„Sicherheit für Netze, Daten, Informationen“

Andrea 'Princess' Wardzichowski

Chaos Computer Club Stuttgart e.V.

http://www.cccs.de/

princess@bofh.de

Themenabend des Verbandes Freier Lektorinnen und Lektoren

25.10.2012, 19:30 Uhr
Jugendhaus Mitte, 2. OG (kleiner Saal)

Über den CCCS / über mich

Über den CCCS:

- seit Sommer 2001 Treffen
- seit Oktober 2003 monatliche Vortragsreihe
- Spaß am Gerät, aber auch: Gefahren durch den bedenkenlosen Einsatz von Technik

Über mich:

- seit November 1990 im Netz aktiv (IRC, Mail, News, Relay Parties, CCC)
- heute: CCCS e.V. (Presse), Haecksen, querulantin.de

Der Chaos Computer Club Stuttgart e.V. ist ein „Ableger“ des CCC e.V. aus Hamburg und agiert in seinem Sinne. Jeder Club in den diversen Städten ist verschieden, je nachdem, welche Menschen beteiligt sind.

Ich selber (Princess) bewegte mich schon vor der Entstehung des WWW im Internet und habe daher einige Entwicklungen sehr genau miterlebt.

Dazu gehört die technische Entwicklung ebenso wie zwischenmenschliches und politisches.

Welche Daten werden im richtigen Leben gesammelt?

Dieses „Minimalset“ an Daten ist eigentlich immer vorhanden, auch ohne Netz:

- Einwohnermeldeamt
- Telekommunikationsanbieter
- Bank

Optional, aber praktisch:

- Versandhändler
- Kundenkarten
- ....

Bevor man sich damit befasst, wo Daten im Netz gesammelt werden, muß man sich klarmachen, wo in einem „normalen“ Leben heute in Deutschland überhaupt Daten anfallen.

Um manches (s.o.) kommt man nicht herum, idR. sind diese Daten aber auch nicht öffentlich und meist gut geschützt.

Anders verhält es sich bei den vielen kleinen Dingen, die das Leben leichter machen (können).

Kundenkarten: Verkauf von Einkaufsdaten gegen „Punkte“

Wer sammelt welche personenbezogenen Daten wozu im Netz?

- Newsletterbetreiber (kommerziell, politisch, Hobbybezogen....)
- Forenbetreiber aller Art, wenn Sie an Diskussionen teilnehmen (private Sites, Zeitungen....)
- Alle kommerziellen Händler (Versand)
- Communities, Twitter

=> kurz: immer wenn Sie aktiv werden und nicht „nur-Leser“ sind, werden Daten gespeichert

Wenn Sie nur eine Webseite aufrufen, werden zwar IP-Adresse, Datum, Zeit, evtl. auch ihr Browser mitgeloggt, dies sind aber noch keine personenbezogenen Daten.

Zwar kann aus IP und Zeit bei ihrem Provider Ihr Vertrag ermittelt werden, dies aber nur, wenn eine Anzeige vorliegt.

Nehmen Sie hingegen aktiv am Netz teil, dann muß mindestens ein Pseudonym, oft auch eine Mailadresse angegeben werden.

Legen Sie sich extra Wegwerf-Mailadressen für Shopping und Communities zu, damit Ihre private Adresse nicht zugemüllt wird.

Welche neuen Trends bei der Speicherung von großen Datenmengen gibt es?

In **.de** gilt generell das Bundesdatenschutzgesetz:

- personenbezogene Daten dürfen nur **zweckggebunden** und **datensparsam** erhoben werden
- jede speichernde Stelle ist **auskunftspflichtig**!

Problem: Speicherung außerhalb von .de (facebook)

Technisch gesehen gibt es heute kaum Grenzen, die Datenträger sind uferlos groß. Die Daten der Volkszählung aus den 80ern passen auf einen USB-Stick!

Ob man hier von „Trends“ sprechen kann, möchte ich nicht einmal behaupten. Fest steht aber, daß alles, was öffentlich im Internet zugänglich gemacht wird, auf ewig im Netz gespeichert bleibt.

Für personenbezogene Daten jedoch gilt, daß diese nur zweckgebunden und sparsam und unter Schutzmaßnahmen gespeichert werden dürfen. DIes betrifft z.B. auch Mitgliederdatenbanken von Vereinen.

Jede Stelle (z.B. auch die Schufa) ist verpflichtet, einmal im Jahr kostenlos Auskunft zu geben, welche Daten gespeichert sind.

Wie gefährlich ist Skype?

- Skype Nutzungsbedingungen:
  http://www.skype.com/intl/de/legal/terms/tou/
- Bei Skype wird der eigene Rechner als Resource genutzt
- je länger man eingeloggt ist, desto mehr Gespräche laufen über die eigene Leitung und den eigenen Rechner
- Gespräche können von Behörden belauscht werden

Skype ist zunächst einmal proprietäre Software, d.h. der Quellcode ist nicht offengelegt. Welche Funktionalität Skype hat, und ob die Betreiber alles mitlauschen, kann nicht nachvollzogen werden. Nimmt man an Skype teil, stellt man seinen Rechner und seine Leitung zur Verfügung. Skype ist ebenso bekannt dafür, daß es jede nur erdenklichen Tricks benutzt, um bestehende Firewalls auszuhebeln.

Wenn Skype notwendig ist, nur sehr sparsam einsetzen und anschließend wieder ausloggen.

..alles in die Cloud?

