CARL VON OSSIETZKY universität OLDENBURG
FAKULTÄT II
DEPARTMENT FÜR INFORMATIK

INFORMATIK und Gesellschaft

Wintersemester 2014/2015

AutorInnen: Studierende des Moduls
Informatik und Gesellschaft

Hrsg.: Hans Fleischhack, Gerrit Klasen,
Christin Poloczek, Christoph Simm,
Tobias Wigbers, und Elke Wilkeit

Version 1.0 vom 24. 04. 2015, 17:01 Uhr

Impressum: Dieses E-Book entstand während des Wintersemesters 2014/15 an der Carl von Ossietzky Universität Oldenburg. HerausgeberInnen sind die BetreuerInnen des Moduls Informatik und Gesellschaft, AutorInnen sind Studierende des Moduls.

Inhaltsverzeichnis

Oldenburg. 6:30 Uhr – der Wecker klingelt. Und auch an diesem Morgen muss Anton H. (Name geändert) feststellen, dass die Nacht mal wieder viel zu kurz war. Verträumt geht er in das Badezimmer, um eine Dusche zu nehmen. Bereit für den Tag führt sein Weg in die Küche, wo er sich einen Kaffee kocht. Nebenbei schaltet Anton sein Smartphone ein, vielleicht gibt es Neuigkeiten. Während der Kaffee zubereitet wird, erhält er gleich mehrere Mitteilungen über verpasste Anrufe, neue Textnachrichten und Terminerinnerungen. Er denkt sich im Stillen: Muss das sein? Mit dem Kaffee geht er in sein Arbeitszimmer, setzt sich an seinen Schreibtisch und schaltet seinen Laptop ein. Der Blick aus dem Fenster verrät: Heute wird ein guter Tag! – der Sonnenaufgang ist fantastisch. Schnell muss Anton diesen Eindruck seinen Freunden mitteilen. Er nimmt sein Smartphone zur Hand, macht ein Foto und postet es direkt auf seiner Facebook-Pinnwand. Er ist jedes Mal darüber erstaunt, wie hervorragend die App (Anwendung) von Facebook auf seinem Smartphone funktioniert. In Windeseile erhält er Rückmeldungen auf seinen Post (die gesendete Nachricht). Nach fünf Minuten haben bereits 30 von seinen 1.254 Freunden die Meldung „geliked“. Da Facebook neben dem Foto auch seinen aktuellen Aufenthaltsort anzeigt, wissen seine Freunde genau, wo Anton sich gerade befindet. Schnell schreibt er auch noch per Twitter, dass der heutige Tag ein ganz besonderer wird. Beim weiteren Stöbern auf Facebook wird er darauf hingewiesen, dass es ab sofort auch eine Kaffeemaschine gibt, die mit einem Smartphone kommuniziert. Es sei so möglich, den eigenen Kaffee auf dem Smartphone zu konfigurieren und danach erzeugen zu lassen. Anton findet diese Möglichkeit toll, fragt sich jedoch, warum Facebook ihm eine solche Maschine als Anzeige präsentiert. Er öffnet sein Mailprogramm, um neue Nachrichten abzurufen. Acht neue Mails sind eingegangen. Unter anderem ist eine Einladung zu einer Informationsveranstaltung rund um das Thema „Big Data“ dabei. Dieser Begriff ist ihm fremd. Er beginnt die Nachricht zu lesen: „Big Data – ein Thema, von dem Sie möglicherweise nichts wissen, welches sich allerdings längst auf Sie auswirkt. Ein Thema, dem sich die Forschung interessiert zuwendet und dessen Potenzial die Wirtschaft längst erkannt hat. Ein Thema, welches unsere

Gesellschaft zunehmend beeinflussen wird. Doch was ist Big Data eigentlich?

Big Data (von engl. big = groß, data = Daten) beschreibt zum einen das Vorhandensein einer schieren Unmenge an Daten und zum anderen die Möglichkeiten der Auswertung und Analyse, die diese bietet. Die technische Entwicklung, insbesondere die Entwicklung in der Informations- und Kommunikationstechnologie, macht dieses möglich. Aktuelle Prognosen zeigen: Der Umfang an vorhandenen Daten verdoppelt sich alle zwei Jahre. Das Thema Big Data gewinnt zunehmend an Bedeutung. Ein Großteil der erhobenen Daten wird inzwischen auf Webseiten und durch Apps generiert. Sie ergeben sich aus vom Nutzer eingegebenen, bereitgestellten Daten und aus Daten, die während des Besuchs der Seite bzw. während der Verwendung der App automatisch erzeugt werden. Beispiele sind „Social Media"-Dienste wie Facebook und Twitter. Ein Post bzw. Tweet verrät mehr, als viele Nutzer erahnen. Und auch wenn der Post nur beschränkt einsehbar ist – die Dienstanbieter kennen alle zugehörigen Informationen und wissen diese zu verwenden, auch wenn dieses aufgrund der aktuellen Rechtslage eine diffizile Thematik ist. Nicht nur die Texte können analysiert werden, auch Bilder bieten Möglichkeiten der Auswertung. Neben den offensichtlich veröffentlichten Daten werden bei der Verwendung solcher Anwendungen bzw. Webseiten Daten über das Nutzungsverhalten erhoben. Welcher Link wurde angeklickt, um auf die Seite zu gelangen? Welche Unterseiten wurden besucht? Wie oft wurden diese besucht? Welche Profile hat sich der Nutzer angesehen? Welche funktionalen Elemente, wie Eingabefelder und Buttons, hat er verwendet? Welche Produkte hat er genauer betrachtet? Welche Produkte hat er letztendlich gekauft? All diese Informationen sind wertvoll, da sie einiges über den Nutzer und sein Verhalten verraten. Es kommt nicht von ungefähr, dass Amazon seinen Kunden genau das dritte Buch einer Trilogie anbietet, dessen ersten beiden Teile sie bereits über Amazon bestellt haben. Grundsätzlich müssen solche Funktionen nicht schlecht sein. Es ist schließlich hilfreich, wenn einem direkt die neue Staffel der Serie angeboten wird, die man so gerne mag. Allerdings sollte man sich immer die Frage stellen, welchen Nutzen der Anbieter aus solchen Funktionen zieht. Es ist sicherlich kein Zufall, dass Facebook WhatsApp aufkauft oder dass Google autonom fahrende Autos und internetfähige Brillen anbietet. Google ist insofern ein gutes Beispiel, als dass die Suchanfragen, die in die Suchmaschine von Google eingegeben werden, ein schier unglaubliches Analysepotenzial bieten. Ein Fakt über den man sich bei der Verwendung der Suchmaschine vermutlich nie Gedanken gemacht hat.

Aber nicht nur Internetanwendungen bieten Anwendungsfelder für Big Data. Heutzutage werden Daten in fast jedem Lebensbereich erzeugt und gesammelt. Jedes automatisierte System benötigt Informationen, nach denen es sich richtet. Das Auto, das Sie fahren, verwendet eine Vielzahl von Sensoren und Mini-Computern, die die gesammelten Daten auswerten. Bei einem Aufprall wird der Airbag ausgelöst und der Motor wird automatisch eingestellt je nach Temperatur des Kühlwassers. Die Straße, auf der Sie fahren, wurde wegen des hohen Verkehrsaufkommens durch das Verkehrsleitsystem zum Befahren freigegeben. Ihr Handy fungiert als Navigationsgerät und ermittelt Ihre GPS-Koordinaten. Diese Daten werden heute möglicherweise weder ge-

sammelt noch analysiert. In der Zukunft könnte dieses aber der Fall sein. Auch hier gilt: Es kann nicht schaden, sich zu überlegen, welche Möglichkeiten in solchen Daten stecken. Welches Interesse könnte ein Versicherungsunternehmen an Ihren Fahrdaten haben? Auch im Bereich der Heimautomatisierung, dem Automatisieren von Licht, Heizung und Sicherheitssystemen sowie Geräten und deren Vernetzung im Haus, sollte man sich Gedanken darüber machen, wofür diese Daten noch verwendet werden könnten. Könnte es interessant sein, dass ich ein Frühaufsteher bin, der viel Kaffee trinkt? Könnte jemand wissen, ob ich mich lieber in meinem Fitnessraum oder vor meinem Fernseher auf dem Sofa aufhalte?“

Anton blickt von seinen Computer auf und greift zu seinem Smartphone, um seinen Kalender aufzurufen. Offensichtlich hat er seine E-Mails seit zwei Tagen nicht gelesen, denn die Informationsveranstaltung findet gleich heute statt. Da er Urlaub hat, beschließt er an dieser Veranstaltung teilzunehmen. Er möchte Näheres zur Auswertung seiner persönlichen Daten erfahren. Die Veranstalter haben sich zum Ziel gesetzt, Bürgerinnen und Bürger dahingehend aufzuklären, welche Möglichkeiten Unternehmen haben, den wohl größten Profit durch die Auswertung ihrer Daten zu erwirtschaften und welche gesellschaftlichen Konsequenzen ein Fortdauern dieser Art der Datenerhebung haben wird. Die Veranstaltung scheint auf großes gesellschaftliches Interesse zu stoßen. Anton betritt den Saal und schon beginnt die Eröffnungsansprache.

