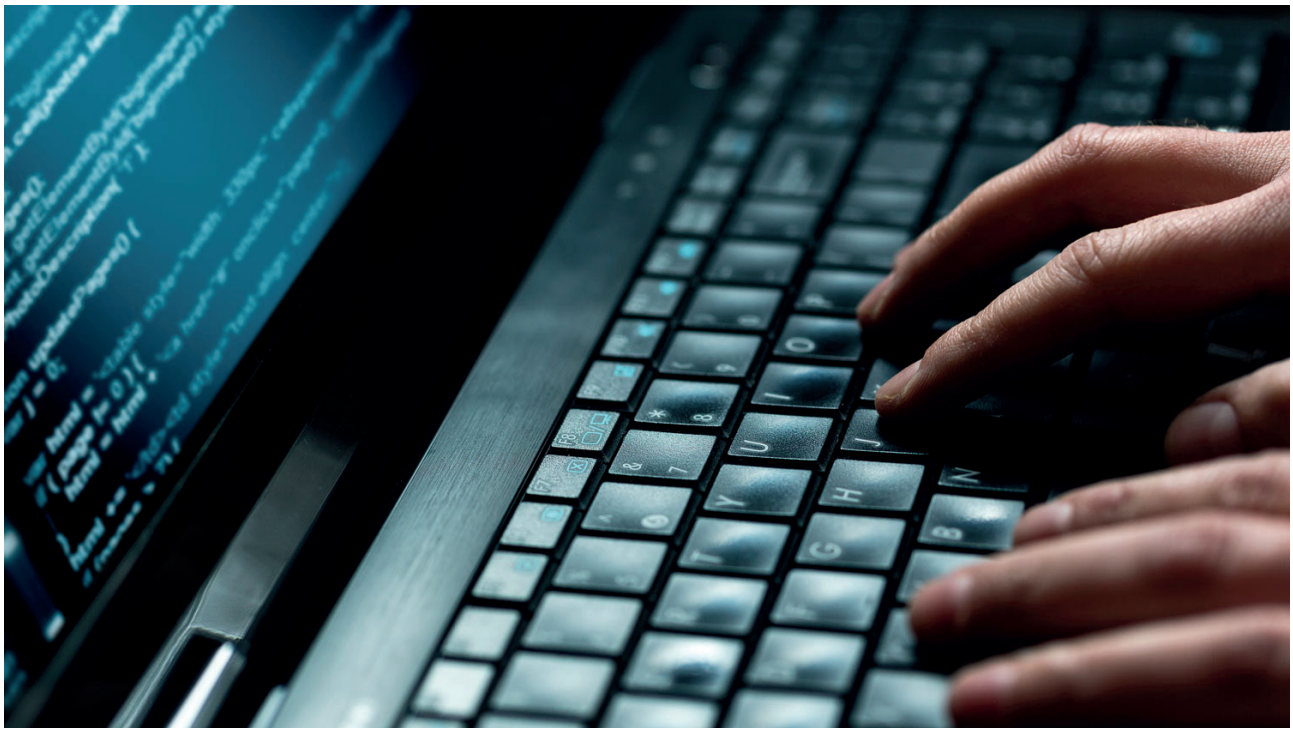
Wochenkommentar 02/2019 von Matthias Zehnder

Schwachstelle Mensch



In den letzten Wochen des vergangenen Jahres haben unbekannte Hacker in Deutschland im grossen Stil vertrauliche Daten von Politikern und anderen Prominenten veröffentlicht. Jetzt hat sich herausgestellt: Es war kein fremder Geheimdienst, der die Menschen im grossen Stil ausspioniert hat und auch keine Verbrecherbande. Es war ein Jugendlicher. Was das bedeutet? Es zeigt vor allem, wieviele Menschen von der computerisierten Umwelt überfordert sind – und wie wenig Anbieter sie unterstützen.

Für viele deutsche Prominente hat das Jahr 2019 schlecht begonnen: Hacker haben im Internet massenweise persönliche Daten von Politikern und Journalisten veröffentlicht, darunter Handynummern, private Adressen, Briefe und Kreditkartendaten. Betroffen waren alle im Bundestag vertretenen Parteien – alle ausser der AfD. Die Daten waren zwar schon vor Weihnachten auf Twitter veröffentlicht worden. Aufgefallen ist es aber erst letzte Woche, weil Politiker wie Martin Schulz (SPD) plötzlich unflätige Anrufe auf ihre eigentlich geheime Handynummer erhielten.[1]

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) nahm Ermittlungen auf. Das Nationale Cyber-Abwehrzentrum übernahm die zentrale Koordination. Die Rede war von einem der grössten Hackerangriffe, die Deutschland je erlebt hatte. BSI-Präsident Arne Schönbohm ging davon aus, dass über 1000 Politiker, Journalisten und Prominente vom Cyberangriff betroffen waren.[2] Natürlich schossen sofort Spekulationen darüber ins Kraut, wer dahinter stecken könnte: Ein Cyberangriff einer fremden Macht? Ein Hacker-Kollektiv? Eine Diebesbande?

