Sicherheit im Internet
Zusammenfassung des Referats
vom 8. Febr. 2022
Aktives Alter Adligenswil
Roland Sigrist

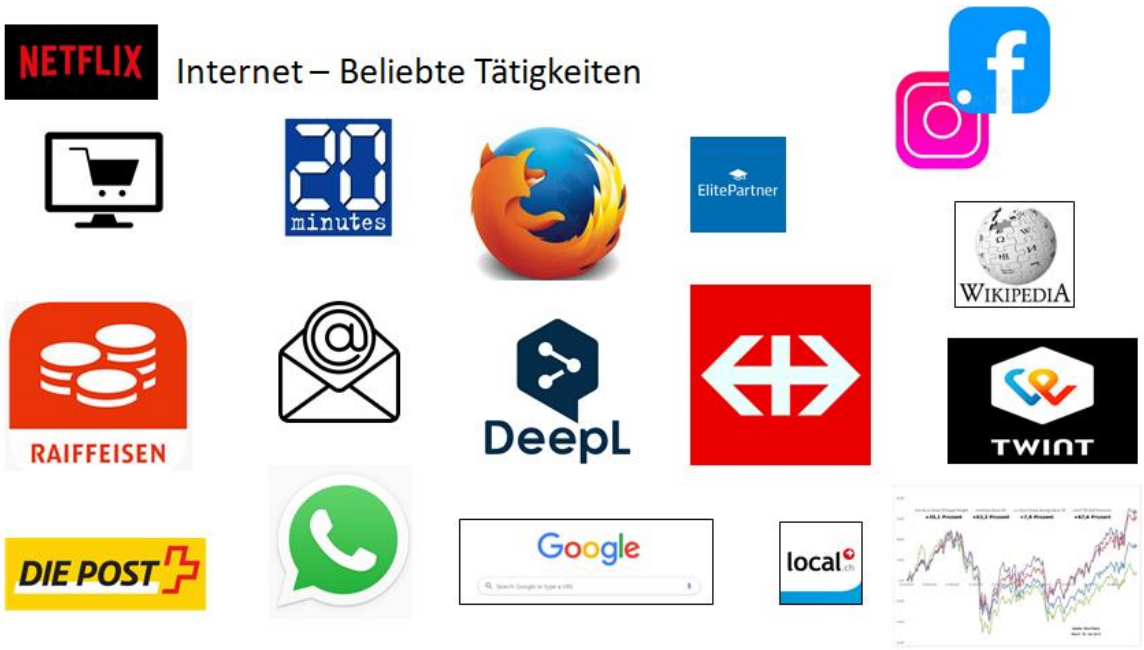
Internet – Mächtig und angreifbar!

- Das Internet ist grundsätzlich nicht sicher!
- Wer sich im Internet bewegt, muss sich bewusst sein, dass er sich damit möglicherweise einer breiteren Öffentlichkeit aussetzt.
- Vorsicht ist geboten, Schutzmassnahmen sind in jedem Fall nötig.
- Persönliche Daten gehören nicht ins Internet.
- Das Internet vergisst nie. Trotz Löschung bleiben Daten, Bilder, etc. weiterhin im Netzwerk.

Internet – Heikle Bereiche

- Supermärkte
- Spitäler, Gesundheitseinrichtungen
- Armee-Einrichtungen
- Regierungsstellen
- Medien
- Öffentlicher Verkehr
- und, und

2021 waren ca. 36% aller KMUs Ziel eines Hackerangriffs!



Internet – Grundlegende Sicherheitsmassnahmen

A. Hardware (PC, Tablet, Notebook):

- Automatische Updates installieren (Windows, IOS, Office, Browser, übrige Programme…)
- Virenschutz und Firewall aktivieren/installieren, Kabel statt Wlan (MS Defender!)
- Veraltete Programme ersetzen/löschen (Windows 7 | 8, Java, Adobe Flash Player…)
- Angebliche Sicherheitsmeldungen genau prüfen
- Bei längeren Arbeitspausen PC herunterfahren
- Kamera bei Notebooks mit Kleber abdecken
- Regelmässige Backups erstellen (auf externe Medien)
- Auf Anrufe von «Microsoft» nicht reagieren, aufhängen (Falle!)