„Sicherlich hat ein Großteil der hier Anwesenden heute bereits sein Facebook-Profil gecheckt und zahlreiche Werbeanzeigen eingeblendet bekommen?“ – Er fühlt sich ertappt. – „Diese sogenannten Facebook-Ads sind Werbeanzeigen, deren Platz Unternehmen für einen bestimmten Preis erwerben können. Auf der Grundlage der über Ihr Klickverhalten erhobenen Daten ist es Facebook möglich, zielgruppenorientierte Werbung zu schalten. Dieses geschieht, indem eine Auswertung in Form von Klick-Pfad-Analysen und Tracking-Analysen sowie auch Third-Party-Cookies vorgenommen wird – doch was versteht man darunter? Wir möchten Ihnen Einblicke geben über die Informationen, die Facebook über Sie erhebt und auswertet, Sie in Zielgruppen einteilt und entsprechend individualisierte Zielgruppenpakete an eine Vielzahl von Unternehmen verkauft. Wenn Sie sich im Internet auf verschiedenen Internetseiten bewegen, ist es möglich, diesen Klick-Pfad nachzuvollziehen und anhand der Aufenthaltsdauer auf verschiedenen Internetseiten Ihre Präferenzen festzustellen. Bei Tracking-Analysen wird Ihnen beispielsweise ein Tracking-Parameter an die URL (Internetadresse) angehängt, welchen Sie Klick für Klick auf Ihrer Reise durch das Web mitnehmen. Theoretisch wäre es möglich Cookies durch entsprechende Einstellungen in Ihrem Internetbrowser zu unterdrücken und zu verbieten – theoretisch. Denn sogenannte Third-Party-Cookies machen es möglich, dass die Werbetreibenden selbst diese Daten auswerten, indem sie die gespeicherten Daten auf einen anderen Server umleiten. So verwundert es also herzlich wenig, dass Sie heute Morgen beim Abrufen Ihrer Facebook-Seite neben den neuen Laufschuhen auch die bekannte Pulsuhr zu Ihrer Sport-Tracking-App eingeblendet bekommen haben. Immerhin haben Sie erst gestern den erfolgreichen Lauf von Ihrer App aufzeichnen lassen, um Ihre Erfolge mit Ihren Freunden auf

Facebook zu teilen und sich durch Likes während Ihres Laufes motivieren zu lassen. Die Wirtschaft hat längst schon das große Potential entdeckt, diese Daten nicht bloß hinsichtlich der Produktentwicklung und zielgerichteter Werbemittel auszuwerten, sondern geht mehr und mehr dazu über, all diese vielseitigen, auf den ersten Blick nicht miteinander in Verbindung stehenden Daten in einen Bezug zueinander zu bringen. Unternehmen können nämlich wichtige Erkenntnisse aus den Verhaltens- und Bewegungsmustern ihrer Kunden gewinnen. So können beispielsweise Datensätze aus Social-Media-Kanälen mit Daten aus Kundendatenbanken und Bestellvorgängen sowie Finanzmarktdaten miteinander verbunden werden. Mehr und mehr wird es für Unternehmen möglich Ihre vorliegenden persönlichen Daten, neben der Produktentwicklung und Optimierung, die Ihnen ja auch einen Vorteil verschaffen, für eigene Zwecke auszuwerten. Dadurch, dass zunehmend umfassendere Algorithmen zur Auswertung vieler verschiedener Formate Ihrer Daten wie beispielsweise Text, Sprache, Audio, Video, usw. entwickelt werden, könnte man sich die Frage stellen, ob wir nicht alle immer mehr zum Spielball werden.

Unternehmen nutzen unsere Daten, um die gewonnen Erkenntnisse in die Marktanalyse einfließen zu lassen und um ihre Position gegenüber den Mitwettbewerbern zu verbessern. Das Tracking unserer Daten ermöglicht es zudem, Risikofaktoren für diverse neue unternehmerische Ansätze zu berechnen und u. a. zu zeigen, wie Trends hinsichtlich Markt und Kunde zeitnah erkannt werden können. Welche Daten miteinander in Verbindung gesetzt werden, ist abhängig vom jeweiligen Unternehmen. Bei einer umfassenden Analyse der vorliegenden Daten kann zudem der Bedarf an weiteren Informationen ermittelt werden. Aus diesen können im nächsten Schritt Analysealgorithmen abgleitet werden. So wird es möglich einen ganzheitlichen Überblick zu gewinnen – über Ihren alltäglichen Lebensablauf, Ihre Gewohnheiten, wann Sie aufstehen, wann Sie zur Arbeit fahren, wie viele Kalorien Sie beim Sport verbrennen, u. v. m. – Man möchte sich nicht ausmalen, welche Möglichkeiten Facebook hat, mit diesen sensiblen Daten zu hantieren, geschweige denn, welche gesellschaftlichen Folgen für die Zukunft entstehen könnten, würden diese Datenmengen in die Hände der falschen Personen gelangen. Ein Knopfdruck und die Analyse all dieser Daten könnte an Behörden, Versicherungen, etc. vermittelt werden. Aufgrund des hohen Potentials der verfügbaren Daten wird Big Data auch gerne als das neue Gold bezeichnet.“

Anton schreckt auf und überlegt, ob er das Licht abgeschaltet hat und ob sich sein Verhalten wohl auf seinen Versicherungsbeitrag auswirken könnte und wie sein Tagesstart in der Zukunft aussehen könnte, wenn Big Data in unserer Gesellschaft Einzug erhalten hat. Bestimmt würde sein Wecker klingeln, ohne dass er ihn gestellt hätte. Der Wecker hätte Zugriff auf Antons geplante Aktivitäten, die aus seinem Kalender ausgelesen werden. Auch Freunde, Kollegen und Familienmitglieder wüssten, was seine Absichten für den Tag sind und könnten so gleich sehen, ob Anton beschäftigt ist. Antons Lieblingsnachrichtensender würde automatisch mit dem Klingeln des Weckers eingeschaltet werden. Dieser Sender ist nicht mehr vergleichbar mit früheren. Er würde Anton flexibel über alle wichtigen Ereignissen, die auf ihn zugeschnitten sind, informieren. So erfährt

er neben den lokalen und weltweiten Nachrichten auch Erinnerungen an Geburtstagen seiner Freunde, Familienmitglieder und Arbeitskollegen. Während er in das Bad geht, würde ihm das Bild des Senders folgen. Alle Spiegel und Glasflächen im Haus würden als Bildschirme dienen. Im Badezimmer angekommen würde Anton gleich angezeigt werden, dass er mal wieder Zahnseide nutzen sollte. Anton würde sie natürlich umgehend nutzen, da sonst seine Versicherung wieder seine Beiträge erhöht. Nach dem Putzen seiner Zähne geht Anton in die Dusche. Diese würde ihn automatisch erkennen und sich auf sein Profil, Duschstrahl und Duschwärme, einstellen. Nachdem Anton seine Dusche beendet hat, würde bereits die Kleidung bereitliegen. Sie würde anhand eines Algorithmus, der seine für den Tag geplanten Aktivitäten und sein Verhalten berücksichtigt, vom Kleiderschrank ausgesucht werden. Dabei würden ihm die neuen Socken ins Auge fallen, die seine Wohnung neu bestellt hätte, da sein älteres Paar ein Loch hatte. Zum Glück könnte Anton Grenzen für die Einkaufswut seiner Einrichtung festlegen. In der Küche stünde Kaffee und Essen bereit. Seine Wohnung wüsste, wonach er sich sehnt.

Anton fühlt sich in eine andere Welt versetzt und verlässt beeindruckt die Veranstaltung. Ihm war bewusst, dass es auch in der Technologiebranche, wie in jeder Branche, Entwicklungen geben würde. Dass sich die Welt durch Big Data aber so grundlegend verändern kann, war ihm vorher nicht bewusst. Und: Wir stehen erst am Anfang der Big-Data-Entwicklung.

Informationen entnommen von der Seite http://www.informatik.uni-oldenburg.de/~iug14/bi/.

Cyberwar

Welche Infrastrukturen sind wie gefährdet?

Hendrik Bodenstein, Frank Juchim, Mark Otten, Daniel Patron, Jonas Retz, Alexander Söker, Robin Speidel, Patrick Wagener

Das Thema Cyberwar wurde in den letzten Monate immer präsenter in den Mainstream-Medien und somit auch transparenter für die Gesellschaft. Die klassischen Methoden, um einen Cyberwar zu führen, liegen darin, den Gegner mit Hilfe von DDoS-Attacken und Defacement moralisch zu schwächen. Mit diesen Methoden werden in erster Linie Websites für kurze Zeit unerreichbar, oder es wird die Meinung der Angreifer auf diesen zu Propagandazwecken veröffentlicht. Das Gefühl, dass auf der eigenen Website die Meinung des Gegners steht, mag vielleicht sehr ernüchternd und provozierend sein, die Frage, die jedoch aufgeworfen wird, ist, inwieweit ein Cyberwar für den Otto-Normal-Verbraucher relevant ist beziehungsweise gefährlich werden könnte. Was ist das eigentliche Horror-Szenario, was ist theoretisch möglich in einem Cyberwar und wieso ist davor niemand wirklich sicher? Anschließend wird geklärt, was die Auswirkungen dieser Attacken sind und wie die Gesellschaft damit umgeht.

