Wenn die Villa Ritter zum Hackertreff wird

Jeweils im Juni treffen sich in Biel, in der Villa Ritter Geeks, Nerds, Hacker, Datenreisende, Diskordianer, Chaoten und andere Interessierte aus der ganzen Schweiz und dem nahen Ausland zur „CoSin“, einem technischen und politischen Event mit Workshops, Diskussionsrunden und anderem Inhalt. Der Anlass ist nicht gewinnorientiert und auch sonst eher chaotisch in der Zielsetzung. Wir trafen zwei Aktivisten vom Chaostreff Bern und Chaos Computer Club Schweiz.

Mögt ihr kurz etwas über euch persönlich erzählen? Wer seid ihr, was macht ihr und was ist der Chaos Computer Club (CCC)?

Niklaus Hofer: Im Umfeld des CCC heisse ich „Vimja“. Gleich hier nebenan an der Fachhochschule habe ich bis vor 2 Jahren Informatik studiert. Heute arbeite ich als Informatiker und bin aktiv im Chaos Treff Bern, den ich ursprünglich gegründet habe.

Rexxnor: Nach einer Informatikausbildung studiere ich jetzt hier in Biel. Seit 3 Jahren bin ich im Chaostreff Bern

involviert.

Ist solch ein Engagement üblich für Informatikstudenten; machen das alle?

Rexxnor: Nein, eher wenig, vielleicht kommen so 5-10% überhaupt mal an einen Chaos-Treff. Aber mittlerweile wissen recht viele davon, weil es immer mehr ein Thema wird.

Vimja: In unserem Jahrgang hatten wir ziemlich Glück, dass wir danach in der Vertiefung während 1,5 Jahren etwa 5 oder 6 Leute aus der Klasse waren und das war recht cool…, aber das ist doch eher die Ausnahme.

Der CCC heute ist sehr divers. Es ging nie nur um technische Details, etwa wie man Sicherheitsmechanismen aushebelt, sondern es hat immer auch einen politischen Anteil gehabt. Viele technische Fragen sind heute auch politische Fragen.

Der CCC hat sich immer schon mit Datenschutz befasst, aber heute geht es noch sehr viel weiter. An der CoSin gibt’s z. B. auch „Foodhacking“, Leute, die Glace aus Flüssig-Stickstoff herstellen, oder eine Gruppe, die mit grossen industriellen Waffeleisen Waffeln herstellen kommt… und andere Sachen, die direkt nichts mit Technik zu tun haben. Wenn Du einmal an eine solche Veranstaltung gehst, so ist das der interessante Teil: nicht an Vorträge zu gehen, sondern Leute aus all den Projekten zu treffen und mit ihnen zu reden.

Der CCC hat eine Hackerethik formuliert; worum geht es? (siehe Infokasten auf dieser Seite).

Vimja: Wer – heute noch mehr als früher – in Computersysteme einbrechen und diese manipulieren kann, hat sehr viel Macht. Und mit sehr viel Macht kommt auch immer sehr viel Verantwortung. Ich denke es geht darum, dass man mit dieser Macht vernünftig umgeht und nicht versucht, Dinge kaputt zu machen und Leuten zu schaden, sondern dass man sein Wissen und seine Macht benützt, um die Welt zu verbessern, darauf

hinzuarbeiten, dass unsere Welt ein besserer Ort wird.

Zurück zur CoSin, die jedes Jahr im Juni in der Villa Ritter statfindet. Findet sie immer hier in Biel statt?

Vimja: Ursprünglich war sie nicht in Biel, aber seit 2011 findet sie nun hier statt, noch bevor wir dazugekommen sind. Die Location ist von jemandem organisiert, der in der Villa Zivildienst gemacht hat. Die CoSin selbst ist von einer losen Gruppe aus ganz vielen Leuten organisiert. Die Leute von der Villa sind super Leute die immer gut zu uns geschaut haben. Es ist sehr angenehm dort.

Die CoSin gibt’s jetzt seit knapp über 10 Jahren und sie fand jedes Jahr statt, ausser 2012, weil im 2012 der „Chaos-Treff Basel“, heute der „CCC Basel“, das „Easterhegg“ veranstaltet hat, das ist eine Oster-Konferenz des CCC…

…das ist eine Anspielung auf die „easter eggs“ von google?

Vimja: …es geht wohl schon in diese Richtung…

Rexxnor: …oder um „hacks“…

Vimja: …und damals wurde die CoSin noch vor allem von den Zürchern und Baslern organisiert und die hatten damals wohl einfach keine Zeit, gleich nach der Easterhegg auch noch die CoSin zu organisieren.

Ich bin dann auch gleich nach der „Easterhegg 2013“ dazugestossen und helfe seither mit. Heute ist die Orga (Organisation, Anm. d. Red.) über die ganze Schweiz verteilt.

Dann ist das ja eigentlich genial, wenn wir so einen Anlass direkt vor der Haustüre haben.

Vimja: Ja und wir hatten die letzten drei, vier Jahre auch immer sehr viel Glück mit dem Wetter, wir sind in diesen letzten Jahren stark gewachsen: noch vor 4 Jahren hatten wir vielleicht 50 Teilnehmer und letztes Jahr hatten wir schon

über 120 Teilnehmer und damit ist nun wirklich auch die Kapazitätsgrenze der Villa erreicht.

2019 findet sie nochmals in der Villa statt, danach schauen wir weiter. (siehe Programm, ab ca. Juni, unter: www.cosin.ch).

Weshalb ist das Wetter so wichtig, ihr seid doch drin?

Vimja: Jaa… (lacht), vor der Villa hat's einen grossen Rasenplatz und anfangs Juni, bei schönem Wetter, sassen viele Leute draussen, haben zusammen geplaudert und gegessen. Draussen haben sie auch Glace gemacht.

Rexxnor: Logistisch wäre es schwierig, bei schlechtem Wetter 120 Leute für's Essen reinzubringen und schönes Wetter hat auch den Vorteil, dass die Leute draussen sitzen oder auf der Wiese liegen können, wenn's drin zuwenig Platz zum Schlafen hat.

Vimja: Wir geben uns Mühe zu kochen: es gibt für alle Teilnehmer Frühstück und freitags und samstags auch Abendessen, damit wir zusammen essen können. Sehr cool ist, dass man kein Hotel suchen, sondern direkt vor Ort übernachten kann; man kann sich einfach hier auf den Boden legen. In der letzten Zeit sind vermehrt Leute aus der Bodenseeregion von Deutschland gekommen.Für diese Leute ist das auch ein Kostenfaktor, weil Ferien in der Schweiz immer sehr teuer sind. Bei uns hier können sie billig essen und übernachten.

