„DigitalKompass -
Sicherheit im Netz:
es geht nicht ohne Passwortsicherheit“

Andrea 'Princess' Wardzichowski
Chaos Computer Club Stuttgart e.V.

http://www.cccs.de/
princess@cccs.de

Ich freue mich sehr über die Einladung diese Online-Veranstaltung.

Normalerweise stelle ich mich und den CCCS kurz vor, aufgrund der Zeitvorgaben entfällt dies heute, in der Kursunterlage finden sich aber diese beiden Folien zum Nachlesen.

Mein Vortrag beginnt mit meinem Nickname. Nur durch dessen (Mit-)Verwendung kann ich andeuten, daß ich privat unterwegs bin.

Über den CCCS / über mich

Über den CCCS:

Seit Sommer 2001 Treffen
Seit Oktober 2003/4 monatliche Vortragsreihe
Spaß am Gerät, aber auch Gefahren beim bedenkenlosen Einsatz von Technik

Über mich:

Seit November 1990 im Netz aktiv
(Mail, News, IRC, Relay Parties, CCC)
Heute: CCCS e.V. (Presse), Haecksen, querulantin.de, Herbstakademie der Alumni der dt. Studienstiftung 2019, XPDays Germany 2019

In vielen großen und inzwischen auch in vielen kleinen Städten gibt es sog. Chaostreffs, die im Sinne des CCC e.V. agieren, der 1986 in Hamburg gegründet wurde.

Ich selber bin auch schon sehr lange im Netz unterwegs und habe meine Homepage aufgebaut, damit man meine aktuellen Veröffentlichungen und Vorträge eher findet, als meine Jugendsünden aus Usenet-Zeiten.

Desweiteren pflege ich selber eine gewisse Paranoia und man findet hoffentlich nur wenige Bilder im Netz, dafür aber meine Veröffentlichungen, nicht jedoch Telefonnummern und meine Wohnadresse.

Man möchte weder, daß die eigenen „Fans“, noch die Menschen, die einen nicht mögen ungefragt vor der eigenen Haustür auftauchen.

Daher drehen sich die meisten meiner Vorträge um den **Datenschutz**, aber auch andere Themen sind spannend!

Eine kurze Agenda

- Passwortsicherheit
- Formulare online und offline
- Digitaler Nachlaß

In nur 20 Minuten wichtige Aspekte der Datensicherheit und des Datenschutzes aufzuzeigen ist eine Herausforderung.

Zwingend notwendig sind aber in JEDEM Fall sichere Passworte.

Desweiteren sollte man selber wachsam bleiben, wieviele Daten man auch auf Anfrage (Formulare) von sich preisgibt.

Gerade für Senioren ist es wichtig, sich mit seinem digitalen Nachlaß zu befassen und was mit Konten, Profilen und Veröffentlichungen passieren soll.

Passwortsicherheit

- Die Grundlage für jedwede Absicherung
- **Niemals ein Passwort an zwei Stellen** verwenden => es wird komplex. Lösung:
- **Passwortsafe**, z.B. keepassx
  Masterpasswort gut verwahren
- **Passwortsystem** mit Gedichten oder Liedern:
  FidEsdF,aLg.
  Ergänzt um 2 Zeichen pro Webseite/Versender
- Wo möglich: **2-Faktor-Authentifizierung**
  (wie bei PIN und TAN beim Banking)

Ein Masterpasswort sollte am besten aus einem ganzen Satz bestehen. Man spricht hier auch oft von einer Passphrase.

Sichere Passworte sollten heute mindestens 12 Stellen haben. Verwendet werden sollte Groß- und Kleinschreibung, Ziffern und die Zeichen . , $! (Punkt, Komma, Dollar, Ausrufezeichen).

Grundlage bildet ein Gedicht oder eine Liedzeile, wie oben werden die Anfangsbuchstaben genommen:
“Festgemauert in der Erden steht die Form, aus Lehm gebrannt.“
Zu dieser Grundlage, die persönlich ist und die man sich gut merken kann, ergänzt man vorne oder hinten 2 Zeichen für den jeweiligen Anbieter, also z.B. AZ für Amazon oder OT für den OTTO Versand usw.
Aus „ein“ könnte die Ziffer 1 werden, aus „to“, „too“, „two“ die Ziffer 2, aus der Silbe „eight“, „late“ die Ziffer 8, bzw. l8.

Viele Versandhändler bieten inzwischen auf eine 2-Faktor-Authentifizierung an, diese muss oft separat eingeschaltet bzw. angefordert werden und bietet mehr Sicherheit.

SingleSignOn

- Im beruflichen Kontext GOLD wert
- Im privaten: Tun Sie es nicht:
  - Mit facebook einloggen
  - Mit Google einloggen
  - Mit Apple einloggen
  - Mit Ebay einloggen
- Ungute Verbindung zwischen unterschiedlichen Unternehmen, Daten besser streng separieren!

