SPIONAGE

Der Tag, an dem ich schwul wurde

Was SPIEGEL-Reporter Uwe Buse bei einem Selbstversuch erlebt hat, kann auch jedem anderen Internetnutzer passieren: Hacker spähten ihn aus, und er verlor die Kontrolle über sein Leben.

An einem Dienstagmorgen, als ich allein vor dem Computer im Arbeitszimmer sitze, hält ein Lieferwagen vor dem Haus. Der Fahrer steigt aus und zieht eine Sackkarre aus dem hinteren Teil des Autos. Dann steigt er in den Laderaum und taucht wenige Sekunden später wieder auf, mit einem großen Karton. Er stellt ihn auf die Sackkarre, schiebt sie über die Straße. Anschließend klingelt er bei mir an der Tür.

„Was ist das?“, frage ich ihn.

„Ein Rasenmäher, von Bosch.“

„Ich habe keinen Rasenmäher bestellt.“

Der Bote schaut auf den Bildschirm seines kleinen Computers. „Doch, haben Sie. Hier steht es“, sagt er.

„Nein“, antworte ich, „ich habe schon einen Rasenmäher und bin sehr zufrieden mit ihm. Ich brauche keinen zweiten.“

„Aha“, sagt der Bote, „und jetzt?“

„Lehne ich die Annahme des Pakets ab.“

Der Bote schiebt den Karton auf die Sackkarre und geht zurück zu seinem Wagen. Ich schließe die Tür und wundere mich, wie schnell die Spione, die ich auf mich angesetzt habe, in mein Leben eindringen konnten. Das Experiment hat also begonnen.

Ich habe mich in die Hände von Hackern begeben, vorsätzlich. Ich möchte,

Gestohlenes Foto von Reporter Buse, Hackerin

CIRA MORO / DER SPIEGEL

dass sie so viel wie möglich über mich herausfinden, über mein privates und mein berufliches Leben, alles soll von ihnen durchleuchtet werden. Dann sollen sie ihr Wissen nutzen, sie sollen versuchen, mir zu schaden, und ich werde versuchen, mich zu wehren. Mein Experiment soll eine Übung in digitaler Selbstverteidigung sein.

Ich habe das Gefühl, dass so etwas jetzt dringend nötig ist, angesichts der Enthüllungen über die NSA, angesichts der Tatsache, dass kriminelle Hacker immer trickreicher werden. Die Profis unter ihnen unterhalten schon Hotlines, um überforderten Nebenerwerbs-Hackern zu helfen.

Es gibt Grenzen für dieses Experiment. Ich will mein Haus nicht verlieren, meine Frau, meine Kinder und Freunde. Ich bin mir allerdings nicht sicher, wie weit die Hacker gehen werden.

Gefunden habe ich diese Spezialisten in Tübingen, bei der Syss GmbH, einem IT-Sicherheitsunternehmen, das von Sebastian Schreiber geführt wird, einem früheren Hacker, der jetzt Unternehmer ist, Krawatte und Anzug trägt und gegen die Kriminellen im Netz antritt. Schreiber hat sich darauf spezialisiert, Netzwerke von Firmen im Auftrag der Eigentümer zu attackieren. Schreiber macht das schon seit über zehn Jahren.

Vor Beginn des Experiments treffen wir uns in Schreibers Firma, um Details

zu besprechen. Ich sitze auf der einen Seite des Konferenztisches, auf der anderen Seite sitzen meine drei persönlichen Hacker, alle jung, alle glücklich darüber, dass sie ihr illegales Hobby in einen legalen Beruf verwandeln konnten. Jeder meiner Hacker hat ein Spezialgebiet. Das Hacken von Handys, das Hacken von Windows-Rechnern, den Umgang mit Linux, einem Betriebssystem, das von Programmierern für Programmierer entworfen wurde.

Die Spione kennen meinen Namen und meinen Arbeitgeber. Sie wissen also, dass ich Journalist bin, aber das erfährt man auch, wenn man meinen Namen googelt. Die Hacker wissen nicht, wo ich wohne, auch nicht, ob ich eine Familie habe. Sie können nichts sagen zu meinen Vorlieben, meinen Gewohnheiten, meinen Finanzen. Ich bin ein Fremder für sie.