Auf der CoSin-Website steht: „Da auch in der Schweiz die politische Realität immer mehr von unseren Idealen wie Informationsfreiheit und Schutz der Privatsphäre abweicht, gibt es je länger je mehr auch politischen Inhalt." Könnt ihr etwas dazu sagen? Was ist eure Position?

Oder: wie steht die Schweiz punkto Datensicherheit da?

Vimja: Bis vor ein paar Jahren war die Schweiz punkto

Datensicherheit sehr vorbildlich; sie war wirklich ganz vorne mit dabei. Das war nicht nur für die Bürger und Bürgerinnen der Schweiz von Vorteil, sondern es ist tatsächlich auch wirtschaftlich ein Vorteil, denn es gibt mehrere Unternehmen, welche in die Schweiz gekommen sind und von hier aus Dienste angeboten haben, aus dem Grund, dass die Schweiz einen sehr guten Datenschutz hat und sie das ihren Kunden anbieten können."

Seither gab's sehr unglückliche Entwicklungen, die den Datenschutz in der Schweiz stark geschwächt haben. Stichwort: BÜPF…

Rexxnor: … das Bundesgesetz zur Überwachung von Post- und Fernmeldeverkehr.

Vimja: Auch das Nachrichtendienstgesetz (NDG): es ist verheerend, was dort eingeführt wurde und zuletzt auch das Geldspielgesetz, über welches Netzsperren eingeführt wurden. Ich denke, heute sind wir gegenüber dem EU-Ausland nicht mehr viel weiter, was Datenschutz anbelangt.

In meiner Vorstellung läuft alles über ausländische Server und der NSA fasst alle Daten ab und speichert sie für alle Ewigkeiten?

Rexxnor: Das war einer der grössten Kritikpunkte beim NDG, das unter anderem die Kabelaufklärung eingeführt hat. Kabelaufklärung heisst, dass man bei unverschlüsselterKommunikation jegliche Internetverbindungen ins Ausland auf ihren Inhalt überwachen muss, sofern möglich. Egal, was kommt, es muss einfach gespeichert werden. Das Problem im Internet ist jedoch: man kann sehr schwer nachweisen, ob die Daten nun ins Ausland gegangen sind oder nicht. Datenpakete benötigen dafür nur paar Millisekunden, die Grenzen sind fast ein wenig fliessend. Man könnte sie auch absichtlich umleiten, damit sie zwangsläufig aufgezeichnet werden. Sobald sie an einem abgehörten Knotenpunkt

vorbeikommen, haben sie zumindest die Umstandsdaten, die sogenannten Metadaten.

Vimja: Was machen wir dagegen? Wir sind – gerade gegen solche Gesetze – vorgegangen, in Zusammenarbeit mit anderen Organisationen: der Piratenpartei und der „Digitalen Gesellschaft Schweiz“. Wir haben unter anderem versucht, die Leute auf die Problematik aufmerksam zu machen, aber dann auch mitgeholfen, Referenden gegen diese Gesetze zu organisieren, Unterschriften zu sammeln und im Fall des NDG haben wir uns am Abstimmungskampf beteiligt, um das zu verhindern.

In der Schweiz ist es schon toll und sehr wertvoll, demokratische Mittel zu haben, um wirklich etwas aktiv dagegen machen und sich wehren zu können. Man muss nicht einfach zuschauen, wie alles kaputt gemacht wird und kann nichts dagegen unternehmen.

Wie schützt ihr eure persönlichen Daten?

Rexxnor: Beim Schutz der persönlichen Daten gilt, wie für andere Dinge auch: wenn keine oder kaum Daten vorhanden sind, muss man diese auch nicht speziell schützen. Das heisst: Datenverminderung ist sicher schon mal ein guter Ansatz. Aber für die Daten, die man irgendwo, auch im Internet hat, gilt es Grundregeln zu beachten. Wenn z.B. auf einer Website plötzlich Name, Adresse, Geburtsdatum, lediger Name der Mutter abgefragt werden, dann bin ich zuerst einmal skeptisch und überlege mir, ob ich über diese Site überhaupt etwas kaufen oder machen will, ob das nötig ist, ob ich den Newsletter brauche und dann entscheide ich eigentlich schon im Voraus. Und wenn ich mich beispielsweise irgendwo einschreiben müsste, zwangsläufig, dann schaue ich, dass ich eine separate E-Mailadresse habe, die ich nicht wirklich brauche. Einfach, damit es nicht mit meiner Person zu verbinden ist, oder wenn doch, damit ich wenigstens weiss, woher das kam.

Vimja: Ich denke, der Schutz der persönlichen Daten geschieht

auf sehr vielen Ebenen. Einerseits indem man sich überlegt, wem man überhaupt welche Daten geben will und welche Implikationen das hat.

Durch Mechanismen, wie das neue Datenschutzgesetz der EU, sind Firmen eigentlich dazu gezwungen, den Nutzern mehr Kontrollmöglichkeiten anzubieten. Gerade wenn man heute einen Computer kauft und auf Windows einrichtet, dann ist Windows standardmässig so eingestellt, dass Daten an Microsoft weitergegeben werden. Das Gleiche gilt auch für ein Android-Telefon, das standardmässig sehr viele Daten an Google und so weitergibt. Es macht Sinn, sich einmal hinzusetzen, die Privatsphären-Einstellungen des Betriebssystems zu öffnen und dort reinzuschauen. Schon nur um einen Eindruck zu erhalten: was gibt der Computer eigentlich alles von mir an den Hersteller? Will ich wirklich, dass er das weitergibt? Und dann nimmt man das mal „zack!“ raus. Dies sind recht simple Massnahmen; jeder kann sich mal hinsetzen und sich Gedanken machen.

Und dann halt die Verschlüsselung von allem, was privat bleiben soll. Klar, wenn Du ein Facebook-Posting machst: das soll auch öffentlich sein, das soll jeder lesen können. Aber der Chat mit deiner Freundin oder den Eltern, das sollte vielleicht nicht jeder lesen können und dann ist auf jeden Fall eine Verschlüsselung angesagt.