Die Frage nach einem solchen Horror-Szenario soll nun in drei Schritten beantwortet werden. Zunächst bedarf es einer sogenannten Einstiegsphase. Innerhalb dieser wird die Gesellschaft nichts von einer drohenden Gefahr erahnen können. In einem fiktiven Szenario, bei dem die Bundesrepublik Deutschland Ziel einer Cyberattacke und somit auch Teil eines Cyberwars wird, könnte ein Auslöser beispielsweise auf der wirtschaftlichen Ebene genügen. Die Bundesrepublik Deutschland vernachlässigt die diplomatischen Verbindungen zu Russland und kritisiert die Politik Putins. Mehrere Unternehmen boykottieren den Export nach Russland. Diese Punkte könnten einen Cyberwar auslösen. Die russische Regierung lässt sich dadurch so sehr provozieren, dass sie die regierungseigene Hackergruppe beauftragt, sich Zugang zu deutschen Kraftwerken und der Stromversorgung zu verschaffen. Mit Hilfe eines ausgeklügelten Wurmes werden diverse Steuerungselemente der Kraftwerke, ähnlich wie es bei dem realen Vorfall des Stuxnet-Wurmes der Fall war, ins Visier genommen.

Im privaten Rahmen besuchen einige Mitarbeiter eines brandenburgischen Erdgas-Kraftwerkes die internationale Computerausstellung CeBit. Dort wird ihnen an einem Stand ein Werbegeschenk in Form eines USB-Sticks überreicht. Ahnungslos benutzen sie diesen vorwiegend für den privaten Gebrauch, jedoch auch für den Datentransfer von Dokumenten im Firmennetzwerk. Normalerweise sollten die Mitarbeiter eines strategisch wichtigen Unternehmens durch Lehrgänge und Seminare darüber informiert werden, welche Aktionen innerhalb eines Firmennetzwerkes erlaubt sind beziehungsweise als gefähr-

lich eingestuft werden, wie zum Beispiel das Installieren von fremder Software aus dem Internet oder das Anschließen ungeprüfter Datenträger und Endgeräte innerhalb des Firmennetzwerkes. Aufgrund von Organisationsproblemen fand eine solche Sicherheitsbelehrung der Mitarbeiter bisher in diesem Kraftwerk noch nicht statt. Ein folgenschwerer Fehler: Da auf dem präparierten Werbegeschenk Schadsoftware in Form des zuvor erwähnten Wurmes installiert wurde, kann sich dieser nun unkontrolliert im gesamten Firmennetzwerk ausbreiten. Somit ist der Zugang für die russische Hackergruppe gelegt und weitere Attacken und Angriffe können nun ohne größeren Aufwand gestartet werden.

In betroffenen Erdgas-Kraftwerk kommt es nun zu einem Defekt in der Technik, sodass zunächst 500 Haushalte für mehrere Stunden ohne Strom auskommen müssen. Dies könnte ein erstes Testen der Wirksamkeit des Wurmes, den die russische „Hackerarmee“ eingeschleust hat, sein. Somit ist klar, das Projekt „Blackout“ kann durchgeführt werden. Innerhalb der Bevölkerung wird dieser Stromausfall nur bei den Betroffenen wahrgenommen und bekommt maximal in der regionalen Zeitung ein wenig Aufmerksamkeit. Die Energie-Experten vor Ort gehen zu diesem Zeitpunkt von einem technischen Defekt aus, der auf Verschleiß gewisser Bauteile zurückgeführt wird. Ein fataler Fehler, wenn man betrachtet, was im Folgenden passieren wird. Zu diesem Zeitpunkt wäre es durchaus noch möglich gewesen, sich gegen den drohenden Blackout zu wappnen.

In einem nächsten Schritt werden immer mehr Kraftwerke in den Fokus der Angriffe genommen. Die Stromausfälle häufen sich und die nationalen Medien werden aufmerksam und befragen Experten nach Gründen für diese Zwischenfälle. Diese fangen langsam an, von einem Fremdverschulden auszugehen, eine genaue Identifikation der Verursacher ist aber noch nicht erfolgt. Die ersten Untersuchungen in diese Richtung laufen aber bereits. Für die Bevölkerung werden diese Energieausfälle immer mehr zu einem Problem. So fallen in der Folge zum Beispiel auch Ampelschaltungen in Großstädten aus, sodass Polizei, Feuerwehr und Rettungsdienste im Dauereinsatz sind. Außerdem kaufen die Krankenhäuser Diesel auf Vorrat an, um so ihre Notstromgeneratoren speisen zu können, damit zum Beispiel die Intensivstation versorgt werden kann. Denn gerade hier ist eine lückenlose Stromversorgung lebenswichtig. Auch andere Einrichtungen wie Banken, Versicherungen und Behörden sind in Sorge, dass die für die dortigen IT-Infrastrukturen installierten USVs (Unterbrechungsfreie Stromversorgung) die immer wieder auftretenden Ausfälle bald nicht mehr kompensieren können. Die Börse und der damit verbundene Aktienmarkt kommt zum schrittweisen Erliegen.

Da die wirtschaftlichen Boykotte und die diplomatische Spannung zwischen Deutschland und Russland weiter anhalten und keine Lösung in Sicht ist, beschließt der russische Präsident, den „Befehl zum Blackout“ zu geben.

Durch den flächendeckenden Angriff auf mehrere große Kraftwerke in Deutschland wird eine folgenreiche Kettenreaktion ausgelöst. Die starken Stromschwankungen, die durch den Ausfall dieser entstanden sind, bewirken eine Abschaltung der Stromversorgung im gesamten europäischen Raum.

Ein Blackout in noch nie da gewesenem Ausmaß!

Das gesamte öffentliche Leben kommt zum Erliegen. Keine Ampel, keine Straßenlaterne und kein Computer funktioniert mehr und auch der Handyempfang ist unterbrochen. Die Bevölkerung weiß nicht, wie sie sich verhalten soll, da eine solche Situation von kompletter Isolation bisher noch nicht dagewesen ist, geschweige denn entsprechende Maßnahmen dazu bekannt sind. Die Bundeskanzlerin spricht zum Volk, nur das Volk kann sie nicht hören. Viele Menschen verfallen bereits nach Stunden in einen panikartigen Zustand. Die Bewohner in Städten versammeln sich an Wahrzeichen und auf Marktplätzen, um sich über die Situation auszutauschen, doch niemand kann Antworten liefern. Ein kompletter Blackout!

Doch das ist nur der Anfang. Am ersten Tag nach dem großen Blackout macht sich die Bevölkerung auf und will sich mit „Hamsterkäufen“ auf eine längere „Durststrecke“ einstellen. Nur öffnet kein Supermarkt seine Pforten, da alle Kassen- und Bezahlsystem ausgeschaltet sind und somit kein Geldtransfer stattfinden kann. In den multinationalen Betrieben, wie VW und Bayer, steht die Arbeit still und von Minute zu Minute werden große Verluste erzielt. Alle Flughäfen schließen, da es ohne den Einsatz von IT vor Ort keine Möglichkeit der Organisation beziehungsweise der Kommunikation gibt. Die Bevölkerung lebt weiter in kompletter Ahnungslosigkeit, da alle Kommunikationskanäle unbrauchbar sind. Die Zeitungspressen stehen still und die Nachrichtensender sitzen ebenfalls im Dunkeln. Experten aus dem gesamten Bundesgebiet befinden sich in den Kraft- und Umspannwerken, um das Problem zu lösen. Erst jetzt wird klar, es handelt sich um einen geplanten Angriff. Die ersten Schätzungen gehen von einer Regenerationszeit von mehr als einer Woche aus. So lange soll Deutschland also noch ohne Strom ausharren.

Doch bereits am zweiten Tag beginnen die ersten kriminellen Gruppen durch die Straßen zu ziehen und Plünderungen sind an der Tagesordnung. Viele Geschäftsleute verteidigen ihren Laden mit Waffengewalt. Es gibt die ersten Toten auf den Straßen Deutschlands. Gerade in den Großstädten und Ballungsgebieten gleicht das Bild immer mehr dem eines Bürgerkrieges. Des Weiteren besteht der psychologische Druck der Bevölkerung, über die Geschehnisse informiert zu werden. Die Bundeswehr wird eingesetzt, um der Bevölkerung helfend zur Seite zu stehen. Jedoch reichen diese Ressourcen gerade einmal aus, um in der Hauptstadt einigermaßen die Ordnung aufrecht zu erhalten.