Zwischen uns auf dem Tisch liegen ein Laptop und ein Handy. Auf beide Geräte haben meine Hacker Spionageprogramme geschleust, die auch im Internet versteckt sind und die sich jeder Benutzer einfangen kann – beispielsweise über eine infizierte Website. Rund 10 000 dieser Seiten, schätzen Experten, werden täglich neu ins Netz gestellt. Es genügt auch schon eine E-Mail, deren Anhang verseucht ist, zehn Milliarden dieser Mails tauchen jeden Tag im Internet auf. Niemand, der sich im Internet bewegt, ist vor dieser Gefahr geschützt. Im Google Play Store werden auch immer wieder bösartige Apps entdeckt, darunter solche, die das Handy und den Computer zugleich infizieren.

Nach Angaben des Bundesamts für Sicherheit in der Informationstechnik wurden in einem Vierteljahr 250 000 Menschen in Deutschland Opfer von Hackern. Das sind rund 2750 Internetnutzer am Tag. Und ich bin nun einer von ihnen.

Ich schalte das Handy ein, danach den Laptop, beide Geräte fahren hoch und funktionieren einwandfrei. Der Virenscanner des Laptops meldet: Dieser Rechner ist virenfrei. Meine Hacker lächeln.

Am Morgen des nächsten Tages, um sieben Uhr, sitze ich – rund 500 Kilometer entfernt von meinen Hackern – in meinem Haus, in meinem Arbeitszimmer, schalte den Rechner und das Handy ein. Innerhalb weniger Minuten erfahren meine Hacker in Tübingen, wo ich bin. Im Handy ist ein Programm versteckt, und es schickt die GPS-Daten des Telefons nach Tübingen, und das nicht nur einmal, sondern von jetzt an alle zwei Sekunden. In Tübingen sitzt einer meiner Spione an seinem Rechner und kopiert die Daten. So sieht er, wo ich im Moment bin, in welcher Straße in Bremen-Schwachhausen. Er kann auch das Haus bestimmen und notiert sich die Adresse als meinen mutmaßlichen Wohnort, weil ihm weitere Daten sagen, dass ich gestern, nach meiner Rückkehr nach Bremen, unmittelbar in dieses Haus gegangen bin und es nicht mehr verlassen habe.

Als Nächstes ruft mein Hacker Google Maps auf, klickt auf die Kartenansicht und zoomt sich von oben an mein Haus heran. Er speichert das Bild. Dann ruft er Google Street View auf und weiß, wie mein Haus in der Straßenansicht aussieht. Auch dieses Bild speichert er.

Um 7.56 Uhr verlasse ich das Haus, das Handy habe ich in der Hosentasche. Ich bewege mich rund 500 Meter in westliche Richtung, bleibe an diesem Ort etwa fünf Minuten lang und kehre dann nach Hause zurück. Aus dem Weg, den ich gewählt habe, aus dem Tempo, mit dem ich mich bewegt habe, schließt mein Hacker, dass ich mit dem Rad gefahren bin. Was mein Ziel war, kann er nicht sagen. Das GPS-Signal wird von den Häuserwänden reflektiert und springt wild herum. Möglicherweise bin ich zum Bäcker gefahren.

Gegen 8.15 Uhr erfährt mein Hacker, dass ich Vater bin und eine schulpflichtige Tochter habe. Sie ruft mich auf meinem Handy an und sagt, dass sie gut mit dem Rad an der Schule angekommen ist, die in Bremen-Findorff, einem anderen Stadtviertel, liegt. Mein Handy überträgt automatisch die Rufnummer meiner Tochter, und der Hacker kann das Gespräch Wort für Wort mithören. Sein Rechner legt eine Audiodatei des Gesprächs an, auch das geschieht automatisch.

Außerdem sendet ihm mein Handy ein Foto, das meine Tochter mit der eingebauten Kamera von sich gemacht hatte, bevor sie zur Schule fuhr. Jetzt weiß mein Hacker, wie meine Tochter aussieht. Es ist kurz vor neun Uhr. Die Überwachung läuft seit knapp zwei Stunden.