Viele Plattformen bieten inzwischen an, sich gar keinen neues Konto (Login ist ja meist die Mailadresse) anzulegen, sondern sich mit einem bestehenden Konto wie facebook, google, apple, Ebay einzuloggen. Im beruflichen Rahmen ist dies angesagt, vor allem weil hier der Anbieter nur einer ist, nämlich die Firma/der Arbeitgeber. Im Privaten aber können wir von so einer Verbindung nur abraten, es entsteht eine ungute Verbindung von Firmen, die sonst nichts miteinander zu tun haben und wir wissen nicht, welche personenbezogenen Daten in den USA zusammengeführt werden, denn dort gilt die EU-DSGVO nicht!

Es gilt: separate Passworte verwenden!

Formulare online und offline

- Wir sind so ordentlich, immer **alles** akkurat auszufüllen.
  Es gilt aber: Datensparsamkeit!
  Z.B. muss die **Telefonnummer meist nicht** zwingend bei Bestellvorgängen angegeben werden.
- **Aktuell: Restaurantdaten** wg. Corona:
  es reicht Name und eine der drei Angaben:
  Wohnadresse, Telefonnummer, Mailadresse

Seien wir ehrlich: „wir Deutschen“ sind schon wahnsinnig ordentlich, was das Ausfüllen von Formularen angeht. Das wird leider von vielen Anbietern ausgenutzt.

Bei Versandhändlern ist die Angabe der Telefonnummer oft freiwillig, wird aber dennoch oft angegeben. Manche Webformulare lassen leere Felder nicht zu. Hier kann man sich aber oft mit „23456789“ oder „Musterstrasse“ behelfen.

Achten Sie auf Ihre Daten und geben Sie nur das für den Vorgang notwendigste an! Sie können zwar Werbeanrufen immer widersprechen, diese sind aber auch beim ersten Mal schon nervig.

Aktuell: in der Verordnung, die die Erhebung von Gastdaten in Restaurants regelt, ist nur sehr unklar beschrieben, ob alle Gäste am Tisch ihre Daten hinterlassen müssen oder nur einer oder nur einer je anwesendem Haushalt. Ebenso ist nicht geregelt, ob man Wohnadresse, Mailadresse und Telefonnummer angeben muss. Es reicht idR. EINE dieser Angaben, um Kontakt herzustellen. Ich empfehle Mail. Geben Sie Ihre Daten nur auf separaten Blättern an, nicht in Listen, wo jeder Gast Ihre Daten erspähen kann.

Häufig nicht bekannt: wer an Preisausschreiben teilnimmt, stimmt idR. zu, dass seine/ihre Daten weiterverkauft werden und erhält dann oft unerwünschte Werbung.

Gedächtnistraining

- Nach Möglichkeit keine Passworte im Browser oder in anderen Anwendungen abspeichern, statt dessen: Gedächtnistraining :)
- Wenn dennoch Passworte abgespeichert werden, das Addon Masterpassword im **firefox** verwenden, um alle Passworte zu schützen. Das Masterpasswort nicht zu kurz wählen!

  Der chrome/chromium Browser kann leider kein Masterpassword.

Kommt ein Gerät abhanden und knackt jemand Ihr Login-Passwort, kann er/sie beliebig viel Schaden anrichten, wenn alle Passworte für Social Media und Versandhändler im Browser gespeichert sind. Bestellorgien und Beleidigungen in Ihrem Namen können die Folge sein.

Daher die Passworte im Browser schützen oder noch besser: auswendig lernen mit dem erklärten Konzept.

Digitaler Nachlass

- Denkt man nicht gern drüber nach
- Einige Anbieter (facebook) setzen Profile in einen Gedenkstatus, Erben können dies dann nicht mehr löschen
- Passworte in einem versiegelten Umschlag hinterlegen, z.B. zusammen mit der Patientenverfügung
- Einer Person des Vertrauens sagen, dass der Umschlag existiert
- Angaben, was mit Konten und Profilen passieren soll

Regeln Sie, was von Ihren Veröffentlichungen übrig bleiben soll, auch wenn es schwerfällt.

Veranstaltungstips

Cryptoparty: fallen bis auf weiteres leider aus

Regelmäßige **Vorträge**: idR. 2. Donnerstag im Monat, Stadtbibliothek, 19:30
Donnerstag, 8.10.2020: Die Datenbanken der Polizei
Anmeldung erforderlich, Audio wird gestreamt

PDF mit Notizen zu diesem Vortrag unter

http://www.querulantin.de/Vortraege/

Derzeit können nicht alle unsere Veranstaltungen wie gewohnt stattfinden, aber wir beraten gern im Rahmen unserer Möglichkeiten.

Fragen / Diskussion

?

?

?