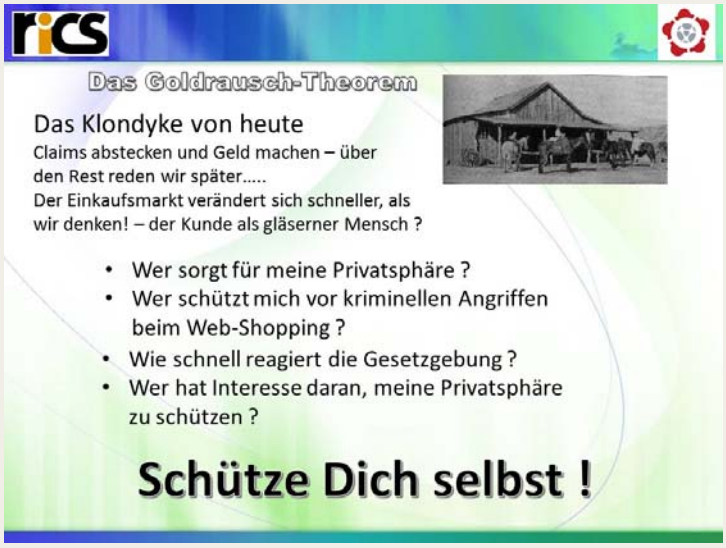
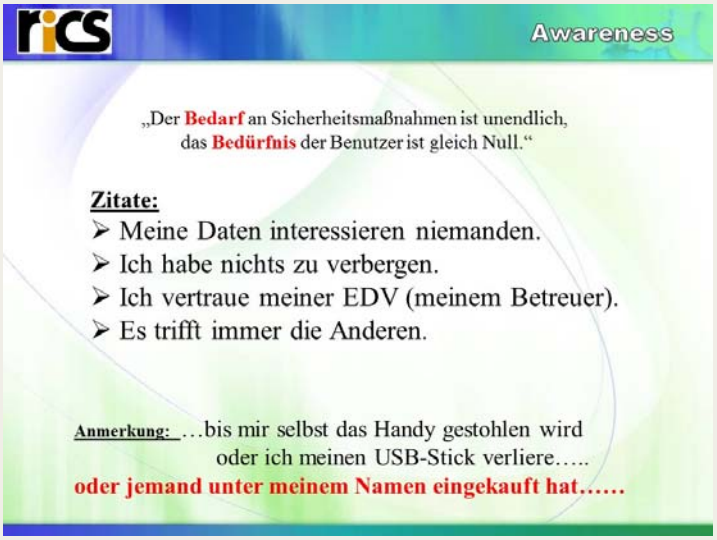
Sicherheit und Risiken beim Onlineshopping

Was ist beim Online-Einkauf zu beachten?

Manfred Wöhrl





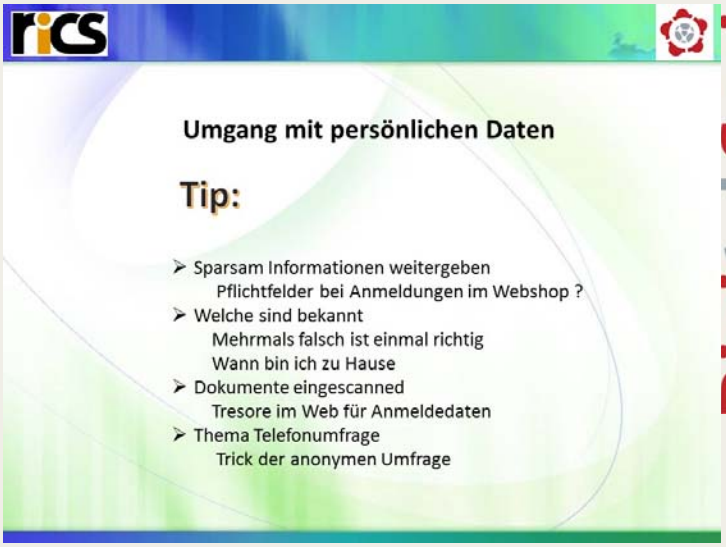
Alles, was wir im täglichen Leben vorfinden, gibt es inzwischen auch im Internet. Dazu gehört leider auch das ungesetzliche Verhalten der Benutzer. Betroffen von der sogenannten „Cyberkriminaltät" sind nicht nur lohnende Ziele für Hacker wie das Pentagon oder große Konzerne sondern zunehmend auch kleinere und mittlere Betriebe und vor allem auch der einzelne Benutzer.

Panama ist überall - wann immer ich Informationen - welcher Art auch immer - im Internet bekannt gebe muss ich damit rechnen, dass meine Daten von Unbefugten benutzt werden. Internet ist ein weltumspannendes Netzwerk und noch so viele Datenschutzgesetze auf nationaler Ebene sind de facto nutzlos. Problematisch ist vor allem, dass eine Datensicherheit sich auch mit komplexen Maßnahmen auf technischer Ebene kaum realisieren lässt, wenn Mitarbeiter von Unternehmen - bei denen die Daten gespeichert sind - teils auch unbewusst „Leaks" verursachen, d.h. persönliche Informationen publik werden. Dabei werden nur einige wenige Vorfälle bekannt und pressewirksam ausgeschlachtet, wie die sogenannten Panamapapiere. In den meisten Fällen werden Vorkommnisse unter den Tisch gekehrt, auch wenn es bereits Gesetze gibt, dass erfolgreiche Angriffe auf persönliche Daten zu veröffentlichen sind. Es betrifft schlussendlich wieder nur Unternehmen, die im „öffentlichen Interesse" tätig sind.