Am dritten Tag herrscht in den Städten die Anarchie. Das Recht des Stärkeren. Die Bevölkerung scheint zurückversetzt in das Mittelalter. Nun führt Deutschland einen Krieg an zwei Fronten: Zum einen den Cyberwar gegen Russland und zum anderen den „Krieg“ gegen sich selbst, weil die Probleme im Inland durch eine unorganisierte und uninformierte Exekutive momentan nicht bewältigt werden können, da sich Bundeswehr, Polizei und Feuerwehr nur lokal organisieren, weil eine bundesweite Organisation dieser ohne Informations- und Kommunikationsnetze nicht möglich ist.

Die Experten und Spezialisten konnten nun durch weitere Recherche die defekten und zerstörten Teile im Erdgas-Kraftwerk ausmachen und diese untersuchen. Dabei bestätigt sich der erste Verdacht, dass ein Fremdverschulden für den Ausfall gesorgt hat. Durch Überwachungskameras wird der Mitarbeiter des Kraftwerkes identifi-

ziert und auch die Quelle für die Beschädigungen wird erkannt: Der USB-Stick. Dieser wird sofort sichergestellt und bei der anschließenden Untersuchung wird die Schadsoftware auf dem Datenträger enttarnt. Jedoch kann der Urheber nicht sicher zurückverfolgt werden, Vermutungen bestehen allerdings.

Nach einer Woche kann das Stromnetz und die Versorgung der Bevölkerung wieder sichergestellt werden, die Informations- und Kommunikationsnetze funktionieren wieder und Feuerwehr, Polizei und Bundeswehr sorgen im möglichen Rahmen wieder für Ordnung, damit die Strukturen innerhalb der Gesellschaft wieder aufgebaut werden können. Unternehmen können wieder anfangen, Güter zu produzieren und die Krankenhäuser werden mit Strom versorgt und somit können die Opfer der Ausschreitungen versorgt werden.

Der wirtschaftliche und gesellschaftliche Schaden für Deutschland lässt sich zu diesem Zeitpunkt noch nicht einmal annähernd abschätzen. Bis sich die Bevölkerung in psychischer Sicht von diesem Ereignissen erholen kann, wird vermutlich auch einige Zeit vergehen, wann und ob sich die Wirtschaft in Deutschland wieder normalisieren wird, bleibt fraglich.

Zum Glück ist dies nur ein Horror-Szenario, aber es zeigt auch, dass wir Cyberwar nicht auf die leichte Schulter nehmen dürfen. Die Regierung Deutschlands sollte sich für die Sicherheit der Bevölkerung auch in Bezug auf einen potentiellen Cyberwar einsetzen, aber auch die Unternehmen in Deutschland, vor allem jene, die eine wichtige strategische Position innehaben, sollten besonderes Augenmerk auf dieses Thema legen. Die Auswirkungen eines solch massiven Angriffes könnten das gesamte Gefüge der Gesellschaft ins Wanken bringen. Dass sich ein Land wie Deutschland von einem solchen Angriff erholt, ist sehr unwahrscheinlich. Selbst die Auswirkungen auf Europa, sogar auf die Weltwirtschaft, wären verheerend.

Weitere Informationen zum Thema auf der Webseite des Teams http://www.informatik.uni-oldenburg.de/~iug14/cy/

Zur Alternative greifen

Essay der Gruppe „Freie Software, freie Menschen“
Johannes Aßmann

Einleitung

In der heutigen Zeit stehen wir einem großen Aufgebot an Softwareprodukten gegenüber. Für die Dienste, die wir auf dem PC nutzen, stehen uns meistens mehrere Möglichkeiten zur Verfügung.

In diesem Artikel geht es um die Software-Alternativen „Freie Software“ und „Open Source“. Für beides gilt:

Der Quellcode des Programms muss für jeden kostenlos zur Verfügung stehen, zum Beispiel auf einer Website. Somit hat man die Möglichkeit, das Programm um Code zu erweitern oder den Code zu überprüfen.

Dabei soll die Freiheit des Nutzers gewährleistet sein. Der Nutzer hat die Möglichkeit, das Programm zu erweitern und selbst zu vertreiben. Viele Lizenzen erlauben darüber hinaus, dass das neu entstandene Produkt als „Closed Source“ (Code nicht frei verfügbar) vertrieben und sogar verkauft wird.

Dementsprechend werden dem Nutzer so wenige Grenzen wie möglich gesetzt.

Erst wenn man sich mit freier Software beschäftigt, wird einem klar, wie wichtig das Thema ist. Besonders wenn man selbst viel Software benutzt und nicht die finanziellen Mittel hat, sich teure proprietäre Software (Payware) zu kaufen.

Es wird einem bewusst, was man selbst bereits an freier Software benutzt und wie brisant die Frage nach Freiheit ist.

Paint a picture

Bei den Halloween-Dokumenten, die 1998 veröffentlicht wurden, handelt es sich um vertrauliche Schreiben eines Microsoft-Mitarbeiters, die nicht für die Öffentlichkeit bestimmt waren. Diese Dokumente wurden geleaked. Als „Leak“ bezeichnet man die Veröffentlichung von Dokumenten, die nicht für eine solche bestimmt waren. Ein bekannter Fall ist das Leaking durch Edward Snowden.

Im Zuge dieser Veröffentlichung wurde klar, dass Microsoft Open Source als ernstzunehmende Konkurrenz sieht. Darüber hinaus bezeichnete ein Manager bei Microsoft die Open-Source-Bewegung als „Robin Hood und seine Gefährten“, die die Armen beschützen wollen [1]:

„Complex future projects [will] require big teams and big capital. These are things that Robin Hood and his merry band in Sherwood Forest aren't well attuned to do.“

Man kann interpretieren, dass Microsoft sich finanziell durch Open Source bedroht fühlt, da diese die „Armen“ (also die Softwarenutzer) beschützen und ihre Software herausgeben, ohne einen Gegenwert zu fordern.

Eine durchaus treffende und amüsante Vorstellung.

Arten von Software

In der heutigen Zeit läuft man nicht mehr mit einer frisch gebrannten CD nach Hause

und installiert sich die neue Software, für die jemand einmal Geld bezahlt hat.

Nein, es gibt drei Möglichkeiten.

Die Software, die wir nutzen, haben wir gekauft. Auf Lebenszeit oder befristet.

Doch wir wollen kein Geheimnis davon machen, dass viele Leute sich mittlerweile einen Großteil ihrer proprietären Software illegal besorgen und das ist auch schon die zweite Möglichkeit Software zu nutzen. Die dritte Möglichkeit ist kostenlose Software.

Vor- und Nachteile

Wenn man für proprietäre Software zahlt, dann können weitere Kosten entstehen, wenn man auf dem neusten Stand bleiben möchte, oder man zahlt gleich ein langwieriges Abonnement.

Um es kurz zu sagen: Kostenlos ist toll.

Da viele Leute immer noch denken, dass besonders teure Produkte auch besonders viel bieten, versuchen sie, die Software kostenlos zu erwerben, die sie normalerweise Geld kosten würde.

Woran die meisten Leute jedoch oft nicht denken: Cracken von lizenzierter Software in der Zeit von NSA und Co ist gefährlich und kann eben aufgrund dieser Risikos in Arbeit ausarten. Und diese Arbeit wiederholt sich, wenn man auf dem neusten Stand bleiben möchte. Das einzige, was all diesen Ärger erspart, ist kostenlose Software.

Das Problem hierbei ist, dass viele Hersteller kostenloser Software trotzdem auf Finanzierung angewiesen sind. Dafür gibt es verschiedene Möglichkeiten.

Beispielsweise durch zusätzliche Software, die bei der Installation angeboten wird oder durch Spionage, die in der Software versteckt eingebaut ist.

Man kann sich nur wirklich sicher sein, dass man nicht in eine Falle gerät, wenn man es im Quellcode einer Software überprüfen kann.

Darum also freie Software

Ein einlesbarer Quellcode ist die einzige wirklich sichere Möglichkeit, sich vor Spionage zu schützen.

Und damit kommt man auch direkt zur Frage, warum man sich vor Spionage schützen sollte: Heutzutage trifft man ja auf immer mehr Menschen, denen es egal ist, wenn in ihre Privatsphäre eingedrungen wird.

„Ich hab' ja nichts zu verbergen!“, heißt es dann.

Das mag ja auch richtig sein, nur ist diesen Leuten nicht klar, dass damit eines ihrer Grundrechte, nämlich das Persönlichkeitsrecht, verletzt wird.

Das spionierende Programm hat die Möglichkeit, private Daten auszulesen, an denen man selbst einzig und allein das Recht besitzt.

Es wurde bereits bestätigt, dass einige closed source Programme bewusst Hintertüren für die NSA offenlassen.

Da kann von einem freien Menschen mit freier und geschützter Entfaltung kaum die Rede sein.

Generell schränken Geheimdienste unsere Freiheit enorm ein und trotzdem passieren Attentate.

Darum ist es sinnvoll, wenn man ein freierer Mensch sein möchte, dass man durchaus des Öfteren zur freien Software greift.

Wie können wir helfen?

Die Frage ist, wie wir Softwarenutzer helfen können, freie Software in das Bewusstsein der Menschen zu bringen.

