Internet-Sicherheit

Das Internet hat für uns persönlich und insbesondere für unsere Gesellschaft eine immer höhere Bedeutung bekommen und diese könnte sich aus heutiger Sicht noch deutlich steigern. Aber die Sicherheit und die Vertrauenswürdigkeit des Internets spielen eine wichtige Rolle bezogen darauf, wie sich das Internet für uns weiterentwickeln wird.

Das Internet mit seinen vielfältigen innovativen Möglichkeiten hat eine hohe Relevanz in unserer modernen Gesellschaft erreicht, die noch weiter steigen wird.
Die deutsche Wirtschaftsleistung ist enorm und das unternehmerische Wissen, das hinter diesen Produkten und Abläufen steckt, wird - vom Großkonzern bis zu den Hidden Champions bei den kleinen und mittelständischen Betrieben - fast ausschließlich mit Hilfe von IT-Systemen verwaltet. Wir beobachten aber gleichzeitig, dass die Angriffsflächen der IT- und Internet-Technologie durch komplexere Software und kompliziertere Zusammenhänge zwischen Protokollen, Diensten und Infrastrukturen vielfältiger und deutlich größer werden. Die Angriffe auf unsere immer höheren Werte auf den IT-Systemen und deren Verfügbarkeit werden verteilter, raffinierter, professioneller und sehr erfolgreich ausgeführt. Die IT-Kriminalität erfährt eine zunehmende Industrialisierung und damit eine nicht zu unterschätzende und nie dagewesen professionalisierte Nachhaltigkeit. Allein die Verluste im Bereich der Wirtschaftsspionage werden auf 50 Mrd. Euro im Jahr geschätzt (Friedrich 2013).
Eine kritische Beurteilung der aktuellen IT-Sicherheitssituation des Internets zeigt, dass wir uns zurzeit nicht angemessen schützen. Welches sind die deutlichsten Sicherheitsgefahren im Internet?

Die Top Internet-Sicherheitsprobleme

In diesem Abschnitt werden die Top Sicherheitsprobleme dargestellt, um die Beurteilung der IT-Sicherheitssituation im Internet und die möglichen Gegenmaßnahmen einschätzen zu können.

„Einfallstor Software“: Die Software stellt in allen Branchen einen immer größeren Wertschöpfungsanteil dar. Wir nutzen Software in PCs, Notebooks, Smartphones, in sehr großen Rechnerzentren, aber auch immer mehr in Autos, in Industrieanlagen, im Haus und vielen weiteren Lebensbereichen. Ein großes Sicherheitsproblem ist, dass in der aktuell genutzten Software zu viele Schwachstellen vorhanden sind. Die Software-Qualität der Betriebssysteme, Anwendungen und Dienste reicht bei der heutigen Bedrohungslage nicht mehr aus. So liegt die Fehlerdichte, also die Anzahl an Softwarefehlern pro 1.000 Zeilen Code, in qualitativ hochwertiger Software heute im Schnitt bei 0,3. Da gängige Betriebssysteme zehn Millionen Zeilen Code und mehr haben, sind danach durchschnittlich 3.000 Software-Fehler zu finden. Teile von diesen Softwarefehlern sind Ziele für erfolgreiche Angriffe. Bei den großen Betriebssystemen, Anwendungen und Diensten ist in den nächsten zehn Jahren auch mit keiner sprunghaften Verbesserung der Software-Qualität zu rechnen und selbst wenn: Auch bei verbesserter Software-Qualität werden die Angreifer noch vorhandene Software-Schwachstellen professioneller ausnutzen.
Die Hersteller von Software müssen ihre Softwareentwicklungsprozesse weiter optimieren, um eine höhere Qualität zu erreichen und die Nutzer sollten pro-aktive

Sicherheitssysteme verwenden, damit ihre IT-Systeme robuster, sicherer und vertrauenswürdiger werden.