Immer häufiger gibt es Verschlüsselungssysteme, sei’s für E-Mail oder für Messenger, oder für was auch immer, mit einer gewissen Nutzerfreundlichkeit.

Wenn Du vor ein paar Jahren verschlüsseln wolltest, dann war das eine absolute Katastrophe und du musstest wirklich ein Profi sein, um zu wissen, wie das geht. Aber heute ist es immer mehr als Standard eingebaut und einfach zu bedienen.

Wie verschlüssle ich denn z. B. Whatsapp?

Vimja: Whatsapp ist heute standardmässig end-zu-end

verschlüsselt. Das heisst, es ist wirklich von deinem Gerät bis zum Gerät der Person, mit der du kommunizierst, verschlüsselt. Die Nachricht geht zwar über die Server von Whatsapp, aber Whatsapp sieht nicht, was in dieser Nachricht drin ist.

Die haben keine Hintertürchen?

Vimja: Man nimmt an, dass es keine hat, einfach aufgrund der Herkunft der benützten Technologie.

Es gilt da natürlich zu beachten, dass – obschon du verschlüsselt kommunizierst –trotzdem Metadaten anfallen. Whatsapp sieht, mit wem Du um welche Zeit wieviele Nachrichten schreibst.

Wichtig ist auch zu verstehen, wovor wir uns schützen wollen. Versuche ich mich davor zu schützen, dass Whatsapp diese Nachrichten sieht, oder der Typ, der neben mir im Starbucks sitzt? Gegen diesen Typen ist das bestimmt ein wirksamer Schutz. Aber wenn du dich vor staatlichem Zugriff schützen willst, dann ist das kein wirksamer Schutz. Der amerikanische Staat kann z. B. Whatsapp per richterlichem Beschluss dazu zwingen, eine modifizierte Version der Whatsapp-App zu machen, die per automatischem Update nur auf dein Android-Telefon ausgeliefert wird, spezifisch für dich. So bekommen sie Deine Daten trotzdem. Solche Angriffe hat’s gegeben.

Also: es ist wichtig, dass man sich immer die Überlegung anstellt: vor wem versuche ich mich zu schützen und welche Massnahmen sind dafür genügend oder ungenügend?

Es gibt ja Alternativen wie Threema oder Telegram…

Rexxnor: Das traurige Problem bei Telegram ist: sie behaupten jedes Mal, sie wären sehr sicher. Doch die normalen Chats und die Gruppen-Chats bei Telegram sind eigentlich unverschlüsselt, also im Klartext abgelegt: im Gerät, auf den Servern von Telegram und den anderen Geräten. Das einzige, was

end-to-end verschlüsselt ist, sind die „Secret Chats“. Der Daten-Transport zu den Telegram-Servern und zum Gesprächspartner ist immer verschlüsselt. Aber bei end-zu-end Verschlüsselung wird wirklich noch über ein eigenes Protokoll, das Telegram selbst designt hat, ein symmetrischer Schlüssel ausgehandelt und dann damit verschlüsselt. Aber Telegram stand auch sehr in der Kritik dafür, weil die erste Regel für Verschlüsselungsalgorhythmen und Verschlüsselungstechnologien lautet: mach’ kein eigenes Gebastel! Telegram hat das jedoch gemacht und deshalb sagt man, dass ihre end-zu-end Verschlüsselung nicht wirklich ideal ist.

Ich habe gerade mal zwei Kontakte, die bei Telegram sind.

Rexxnor: Es kommt natürlich sehr auf das eigene Umfeld an: da sind vielleicht Messaging-Dienste aus anderen Gründen beliebter.

Ich habe mitbekommen, dass Apple jetzt z. B. bei Telegram die Gruppenchats, die inhaltlich gegen die Nutzungsbedingungen verstossen, gesperrt werden. So eine Zensur vom Anbieter finde ich ziemlich schockierend.

Vimja: Dass Apple alles zensiert, ist ja schon lange bekannt.

Rexxnor: Das war mir nicht bewusst, bis vor kurzem. Ich selbst bin nicht davon betroffen. Ich habe mal von einem Dienstleister gehört, der solche Nutzungsbedinungen anschaut und ein paar „Bullet Points“ gibt, was positiv und negativ ist. So eine Art „Ampel“ der Nutzungsbedingungen…

Vimja: Ja, das ist einfach eine Website, die heisst „Terms of Service Did not read“ (https://tosdr.org/).

Rexxnor: Ah, das ist sogar communitymässig, also nicht einmal ein Dienstleister, der das macht. Super, wenn Du eine Site hast, die das quasi für Dich übernimmt und dir sagt, wo du aufpassen sollst. Etwa wenn Du die Rechte an Deinen Bildern beim Hochladen abgibst, oder so.

Etwa bei Facebook: wenn man da Bilder hochlädt, verliert man seine Rechte an den Bildern…

Rexxnor: Da sieht man: die Nutzungsbedingungen sind sehr heikel.

Max Schrems schreibt in seinem Buch, wie etwa bei Facebook die Voreinstellungen gegen Dich sind. Die Einstellungen für die Privatsphäre sind an vielen verschiedenen Orten versteckt, es ist gegen Dich und das ist fies.

Rexxnor: Das gibt’s auch bei anderen Diensten, etwa wenn man sich abmelden oder das Konto löschen will, da machen sie es dir sehr schwer, dass du überhaupt an einen Punkt kommst, an dem du aussteigen kannst: „ich möchte nicht mehr auf dieses Konto zugreifen können“.

Das geht soweit, dass Du – Amazon ist ein krasses Beispiel – auf sieben verschiedenen Seiten, an verschiedenen Orten sagen musst: „ich will nicht mehr“. . Nach drei Schritten denkst du: „jetzt habe ich’s dann“, aber bist du dann wirklich gekündet hast, geht’s noch viel länger. Wieder andere Dienste drücken auf die Tränendrüse und sagen: „bitte gehe nicht!“. Ich finde das unfair gegenüber dem Benutzer.

Vimja: Ich denke, die Datenauskünfte sind mit der neuen DSGVO (Datenschutz-Grundverordnung) viel besser geworden. Die Firmen sind dort jetzt stärker dazu verpflichtet, dir deine Daten zu geben und es ist sehr interessant, zu sehen was da kommt. Kürzlich hat einer mit eBook-Reader bei Amazon alle seine Daten angefordert und gesehen: die speichern alles! Wann hast du welche Seiten angeschaut?Wie lange hast du diese Seiten angeschaut? Was genau, welchen Text hast du markiert? Wie hell war der Bildschirm, als Du sie angeschaut hast? Wann hast du weitergeblättert? Die speichern einfach alles.