Freie Software fordert häufig vom Nutzer sogar, dass er das Produkt verbreiten soll. Genau das können wir auch tun. Wir können anderen Nutzern qualitativ hochwertige freie Software ans Herz legen und sie über die Vorteile aufklären.

Wir können in Diskussionen die Vorurteile gegen freie Software bekämpfen.

Wertigkeit freier Software

Das wohl meist gehörte Vorurteil ist beispielsweise: „Was nichts kostet, ist nichts wert." Jedoch kann man leicht die Gegenfrage stellen. Ist Luft nichts wert, weil es nichts kostet? Wir brauchen sie zum Leben und damit hat sich die Frage erübrigt.

Was sich in den Köpfen der Menschen noch zu selten manifestiert, ist, dass nicht jeder Dienst einen Gegenwert braucht. Man geht davon aus, dass niemand einen hochwertigen Dienst leistet, ohne sich selbst dadurch zu bereichern. Was diese Leute aber vergessen ist, dass die Entwickler das Programm oft für ihre eigenen Belange entwickeln und offenbar kein Problem damit haben, es einer breiten Masse kostenlos zur Verfügung zu stellen. Mit dem freien Zugriff auf den Quellcode steckt indirekt die Aussage dahinter: „Fühlt euch frei, damit zu tun, was ihr wollt." Die einzige Einschränkung dabei ist die Lizenz, unter der die Software veröffentlicht wird, was jedoch eine übersichtliche Anzahl an Verboten beinhaltet (oder gar keine).

Daher sollte man dieses Geschenk dankend annehmen und im Hinterkopf behalten, dass jemand diese Software entwickelt hat, weil sie für ihn einen bestimmten Zweck erfüllt. Wenn man ähnliche Ansprüche hat, kann es sein, dass das Programm genau für einen selbst zugeschnitten ist. Das ist ein großer Unterschied zu vielen Anbietern proprietärer Software. Bei freier Software wurde das Produkt oft von Entwicklern programmiert, die aus Eigeninteresse eine bestimmte Funktionalität implementieren.

Dies ist auch der Grund dafür, dass für freie Software oft schneller ein Update bereitgestellt wird als für proprietäre. Die Nutzer sehen das Problem selbst und arbeiten daran es zu beheben. Es muss kein Unternehmen benachrichtigt werden, was die unliebsame Aufgabe an seine Angestellten weitergeben muss.

Natürlich gibt es auch das Problem, dass freie Software oft aus einer kleinen Gemeinschaft hervorgeht, die nicht so schnell auf ein Problem reagieren kann.

Fazit

Freie Software muss in Zukunft noch viel mehr unterstützt werden, um die Vorteile voll nutzen und sich von der Abhängigkeit großer Konzerne befreien zu können.

Dazu kann jeder seinen Teil beitragen, und das muss nicht einmal in Form von Spenden erfolgen.

Weitere Informationen zum Thema auf der Webseite des Teams http://www.informatik.uni-oldenburg.de/~iug14/fr/

Quelle

[1] Raymond, Eric S.: *Halloween IV: When Software Things Were Rotten.* http://www.catb.org/esr/halloween/

halloween4.html, 1998.
Stand: 31. 01. 2015.

Industriespionage und Angriffe auf Firmen

Gerd Backenköhler

26,9 Prozent der in Deutschland befragten Unternehmen sind in den Jahren 2012 und 2013 von Industriespionage heimgesucht worden. Das geht aus der im vergangenen Sommer veröffentlichten Studie *Industriespionage 2014* des Instituts *Corporate Trust* hervor. Corporate Trust ist eine Unternehmensberatung für Sicherheitsleistungen aus München und präsentiert alle zwei Jahre die Untersuchung, bei der insgesamt 300000 Unternehmen in Deutschland befragt wurden.

Unter Industriespionage, die auch Konkurrenz- oder Wettbewerbsspionage genannt wird, versteht die Wissenschaft die Ausforschung, die ein konkurrierendes und privates Unternehmen gegen ein anderes betreibt. Streng davon abzugrenzen ist die Wirtschaftsspionage, die nach der Definition des Bundesamtes für Verfassungsschutz die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Forschungseinrichtungen beinhaltet. Der Hauptunterschied zwischen Wirtschafts- und Industriespionage besteht also darin, ob es sich um staatlich ausgelöste Spionage handelt oder ob sie von der privaten Wirtschaft ausgeht. Die Spionageaktivität der konkurrierenden Unternehmen beschränkt sich dabei nicht allein auf Konkurrenten im engeren Sinne, sondern bezieht sich auf das gesamte Wettbewerbsumfeld, zu dem auch Lieferanten, Abnehmer und Hersteller von Ersatzprodukten zählen. Gerade kleine und mittelständische Unternehmen betreiben oft nur sehr wenig Aufwand, um betriebsinterne Informationen zu schützen, sodass sie besonders von Spionageangriffen betroffen sind. Ziel einer solchen Spionage ist es, unbemerkt an Informationen zu gelangen, die die Wirtschaftskraft des eigenen Unternehmens verbessern und vor unerwarteten Entwicklungen schützen. Neben Kenntnissen über neue Produkttechnologien können auch Informationen über innovative Produktionsabläufe von Interesse sein.

Der durch Industriespionage entstandene Schaden ist immens, da er sich nach Angaben von Corporate Trust auf jährlich 11,8 Milliarden Euro beläuft. 75 Prozent der befragten Unternehmen hatten einen Schaden, bei einem Großteil von ihnen zwischen 10000 und 100000 Euro. Außerdem beklagten 40,8 Prozent der befragten Unternehmen materielle Schäden. Am meisten hatten die Unternehmen mit dem Ausfall bzw. Diebstahl oder der Schädigung von IT- oder Telekommunikationsgeräten zu kämpfen (53 Prozent). An zweiter Stelle lagen in Deutschland mit 26,8 Prozent die Umsatzeinbußen durch den Verlust von Wettbewerbsvorteilen.

Nach wie vor steht der Mittelstand verstärkt im Fokus der Angreifer: Die Beteiligung mittelständischer Unternehmen an der Studie war mit 67,7 Prozent zwar am stärksten, jedoch im Verhältnis zur Beteiligung waren hier die Schäden auch am höchsten. In Deutschland wurden 30,8 Prozent der mittelständischen Unternehmen, 23,5 Prozent der Konzerne und 17,2 Prozent der Kleinunternehmen geschädigt. Aufgrund dieser Zahlen kann davon ausgegangen werden, dass Kleinunternehmen

nicht so interessant für die Spione erscheinen, Konzerne besser gesichert sind und Mittelständler zu wenig für die Prävention tun.

Unternehmen wurden vor allem in Asien, Osteuropa und den Staaten der ehemaligen Sowjetunion durch Spionage geschädigt. An erster Stelle der Branchen stand der Automobil-, Luftfahrzeug-, Schiffs- und Maschinenbau mit einem Schädigungsgrad von 22,5 Prozent aller Schäden. Auf den weiteren Plätzen folgten Chemie, Pharma und Biotechnologie (17,1 Prozent), Elektro, Elektronik, Feinmechanik und Optik mit 12,6 Prozent sowie Eisen und Stahl, Metallverarbeitung und Grundstoffe mit 8,1 Prozent. Wahrscheinlich für viele überraschend erscheint die Tatsache, dass die Branche Computer und Software mit einem Anteil von 6,3 Prozent nur auf dem siebten Platz und Telekommunikation bzw. Internet mit 4,5 Prozent auf dem neunten Platz unter 13 aufgeführten Branchen landete.

Ein klassischer Fall von Industriespionage ist die Geschichte der *clearaudio electronic GmbH* in Erlangen aus dem Jahr 2012. Das Unternehmen, das sich auf Hightech-Plattenspieler spezialisiert hat, hatte damals ein Patent auf ein neues Plattenspielerlager erteilt bekommen. Als sie dieses auf einer internationalen Messe vorstellen wollten, mussten sie feststellen, dass ein chinesischer Stand auf derselben Messe ein baugleiches Modell präsentierte. Da war dem Unternehmensführer Robert Suchy bewusst geworden, dass er ausspioniert worden war. Er schaltete einen Rechtsanwalt ein und beantragte eine einstweilige Verfügung. Durch einen Kontaktmann in China konnte das Unternehmen schließlich ermitteln, wann die nächste Lieferung des Plagiats in Deutschland ankommen sollte, um es vom Zoll abfangen zu können und den Schaden zu verhindern.

Auch der Nordwesten Deutschlands war schon einmal von einem größeren Fall von Industriespionage betroffen – genauer gesagt die Windenergieanlagenhersteller *Enercon* aus Aurich. Beim Fall aus dem Jahr 1994 war es einem Abgesandten des amerikanischen Konkurrenzunternehmens gelungen, mit einem Computer wichtige Daten über die Windkraftturbine *E 40* zu stehlen. Enercon konnte darauf hin keine weiteren Anlagen mehr nach Amerika verkaufen, da das amerikanische Unternehmen behauptete, die Turbine sei von ihnen entwickelt worden. Enercon beklagte einen Umsatzverlust in Höhe von 200 Millionen DM.