A. Hardware (Smartphone):

- Automatische Updates des Betriebssystems installieren (Achtung: Ältere Handys lassen oft keine Updates zu!)
- Event. Virenschutz installieren
- Veraltete, ungenutzte Apps löschen
- Vorsicht bei ungeschützten Netzwerken (Hotels, Flughäfen, ect.)
- Vorsicht vor Kosten durch Roaming
- Ev. automatische Ortung aktivieren (Apple: *Wo ist*, samsung: *Find my Mobile…)*
- Regelmässige Backups erstellen (Cloud oder PC)

B. Anwendungen (e-Banking):

- Nicht in öffentlichen Netzwerken oder auf öffentlichen Geräten benutzen
  Achtung: **Phishing** (Bankdaten abfangen, «fischen»)
- Link eintippen und beachten, dass man auf einer Seite mit https:// surft
- Zwei-Faktor-Authentifizierung verwenden (SMS-Code, FotoTAN, Fingerabdruck…)
- Verweildauer auf der Bankseite kurz halten
- Am Ende sauber abmelden (Button)
- Chronik/Verlauf löschen

B. Anwendungen (Online-Shopping):

- Nicht in öffentlichen Netzwerken oder auf öffentlichen Geräten benutzen
- Vergewissern, dass es sich um eine seriöse, bekannte Firma handelt (googeln), besonders tiefe Preise bei unbekannten Anbietern sind oft Lockvogelangebote.
- Bewertungen im Internet sind oft manipuliert oder sogar Fakes.
- Vorsicht bei Auslandbestellungen (z.T. horrende Zollgebühren!)
- Zurückhaltung bei Bezahlung mit Kreditkarte/Vorauskasse
- Ev. Ist die Eröffnung eines Kundenkontos von Vorteil (Bestellungsverlauf)
- www.toppreise.ch zeigt besonders günstige Angebote. (Preisalarm! Sich per Mail informieren lassen, wenn ein angestrebter Preis erreicht wird)

B. Anwendungen (e-Mail):

- Nicht in ungesicherten Netzwerken oder auf öffentlichen Geräten benutzen (Hotels, Flughäfen, etc.)
- E-Mails haben etwa die gleiche Vertraulichkeitsstufe wie eine Ansichtskarte! Heikle Daten gehören nicht in Mails. Senden Sie ein verschlüsseltes Pdf-Dokument!
- Regelmässig Passwörter ändern. Bei Melani überprüfen, ob die Mailadresse gehackt wurde.
  https://www.ibarry.ch/de/sicherheits-checks/
- Unbekannte Mails löschen, keine Anhänge öffnen
- Banken verlangen nie per Mail, dass Kontoangaben gecheckt werden müssen oder dass ein Konto gesperrt wurde!! Die Hacker versuchen an Bankdaten zu gelangen.
- Fakemails verlangen oft rel. kleine Beträge für z.B. die Zustellung von Postpaketen (€ 2.99 oder ähnlich) Der Auftritt wirkt echt und professionell, Adresse «kryptisch"
- Auf Drohmails von Anwälten, Inkassobüros usw. nicht eingehen/nicht antworten, ev. Polizei zuziehen.
- Gerne wird auch damit gedroht, dass bei Nichtbezahlen eines Betrags, Daten und intime Bilder an alle meine Mailadressen (Kontakte) geschickt werden. Der Absender behauptet, die Kontrolle über mein E-Mailkonto zu haben! (nicht reagieren, ev. Passwort ändern!)
- Unerwünschte Mails in Spamordner verschieben. So besteht die Chance, dass gleiche Mails beim nächsten Mal als Spam erkannt werden. Spamordner regelmässig löschen.
- Wird ein privates Mailkonto gehackt, wird ev. ein Massenmail an meine Kontakte geschickt, welches vorgaukelt, ich sei in Not und würde dringend Bargeld benötigen.
- Mailadressen nicht auf Webseiten angeben. Alternative Mailadresse einrichten.
- Massenmails an sich selbst (mit Adressen im BCC) versenden (Persönlichkeitsschutz)

B. Anwendungen (WhatsApp, ähnliches gilt für SMS):

- Beliebt für Chats, Videoübertragung, Bilder, kostenlose Telefonie
- Viele Nutzer misstrauen WhatsApp, da sich die Datenserver in den USA befinden. Die Sicherheitsrichtlinien sind weniger streng als in Europa, zudem ist WhatsApp mit Facebook verbandelt und die Sperrung von persönlichen Daten ist nicht gewährleistet.
- Über WhatsApp werden oft Malware, unseriöse Kettenbriefe, Cyberkriminalität («Ihr WhatsApp- Abo läuft ab – jetzt hier klicken» – Abokosten CHF 5.--/Monat))
- Unter Jugendlichen ist WhatsApp berüchtigt für Cybermobbing.
- Angesichts dieser Gefahren wechseln immer mehr User zu Threema (Schweizer Unternehmen, besserer Datenschutz, ähnliche Funktionen)