Um kurz nach neun setze ich mich an meinen Computer und denke, dass ich allein bin, aber da täusche ich mich. Die eingebaute Kamera meines Laptops schießt alle fünf Minuten ein Bild von mir und schickt es an meine Hacker.

Der Rechner sendet ihnen jeden meiner Anschläge auf der Tastatur des Rechners, die Liste erreicht meinen Hacker als übersichtliche Excel-Tabelle, die den Programmnamen, das geöffnete Fenster auf dem Computerbildschirm ebenso nennt wie die Tastatureingaben und die Uhrzeit, zu der sie erfolgten. Außerdem erfahren meine Hacker, wann die Daten an sie abgeschickt werden. Dies geschieht etwa alle fünf Minuten.

Innerhalb der nächsten Stunde erhalten meine Hacker die Zugangsdaten für mein Amazon- und mein E-Mail-Konto bei Google. Sie loggen sich in beide Konten ein.

Die Einstellungen des Amazon-Kontos bestätigen, dass ich dort wohne, wo ich heute Morgen aufgewacht bin. Außerdem können sich meine Hacker den Verlauf meiner Amazon-Käufe anschauen. Sie wissen jetzt, dass ich Motorrad fahre und sehr wahrscheinlich trockene Haut habe. In der Liste meiner Einkäufe bei Amazon finden sich Ersatzteile für meine Honda CRF450 und mehrere Packungen Urea-Creme.

Den Hackern werden all diese Informationen auf sehr komfortable Weise geliefert. Es ist kaum Expertenwissen vonnöten. Das haben meine Hacker Entwicklungen zu verdanken, die den globalen Markt für Viren, Trojaner und Spionageprogramme geprägt haben. War kriminelles Hacken früher eine mühselige Angelegenheit, ist es heute eine professionelle Dienstleistung, Anbieter werben im Netz mit dem Akronym Caas, „crime as a service“.

Die Spähprogramme werden auf Bestellung geschrieben. Virenbaukästen und Angriffs-Kits kann man im Internet einsatzfertig kaufen, sie werden mit bequemen Bedienungsoberflächen geliefert, günstige Basisvarianten sind für rund tausend Dollar zu haben. Die Programme wurden in der Regel ausgiebig getestet, sie sind zuverlässig und werden oft aktualisiert. Hotline-Unterstützung kann auf Wunsch dazugebucht werden.

Verschwinden einzelne Programme zeitweise vom Markt, weil Strafverfolger

Gegen 8.15 Uhr erfährt der Spion, dass ich Vater bin und eine schulpflichtige Tochter habe.

Hacker-Jäger Schreiber

CIRA MORO / DER SPIEGEL

erfolgreich gegen sie vorgegangen sind, dann heuern kriminelle Risikokapitalgeber routinierte Programmierer an, um die Lücke im Sortiment zu schließen. In Hacker-Foren wird zurzeit für ein Programm namens Kins geworben, das an die Stelle des früheren Bestsellers Zeus treten soll, eines Programms, das darauf spezialisiert ist, Zugangsdaten für Bankkonten zu erbeuten. Kins wurde wahrscheinlich in Russland programmiert und besitzt eine Eigenschaft, die Strafverfolger dort milde stimmen soll: Die Programmierer versichern, dass sich das Programm deaktiviert, sollte es gegen Computer in Russland oder in anderen Ländern der ehemaligen UdSSR eingesetzt werden.

Nachdem die Hacker auch meine E-Mails durchforstet haben, wissen sie, dass ich verheiratet bin, zwei Kinder habe, eine Tochter und einen Sohn, der noch in den Kindergarten geht. Meine Hacker kennen den Namen meiner Frau, Birgit. Die Spione kennen Birgits private E-Mail-Adresse, ihre private Handy-Nummer, sie wissen, wo sie arbeitet, wie sie aussieht, und sie haben mitgehört, als ich sie beim Frühstück gefragt habe: „Schatz, bringst du Max heute bitte in den Kindergarten?“

Am Abend fahre ich zu einem See, spiele Fußball mit meinem Sohn. Der Hacker ist über alles informiert.