Jedoch ist Industriespionage auch schon fast so alt wie die Menschheit selbst, bereits die Fugger spionierten im 15. Jahrhundert das Geheimnis des Monsunwindes aus. Der Überlieferung nach verriet ein osmanischer Seemann den Fuggern das Geheimnis des Monsunwindes, was es den Fuggern ermöglichte, regelmäßig Handel mit Asien zu treiben. Zu Beginn der Krupp-Dynastie 1811 versuchte Friedrich Krupp durch Einsatz von Spionen an die Rezepte für englischen Stahl zu gelangen; jedoch erst sein Sohn Alfred Krupp konnte Jahre später durch eigene Spionage in deren Besitz gelangen. Ebenso markant war die Zeit nach 1841 als Charles Goodyear das Vulkanisieren entdeckte, doch trotz Patentschutz wurde es vielfach von der Konkurrenz ausspioniert und auch kopiert. Der wohl älteste bekannte Fall resultierte aus dem Seidenmonopol der Chinesen bis zum sechsten Jahrhundert, als die Seide in Europa als minderwertig galt. Um 176 nach Christus wurde die Seidenstraße eröffnet, welche eine Handelsroute zwi-

schen dem damaligen Römischen Reich und China darstellt. Geschichten zufolge hielt im Jahr 200 nach Christus der Fürst von Khotan (heute westliche Grenze China) die Hand um eine chinesische Prinzessin an. Da die Prinzessin nicht auf Seidenkleider verzichten wollte, schmuggelt sie Maulbeersamen und Seidenspinneneier in ihrem Haar aus China heraus. Dadurch verließ das Geheimnis der chinesischen Seide erstmals die heutige Volksrepublik. Im sechsten Jahrhundert entsandte Kaiser Justinian zwei Mönche gen Osten, um dieses zu stehlen. Auch Mönche wurden zu jener Zeit und auch später gerne aufgrund ihres Rufes für Spionagezwecke entsandt, da man davon ausging, dass sie nur Prediger ihrer Kirche seien. Die Mönche mussten jedoch nicht bis nach China reisen, da das Geheimnis sich bereits in der Region um Khotan und Indien verbreitet hatte. Nachdem die Mönche das Wissen um die chinesische Seide nach Europa brachten, war Kaiser Justinian nicht mehr auf teure Importe angewiesen und konnte eine eigene Seidenproduktion aufbauen. Das Geheimnis war keines mehr und das Wissen verbreitete sich von Konstantinopel (dem heutigen Istanbul) aus in ganz Europa.

Diese Fälle sollen die Verbreitung von Industriespionage verdeutlichen. Für viele Unternehmen ist das Thema *Industriespionage* aber viel zu weit weg und nicht von Relevanz. Jedoch sehen das die Konkurrenten meist anders, sodass die Ausspähung von Daten zur täglichen Praxis gehört. Bezüglich der Methoden wird unterschieden zwischen Human Source Intelligence (HUMINT), Technical Intelligence (TECHINT), Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), Measurement and Signature Intelligence (MASINT) und Computer Intelligence (COMPINT), wobei das HUMINT als das größte Risiko gilt. HUMINT lässt ich wiederum unterscheiden in die Methoden durch interne Täter, Angeberei und Leichtfertigkeit, den Wechsel von Mitarbeitern sowie Social Engineering.

Dabei ist der Mensch das größte Risiko bei der Industriespionage, da in der Regel alle Mitarbeiter Vollzugriff auf alle Informationen haben und auch vollstes Vertrauen genießen. So hilft auch die beste Firewall nicht, wenn der Täter sich im Unternehmen befindet. Dabei sind mit Mitarbeitern nicht nur die eigenen gemeint, sondern auch externe Kräfte, wie zum Beispiel Lieferanten oder Reinigungskräfte.

Eine weitere Methode, um an Informationen zu gelangen, ist das Ausspionieren von Mitarbeitern, die leichtfertig Daten öffentlich publizieren.

Ebenso ist das Social Engineering eine Methode, bei der versucht wird, durch geschickte Interaktionen mit Mitarbeitern, Informationen zu erlangen. Auch der Wechsel von Angestellten sollte nicht unterschätzt werden, da hier nicht nur das Wissen, sondern auch die Schwächen des ehemaligen Unternehmens mitgenommen werden.

Interne Täter: Die eigenen Mitarbeiter genießen hohes Ansehen im Unternehmen und ihnen wird ohne Einschränkungen vertraut. Ein Mitarbeiter kann entweder eigenaktiv handeln oder er wird angeworben, um Daten zu stehlen. Handelt er eigenaktiv, so will er in der Regel dadurch Eigenprofit erlangen. Die Gründe dafür sind oft finanzieller Natur, Verärgerung oder Wut. Sollten es die beiden letztgenannten Gründe sein, hat der Mitarbeiter in der Regel meistens schon seine innere Kündigung vollzogen und der Verluste von Informatio-

nen ist vorprogrammiert. Wird der Mitarbeiter angeworben, so geschieht dies in der Regel durch Außenstehende, die Interesse an Informationen haben, und versuchen eine Schwachstelle bei einem Mitarbeiter zu finden, denn ein Industriespion versucht das schwächste Glied im Unternehmen zu finden.

Angeberei bzw. Leichtfertigkeit: Ein weiteres Risiko sind Mitarbeiter wie *Herr Wichtig* oder *Herr Leichtsinnig*. Ersteres sind Personen, die zum Beispiel lautstark im Zug telefonieren und dabei heikle Daten über das Unternehmen von sich geben. Die andere Kategorie sind Personen, die leichtsinnig handeln und zum Beispiel einen Laptop öffnen und frei einsehbar in der Öffentlichkeit platzieren. Dadurch kann der Spion gezielt Informationen sammeln und viel über die Person bzw. das Unternehmen erfahren. Das größte Problem bei diesen Mitarbeitern ist die Arglosigkeit und das fehlende Bewusstsein, da diese in der Regel nicht böswillig handeln.

Social Engineering: Bei dieser Methode manipuliert eine Person anhand von psychologischen Tricks, sodass niemand davon etwas merkt. Beispielsweise könnte sich eine Person als Mitarbeiterin der IT-Abteilung ausgeben, um so persönlich oder auch telefonisch an Daten zu kommen. Der Angriff erfolgt in drei Phasen: In Phase eins erfolgt eine gezielte Informationsrecherche, in Phase zwei wird versucht sich Zutritt und Zugang zu verschaffen, in Phase drei findet der Informationsdiebstahl statt.

Wechsel von Mitarbeitern: Der häufigste Verlust von Informationen an andere Unternehmen geschieht durch den Wechsel von Mitarbeitern. Diese nehmen zum Teil ganze Datenbanken, Aufzeichnungen, Beschreibungen von Produkten und vieles mehr mit. Dabei haben die meisten Mitarbeiter den Wechsel schon vorher lange geplant und versuchen den Noch-Arbeitgeber zu schaden, um das Wissen in das neue Unternehmen einzubringen.

Was können nun aber Unternehmer bzw. leitende Angestellte tun?

1. Führen Sie ein Sicherheitsaudit mit Experten durch, um Schwachstellen aufzudecken.
2. Stellen Sie Regeln mit ihren Mitarbeitern auf und überprüfen sie deren Einhaltung.
3. Ermöglichen Sie jedem Mitarbeiter nur den Zugang zu denjenigen Informationen und Räumlichkeiten, die er zur Erfüllung seiner Aufgaben benötigt.
4. Sorgen Sie für regelmäßige Schulungen, in denen Mitarbeiter auf die aktuellen Methoden der Spione aufmerksam gemacht werden.
5. Beobachten Sie die Loyalität der Mitarbeiter.
6. Seien Sie bei der Einführung neuer Informationssysteme vorsichtig und prüfen Sie das Schadenspotenzial.
7. Errichten Sie ein anonymes Meldesystem für Verdachtsfälle.

Insgesamt kann festgehalten werden, dass nicht nur früher Industriespionage vorhanden war, sondern diese heute immer mehr zu nimmt. Daher ist es von großer Wichtigkeit, dass Unternehmen ihre Daten und vor allem Innovationen durch präventive Maßnahmen schützen.

Weitere Informationen zum Thema auf der Webseite des Teams http://www.informatik.uni-oldenburg.de/~iug14/is/

Literatur

[1] Ann, Christoph, Michael Loschelder und Marcus Grosch (Herausgeber): *Praxishandbuch Know-How-Schutz*. Carl Heymanns, 2010.

[2] Christian, Schaaf: *Der große Angriff auf den Mittelstand*. Richard Boorberg, 2009.

[3] Friedrich Wimme, Alexander Tsolkas und: *Wirtschaftsspionage und Intelligence Gathering*. Vieweg und Teubner, 2013.

[4] Fussan, Carsten: *Managementmaßnahmen gegen Produktpiraterie und Industriespionage*. Gabler, 2010.

[5] Heißner, Stefan: *Erfolgsfaktor Integrität*. Springer, 2014.

[6] Hlavica, Christian, Uwe Klapproth und Frank Hülsberg (Herausgeber): *Tax Fraud and Forensic Accounting*. Gabler, 2011.