B. Anwendungen (Telefon):

- Durch die Verbindung von Telefonie und Internet ist es möglich, dass Hacker irgendwelche Telefonnummern generieren und uns damit anrufen.
- Beliebt sind Anrufe unter der Nummer 117 (Polizei). Damit gaukelt der Anrufer vor, er möchte mich vor einer kriminellen Tat schützen. Er gibt z.B. vor, mir grösstmöglichen Schutz zu bieten (Verwahrung von Geld, Wertgegenständen, usw.)
- Bei Werbeangeboten tappt man häufig in eine teure Abofalle. Angebote immer zuerst prüfen, keine raschen Zusagen…
- Mit dem «Enkeltrick» wollen Kriminelle an mein Geld kommen. Aufhängen!!
- Ping Call: Eine unbekannte Nummer lässt einmal klingeln und erwartet dann, dass ich zurückrufe. Abhilfe: Unbekannte Tel.-Nummern nicht zurückrufen. Der Anruf kann sonst sehr teuer werden.

B. Anwendungen (Passwörter):

- Jeder Internetuser hat unzählige Passwörter zu verwalten.
- Passwörter sollen stark und möglichst komplex sein. (mind. 8-10 Zeichen, Gross- und Kleinbuchstaben, Zahlen, Sonderzeichen) Sünden: 123456, Namen, qwertz
- Ev. Merksatz für die Bildung eines Passwortes verwenden: Ich mag Pizza seit meiner Jugend vor 30 Jahren (ImPsmJv@30J)
- Für verschiedene Dienste nicht die gleichen Passwörter verwenden.
- Passwörter nicht auf dem PC verwalten oder speichern (Excel- oder Wordlisten).
- Passwörter regelmässig ändern, Hacking prüfen (vgl. Kap. E-Mail)
- Ev. einen Passworttresor verwenden (Liste in einer Anwendung, die nur ein starkes Passwort braucht, z.B. KeePassXC) (kostenlos)

B. Besondere Gefährdungen:

- Darknet: Bereiche ausserhalb des www. können mit speziellen Browsern aufgerufen werden. Bekannt als Tummelplatz für Kriminelle.
- Spyware: Bösartige Software, welche Geräte infiziert, diese ausspioniert und Daten sammelt und weitergibt.
- Trojaner: Werden über Dateien auf den PC eingeschleust und können dann aktiviert werden und Schaden verursachen. Achtung bei Dateien mit *.exe, *.bat, *.docx, *.xlsx
- Viren: Programme mit zerstörerischer Wirkung. Eingeschleust über Dateien, Downloads, etc. (Virenschutzprogramme verwenden!) →täglich ca. 350’000 neue Viren/Varianten
- Würmer: Schadsoftware, welche Sicherheitslücken aufspürt, sich selbst reproduziert und Daten zur Weitergabe sammelt.
- Ransomware: Stellt eine Art digitaler Erpressung dar. Ein Programm greift auf die persönlichen Daten zu und verschlüsselt diese. Um den Zugriff freizuschalten, wird ein Lösegeld verlangt.

C. Kleine Helferlein:

- **Cookies**: Sie sind in der Regel unproblematisch und helfen, bereits einmal aufgerufene Inhalte schneller zu finden. Oft speichern sie Spracheinstellungen und sorgen dafür, dass wir z.B. im Online-Banking angemeldet bleiben. Ebenso können so auch Passwörter gespeichert werden.

- Bei gewissen Anwendungen (z.B. Google, Amazon…) werden aufgerufene Seiten an den Dienst weitergeleitet und mir entsprechende Werbung eingeblendet.
- Cookies können im Browser verwaltet und gelöscht werden. (z.B. z.B. im Firefox-Menü unter ***Einstellungen – Datenschutz und Sicherheit***). Gleichenorts kann eingesehen werden, welche Passwörter auf dem PC gespeichert wurden. Dort können auch Einträge angesehen und gelöscht werden.

Internet – eine tolle Erfindung

C. Nur noch mit Angst ins Internet?

- Das Internet ist und bleibt eine grossartige und nützliche Erfindung!
- Mit einer gewissen Zurückhaltung und einigen wichtigen Sicherheitsvorkehrungen dürfen wir das Internet mit ruhigem Gewissen einsetzen. Als Zielgruppe für Hacker sind wir eher nicht interessant.
- Lieber einen Klick weniger als einen zu viel. Im Zweifelsfalle gibt es auch in Ihrem Freundeskreis Leute, die über grosses Wissen rund um den PC, u.a. verfügen.
- Wegen der Unterschiedlichkeit der Gerätekonfigurationen ist es unmöglich, an dieser Stelle technische Lösungen vorzustellen. Fragen Sie jemanden, der/die in diesen Dingen versiert ist.
- Stellt sich ein ungewöhnliches Ereignis ein, lassen Sie sich von einer Fachperson beraten.