Bilder aus Überwachungsprotokoll

Meine Hacker wissen, dass wir kein Auto haben, sondern Carsharer sind, dass wir zuletzt am 3. August Auto gefahren sind, von 12.45 bis 13.45 Uhr, und dass wir in dieser Zeit zwölf Kilometer zurückgelegt haben. Meine Hacker fanden heraus, dass wir eine tägliche Ausgabenliste auf Google Docs führen, dass wir selten bei Discountern kaufen, meist bei Rewe und sehr selten beim Bio-Supermarkt Aleco. Außerdem haben sie erfahren, dass wir am kommenden Wochenende nicht zu Hause sein, sondern Verwandte besuchen werden – in Berlin.

Die kommenden sechs Stunden verbringe ich im Haus und arbeite. Im Abstand von fünf Minuten erhält mein Hacker ein neues Datenpaket, und die Kamera des Laptops macht ein neues Foto. Dann schicken meine Hacker eine stille SMS, die – von mir unbemerkt – das Mikrofon des Handys anschaltet. Mein Telefon ist jetzt ihre Wanze. 30 Minuten lang wird sie alles aufnehmen, was zu hören ist. Im Protokoll wird später stehen: Stille und Tippen, Zielperson arbeitet wohl.

Am Abend fahre ich zu einem nahe gelegenen See, mein Hacker dokumentiert auch das. Wenig später komme ich zurück, esse Abendbrot mit der Familie, spiele Fußball mit meinem Sohn. Meine Frau bringt ihn ins Bett, danach meine Tochter. Mein Hacker ist über alles informiert, er hört mit, macht sich Notizen: Zielperson telefoniert mit einem Mann namens „Hauke“, das Gespräch dreht sich um berufliche Termine. In seinem Tagesprotokoll notiert der Hacker auch, dass sich die Zielperson mit der Tochter über den Kauf einer Luftmatratze unterhält. Um kurz nach elf ist für meinen Hacker erst einmal Sendeschluss, für mich auch, ich schalte das Handy und den Rechner aus.

Ich werde von meinen Hackern mit einem Programmpaket ausspioniert, das von den USA aus angeboten wird. Es trägt den Namen Mobistealth, wird von Kennern gelobt und ist in mehreren Varianten erhältlich. Es gibt Software-Pakete für Android-Smartphones, für iPhones, für BlackBerrys und Nokia-Geräte, auch Windows-Rechner und Apple-Computer können überwacht werden. Fast niemand ist vor diesen Angriffen sicher, nur die Benutzer des Linux-Betriebssystems.

Das Paket kann man nicht kaufen, nur mieten, es ist ein echtes Dumping-Angebot, drei Monate kosten 99 Dollar, und die Programme funktionieren tadellos. Es bietet einen Keylogger, der alle Tastenanschläge protokolliert, verschiedene Chatlogger, Fotos des Nutzers werden geschossen, ohne dass der etwas davon merkt, die Position des Rechners oder Handys wird übertragen, und bei Bedarf lassen sich die Mikrofone in dem Computer und dem Handy aktivieren. Man bezahlt den Service ganz einfach mit der Kreditkarte.

Wie andere Anbieter wirbt die Firma, mit deren Produkt ich ausspioniert werde, öffentlich im Internet. Besorgte Eltern, misstrauische Ehepartner und überforderte Chefs werden dort ermuntert, ihre Mitarbeiter, Ehepartner und Kinder auszuspionieren. Den Hinweis, dass der Einsatz aller Mobistealth-Programme in fast allen Ländern illegal ist, versteckt die Firma im Kleingedruckten.

