zu kopieren. Dadurch verbreiten sie sich deutlich schneller als Computerviren. Viele Würmer verbreiten sich per E-Mail: Ist ein solcher Wurm einmal aktiv, durchsucht er beispielsweise das Adressbuch des E-Mail-Programms und schickt sich an alle darin gespeicherten Adressen weiter.

Aber auch über eine normale Internetverbindung finden einige Würmer den

Weg auf andere Computer. Allein der Aufbau einer Verbindung reicht dazu aus. Um die Zugriffskontrolle auf den fremden Computer auszuhebeln, werden bestehende Sicherheitslücken in den jeweiligen Betriebsprogrammen und auch in den Schutzprogrammen ausgenutzt.

Vorsicht: Wenn Sie ohne jegliche Schutzmaßnahmen (etwa Virenscanner und Firewall) ins Internet gehen, dauert es meist nur wenige Minuten, bis sich Ihr Rechner den ersten Wurm eingefangen hat!

Sogenannte „Hintertür-Programme“

Sie öffnen, wie der Name schon sagt, eine Hintertür zum Computer. Ist ein solches Programm auf dem PC installiert, kann sich der Hacker bei bestehender Internetverbindung an Ihrem Computer anmelden und auf Ihre Daten zugreifen, Programme ausführen, Windows-Einstellungen ändern und sogar beliebige Programme installieren.

Rootkits

Dies sind Programme, die die Spuren von Fremdeinwirkungen auf Ihren Computer verstecken. Solche Programme löschen zum Beispiel Einträge in den Protokolldateien von Windows, verstecken verdächtige Dateien oder machen im Hintergrund laufende Programme für Windows unsichtbar.

Spionage-Programme durchschnüffeln Computer nach vertraulichen Informationen und versenden diese.

Alle Spionage-Programme haben eines gemeinsam: Sie durchsuchen den Computer nach vertraulichen Informationen, sammeln diese und geben sie übers Internet weiter. Die Urheber der Spione nutzen diese Informationen, um auf Ihre Kosten zu Geld zu kommen. Etwa durchs Plündern des Bankkontos oder durch gezielte Werbeattacken.

Die meisten Spionage-Programme gelangen in Trojanern auf den Computer. Es gibt aber auch viele „normale“ kostenlose Programme, die Spionage-Funktionen eingebaut haben. Lange Zeit war sogar der Windows-Hersteller Microsoft in Verruf, mit seinem Musik-Abspielprogramm „Windows Media Player“ die Benutzer auszuspionieren.

Diese unterschiedlichen Arten von Spionage-Programmen gibt es:

Keylogger

Diese speziellen Spionage-Programme protokollieren alle Tasteneingaben am Computer und schicken die Informationen per Internet an den Urheber. Das ist eine sehr heimtückische Methode, um etwa Kennwörter zu stehlen.

Datendiebe

Das Spionage-Programm durchsucht die auf der Festplatte Ihres Computers gespeicherten Dateien nach Zugangsdaten, Kennwörtern oder Kreditkartennummern. Hat es die gefunden, schickt es sie übers Internet an seinen Absender, der dann beispielsweise auf Ihre Kosten im Internet einkaufen kann.

Schnüffelprogramme

Einige Spionage-Programme untersuchen, welche Internetseiten Sie besuchen, welche Waren Sie bestellen und was Sie noch interessiert. Diese Informationen werden dann per Internet an unseriöse Firmen weitergeleitet und von denen missbraucht, um Sie gezielt mit Werbung zu bombardieren.

Vermehrungsfunktion

Viren bauen sich in andere Dateien ein, meist in Programme („Wirte“). Sobald man den Wirt startet, wird auch der Virus aktiv und nistet sich unbemerkt im PC-Arbeitsspeicher ein. Dann sucht er auf der Festplatte nach noch nicht infizierten Programmen und baut sich dort ebenfalls ein. Dazu muss der Virus erkennen können, ob eine Datei bereits befallen ist. Er muss seine Wirte also kennzeichnen. Hier setzen Virenschutz-Programme an: Deren Hersteller suchen nach diesen Kennzeichnungen. Die daraus zusammengestellten Listen („Virendefinitionsdateien“) müssen Sie regelmäßig aus dem Internet auf Ihren PC überspielen. Das Schutzprogramm durchsucht dann alle Programme auf dem Computer nach den in der Liste enthaltenen Kennungen.

Schadfunktion

Viele Viren machen sich nicht sofort bemerkbar, sondern werden nur an einem bestimmten Tag aktiv, der „Michelangelo“-Virus zum Beispiel an jedem 6. März. In der „Wartezeit“ können sie mehr Dateien befallen. Bricht die Schadfunktion aus, kommt es oft weltweit zu großen Schäden.

Tarnverfahren von Viren

Viren können sich nur so lange weiterverbreiten, wie sie nicht entdeckt und gelöscht werden. Daher haben die Urheber moderner Viren verschiedene Tarnverfahren entwickelt, um ihre Schädling vor der Entdeckung zu schützen. Hier die wichtigsten:

Einige Viren können sich selbst verändern („poly- und metamorphe Viren“). Ihre Funktion bleibt trotz des geänderten „Aussehens“ erhalten. Solche Viren sind für Schutzprogramme nur schwer zu erkennen und kaum auszurotten, ähnlich wie der Grippevirus beim Menschen, der auch in immer neuen Mutationen auftaucht.

Andere Viren können ihre Spuren, also die Veränderung befallener Dateien, verschleiern („Stealthviren“). Dazu greifen sie beispielsweise in die Funktionen des Betriebsprogramms ein. Das meldet dem Virenschutz-Programm bei der Abfrage der Dateigrößen bei infizierten Dateien die ursprüngliche Größe. Damit fällt die Größenveränderung für die Virenerkennung flach.

Besonders tückisch sind die sogenannten „Retroviren“. Sie versuchen häufig erfolgreich, die auf dem Computer installierten Schutzprogramme zu deaktivieren. Dadurch schützen sie sich nicht nur selbst vor Entdeckung, sondern öffnen auch anderen Schadprogrammen Tür und Tor.

Was für Virenarten gibt es?

Programmviren brauchen als Wirt ein Programm (Datei-Endung „.exe“, „.com“ oder „.dll“). Sie werden aktiviert, wenn eine befallene Datei ausgeführt wird.

Skriptviren befallen Skripte, die zum Beispiel in vielen Internetseiten eingebaut sind. Sie sind oft in der Programmiersprache „Javascript“ geschrieben. Denn diese Sprache verstehen die gängigen Internet- Browser, zum Beispiel der Internet Explorer. Die führen dann das schädliche Skript aus, und schon ist der PC infiziert.

Bootviren schreiben sich in den Bootsektor von Festplatten, Disketten oder Speicherkarten beziehungsweise -sticks. Sie werden aktiv, sobald der Computer von solch einem infizierten Datenträger gestartet wird. Daher sollte man einen unbekannten USB Stick vor dem Ausschalten des PCs entfernen.

Makroviren brauchen als Wirt Dateien, die Makros enthalten können, beispielsweise Word und Excel-Dateien. Die Schadmakros werden beim Öffnen der Datei automatisch mit gestartet und spulen dann ihre Befehle ab.