Ideen und Konzepte der Informatik

Sicherheit und Privatheit

Praktische Tipps

Kurt Mehlhorn

Überblick

- Sicherheit:
  - Absperren von Geräten
  - Back-Ups (Datensicherung)
  - Passwörter
  - Soziale Attacken, Phishing,
- Privatheit
- Ich bin nicht paranoid bezüglich Sicherheit und Privatheit, aber vorsichtig. Ich werde immer vorsichtiger (Missbrauch einer Kreditkarte, Einbruch in mein Opodokonto, Bewusstheit meiner Abhängigkeit).

Sicherheit

Eine Kette ist nur so stark wie ihr schwächstes Glied.

Passwörter I

- Für meine Anwendungen (Banken, Internetstores, Zeitungen, GPSies, Datenbank des Fachbereichs, ….) habe ich Passworte unterschiedlicher Qualität benutzt. Für wichtige Dienste (hoher Schaden) jeweils ein eigenes Passwort. Für unwichtige Dienste (kleiner Schaden) einige wenige Passworte. Alle Passworte sind 8 Zeichen oder länger. Wichtige Passworte sind 12 und mehr Zeichen.

- Alle neuen Passworte sind zufällige Worte aus 16 Buchstaben. Die alten stelle ich gerade um. Ich bin mir nicht mehr sicher, ob die Unterscheidung wichtig/unwichtig sinnvoll ist.

- Muss mehrmals am Tag im Passwortsafe nachschauen.

- https://sec.hpi.de/ilc/search?lang=de, Liste von kompromitierten Passwörtern.

Passwörter II

- Ich benutze einen Passwortsafe (Keepassx), den ich zwischen meinen verschiedenen Geräten automatisch synchronisiere.
- Dafür benutze ich ein langes Passwort (14 Zeichen).
- Das Passwort ist im Safe des Instituts hinterlegt.
- Den Passwortsafe in meinem Browser benutze ich nur für unwichtige Passworte.
- Zweifaktorauthorisierung, wenn immer möglich.

Absperren von Geräten

- Meine Geräte werden gesperrt, wenn ich sie 60 Sekunden nicht benutze
- Iphone, Ipad: 4stelliger Code, 3mal falscher Code führt zum Löschen aller Inhalte
- Notebook: Passwort mit 12 Zeichen
- WLAN zu Hause: Passwort mit 12 Zeichen

Datensicherung (Back-Up)

- Machen sie regelmäßig eine Datensicherung auf ein Medium, das getrennt von ihrem Rechner ist.
- KM in der Arbeit: automatisch, wenn immer ich mehrere Stunden im Büro bin.
- KM zu Hause: wöchentlich oder öfter bei Bedarf auf Festplatte, die ich nur dazu mit dem Rechner verbinde.
- Telefon und Tablett: regelmäßig in der Cloud´.

Weitere Maßnahmen

- HTTPS Everywhere
- Vorsicht beim Öffnen von Attachments und Verfolgen von Links. Besondere Vorsicht, wenn Absender oder Webseite unbekannt. Phishing Angriff.
- Aktueller Virenscanner, aktuelle Version des Betriebssystems und aller Programme (automatische Updates).
- Uni Bielefeld: 10 goldene Regeln für Computersicherheit.

Privatheit

Im Internet scheint vieles umsonst (Suchmaschinen, soziale Netzwerke, Streamingdienste). Es gibt aber wenig umsonst im Internet. In der Regel zahlen wir

- mit Daten, die eine gezieltere Werbung erlauben oder
- mit erhöhter Verwundbarkeit/Beeinflussbarkeit

Das Internet vergisst nicht. Was wir heute lustig finden, finden wir in 10 Jahren vielleicht peinlich.

Der digitale Fußabdruck verrät viel

We show that easily accessible digital records of behavior, Facebook Likes, can be used to automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender. The analysis presented is based on a data set of over 58,000 volunteers who provided their Facebook Likes, detailed demographic profiles, and the results of several psychometric tests. The derived model correctly discriminates between homosexual and heterosexual men in 88% of cases, African Americans and Caucasian Americans in 95% of cases, and between Democrat and Republican in 85% of cases. For the personality trait “Openness,” prediction accuracy is close to the test–retest accuracy of a standard personality test. We give examples of associations between attributes and Likes and discuss implications for online personalization and privacy.

Kosinski et al: Private traits and attributes are predictable from digital records of human behavior, PNAS 2013

Dienste

- Ich benutze Browser, Google, WhatsApp, email (immer weniger gmail), Dropbox.
- Browser: maximale Sicherheits- und Privatheitseinstellungen.
- Browsererweiterungen Adblock, HTTPS Everywhere, Privacy Badger (protection against trackers), Google Analytics Opt-Out, NoScript.
- Google Privatsphärecheck: habe die Rechte von Google zur Auswertung meines Browserverhaltens weit möglichst eingeschränkt.

Email

- Ich signiere meine Emails. (Elektronische Unterschrift)
- Manche Emails verschlüssele ich. Wenn immer der Empfänger es so eingerichtet hat.

Zusammenfassung

- Benutzen Sie die Segnungen des Internets bewusst.
- Treffen Sie Vorkehrungen gegen Missbrauch.
- Missbrauch bedeutet Ärger, Verlust von Zeit und/oder Geld, Ansehen, ….