[7] Meissinger, Jan: *Gefahren und Bedrohungen durch Wirtschafts- und Industriespionage in Deutschland*. Dr. Kovac, 2005.

[8] Schnitzer, A. und M. Hochenrieder: *Anatomie eines Industriespionage-Angriffs (I)*. Datenschutz und Datensicherheit – DuD, 31(12):927–930, 2007.

[9] Trust, Corporate: *Studie Industriespionage*, 2012. https://corporate-trust.de/pdf/CT-Studie-2012_FINAL.pdf, (2015-01-31).

[10] Trust, Corporate: *Studie Industriespionage*, 2014. http://www.corporate-trust.de/pdf/CT-Studie-2014_DE.pdf, (2015-01-31).

[11] Verfassungsschutz, Bundesamt für: *Wirtschaftsspionage: Risiko für Unternehmen, Wissenschaft und Forschung*, 2014. http://www.verfassungsschutz.de/de/download-manager/_broschuere-2014-07-wirtschaftsspionage.pdf, (2015-01-31).

IT-Sicherheit „Made in Germany“

Eine Arbeitsgruppe des Moduls Informatik und Gesellschaft

***Zusammenfassung*—In Deutschland ist für Fragen der IT-Sicherheit das Bundesamt für Sicherheit in der Informationstechnik (BSI) zuständig. Durch seine Tätigkeiten und Maßnahmen gilt die IT-Infrastruktur Deutschlands zu den sichersten weltweit. Diese Begebenheit wird von einigen Unternehmen ausgenutzt, um mit dem Qualitätssiegel “Deutsche Sicherheit“ für ihre Produkte zu werben. Beispiele dafür sind die De-Mail sowie die Initiative “E-Mail made in Germany“, die nach nach dem NSA-Skandal im Jahr 2013 entstanden ist. Die von den Unternehmen beworbene Sicherheit ist dabei allerdings meist nur unzureichend gegeben.**

Einleitung

Das Internet ist mit seinen Möglichkeiten, aber auch seinem Gefahrenpotential, vergleichsweise jung. So kamen viele Fragen zur IT-Sicherheit in Deutschland erst in Folge der NSA-Späh-Affäre im Sommer 2013 auf. In diesem Artikel wird zunächst aufgezeigt, wer in Deutschland für die Datenschutzgesetze und die IT-Sicherheit verantwortlich ist. Danach werden Datenschutzrichtlinien und -gesetze international verglichen. Abschließend wird gezeigt, wie E-Mail- und Internetdienstanbieter mit Sicherheit werben, welche Sicherheitsmaßnahmen sie dabei umsetzen und wie diese kritisiert werden.

IT-Verantwortliche

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde am 1. Januar 1991 gegründet und gilt als der zentrale IT-Sicherheitsdienstleister des Bundes. Sein Hauptziel ist „die präventive Förderung der Informations- und Cyber-Sicherheit“ Deutschlands. Außerdem ist es für den Schutz der IT-Systeme des Bundes verantwortlich.

Das BSI gehört zum Geschäftsbereich des Bundesministeriums des Innern (BMI). Im Koalitionsvertrag der 18. Legislaturperiode (16.12.2013) wurde festgelegt, dass die Regierung bemüht ist, eine bessere und sicherere digitale Infrastruktur in Deutschland zu gewährleisten [5]. Am 20. August 2014 wurde die „Digitale Agenda“ beschlossen. Eines ihrer Kernziele lautet: „Die Verbesserung der Sicherheit und den Schutz der IT-Systeme und Dienste, um Vertrauen und Sicherheit im Netz für Gesellschaft und Wirtschaft stärker zu gewährleisten [3]“. Außerdem soll im Rahmen des Koalitionsvertrages und der dort geplanten Digitalen Agenda ein IT-Sicherheitsgesetz durchgesetzt werden [4].

Am 17. 12. 2014 wurde das IT-Sicherheitsgesetz (ITSIG) von der Regierung beschlossen [2]. Um den Vereinbarungen des Koalitionsvertrages gerecht zu werden, sind im ITSIG Anforderungen an kritische Infrastrukturen (KRITIS) enthalten. Hierzu zählen Einrichtungen und Anlagen aus den Bereichen Energie, Informationstechnik und Telekommunika-

tion, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie dem Finanz- und Versicherungswesen. Den Betreibern kritischer Infrastrukturen wird eine Meldepflicht auferlegt, nach der sie dem BSI Störungen durch Schadprogramme oder Hackerattacken melden müssen.

Der Bund plant bis zu 38 Milliarden Euro jährlich für zusätzliche Ausstattung und Personal der zuständigen Sicherheitsbehörden auszugeben.

Datenschutzgesetze

Zwar besitzen die meisten Länder der Welt Datenschutzgesetze, doch sind diese äußerst unterschiedlich ausgeprägt. Wie in Abb. 1 zu sehen ist, haben die wirtschaftlich einflussreicheren Staaten wie die USA, China oder Russland im Vergleich zu anderen Industriestaaten ein eher schlechtes Schutzniveau. In den Entwicklungsländern wird sich dagegen kaum oder gar nicht mit dem Thema Datenschutz beschäftigt.

Seit 1980 gibt es internationale datenschutzrechtliche Richtlinien, die „OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data“. Zu ihren Aufgaben gehören die weitreichende Harmonisierung der Datenschutzbestimmungen, die Förderung eines freien Informationsaustauschs und das Ermöglichen eines uneingeschränkten Handels. Außerdem soll verhindert werden, dass unterschiedliche Datenschutzentwicklungen zu einer Kluft zwischen den Mitgliedsstaaten führen [12].

Deutschland

In Deutschland wird der Datenschutz durch das Bundesdatenschutzgesetz (BDSG) geregelt. Der Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass der Umgang mit seinen personenbezogenen Daten sein Persönlichkeitsrecht beeinträchtigt. Es sieht vor, dass jeder Mensch selbst entscheiden kann, wem wann welche seiner persönlichen Daten zugänglich sein sollen. Ziel ist es, den „gläsernen Menschen“ zu verhindern [13].

Ein wesentlicher Grundsatz ist das „Verbotsprinzip mit Erlaubnisvorbehalt“. Prinzipiell ist es verboten personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen. Es ist erst dann erlaubt, wenn die betroffene Person ihre Zustimmung zur Erhebung, Verarbeitung und Nutzung gegeben hat. Ebenfalls gilt der Grundsatz der Datensparsamkeit und -vermeidung, der besagt, dass nur so viele personenbezogene Daten erhoben werden sollen, wie sie für die Datenverarbeitung notwendig sind. Außerdem soll von Anonymisierung bzw. Pseudonymisierung Gebrauch gemacht werden [15].

Die Europäische Union

Die Europäische Union verabschiedete 1981 die Europäische Datenschutzkonvention, welche eines der ersten internationalen Abkommen darstellt. Die Konvention steht Staaten weltweit offen und gilt heute für mittlerweile 46 Staaten. Die Datenschutzrichtlinien der Europäischen Union hingegen gelten nur für die Mitgliedsstaaten der EU [9], [10].

Die Vereinigten Staaten von Amerika

In den USA gibt es keinen einheitlich gesetzlich verankerten Datenschutz. Weitestgehend ist der Zugriff auf persönliche Daten akzeptiert. Nur einzelne Bereiche sind geschützt wie z.B. „Der Schutz

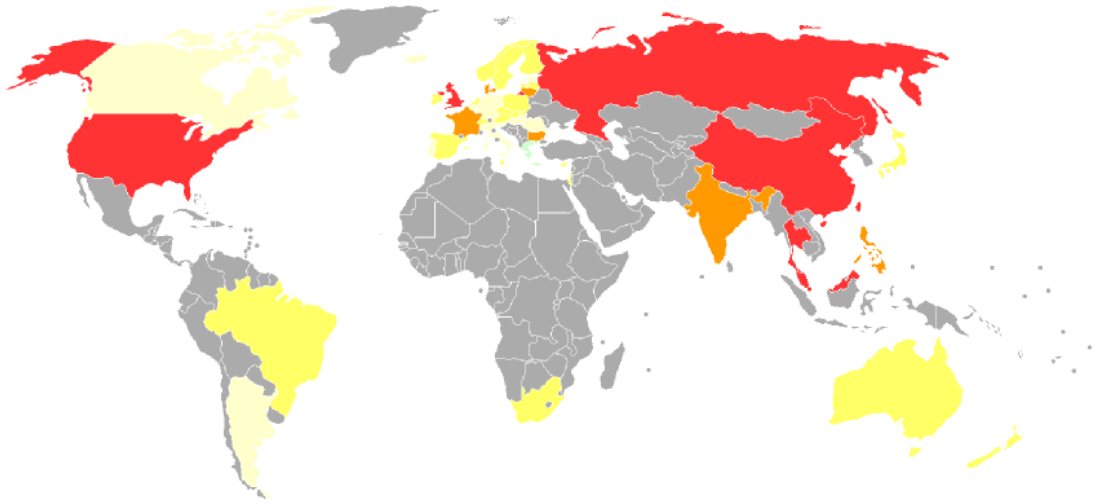

Abbildung 1: Vergleich einiger Staaten im privacy ranking 2007 der Organisation Privacy International [11] (Je heller der Farbton, desto höher ist das Schutzniveau)

der Privatsphäre von Kindern im Internet“. Ein generelles Datenschutzgesetz würde mit den bestehenden Gesetzen (z.B. Meinungsfreiheit) kollidieren. Der oberste Gerichtshof gesteht, nach Interpretation der Verfassung, jedem Einzelnen ein Recht auf Privatsphäre ein. Allerdings wird dies nur von wenigen Bundesstaaten anerkannt. Eine der Ausnahmen bildet hierbei Kalifornien. Auch gibt es in den USA keine unabhängigen Datenschutzbeauftragten. Gegebenenfalls beschäftigt sich die „Federal Trade Commission“ mit Datenschutzproblemen. Sie kann allerdings nur eingreifen, wenn ein Unternehmen seine eigenen Datenschutzrichtlinien verletzt. Verpflichtet sich demnach ein Unternehmen nicht selbst zum Datenschutz, kann kein Eingriff von staatlicher Seite erfolgen. Zwischen 1998 und 2000 wurde vom US-Handelsministerium das „Safe-Harbor“ entwickelt, an welchem die Unternehmen freiwillig teilnehmen können, um einen Umgang mit europäischen Geschäftspartnern zu vereinfachen [16].