Doxing aus Ärger

Alles falsch: Es war ein Jugendlicher, ein knapp 20 Jahre alter Schüler. Er

lebt noch bei seinen Eltern in Mittelhessen, also in der Region zwischen Frankfurt, Düsseldorf und Kassel mitten in Deutschland. Die Generalstaatsanwaltschaft Frankfurt am Main gab Anfang der Woche bekannt, das Bundeskriminalamt (BKA) habe die Wohnung des Jugendlichen durchsucht und ihn vorläufig festgenommen. Der Verdächtige sei geständig: Er habe *die gegen ihn erhobenen Vorwürfe umfassend eingeräumt und über eigene Straftaten hinaus Aufklärungshilfe geleistet*, teilt die Generalstaatsanwaltschaft etwas umständlich mit.[3]

Der jugendliche Hacker hatte sich offenbar über öffentliche Äusserungen der betroffenen Politiker, Journalisten und Prominenten geärgert und aus Rache persönliche Informationen der Promis veröffentlicht. «Doxing» heisst das im Cyber-Jargon. Ziel von Doxing ist es, die Privatsphäre aufzubrechen und die Opfer blosszustellen, indem Fotos, Kontaktangaben und private Daten aus E-Mails oder aus Chats veröffentlicht werden. Doxing ist also eine Art «Cyber-Mobbing». Veröffentlicht hatte der Hacker die Daten unter anderem über ein Twitter-Konto, auf dem er sich «God» nannte – mit der Adresse «@_Orbit».[4]

Gott bekam kalte Füsse

Als plötzlich die Bundespolizei in ganz Deutschland nach ihm fahndete, bekam «God» kalte Füsse. Er versuchte, seine Spuren zu verwischen, die Festplatten zu löschen und die Computer auf einem Recycling-Hof zu entsorgen.[5] Bloss ist es in der digitalen Welt nicht ganz so einfach, Spuren und Indizien auszumerzen. So kamen die Beamten dem jungen Mann rasch auf die Spur. Laut BKA hatte er keinerlei Informatikausbildung, er hat sich das Hacken selber beigebracht.

Der junge Mann ist inzwischen wieder zu Hause. Er zeige Reue und es bestehe keine Fluchtgefahr. Martin Schulz hat eine neue Handy-Nummer und wieder seine Ruhe, viele andere Politiker rund Prominente sind mit dem Schrecken davongekommen. Für den einen oder die andere mögen die Daten, die der Hacker veröffentlichte, peinlich oder ehrenrührig sein. Die Verletzung der Privatsphäre ist auch dann schmerzhaft und unangenehm, wenn sie «nur» elektronisch erfolgt. Und jetzt? Was geht uns das an? Und in der Schweiz?

Wir überforderten Benutzer

In erster Linie zeigt der Fall, dass sehr viele Benutzerinnen und Benutzer im Umgang mit Computer, Handy und Internet überfordert sind. Der junge Hacker konnte sich persönlicher Daten bemächtigen, weil die Promis auch einfachste Sicherheitsregeln nicht beachteten. Ein Beispiel: Das am häufigsten verwendete Passwort ist nach wie vor «123456». Das ist so absurd, wie wenn man sein Einfamilienhaus mit einem Spielzeugschlüssel von IKEA abschliessen würde. Auf der Liste der beliebtesten Passwörter befinden sich laut Hasso Plattner Institut der Universität Potsdam weitere Zahlenreihen – und das Wort «Passwort».[6] Zweiter Kardinalfehler: Viele Benutzerinnen und Benutzer setzen bei allen Diensten dasselbe Passwort ein. Stösst ein Hacker auf dieses Passwort, kann er sich wie mit einem Generalschlüssel überall Zutritt verschaffen.

Die meisten Menschen nutzen Computer wie ein Auto oder die Stereoanlage: als nützliche Geräte, die man nicht weiter verstehen muss. Das ist gefährlich, weil sich die Computertechnik extrem schnell entwickelt. Alle

eineinhalb Jahre verdoppelt sich die Rechenkraft, die man für das gleiche Geld kaufen kann. So lautet Moores Gesetz, das nach Gordon Moore benannt ist, einem der Gründer der Chipfabrik Intel. Wir sind uns gar nicht bewusst, dass wir mit unseren Smartphones eigentlich kleine Supercomputer in der Westentasche herumtragen. Noch vor 20 Jahren wären Spezialgeräte von der Grösse eines Familienkühlschranks nötig gewesen, um diese Power anzubieten – Spezialgeräte, die von Spezialisten betreut wurden. Heute hat jeder so einen Supercomputer in der Hosentasche – freilich ohne jegliche Spezialausbildung. Das ist, wie wenn man einen Fahrschüler in ein Formel 1-Auto setzen würde – oder einen Kindergärtner bitten würde, mal eben die Dogge zu halten.