+ Zugriff auf Daten von „überall“
  Smartphone, Tablet, PC
+ Backup beim Anbieter (hoffentlich)

- Daten lagern extern
- wie vertrauenswürdig ist der Anbieter
- was tun bei Netzstörungen, kein Zugriff auf (Arbeits-)Daten

Populär ist heute auch das Auslagern von Daten in die „Cloud“. Hierbei stellt ein Anbieter große Mengen Plattenplatz und einen guten Netzanschluß zur Verfügung. Ein Foto beispielsweise, vom Smartphone in die Cloud geladen, kann sogleich von anderen Rechnern aufgerufen werden.

Es stellt sich hier aber auch die Frage der Vertrauenswürdigkeit des Anbieters und Regelung der Zugriffsrechte.

Ferner muß geprüft werden, was bei Netzausfall geschieht, die Daten sind dann nicht zugreifbar.

Technische Maßnahmen

- Virenschutz (z.B. Microsoft Security Essentials, Avira)
- Firewall (bei Windows 7 inklusive)
- regelmäßiges Update
- regelmäßiges Backup
- restriktive Dateifreigaben
- nicht Outlook Express für Mail nutzen (sondern z.B. Thunderbird)
- personenbezogene Daten nur mit **https** in Webseiten eingeben!

Seinen Rechner zu schützen, ist leider keine einmalige Aufgabe, sondern ein Prozeß.

Das meiste muss regelmäßig erfolgen, gerade wenn man als Freiberufler den Rechner als Werkzeug nutzt und dieser nicht ausfallen darf. Backup kann z.B. auf eine USB-Festplatte gemacht werden, Archivierung auf CD/DVD. Wichtig ist, nicht immer nur die letzte Version eines Dokuments zu überschreiben, es sollten Versionen jedes Tages rückholbar sein.

Auch sollte überdacht werden, ob der Rechner und das DSL den ganzen Tag laufen müssen (breiteres Angriffziel ,wenn den ganzen Tag die gleiche IP verwendet wird) oder eben nur nach Bedarf (-> Strom!).

..nur allzu menschliches

„Soziale Probleme lassen sich nicht mit Technik lösen“

- nicht auf alles klicken was nicht bei “drei“ auf dem Baum ist.
- Wenn man noch nie Mail von seiner Bank bekommen hat, wieso sollten die plötzlich mit Newslettern anfangen?
- Links LESEN

Man sollte beim Nutzen von Rechner, Internet und Navi (!) den gesunden Menschenverstand eingeschaltet lassen!

Lesen Sie Mails und Links genau! Wenn Ihre Bank mit Ihnen bisher nie per Mail kommuniziert hat, wird sie dies von sich aus nicht plötzlich tun!

Klicken Sie nicht auf jeden Link, der Ihnen unterkommt.

Erledigen Sie wichtige Dinge nach wie vor auf Papier.

Wie kann ich mich vor Hackern schützen?

Zunächst: private Daten eines einzelnen Menschen sind selten das Ziel!

- **Bots:** tun ihren Daten nichts, nutzen „nur“ ihren Rechner um Botnetze zu steuern
- **Trojaner** zerstören Daten (bei Verdacht: Rechner neu aufsetzen, Backup einspielen)
- immer selber **datensparsam** agieren (wenn ein kostenloser Download angeboten wird, warum dann Name und Adresse angeben?)

IdR. wird Ihr privater Rechner seltenst Ziel eines Hackerangriffs sein. Angriffe richten sich gegen Einrichtungen, wo es um Patente und Wirtschaftsgüter geht.

Ärgerlich ist es trotzdem wenn man sich Bots oder Trojaner einfängt. Sollten Zweifel bestehen, setzen Sie das System wieder neu auf und holen Ihre Nutzdaten (E-Mails, Aufträge, Dokumente, Fotos...) aus dem Backup. Dies kann man üben und ist auch nach ein paar Durchgängen nicht mehr so schrecklich.

Geben Sie selber auch nur soviele Daten an, wie nötig. Versandhändler bestehen zwar zuweilen auf eine Telefonnummer, das muss aber nicht ihre richtige sein.

Der Rechner als Werkzeug für das tägliche Einkommen

- Familienrechner von Arbeitsrechner trennen (evtl. sogar steuerlich absetzbar)
- Datentransfer per USB-Stick
- Rechner nur für Updates ans Netz hängen, Mail und surfen vom Familienrechner aus

Wenn Sie freiberuflich und selbstständig tätig sind, dann ist der Ausfall des Arbeitsmittels immer eine (auch finanzielle) Katastrophe. Eine Idee ist, 2 Rechner im Haushalt vorzuhalten. Oft braucht man in Familien ohnehin einen Rechner für die Hausarbeiten der Kinder. Dieser steht dan ohnehin auch zeitlich nicht immer zum Arbeiten zur Verfügung und wird auch gern verkonfiguriert (auch wenn jeder seinen eigenen Account haben sollte!).

Der Arbeitsrechner sollte einer höheren Sicherheit unterliegen und Backup täglich gemacht werden (USB Platte, CD).

Zum Schluß....

.....haben wir noch Zeit für weitere Fragen!

Heute konnte nur ein kleiner Überblick in die wunderbare Welt der IT und des Netzes gegeben werden.

Aber mit ein paar einfachen Maßnahmen kann man sich gut schützen und dennoch die Welt des Netzes und den Rechner als Werkzeug und Arbeitserleichterung genießen.