Und das wird auch alles analysiert?

Vimja: Auf jeden Fall.

Rexxnor: Grundsätzlich: Wo Daten existieren, werden Daten angeschaut und analysiert. Ich glaube, das Ausmass dieser Analyse wird einem gar nicht bewusst, eigentlich bis es zu spät ist.

Gibt es nicht auch Authentifizierungs-Methoden, bei welchen geschaut wird, wie wir mit der Maus über eine Seite fahren?

Rexxnor: Genau, Google-Captchas! Das ist interessant: bei der ersten Generation war gefragt: „erkenne diesen Text hier“, jetzt, bei der zweiten Generation muss man diese Kacheln anklicken: „Erkenne die Ampeln, Autos, usw, …“. Bei der dritten Generation wollen sie sich nun eben die Mausbewegung anschauen.

Vimja: Nein, dass das Nutzerverhalten analysiert wird, wurde tatsächlich bereits 2014 unter dem Namen „No-Captcha“ eingeführt: das ist immer dann, wenn der Knopf „I’m not a robot“ erscheint. Der Entscheid, ob dieser Knopf angezeigt wird, fällt aufgrund der Art, wie du eine Website benützt.

Das ist auch ein endloser Battle gegen die Bots im Internet. Ein Google-Team hat selbst ein Programm geschrieben, das besser darin ist, Captchas zu lösen als 98% der Menschen (lacht). Das ist leicht problematisch, wenn Du ein Programm hast, das den Test besser lösen kann, als Menschen.

Andere Frage: sind Trolle, Hater und Fake News für euch ein Thema?

Vimja: Das ist für uns glücklicherweise weniger ein Thema, sondern für youtube oder so. Was für uns aber ein Thema ist, sind Fake News, gerade im Zusammenhang mit der Entwicklung, wie die Russen offenbar massiv Geld in die Hand genommen haben, um in den USA die Wahlen zu manipulieren. Das ist ein sehr bedenkliches Thema, zu sehen, dass Staaten bereit sind, sehr viel Geld in die Hand zu nehmen, um über Computer Wahlen zu manipulieren.

Es ist auch bedenklich, wenn man sieht, dass heute in der Schweiz eine offensive Cyberforce gefordert wird, die andere Staaten hacken und angreifen kann. Oder wenn du siehst, wie abhängig wir heute von Computersystemen sind, die jeden Teil unseres Lebens regeln. Unsere Stromnetzwerke, unsere Wasserversorgung, unseren Verkehr, alles. Wenn Staaten wirklich bereit sind, Geld in die Hand zu nehmen, um solche Systeme aktiv kaputt machen zu können, dann müssen wir alle uns Gedanken und Sorgen darüber machen.

Ich denke, da wäre es wichtiger, dass der Staat Geld in die Hand nimmt, um die Sicherheit der Systeme zu verbessern, damit nicht andere Staaten, Verbrecher, oder wer auch immer, uns schaden können.

Rexxnor: Es ist sehr bedenklich. Es wurde ja gesagt, dass es bei dieser Wahlmanipulation mehr darum ging, über gezielt geschaltete Werbung, z. B. auf Facebook, gewisse Wählergruppen in eine Richtung tendieren zu lassen, und so auf einen Hass abgezielt hat oder so eine Neigung noch zu verstärken. Das habe erstaunlich gut funktioniert. Und das Mittel zum Zweck, nämlich dass Facebook gezielte Werbung schalten kann, macht sie meiner Meinung nach mitschuldig. Es war zwar eine andere Instanz, die Geld gegeben hat und diese Werbungen geschaltet hat. Aber wenn die Plattform zulässt, dass Werbung geschaltet wird, dann hast du diese Gefahr. Man sollte da Facebook auf die Finger schauen.

Vimja: Das wird ja auch gemacht, die wurden vor den Kongress zitiert…

Rexxnor: Auch in der EU war das so…

Das fand ich faszinierend: wenn du das Hearing in den USA anschaust – es gab ja Aufnahmen davon – und dann in der EU: sie stellen komplett verschiedene Fragen, die Senatoren und die Leute aus dem EU-Parlament! Der Unterschied ist wie Tag und Nacht: in den USA mehr ging es mehr um Implikationen und

so, aber in den EU hat man sich noch um den Datenschutz und private Daten gekümmert.

Vimja: Etwas anderes, was ich bei solchen Vorwürfen wie jetzt gegen Russland auch immer sehe: es ist sehr praktisch ist, den Russen die Schuld zu geben. Wenn es heute einen Angriff in den USA gibt, dann heisst es: „das sind die Russen gewesen, oder: „das sind die Chinesen gewesen…“. Ich meine, solche Aussagen sind häufig sehr politisch motiviert. Da sind viele Aussagen von Leuten, die nicht dazu qualifiziert sind, solche Aussagen überhaupt zu machen, oder Aussagen, die gemacht werden, obschon die ermittelnden Behörden gesagt haben: „nein, das kann so nicht sein“. Man muss aufpassen, was man glauben will. Es gibt Leute, die ein Interesse daran haben, dass die bösen Russen Schuld sind.

Und dann kann man es auch noch so aussehen lassen, als wären’s die Russen gewesen?

Vimja: Genau und gerade die Amerikaner sind dort natürlich sehr heuchlerisch; die machen genau dasselbe auch. Der Stuxxnet, mit dem sie in die iranischen Zentrifugen zerstört haben…

…in den Atomanlagen…

Vimja: …dort haben sie am Schluss zugegeben, dass sie das waren. Da muss man dann nicht auf die bösen Russen zeigen.

Wir sehen, wie die Digitalisierung jeden Bereich unseres Lebens mit einer wahnsinnigen Geschwindigkeit verändert und beeinflusst. Was denkt ihr, wie diese Welt in 20 oder 50 Jahren aussieht; wo geht das hin, haben wir bis dahin den totalen Überwachungsstaat, wie jetzt schon teilweise in China, oder schaffen wir’s wirklich, dass diese Technik uns zu einer faireren, sozialeren, gerechteren Welt verhilft? Das kann sehr visionär sein: wo gehen wir hin?