Am zweiten Tag des Experiments logge ich mich bei meiner Bank ein, der Keylogger im Laptop leitet die Kennwörter an meine Hacker weiter. Als ich mich ausgeloggt habe, inspizieren sie mein Konto, erfahren mein monatliches Gehalt, die wiederkehrenden Ausgaben für das Haus. Auf dieselbe Weise verschaffen sie sich Zugang zu meinem Facebook-, meinem PayPal-, meinem iTunes-Account. Sie wissen jetzt, dass ich auf amerikanisches Popcorn-Kino stehe, auf Songs von Peter Fox, Keb’ Mo’ und Nickelback. Sie kennen das Geburtsdatum meiner Frau, das Alter meiner Kinder, meines Hundes. Sie wissen, dass unser Hund Jackie heißt und dass wir vor kurzem rund tausend Euro für Jackies Operation bei der Kleintierklinik Bremen bezahlt haben.

Am dritten Tag beenden meine Hacker das Datensammeln und schalten auf Angriff. Zunächst schreiben sie in meinem Namen eine Mail an die Carsharing-Firma, bei der meine Frau und ich unsere Autos mieten.

„Sehr geehrte Damen und Herren, am Sonntag den 4. August habe ich von 12 Uhr bis 14 Uhr den Ford Fiesta von der Station GEORG gemietet. Ich habe einen kleinen Unfall gehabt, dem Auto fehlen beide Außenspiegel. Das ist nicht schlimm, denn generell braucht man die Spiegel ja nicht, der Rückspiegel ist ja noch dran. Eigentlich wollte ich noch mal hingehen und den Spiegel wieder festkleben. Zeitlich schaffe ich es aber nicht. Melden Sie sich gern bei mir, am besten telefonisch auf meiner mobilen Nummer, dann kann ich Ihnen den Kleber übergeben. Beste Grüße, Uwe Buse.“

Dann wenden sich die Hacker meinem Amazon-Konto zu, bestellen eine Waschmaschine im Wert von 415,39 Euro und lassen Amazon wissen, dass ich mit meiner Kreditkarte zahlen werde.

Wenige Minuten später verschickt Amazon die Bestellbestätigung. Meine Hacker löschen sie in der Sekunde, in der die E-Mail auf meinem Konto eintrifft. Auf die Bestellbestätigung folgt eine Versandbestätigung. Sie erreicht mein Konto mitten in der Nacht, keiner meiner Hacker ist im Dienst, und am nächsten Morgen bin ich der Erste, der die E-Mail sieht.

Ich rufe bei Amazon an und lasse die Frau am anderen Ende der Leitung wis-

sen, dass ich die Annahme der Waschmaschine verweigern werde, weil ich sie nicht bestellt habe. Mein Konto, sage ich, sei offensichtlich gehackt worden.

Die Amazon-Mitarbeiterin scheint das nicht zu überraschen, sie rät mir, mein Passwort zu ändern, dann sollte das Problem aus der Welt geschafft sein.

Ich folge ihrem Rat, aber das Problem verschwindet nicht, denn Minuten nachdem ich das neue Passwort eingetippt habe, kennen es dank des Keyloggers auch meine Hacker.

Ich rufe wieder bei Amazon an. Dieses Mal verbindet mich die Frau von der Hotline mit der Sicherheitsabteilung des Unternehmens. Dort wirft jemand einen Blick auf mein Konto, sagt, das daure jetzt ein wenig, und verspricht zurückzurufen.

Zwei Stunden später klingelt mein Telefon, und ich erfahre, dass mein Amazon-Konto „total zerschossen“ sei und nicht mehr zu retten. Man rät mir, es aufzugeben und beim Surfen im Netz künftig vorsichtiger zu sein. Außerdem sei es sinnvoll, Anzeige bei der Polizei zu erstatten, gegen unbekannt. Eventuell würden die Beamten auch meinen Rechner untersuchen, in der Hoffnung, Hinweise auf die Täter zu finden.

Zeitgleich zur Amazon-Attacke greifen meine Hacker meinen Facebook-Account an. Zunächst haben sie vor, alle Bremer zu einer Party bei mir zu Hause einzuladen, dann haben sie eine andere Idee.

Da der infizierte Laptop ihnen die Zugangsdaten für meinen Facebook-Account geliefert hat, loggen sie sich problemlos ein, erweitern die Einstellungen zur Privatsphäre, loggen sich aus, damit die Einstellungen übernommen werden, und versuchen, sich dann erneut einzuloggen, aber das misslingt.