Daher die erste und wichtigste Regel beim Internet Shopping: nur die notwendigsten Daten bekannt geben und vorsichtig bei der Wahl eines Webshops sein! Diese entstehen derzeit in einer großen Zahl neben den renommierten und bekannten wie Amazon. Ohne großen Aufwand kann heute jedermann weltweit seine Produkte zu minimalen Kosten vermarkten und träumt vom großen Geschäft. Wir befinden uns in einer neuen Goldgräberstimmung.

Die größte Gefahr beim Internetkauf ist die Sorglosigkeit ungeübte Benutzer. Es fehlt am Bewusstsein (der sogenannten „Awareness"), was alles passieren kann, bis es oft zu spät ist. Der Mensch ist von Natur aus nicht imstande mit Risiken richtig umzugehen... „Mir wird schon nichts passieren".

In einem einfachen Fall kann meine Sorglosigkeit dazu führen, dass zum Beispiel ein naher Verwandter mein Passwort ausspäht und unter meinem Namen Geschäfte tätigt. Dieser „Identitätsdiebstahl" kann in einem kriminellen Umfeld bis zur Gefährdung meiner Existenz führen. Diesem Punkt hat zum Beispiel das DoD (Department auf Defense) in den USA eine eigene Abteilung gewidmet, an die ich mich im Fall eines Cyberangriffs wenden kann.



Was ist ein sicheres Passwort ?

- **Länge**
  20+
- **Zeichen mischen, Merksatz**
  Ziffern, Buchstaben, Sonderzeichen
- **Keine Verbindung zur Person**
  Geburtstag, Haustier.....
- **Nach Möglichkeit Wechsel zur HW-Lösung**
  „Token"
- **Anti-Lexikon-und-Phrasen-Prüfung**
  „Brute-Force-Checker"
  http://password-checker.online-domain-tools.com/

Wie merke ich mir einen PIN ?

- **Niemals aufschreiben**
  Umfeld Arbeitsplatz....Bankomartkarte
- **Umkehrbare pers. Algorithmen definieren**
  Spiegeln
  3412 → 2143 → 3412
  Positionstausch (z.B. aussen)
  3412 → 2413 → 3412
  Rotieren im Kreis um x Positionen
  (1 x rechts) 3412 → 2341 → 3412 (1 x links)
  9-Komplement
  3412 → 6587 → 3412
- **Algorithmen kombinieren**
  zB. Spiegeln + 9-Komplement 3412 → 2143 → **7856**
- **Coded-PIN 7856 notieren**
  Verwenden auch als Teil eines Passwortes

Security-Forderung

Identifikation des Benutzers durch **Wissen** & **Besitzen**

Ziel: Kundenkarten mit Chip
Device (z.B.: Handy) mit Challenge-Response-Verfahren
RFID-subdermales-Implantat?

http://lines-and-dots.com/bodymod/rfid-implantat/

Die 10 Gebote der Shopauswahl

1. Die Anbieterin/der Anbieter ist eindeutig durch Firmenname, Anschrift, Telefonnummer, E-Mail-Adresse, Nennung einer Kontaktperson und Firmenbuchnummer zu identifizieren.
2. Die Anbieterin/der Anbieter stellt leicht zugängliche und transparente Vertragsbedingungen für das Online-Shopping bereit.
3. Die Leistungsmerkmale der angebotenen Produkte und die Garantiebedingungen sind genau und übersichtlich dargestellt.
4. Der Produktpreis enthält – einzeln aufgelistet – sämtliche Zusatzkosten für Lieferung, Verpackung, bestimmte Zahlungsformen etc.
5. Eine technisch sichere, für die Konsumentin/den Konsumenten nachvollziehbare Zahlungsmöglichkeit ist gewährleistet

Quelle: https://www.help.gv.at/

Conclusio

Brave new world.

Vom Einkaufen zum Eye-Shopping

→ das Lusterlebnis "Einkaufen" wird auf Gustier-Ausflüge reduziert

Die Vereinsamung ist vorprogrammiert

→ auch das Eye-Shopping wird zum virtuellen Einkaufsspaziergang im Netz mit Google-Brille, Augmented Reality & Cyber-Gloves

...wer entscheidet, welche Daten ich sehe ?