Rexxnor: Ich empfinde diese Frage – ehrlich gesagt – immer ein

wenig deprimierend, wenn ich so in die Zukunft schaue. Was die Zukunft angeht, vor allem einen Zeitraum von 20 oder mehr Jahren, bin ich ziemlich pessimistisch. Wir haben schon in den letzten paar Jahren gesehen, dass es bei allem, was politische Entscheide anging, wie NDG, BÜPF, Geldspielgesetz, dass es überall, wo's um digitale Themen geht oder diese anschneidet, nur in eine Richtung geht: nämlich dass es einem egal wird, was mit den Daten passiert. Ich habe grosse Bedenken, wir kommen einmal an diesen Punkt: „es ist doch egal, es ist gut und wir müssen denen einfach nur vertrauen" und man sich ausgeliefert fühlt und denkt: „Ich kann sowieso nichts daran ändern". Es führt in eine Richtung, die für mich unangenehm wird.

Vimja: Ich habe starke Bedenken. Etwa vor einem Jahr sind „Spectre" und „Meltdown" öffentlich bekannt geworden, zwei wirklich grundlegende, verheerende Fehler in den Prozessoren unserer Computer selbst. Das sind Fehler, die seit 15 Jahren in alle neuen Prozessoren eingebaut worden sind. Prozessoren, die von den grössten Herstellern der Welt gebaut werden, von den besten Spezialisten, die es gibt. Und über 15 Jahre hinweg hat niemand realisiert, dass die Prozessoren grundlegende Sicherheitsprobleme haben, die alle anderen Sicherheitsmechanismen, die du darüber aufbaust, komplett unterwandern.

Könnte das Absicht gewesen sein?

Vimja: Nein, das ist einfach dadurch bedingt, wie diese Prozessoren aufgebaut sind. Ich denke, wichtiger noch als das ist, dass es zeigt, wie wenig Verständnis wir darüber haben, wie Computer tatsächlich funktionieren. Man hat solche grundlegenden Probleme nicht erkannt und gleichzeitig baut man immer weitere Schichten der Abstraktion und Komplexität obendrauf. So haben wir heute das Problem, dass wir immer mehr Aufgaben an Computersysteme übergeben, die wir immer schlechter verstehen und immer schlechter kontrollieren können. Das ist an sich bedenklich. Man sieht immer wieder,

dass wir massive Sicherheitsprobleme haben und trotzdem füttern wir immer mehr Daten in diese Systeme rein und übertragen mehr Macht an diese Systeme, die offensichtlich problematisch sind.

Stichwort „künstliche Intelligenz“? Dass diese Systeme dann aufgrund von irgendwelchen Informationen oder Algorhythmen selbst Entscheidungen treffen?

Vimja: Genau, Systeme, die wir nochmal viel schlechter verstehen, als herkömmliche Computer. Das ist das, worüber ich mir Gedanken mache, wenn ich in die Zukunft schaue. Dass man einfach heute sehr bereitwillig Sachen digitalisiert, ohne sich die langfristigen Folgen zu überlegen.

Ganz andere Probleme stellen sich etwa den Gerichten. Manche Entscheide müssen über viele Jahrzehnte aufbewahrt werden. Es hat aber niemand Computersysteme, welche Daten über so lange Zeiträume speichern können.

Wir rennen in die Digitalisierung hinein und haben dabei grundlegende Probleme nicht gelöst. Vielleicht wär’s richtig, mal einen Schritt zurück zu machen und zu sagen: „Jetzt gehen wir das Ganze einmal von Vorne an und überlegen uns, wie wir’s richtig machen wollen, bevor wir einfach drauflos rennen und dann erst schauen, was passiert“.

Das ist aber utopisch, nochmal von Vorne anzufangen…

Vimja: Ja klar, das wird nicht passieren, aber der eine oder andere wird fürchterlich auf die Fresse fallen, bis gemerkt wird, dass man besser aufpassen sollte. Ich denke es wird noch recht knallen, bevor wir anfangen, das wirklich seriös zu machen.

Wir sind aber wohl schon auf dem Weg dorthin: In den letzten Jahren, haben es Hacks von grossen Firmen und Industrieanlagen immer mehr in die Medien geschafft und Staaten, fordern höhere Sicherheitsstandards und dass besser geprüft wird, wie

Sicherheitssysteme von Computern gewährleistet werden. Auch aus dem CCC-Umfeld kommt viel Kritik, weil viele der Versuche, die die Politik heute unternimmt, um die Sicherheit der Computersysteme zu regeln, völlig unzulänglich sind. Aber sie versuchen es immerhin. Nun muss man schauen, dass es in die richtige Richtung geht. So besteht die Hoffnung, dass es gut kommt und am Schluss die Politik von der Industrie und von den Betreibern sichere Computersysteme fordert und dass man das vernünftig kontrollieren kann.

Sind „Rohstoffe und Nachhaltigkeit“ für euch ein Thema? Und der ganze Elektroschrott?

Die ganze Digitalisierung ist extrem rohstoffintensiv; schon jetzt werden Kriege um die Rohstoffquellen geführt, wo alle die „seltenen Erden“ sind. Oder wie die Umwelt damit verschmutzt wird, mit der Förderung dieser Metalle. Ist das ein Thema oder noch nicht?

Vimja: das ist auf jeden Fall auch ein Thema. Es gibt schon – jetzt nicht direkt von uns – Bewegungen, die in die richtige Richtung gehen: das „FairMouse“ (*www.nager-it.de, Anm. d. Red.) oder das „FairPhone“-Projekt aus Holland. Die geben sich Mühe, dort zu schauen. Interessant sind dabei nicht so sehr die Produkte – die machen Produkte und das geht in die richtige Richtung – sondern wie die aufzeigen, wo die Rohstoffe wirklich herkommen. FairPhone steckt sehr viel Energie rein, aufzuzeigen, woher die Rohstoffe kommen, woher das Metall kommt und woher der Lieferant das Metall hatte. Das zeigt einfach, wie komplex das Thema ist und wie du – wenn du diesen Wegen nachgehst –schlussendlich immer an die schlimmsten Orte dieser Welt kommst, wo die Leute am schlechtesten behandelt werden. Das ist sehr bedenklich. Die Leute sagen, es wäre ihnen wichtig und dennoch will jedeR jedes Jahr ein neues iPhone, ein neues Laptop, ein neues Tablet.