Facebook fordert meine Hacker auf, sich zu legitimieren. Das Unternehmen stellt die Sicherheitsfrage und will den Geburtsort meiner Mutter wissen. Meine Hacker arbeiten sich durch ihre Daten, sehen, dass ich in Ostfriesland geboren bin, und geben drei Städtenamen in Ostfriesland an. Sie liegen dreimal daneben. Facebook sperrt daraufhin den Zugang zu meinem Konto und fragt mich Sekunden später in einer E-Mail, ob ich gerade versucht hätte, meinen Account von Stockholm aus zu öffnen – mit einem Firefox-Browser, der auf einem Rechner installiert ist, auf dem Windows 7 läuft. Meine Hacker haben offenbar einen Anonymisierungsdienst benutzt, um ihre Identität und ihren Standort zu verschleiern.

Nachdem ich mein Konto wieder freigeschaltet habe, versuchen es meine Hacker erneut, raten dieses Mal bei der Sicherheitsfrage richtig und kapern meinen Account. Sie schreiben in meinem Namen: „Bewegend für mich, und vielleicht wisst ihr es ja längst. Ich bin schwul und habe jetzt auch einen Partner.“

Einer Freundin gefällt diese Mitteilung offenbar, sie zeigt es mit dem Symbol „Daumen hoch“. Eine andere Freundin bietet mir an, zur Verfügung zu stehen, wenn ich mich mal aussprechen wolle. Meine männlichen Freunde schweigen irritiert. Es ist der 14. August, von nun an gelte ich als schwul.

Das ist der Punkt, an dem ich mich frage, ob mir das Experiment über den Kopf wächst. Was wird wohl als Nächstes geschehen? Wird es mir überhaupt gelingen, die im Netz verstreuten Falschinformationen einzufangen und zu löschen? Es ist einfach, einen Rasenmäher zurückzuschicken, aber es ist schwierig, die eigene Identität zurückzubekommen, nachdem sie gekapert worden ist. Ich interessiere mich für Computer und Software, ich beschäftige mich seit Jahren damit, aber ich hätte nicht geglaubt, dass die Hacker mich derart hilflos machen könnten. Für die Welt da draußen bin ich jetzt schwul.

In den folgenden Tagen versuche ich, die Kontrolle über mein Facebook-Konto zurückzubekommen, aber das klappt nicht. Die Hacker haben alle persönlichen Daten geändert, für Facebook bin ich plötzlich ein Fremder, dem der Zugriff auf das Konto verweigert wird. Ich kann mein Konto nicht einmal mehr löschen. Ich kann auch niemanden bei Facebook um Hilfe bitten, weil Facebook keine telefonische Hilfe anbietet.

Während ich noch um mein Facebook-Konto kämpfe, loggen sich die Hacker in mein Bankkonto ein, schreiben eine Überweisung, fangen die TAN der Banküberweisung ab, die als SMS auf mein Handy geschickt wird, und leeren mein Konto. Das Geld parken sie auf Prepaidkarten, die nicht zu ihnen zurückverfolgt werden können.

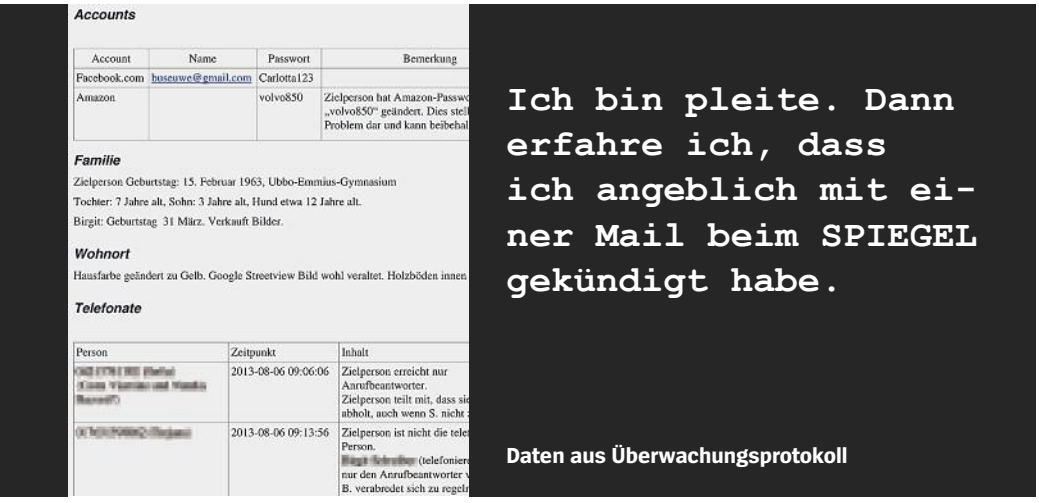
Ich rufe meine Bank an. Dort sagt man mir, dass ich zunächst eine Strafanzeige bei der Polizei stellen müsse, danach könne man versuchen, das Geld zurückzuholen. Außerdem werde man mir neue Zugangsdaten für mein leeres Konto schicken, mit der Post.