“Schlechter Schutz vor Malware“: Malware ist der Oberbegriff für "Schadsoftware" wie Viren, Würmer, Trojanische Pferde und andere. Angreifer - wie kriminelle Organisationen, Spione oder Terroristen - nutzen Software-Schwachstellen aus, um Malware auf IT-Endgeräten zu installieren. Hauptsächlich über E-Mail-Anhänge oder unsichere Webseiten mit Hilfe von sogenannten Drive-by Downloads wird Malware in IT-Endgeräte unbemerkt eingeschleust. Das Institut für Internet-Sicherheit geht zurzeit davon aus, dass auf jedem 25. IT-Endgerät in Deutschland ungewollte Malware vorhanden ist, die über ein Botnetz gesteuert wird (Pohlmann 2013). Ein Botnetz ist eine Gruppe von IT-Endgeräten, die unter zentraler Kontrolle eines Angreifers steht und von ihm für Angriffe genutzt wird. Dadurch können Angreifer Informationen von IT-Endgeräten auslesen (Keylogger, Trojaner), IT-Endgeräte für die Spam-Verteilung und DDoS-Angriffe nutzen und zum Beispiel Daten verschlüsseln und Lösegeld für die Entschlüsselung verlangen. Bei Lösegeldforderungen verschlüsseln die Angreifer mit Hilfe der Malware wichtige Daten auf dem IT-Endgerät und verlangen vom Besitzer eine Summe für die Informationen, mit denen die Daten wieder entschlüsselt werden können.
Wir müssen kritisch feststellen, dass die Anti-Malware-Produkte heute mit 75 bis 95 Prozent eine zu schwache Erkennungsrate haben. Bei direkten Angriffen auf ein IT-System liegt Erkennungsrate im Schnitt sogar nur 27 Prozent.
Advanced Persistent Threat (APT) ist die Begrifflichkeit, die sich für intelligente Malware wie Stuxnet international etabliert hat. Unter dem Namen Stuxnet wird ein Botnet mit einer qualitativ sehr hochwertigen Malware verstanden, die speziell für Produkte zur Überwachung und Steuerung technischer Prozesse (SCADA-System) der Firma Siemens entwickelt wurde. Stuxnet wurde mit dem Ziel geschrieben, die Leittechnik einer Anlage zur Uran-Anreicherung im Iran zu sabotieren. Stuxnet hat eine neue Qualität an Malware eingeleitet, die sehr viel intelligenter ist, viel gezielter vorgeht und vor allem einen sehr viel größeren Schaden anrichten kann. Stuxnet markiert den Startpunkt der Entwicklung von qualitativen Cyberwaffen, die Industrien und Infrastrukturen ganzer Länder lahmlegen können.
Allgemein wird der Begriff Advanced Persistent Threat (APT) in der Regel als ein gezielter Angriff mit komplexen Angriffstechnologien und -taktiken sowie aufwendigen Hintergrundinformationen eines Opfer-IT-Systems und dessen Umgebung verstanden. Dabei nimmt der professionelle Angreifer einen großen Aufwand auf sich (Advanced), um erfolgreich auf ein Opfer-IT-System zuzugreifen und dabei möglichst lange (Persistent) unentdeckt zu bleiben. So ist es möglich, über einen längeren Zeitraum Informationen auszuspähen oder Schaden anzurichten. Gegen diese Art von hochentwickelten und professionellen Angriffen mit intelligenter Malware haben wir im Prinzip heute keine passenden Abwehrtechnologien im Einsatz!

„Keine internationalen Lösungen für Identifikation und Authentifikation“. Im Jahr 2013 werden immer noch Passworte für die Authentifikation im Internet genutzt. Die Probleme sind bekannt: Verwendet werden oft schlechte Passwörter oder ein gutes Passwort für viele Anwendungen. Passworte werden zum Beispiel im Klartext in E-Mails durch das Internet übertragen. Durch die Nutzung dieser unsicheren Authentifikation-Technologien entstehen jährlich hohe Schäden von 1,9 Milliarden Euro (Verisign Fraud Barometer, 2009). Dabei sind sehr gute Identifikations- und Authentifikationslösungen vorhanden, wie zum Beispiel die ID-Funktion des neuen

Personalausweises in Deutschland. Nur werden diese kaum von Internet-Diensten angeboten oder genutzt und haben international wenig Bedeutung.