Sicherheit als Werbemittel

Bereits seit längerem werden verschiedene elektronische Dienstleistungen mit dem Gütesiegel „Made in Germany“ beworben. Auch schon vor Beginn der NSA-Späh-Affäre im Jahr 2013, auf die als Reaktion die Initiative „E-Mail Made in Germany“ ins Leben gerufen wurde, existierte das Kommunikationsmittel „De-Mail“, das laut Anbieter einen sicheren und nachweisbaren Versand von Mails ermöglichen soll [6].

E-Mail made in Germany

„E-Mail Made in Germany“ ist eine Initiative, die von den Internetanbietern Deutsche Telekom und United Internet ins Leben gerufen wurde und seit Ende April 2014

durch eine deutschlandweite Werbekampagne begleitet wird. Die beteiligten Unternehmen werben damit, dass E-Mails zwischen ihren Diensten „T-Online E-Mail“, „Web.de“ und „GMX“ sicher versendet werden. Die Verschlüsselung der E-Mails erfolgt dabei über das Verschlüsselungsprotokoll SSL. Gesichert werden die Übertragungen zwischen dem Endgerät und dem E-Mail-Server eines Anbieters und zwischen den E-Mail-Servern der Anbieter untereinander. Außerdem findet laut der Initiative die Datenverarbeitung ausschließlich in Deutschland statt [14].

De-Mail

De-Mail ist ein der E-Mail ähnliches Kommunikationsmittel, das die elektronische Version des Briefes darstellen soll. Wie bei „E-Mail Made in Germany“ erfolgt auch hier die Verschlüsselung über SSL. Ein Vorteil der De-Mail gegenüber normalen E-Mails ist die vorherige Überprüfung der Identität der Nutzer. Dadurch können Sender und Empfänger jeder versendeten De-Mail sicher festgestellt werden. Als Folge davon werden auch Spam und Phishing vermieden. Weiterhin existiert die Möglichkeit Nachweise für den Empfang und Versand von De-Mails zu erhalten. Zusammen mit der Nachweisbarkeit der Identität erzeugt dies die notwendige Beweiskraft für das Abschließen von Rechtsgeschäften oder anderen wichtigen Vorgängen [7].

Kritiken

Sowohl „E-Mail Made in Germany“ als auch De-Mail wurden mehrfach vom Chaos Computer Club kritisiert. Es wurde vor allem darauf hingewiesen, dass die beworbene Verschlüsselung durch das Protokoll SSL erfolgt - ein bereits seit über 10 Jahren existierender RFC-Standard, der bei den Anbietern schon seit Jahren hätte Anwendung finden sollen. Nutzern wird dabei vorenthalten, dass E-Mails mit einer SSL-Verschlüsselung nur auf dem Transportweg geschützt werden, aber auf den Servern der Anbieter noch immer ausgespäht werden können. Eine Ende-zu-Ende-Verschlüsselung wird als einzig sinnvolles Mittel empfohlen, um einen fremden Zugriff auf E-Mails zu verhindern. Diese ist bei der De-Mail zwar optional anwendbar – sie sollte aber als Standard eingeführt werden, um echte Sicherheit zu gewährleisten [1], [8].

Zusammenfassung und Fazit

Die IT-Sicherheit und der Datenschutz werden in Deutschland durch Gesetze und Richtlinien bestimmt, die auch unter Einfluss der EU entstanden sind. Dabei wird vor allem Fokus auf den Schutz des „Betroffenen“ gelegt. Im internationalen Vergleich sind Deutschland und die EU bezüglich des Datenschutzes führend. Bei den Wirtschaftsmächten außerhalb der EU wird Datenschutz dagegen gerne vernachlässigt – unter anderem da er mit hohen Kosten verbunden ist. Entwicklungs- und Schwellenländer beschäftigen sich kaum oder gar nicht mit Datenschutz.

Zwar hat der 2013 aufgedeckte NSA-Skandal wichtige Fragen zur IT-Sicherheit in Deutschland aufgeworfen und das Problembewusstsein von Politik, Bürgern sowie Unternehmen gesteigert. Doch die Folgen beschränken sich bislang weitgehend auf die kommerzielle Nutzung des gewachsenen Bewusstseins für Sicherheitsfragen.

Weitere Informationen zum Thema auf der Webseite des Teams http://www.informatik.uni-oldenburg.de/~iug14/sm/

Literatur

[1] 46halbe, Chaos Computer Club: *„E-Mail Made in Germany“: Das Sommermärchen von der sicheren E-Mail*. http://ccc.de/de/updates/2013/sommermaerchen, besucht: 04.01.15.

[2] Bundeministerium des Innern: *Bundesregierung beschliesst IT-Sicherheitsgesetz*. http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/12/bundeskabinett-beschlie\T1\sst-it-sicherheitsgesetz.html, besucht: 04.01.15.

[3] Bundeministerium des Innern: *Digitale Agenda*. http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/Digitale-Agenda/digitale-agenda_node.html, besucht: 04.01.15.

[4] Bundeministerium des Innern: *Friedrich stellt Wirtschaft IT-Sicherheitsgesetz vor*. http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2013/03/eco_mmr_itsicherheitsgesetz.html, besucht: 04.01.15.

[5] CDU, CSU, SPD: *Deutschlands Zukunft gestalten – Koalitionsvertrag zwischen CDU, CSU und SPD, S.138ff*. http://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf, besucht: 04.01.15.

[6] Die Beauftragte der Bundesregierung für Informationstechnik: *De-Mail – Häufig gestellt Fragen*. http://www.cio.bund.de/Web/DE/Innovative-Vorhaben/De-Mail/Haeufig-gestellte-Fragen/haeufig_gestellte_fragen_node.html, besucht: 12.12.14.

[7] Die IT-Beauftragte der Bundesregierung für Informationstechnik: *De-Mail*. http://www.cio.bund.de/Web/DE/Innovative-Vorhaben/De-Mail/de_mail_node.html, besucht: 04.01.15.

[8] erdgeist, Chaos Computer Club: *Bullshit made in Germany: Chaos Computer Club warnt vor Mogelpackung „E-Mail made in Germany“*. http://ccc.de/de/updates/2013/bullshit-made-in-germany, besucht: 04.01.15.

[9] Europe, Council of: *Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten*. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=&CL=GER, besucht: 14.01.15.

[10] Europe, Council of: *Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten*. http://conventions.coe.int/Treaty/ger/Treaties/Html/108.htm, besucht: 14.01.15.

[11] Inc., Wikimedia Foundation: *Datenschutz*. http://de.wikipedia.org/wiki/Datenschutz, besucht: 03.01.15.

[12] OECD: *Kurzfassung OECD – Richtlinien über Datenschutz und grenzüberschreitender Ströme persönlicher Daten*. http://www.oecd.org/internet/ieconomy/15589558.pdf, besucht: 03.01.15.

[13] Ruland, Eva, Birte Ziegler und Moyra Rojas: *Zusammenfassung des BDSG*. http://iwi-project.jimdo.com/der-rechtsschutz/der-datenschutz/zusammenfassung-des-bdsg/, besucht: 03.01.15.

[14] Telekom Deutschland GmbH / 1&1 Mail & Media GmbH: *E-Mail Made in Germany*. http://www.e-mail-made-in-germany.de/Verschluesselung.html, besucht: 04.01.15.

[15] Verbraucherschutz, Bundesministerium der Justiz für: *Bundesdatenschutzgesetz*. http://www.gesetze-im-internet.de/bdsg_1990/index.html, besucht: 03.01.15.

[16] Weichbrodt, Paul: *Datenschutz im internationalen Vergleich*. 2010. http://www.wi.hs-wismar.de/~laemmel/Lehre/WA/Artikel1206/weichbrodt_DS.pdf, besucht: 03.01.15.