Die 10 Gebote der Shopauswahl

6. Jede Bestellung wird von der Anbieterin/dem Anbieter nochmals per E-Mail bestätigt
7. Ein Rücktritts- und Rückgaberecht wird der Konsumentin/dem Konsumenten ausdrücklich zugestanden und die Bedingungen dafür werden genau erläutert
8. Die voraussichtliche Lieferzeit ist exakt angegeben
9. Die Anbieterin/der Anbieter verpflichtet sich, keine Kundendaten an Dritte weiterzugeben
10. Angebote, Produktbeschreibungen und Support erfolgen durchgängig in der jeweiligen Landessprache der Anbieterin/des Anbieters bzw. in der Sprache, in der die Bestellung abgewickelt wird

Quelle: https://www.help.gv.at/

Conclusio

Brave new world.

Nach einem Einkauf über ein Webshop wird die Lieferung erfolgen

- durch Dienstleister
- in Abholcontainer
- in den Kofferraum meines Autos
- durch Drohnen
- durch autonome Roboter-Fahrzeuge
- Downloads eines Konfigurationsfiles und Ausgabe des Produktes am 3D-Drucker zu Hausen

Conclusio

Brave new world. 1932

Eine Gesellschaft, in der „Stabilität, Frieden und Freiheit" gewährleistet scheinen.

Mittels mentaler Indoktrinierung bereits der Kleinkinder werden die Menschen in gewisse Gruppen (Kasten) geprägt.

Allen Kasten dieser visionären Gesellschaft gemeinsam ist die Konditionierung auf eine permanente Befriedigung durch Konsum, Sex und die Droge ***Soma***, die den Mitgliedern dieser Gesellschaft das Bedürfnis zum kritischen Denken und Hinterfragen ihrer Weltordnung nimmt.

International muss man leider feststellen, dass die Gesetze den Angriffen meistens hinten nach hinken und vor allem die Zusammenarbeit zwischen den Staaten sehr langsam anläuft. Zumindest auf europäischer Ebene werden schon gemeinsame „Task-Forces“ zur Abwehr von Cyberattacken gebildet.

Neben den bereits geschilderten Problemen bei der Bekanntgabe persönlicher Daten gibt es noch allgemeine Risiken beim Internet Shopping, die vor allem auf altbekannte Probleme bei der Nutzung von Webseiten generell zurückzuführen sind. Dazu gehört vor allem auch die Abwicklung von Zahlungen per Kreditkarte im Web.

Es soll nicht unerwähnt bleiben, dass Webshop-Betreibern natürlich bekannt ist, dass manche ihrer Kunden teilweise unwichtige Daten eingeben, um ihre Anonymität zu bewahren. In Kombination mit einer freien E-Mail-Adresse ist das im Normalfall recht wirksam. Es hat sich aber nun gezeigt, dass es statistische Modelle gibt - wenn ein Benutzer mehrmals falsche Daten eingibt ein Webshopbetreiber statistisch doch gewisse Rückschlüsse auf den Kunden ziehen kann. Speziell mit zusätzlichen Methoden wie Telefonumfragen können Benutzerprofile über ein Kaufverhalten aber auch andere persönliche Daten erstellt werden.

Ein weiteres Problem bei Benutzung verschiedener Webshops ist die Kombination Benutzername-Passwort-PIN. Einerseits sollte diese aus Sicherheitsgründen bei jeder Benutzung auf einer Webseite unterschiedlich sein, gleichzeitig muss man sich diese Kombination merken und sollte sie keinesfalls aufschreiben.

Es gibt einfache Methoden dem Dilemma der sicheren Passwortgestaltung ohne aufzuschreiben zu entgehen, indem man - jeder für sich selbst - Regeln aufstellt, nach denen Passwörter - als Kombination von Buchstaben und Ziffern – generiert. Gedächtnisstützen dafür kann man durchaus schriftlich festhalten. Im einfachsten Fall kann ich bei einem PIN, zum Beispiel 1234, die äußeren Ziffern tauschen und diese Zahl (4231) notieren. Wenn ich den echten PIN benötige brauche ich nur meine Notiz zurate ziehen und wieder die beiden äußeren Ziffern tauschen. Nachdem diese Vorschrift zu einfach ist, kann ich auch noch andere Algorithmen zurate ziehen, wenn diese ebenfalls „symmetrisch“ sind. Dazu gehört vor allem die einfache Regel „ergänze jede Ziffer auf neun“ (…sogenanntes 9-er-Komplement) - sehr einfach und umkehrbar! Wenn ich jetzt die hier bereits erwähnten zwei Regeln kombiniere wird mein PIN für einen unbedarften Angreifer kaum erkennbar sein. Mit ein wenig Übung kann man damit in einer Kombination von einfachen merkbaren Regeln eine Vielzahl von unterschiedlichen Passwörtern und Pins verwenden und auch notieren.

Manfred Wöhrl
Beirat bei Digital Society

Follow me

Gerichtlich beeideter und zertifizierter Sachverständiger; seit mehr als 30 Jahren im Bereich der IT mit den Spezialgebieten Innovative Technologien (derzeitiger Schwerpunkt Digital Signage) und IT-Security tätig; war Gründer und Leiter der staatlichen Versuchsanstalt für Datenverarbeitung an der HTL-Spengergasse,Lehrbeauftragter an der Fachhochschule Krems, sowie Lektor an der Universität Wien, der Donauuniversität und der Wirtschaftsuniversität Wien.