So müsste man bei den Produzenten den Finger drauf halten und

verlagen: „hört mal Leute, wir wollen Computer, die länger als drei Jahre halten“? Die könnten doch Computer herstellen, die einfach 10 Jahre laufen, oder?

Rexxnor: Spezifisch im Fall von Apple ist es so, dass Apple Vieles gegen das „Recht zum Reparieren“ getan hat: z. B. haben sie den Akku eingeklebt, oder beim iPhone ist es jetzt so, dass sich seit der touch-ID das Display nicht mehr austauschen lässt, ohne gleichzeitig auch den Fingerabdruck-Scanner auszutauschen. Oder bei Macbooks: es ist meist so, dass sie sehr viel Geld verlangen, um etwas zu ersetzen, das man mit dem richtigen Equipment und etwas Erfahrung selbst reparieren könnte.

Das ist auch das Problem punkto Nachhaltigkeit: wenn man etwa sagt: „das Mainboard ist kaputt“, aber es ist nur ein elektronisches Bauteil kaputt und dann trotzdem das ganze Board austauscht und wegwirft, ist das ökologisch gesehen absurd.

Jetzt gibt es die Repair-Café-Bewegungen in der Schweiz oder auch international.

Nächsten Samstag ist gerade wieder eins, in Bern in der „Turnhalle“, wo ich auch dabei bin. Repair-Cafés sind eigentlich ein Schritt in die richtige Richtung, aber man müsste trotzdem die Hersteller…

Vimja: Es kann doch nicht sein, dass dir die Hersteller immer „mülligere“ Geräte verkaufen, die immer schneller kaputt gehen und dann sollen Leute wie rexxnor in ihrer Freizeit dorthin gehen und das Gerät flicken, das du von einem Hersteller gekauft hast. Hier ist die Politik gefragt, welche die Hersteller dazu zwingt, bessere Garantieleistungen zu bieten, Geräte herzustellen, die länger halten und auch, dass man die Geräte flicken kann mit den nötigen Anleitungen und Werkzeugen.

Dann kommt natürlich sofort Apple, betreibt in den USA aktiv

Lobbying-Arbeit gegen solche Politik und ich frage mich: weshalb eigentlich? Der Staat ist doch Vertreter der Bürger, nicht von Apple.

Die bezahlen ja auch keine Steuern…

Vimja: Die Politik befürchtet dann bei der Einführung solcher Gesetze immer einen Standortnachteil, aber ich denke mit dem DSGVO hat die EU gezeigt, dass Europa sehr wohletwas tun kann. Europa ist genug gross, hat genügend Macht, um auch amerikanische Hersteller dazu zu zwingen, sich zu bewegen. Wenn wir wieder Geräte wollen, die funktionieren, die wir flicken können und die zuverlässig sind, dann ist auf jeden Fall die Politik gefragt. Von den Herstellern wird's nicht kommen. Die Entwicklung geht definitiv in die falsche Richtung, es wird immer schlechter.

Also müsste man auf der grossen Ebene versuchen eine Veränderung zu bewirken und bis das durch ist, sind die Repair-Cafés super?

Rexxnor: Bei den Repair-Cafés geht's um dieses Sich-Selbst-Helfen. Was wir dabei öfter machen, ist, dass wir auf ein kaputtes Windows-Laptop ein Linux darauf installieren. Da geht es uns nicht darum, dass dieses Gerät schon nach diesen zwei, drei Jahren kaputt ist". Ab und zu gibt's auch mal ein Macbook mit Altersschwäche; da installiere ich meistens ein Linux drauf, wenn das Mac-System nicht mehr passt.

Stichwort „Bargeldabschaffung", ist das ein Thema für euch, oder nicht?

Rexxnor: Digitale Zahlungen jeglicher Art hinterlassen Spuren. Man kann damit alle Zahlungen an jeden Punkt und an jede Person verfolgen und ganze Bewegungsabläufe erstellen. Bargeld hat – das ist meine Meinung – den entscheidenden Vorteil, dass es quasi nicht nachverfolgbar ist und man kann quasi anonym etwas kaufen. Das würde ich vermissen, wenn das Bargeld abgeschafft würde.

Vimja: Soviel ich weiss, hat schon vor Jahren, das amerikanische Innenministerium in ihrem Wahn gegen die Terroristen Infoblätter für Flughäfen und andere gefährdete Stellen veröffentlicht: Leute, die ihren Kaffee nicht mit der Kreditkarte bezahlen sind verdächtig! Das ist doch bedenklich!

Es ist zum Teil absurd, was gefordert wird: die EU hat die die grösste Note abgeschafft, die 500-er Euro-Note, weil damit der Terrorismus finanziert würde. Bin Laden hatte also die X Milliarden in 500-Euro Noten mit sich, um damit Kriegs-Maschinerie zu kaufen. Das ist absolut absurd. Auch die Mafia finanziert sich nicht so. Das organisierte Verbrechen ist der drittgrösste Wirtschaftszweig weltweit, direkt hinter der Autoindustrie. Du kannst eine solche Wirtschaft gar nicht mit Bargeld finanzieren; das ist hirnverbrannt. Das sind Beträge, die weit über alles Bargeld hinweggehen.

Andere Dinge betreffen uns sehr direkt: Wenn ich etwa in den Laden gehe und ein Sexspielzeug kaufe, dann will ich das nicht mit der Kreditkarte kaufen.

Das geht niemanden etwas an…

Vimja: Ja, das geht niemanden etwas an, das will ich mit Bargeld bezahlen können, wie andere Dinge aus dem Alltag, die jeden betreffen. Man kauft Dinge und denkt „das geht jetzt niemanden etwas an, dass ich das gekauft habe“.

Wie denkt ihr über Online-Abstimmungen und Wahlen?

Rexxnor (lacht): Das ist ein sehr brisantes Lieblingsthema von uns! Weil ich hier studiere und die Security-Vertiefung mache, habe ich mich auch mit e-voting auseinandergesetzt, unter anderem auf der Protokoll-Ebene. Für Leute, die das interessiert: die Protokolle sind alle ganz schön. Wow, das kann funktionieren! Auf rein technischer Ebene ist das faszinierend. Aber die zwei grössten Probleme, die sich immer zeigen sind einerseits die Umsetzung: du musst immer noch

vertrauenswürdige Parteien haben, Wahlbeobachter, die alles verifizieren, die sich z. B. auch darum kümmern, dass alles sauber abläuft. Man muss Leuten vertrauen.