Schwachstelle Mensch

Deshalb wären eigentlich die Anbieter gefordert, ihre Dienste so auszugestalten, dass man sie nur sicher benutzen kann. Es wäre zum Beispiel relativ einfach für einen Mail-Dienst oder einen Onlineshop, prinzipiell nur sichere Passwörter zuzulassen. Ausser Onlinebanken hat jedoch kaum ein Anbieter Restriktionen eingebaut. Onlineshops wollen es ihren Kundinnen und Kunden so einfach wie möglich machen. Nur ja keine Hürden aufbauen, der Kunde könnte sich den Kauf sonst noch einmal überlegen. Dazu kommt, dass viele Anbieter selbst hoffnungslos überfordert sind.

Bei Anbietern und bei Konsumenten gilt deshalb: Computer könnten sicher sein, die eigentliche Schwachstelle aber ist und bleibt der Mensch. Das ist nichts Neues. Als einer der bekanntesten und gefährlichsten Hacker der Welt galt und gilt Kevin Mitnick. [7] Als er nach einer langen Haftstrafe 2003 auf Bewährung in die Freiheit entlassen wurde, habe ich ein Interview mit ihm geführt. Er sagte mir damals, dass das wichtigste Arbeitsprinzip eines Hackers nicht Geheimprogramme oder spezielle Programmierkenntnisse seien, sondern das so genannte «Social Engeneering» sei: *Die Bandbreite reicht dabei vom einfachen Anruf bei einem vertrauenswürdigen Angestellten einer Firma und einem lockeren Gespräch über Passworte bis zum komplexen, mehrschichtigen Angriff wie in einem Schachspiel,* erklärte mir Mitnick. Social Engeneering, das Erschleichen von Passwörtern und Zugängen über Menschen, sei meist viel einfacher, als das Knacken von Sicherheitstechniken.

Der versteckte Preis der Computerei

Wir staunen manchmal, wie günstig heute superschnelle Computer sind, wie einfach wir an Hochleistung durch Rechner kommen, was unsere Handydienste alles fertigbringen. Das Beispiel des deutschen Kinderzimmer-Hackers zeigt, dass wir den Preis für diese supergünstige Supertechnik möglicherweise auf einer ganz anderen Ebene bezahlen, als uns bewusst ist. Nötig im Umgang mit Computer, Handy und Internet wäre deutlich mehr Respekt und Vorsicht – und eine sehr viel bessere Ausbildung, bei Anbietern und bei Benutzern. Wer möchte sich schon ohne Vorbereitung in einen vollgetankten Formel-1-Boliden setzen.

Basel, 11. Januar 2019, Matthias Zehnder **mz@matthiaszehnder.ch**

PS: Nicht vergessen – **Wochenkommentar abonnieren.** Kostet nichts, bringt jede Woche ein Mail mit dem Hinweis auf den neuen Kommentar und einen Buchtipp. Einfach **hier klicken.**

Ein Tipp zu sicheren Passwörtern

Sichere Passwörter bestehen aus einer zufälligen Folge von Buchstaben, Zahlen und Sonderzeichen. Sie sehen also zum Beispiel so aus: *W6TjAmufsA* Dieses Passwort habe ich mir nicht selbst ausgedacht: Solche Passwörter lasse ich mir von meinem Passwortmanager generieren. Das ist eine App, mit der ich die Benutzernamen und Passwörter all der Webseiten und Dienste verwalte, die ich benutze. Ohne einen solchen Passwortmanager geht es heute nicht mehr. Denn sichere Passwörter kann man sich fast nicht merken – schon gar nicht, wenn es für jeden Dienst ein neues Passwort sein soll, das auch noch regelmässig ausgewechselt wird. Die beiden bekanntesten Passwortmanager sind LastPass und OnePassword. Beide gibt es als App für das Handy, als Programm für den Computer und als Plugin (Zusatz) für den Webbrowser.

LastPass: https://www.lastpass.com/de

OnePassword: https://1password.com/de/

Quellen

1 Vgl. «Der Spiegel», 4.1.2019, http://www.spiegel.de/politik/deutschland/medienbericht-ueber-hacker-angriff-auf-hunderte-deutsche-politiker-a-1246359.html
2 Vgl. Zeit Online, 4.1.2019, https://www.zeit.de/video/2019-01/5986019427001/datendiebstahl-eine-hoehere-zweistellige-zahl-von-angriffen-die-sehr-erfolgreich-waren
3 Vgl. Pressemitteilung des BKA vom 8. Januar 2019: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2019/Presse2019/190108_FestnahmeDatenausspaehung.html
4 Vgl. «Spiegel» vom 8.1.2019; http://www.spiegel.de/netzwelt/web/hackerangriff-tatverdaechtiger-ist-wieder-auf-freiem-fuss-a-1246965.html
5 Vgl. «Spiegel» vom 10.1.2019: http://www.spiegel.de/netzwelt/web/daten-leak-so-wollte-0rbit-seine-spuren-verwischen-a-1247415.html
6 Vgl. Pressemitteilung des HPI vom 18.12.2018: https://hpi.de/pressemitteilungen/2018/die-top-ten-deutscher-passwoerter.html
7 Wie viele andere, ehemalige Hacker führt Mitnick heute eine eigene Sicherheitsfirma: https://mitnicksecurity.com/about/kevin-mitnick-worlds-most-famous-hacker-biography