Bevor ich zur Polizei gehen kann, erfahre ich, dass ich angeblich gekündigt habe. Mein Ressortleiter beim SPIEGEL hat eine E-Mail von mir erhalten, in der ich ihm mitteile, dass ich die Nase von ihm voll habe, als Pressesprecher bei der Syss GmbH mehr verdienen könne und deshalb mit sofortiger Wirkung kündigte.

Meine Hacker lassen mich wissen, dass sie mir nun noch Kinderpornos auf den Rechner schieben können, danach könnten sie die Polizei alarmieren. Ich bitte sie dringend, von dieser Idee Abstand zu nehmen.

Ein paar Tage später sitze ich fluchend in meiner Küche und versuche, sämtliche Programme von meinem Laptop und meinem Handy zu löschen. Ich hoffe, dass die Viren danach auch verschwinden, aber optimistisch bin ich nicht. Wahrscheinlich haben sie sich zu tief in die Geräte gefressen. Mein Versuch in digitaler Selbstverteidigung, das ist jetzt klar, endet als totale Niederlage.

Um künftig besser auf solche Angriffe vorbereitet zu sein, frage ich meine Hacker ein paar Tage später, wie ich mich schützen kann. Ich soll ein Leben führen, das mich sehr anstrengen wird. Keine Windows-Rechner mehr benutzen, sagen sie, sondern Linux als Betriebssystem. Software-Updates immer installieren, und zwar schnell, das gilt vor allem für den Viren-Scanner. Eine Firewall einrichten, das Handy verschlüsseln, keine unnötigen Apps installieren. Kein Homebanking mehr, raten sie mir, schon gar nicht über das Handy, sondern immer persönlich zur Bankfiliale gehen und einen Vordruck ausfüllen. Ich soll wieder einem Stück Papier vertrauen.



Accounts

Account	Name	Passwort	Bemerkung
Facebook.com	buseuwe@gmail.com	Carlotta123	
Amazon		volvo850	Zielperson hat Amazon-Passwo „volvo850“ geändert. Dies stel Problem dar und kann beibehal

Familie

Zielperson Geburtstag: 15. Februar 1963, Ubbo-Emmius-Gymnasium

Tochter: 7 Jahre alt, Sohn: 3 Jahre alt, Hund etwa 12 Jahre alt.

Birgit: Geburtstag 31 März. Verkauft Bilder.

Wohnort

Hausfarbe geändert zu Gelb. Google Streetview Bild wohl veraltet. Holzböden innen

Telefonate

Person	Zeitpunkt	Inhalt
[redacted]	2013-08-06 09:06:06	Zielperson erreicht nur Anrufbeantworter. Zielperson teilt mit, dass sie abholt, auch wenn S. nicht
[redacted]	2013-08-06 09:13:56	Zielperson ist nicht die telef Person. [redacted] (telefoniert nur den Anrufbeantworter B. verabredet sich zu regelm

Ich bin pleite. Dann erfahre ich, dass ich angeblich mit einer Mail beim SPIEGEL gekündigt habe.

Daten aus Überwachungsprotokoll

Video: So wurde Uwe Buse gehackt

spiegel.de/app422013hacker
oder in der App DER SPIEGEL