Andereseits und das ist eigentlich das grösste Problem: ich habe das alles studiert und ich verstehe es immer noch nicht ganz. Um das alles in seiner ganzen Komplexität zu verstehen, musst du nicht bloss studiert, sondern dein halbes Leben damit verbracht haben. Wenn wir unsere Demokratie auf ein solch komplexes System abstützen wollen, finde ich das sehr bedenklich!

Dann gäbe es nur noch ein paar wenige Menschen, die das kontrollieren könnten?

Rexxnor: Es geht nicht mal um Kontrolle, es geht um Verständnis. Wenn Du einen Zettel in eine Urne wirfst, wird der gezählt; das versteht jedes kleine Kind. Aber bei digitalen Abstimmungen hast du eine Reihe von Zeichen, eine Zeichenkette, die von Menschen nicht lesbar ist. Dann fragt man sich: „Wie kann das meine Stimme sein, *ist* das meine Stimme, wie kann ich das überprüfen?“ All das ist im Protokoll beschrieben, wie man’s machen muss. Aber wirklich verstehen, was abläuft, tut man dann trotzdem nicht.

Vimja: Es ist die Komplexität dieser E-Voting-Systeme, die immens ist und sie steht in einem krassen Kontrast zu unserem heutigen System. Wenn ich wissen will, ob in meiner Gemeinde die Abstimmung sauber läuft, dann stehe ich ins Wahlbüro und kann zuschauen. Alles was passiert, kann ich nachvollziehen und abends nach Hause gehen und sagen: „Doch ja, ich habe gesehen, was passiert. Ich habe gesehen, dass es sauber abgelaufen ist, es ist gut abgestimmt worden. Ich muss auf der Gemeinde sogar Stimmen auszählen gehen und bin ein Teil des Prozesses. Das ist wirklich etwas, das wir alle verstehen.

Das E-Voting, wie’s heute gemacht werden soll, ist dagegen unverständlich. Bis auf ein paar ganz wenige Kryptografen und

Mathematiker, die den Durchblick haben. Das würde schlussendlich auch das Vertrauen der Leute ins System untergraben, was sehr schade wäre. Wie Rexxnor gesagt hat: das ist mathematisch und kryptografisch sehr interessant, aber ich denke nicht, dass wir unsere Demokratie diesem System anvertrauen sollten. Man sollte weiter Geld reinstecken und weiterforschen, aber nicht eine Demokratie darauf abzustützen; das wäre sehr schade.

Rexxnor: Gerade letzte Woche durfte ich – als benotete Arbeit – ein Protokoll vorstellen, da ging's darum, dass dieses System für Abstimmungen besser bei Mitarbeiter-Umfragen angesiedelt wäre. Weil es funktioniert: du kannst mit dem Protokoll anonym abstimmen und du kannst auch verifiziert sein. Anstatt den Mitarbeitern Anonymisierung zu versprechen, oder irgendwelche Nummern zuzuweisen. Dort geht's dann wirklich darum, dass man dir Deine Aussagen nicht zuweisen kann, weil dich das sonst die Stelle kosten könnte.

Vimja: Das zweite Problem, das wir immer haben, wenn wir etwas digital machen: wenn wir heute eine Wahl manipulieren wollen, ist das sehr schwierig. Es reicht nicht, eine Stimme zu manipulieren, sondern man müsste viele Stimmen manipulieren und das ist ein grosser Aufwand. Je mehr Stimmen man manipuliert: der Aufwand steigt. Ein Briefcouvert bei den Nachbarn aus dem Briefkasten zu nehmen und umzubauen, mag gerade noch gehen, aber hier in Biel 10'000 Stimmen zu modifizieren, dürfte eher schwierig werden. Selbst wenn du es schaffen solltest, dass das nachträglich nicht auffällt: der Aufwand ist hoch. Aber wenn wir in einem digitalen System eine Angriffsmöglichkeit finden, die auf eine Stimme funktioniert, dann funktioniert sie auch auf 10'000 Stimmen, automatisch und ohne Mehraufwand. Angriffe auf's Wahlsystem skalieren mit E-Voting ganz anders.

Rexxnor: Bei dem geplanten Genfer E-Voting-System „ch-Vote" ist es ja grundsätzlich so, dass… …

Vimja: …das wurde abgesagt…

Rexxnor: Das wurde abgesagt; ich möchte es trotzdem kurz erwähnen, weil die Forschung an dem System nicht aufgegeben wird. Grundsätzlich war halt die Idee, dass man eine Card mit Verifikationscoden erhält, die man an gewissen Orten eingeben muss, um ins System zu kommen. Manche Leute haben gesagt, wie man das grundsätzlich angreifen könnte: mit Verschlüsselungstrojanern dein System verschlüsseln und dann gegen Lösegeld den Schlüssel freigeben. Ein solcher Trojaner könnte sich, weil er digital ist, viel einfacher verbreiten und nach diesen Codes fragen, mit denen man sich authentifizieren und eine Stimme abgeben könnte. Aber auf Papier kann man das einfach nicht machen. Das gibt es gar nicht auf Papier.

Vimja: Weiter finde ich bedenklich, dass überhaupt im Raum steht, das von einer gewinnorientierten Firma machen zu lassen. In diesem Fall steht jetzt zur Diskussion, dass die Post das E-Voting für die Kantone betreiben soll. Das ist doch an sich eine bedenkliche Entwicklung. Abstimmungen sind eine wichtige Grundlage unseres Staates, bis jetzt hat das immer der Staat garantiert und nun will man das plötzlich an eine gewinnorientierte Firma ausliefern. Das bedeutet dann, dass das Wichtigste an den Abstimmungen nicht mehr die Abstimmungen für unseren Staat sind, sondern dass die Post damit Geld verdient. Das ist für die Post dann das, was zählt, in diesem System: dass es gewinnbringend ist, weil das ist die Natur jeder Firma ist.

Die Post wiederum kauft die Software von einer spanischen Firma, namens Scytl (https://www.scytl.com/en/) die ebenfalls eine gewinnorientierte Firma ist. Und auf dieser Software, die auch nach kapitalistischen Grundsätzen entwickelt wurde, wollen wir unsere Demokratie aufbauen. So verkaufen wir unsere Demokratie an den Niedrigstbietenden, resp. an den Höchstbietenden.

Rexxnor: Was E-Voting angeht, so gibt es noch ein anderes Problem: das Genfer System wurde bei ein paar Abstimmungen in der Vergangenheit schon für ein paar Testläufe eingesetzt.

In Genf unten?

Rexxnor: Das ist in mehreren Kantonen angewendet worden, beispielsweise im Kanton St. Gallen und die Auswertung dieser Kantone ist dann in Genf passiert. Das heisst, man hast eine Art Zentralisierung dieser Instanzen, was sehr schade ist. Bisher hat das jede Gemeinde so schön selbst gemacht. Man müsste heute soviele Gemeinden infiltrieren und beeinflussen, um Wahlbetrug zu machen. Man kann ja sich ja auch tatsächlich für Wahlbeobachtung anmelden und Wahlbeobachtung machen. Selbst wenn man nun bei E-Voting als Wahlbeobachter hingehen würde: ich habe das Gefühl, als nicht-technikaffiner Mensch wäre es schwierig, etwas beurteilen zu können. Selbst als technikaffine Person habe ich das Gefühl, dass es immer noch ganz kritisch ist. Vor allem wenn man bemerken sollte, dass etwa ein security-affiner Mensch, oder einer, der Security-Vertiefung gemacht hat und Informatik studiert hat, die Sachen so verifizieren, wie man es nicht machen sollte. Als Security-Researcher hätte man dann vielleicht das Eindruck von Grobfahrlässigkeit. Man müsste diesen Leuten dann vertrauen, dass sie es richtig machen.

Rexxnor: Ich möchte auch noch gerne wissen, wie das als Zukunftsbild aussieht. Angenommen in 5 Jahren wird das E-Voting-System eingeführt, und in 15 Jahren, also 10 Jahre nach Einführung des E-Voting erkennt man, dass da vor Jahren einmal eine Abstimmung entscheidend manipuliert worden ist. Was wird dann passieren? Was wird das Volk machen, was der Bundesrat? Welches wird die Reaktion darauf sein? Wird es einfach ein kompletter Verlust des Vertrauens in die Demokratie sein oder werden rückblickend die Entscheide annuliert, obschon sie dann schon ein paar Jahre in Kraft sind? Ich vermute, dass es eine interessante Diskussion erzwingen würde.

Diese Situation möchte niemand. Aber wenn man ein solches E-Voting-System einführt: jede Sicherheitsschranke ist auch zu knacken, oder?

Rexxnor: Das ist dann so eine grundlegende Kryptografie-Sache. Das basiert auf mathematischen Annahmen. Vielleicht muss mich da Niklaus ein wenig korrigieren: man geht von Annahmen aus, aber wenn diese mathematischen Annahmen gebrochen werden, dann verpafft die ganze Kryptographie, die heute existiert, auf einmal.

Ich bin darin auch nicht fliessend, bin bei Weitem nicht Experte der Kryptografie, finde es aber einfach faszinierend, dass das irgendwie funktionieren kann. Ob die Ergebnisse dann stimmen und das System sich behauptet, ist eine komplett andere Diskussion. Es interessiert mich, weil es lustig ist, dass Zahlen solche Eigenschaften haben können.

Gibt's das Büchlein „Digitale Selbstverteidigung" auch auf Französisch? wo können sich Leute informieren?

Vimja: Es gibt sehr viele Anlaufstellen. Das beste, was Dir passieren kann, ist wenn in deiner Nähe eine Kryptoparty veranstaltet wird. Kryptoparties sind Veranstaltungen, speziell mit dem Ziel, den Leuten Kryptographie beizubringen, den Leuten zu zeigen, wie sie E-Mails verschlüsseln können, wie sie ihre Festplatte verschlüsseln können und wie sie sicher kommunizieren können. In der Regel sind an diesen Veranstaltungen auch Leute, die ein Interesse haben, das den Leuten beizubringen, oder sich mit dir hinsetzen, auf deine Fragen eingehen und dir helfen.

Zürich hat schon Kryptoparties gemacht, sonst gibt's das in der Schweiz nicht häufig. Aber ich denke für interessierte Leute gibt's in der Nähe einen Chaos-Treff, einen Hacker-Space. Über die CoSin kann man auch Leute treffen.

Für Französischsprechende ist die beste Anlaufstelle wohl die „quadrature du net"; das ist eine französische

Bürgerrechtsorganisation, die sich vor allem auf europäischer Ebene für Datenschutz und solche Sachen einsetzt, für die auch der CCC einsteht. In Frankreich ist das eine gute Anlaufstelle für alles Mögliche.

Rexxnor: Die „Digitale Gesellschaft“ setzt sich sehr für digitale Rechte im Schweizer Raum ein. Ich glaube, es gibt keine französische Ausgabe. Ich weiss nicht, ob sie eine französische Sparte haben, oder französische Übersetzungen machen, aber ich habe mal gehört, dass sie Mehrsprachigkeit anstreben.

Vimja: Ihr könnt auch den Fix-Me Hackerspace in Lausanne anfragen, den gibt’s schon lange, die sind gross, bieten Workshops und Veranstaltungen an und haben sicher auch Leute, die sich auskennen.

An der EPFL gibt’s die „Gnu-Generation“, das ist die eigene Linux-Usergroup der EFPL; die gibt’s schon sehr lange. Die haben in ihrer Existenz stark geschwankt, wie aktiv sie sind, wieviele Leute wirklich dabei sind und aktiv Sachen machen.

Herzlichen Dank!

CoSin-Event: www.cosin.ch

Chaos Computer Club Schweiz: https://www.ccc-ch.ch

Digitale Gesellschaft: www.digitale-gesellschaft.ch

Französische Bürgerrechtsorganisation (auf französisch): www.laquadrature.net

Hackerspace in Lausanne (auf französisch): https://fixme.ch

Linux-Usergroup der EFPL (auf französisch): https://gnugeneration.epfl.ch/doku.php

Die ethischen Grundsätze des Hackens – Motivation und Grenzen:

• Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
• Alle Informationen müssen frei sein.
• Mißtraue Autoritäten – fördere Dezentralisierung.
• Beurteile einen Hacker nach dem, was er tut, und nicht nach üblichen Kriterien wie Aussehen, Alter, Herkunft, Spezies, Geschlecht oder gesellschaftliche Stellung.
• Man kann mit einem Computer Kunst und Schönheit schaffen.
• Computer können dein Leben zum Besseren verändern.
• Mülle nicht in den Daten anderer Leute.
• Öffentliche Daten nützen, private Daten schützen.