„Unsichere Webseiten im Internet“. Heute wird Malware hauptsächlich über unsichere Webseiten im Internet verteilt. Das Institut für Internet-Sicherheit misst im Projekt „Internet-Kennzahlen-System“, dass auf den deutschen gemessenen Webseiten zurzeit etwa 2,5 Prozent Malware direkt oder indirekt vorhanden sind, die dafür sorgen können, dass die Nutzer der Webseiten infiziert werden (Feld, Pohlmann, Sparenberg und Wichmann 2012).

Unternehmen stellen Webseiten im Internet häufig zu sorglos zur Verfügung. Oft sind diese nicht sicher genug erstellt, so dass Angreifer die Webseiten mit Malware verseuchen können. Der Schwerpunkt in der eigenen Web-Darstellung liegt bei vielen Unternehmen und Behörden hauptsächlich auf der grafischen Darstellung, auf Benutzerführung und Farbgestaltung und nicht auf der IT-Sicherheit, die aber für die Nutzer der Webseite wichtig ist. Die Unternehmen übernehmen keine Verantwortung für ihre eigenen Webseiten und für ihre Kunden!

Vergleichbar ist dies mit einem Logistikunternehmen, das seine LKWs ohne Bremsen im Straßenverkehr nutzt. Auch große Firmen wie Sony wurden schon mehrmals gehackt, weil sie sich und ihre Kunden nicht angemessen geschützt haben. Selbst Regierungsorganisationen lassen erkennen, dass sie geheime Informationen oder datenschutzrelevante Bürgerinformationen nicht angemessen schützen.

„Nutzung mobiler Geräte“. Die Vorteile von mobilen Geräten wie Smartphones und Tablets sind bestechend. Über die vielfältigen Kommunikationsschnittstellen (wie UMTS/LTE, WLAN, Bluetooth, NFC) ist das Internet mit seinen Diensten stets und überall verfügbar. Mobile Geräte sind multifunktional: Handy, Navi, Musik/TV-Gerät, Medizin-/Gesundheitsgerät, Zugang zum Unternehmen, Internet-Dienste, universeller Computer mit Handy-Apps - alles ist in einem Gerät. Mit "Local Based Service” kommen nützliche und innovative Dienste vor Ort hinzu.
Mit diesen mobilen Geräten tauchen aber auch neue Angriffsvektoren auf, die weitere Risiken verursachen. Ständig wechselnde unsichere Umgebungen (Flughäfen, Bahnhöfe, Cafés) erhöhen die Wahrscheinlichkeit des unabsichtlichen Verlustes und des gezielten Diebstahls durch Taschendiebe. Die Gefahr einer Bewegungsprofilbildung und die einfache Möglichkeit, in der Öffentlichkeit Einsicht zu nehmen, sind nicht zu unterschätzen. Die Nutzung von „bösen“ Apps, die unsere Daten auslesen, wird durch das Prinzip „Masse statt Klasse“ und nicht vertrauenswürdige App-Stores wahrscheinlicher und für zu viele real (Achten und Pohlmann 2012). Aber auch die Nutzung von falschen oder manipulierten Hotspots wird durch ein „schnelles E-Mail-checken“ immer häufiger zum Angriffspunkt und mit großen Schäden als Folge. Eine weitere Gefahrenquelle für Unternehmen ist die parallele Nutzung von mobilen Geräten für private und berufliche Zwecke. Ein großes Problem dabei ist, dass die meisten mobilen Geräte für den Verbraucher-Markt erstellt werden. Hier wird von den Anbietern die Strategie verfolgt: Die mobilen Geräte, wie zum Beispiel das iPhone müssen für jeden Benutzer leicht verständlich erstellt werden. Erst mal funktioniert alles, wenn der Benutzer mehr Sicherheit möchte, muss er Einschränkungen vornehmen. Und das kann er meistens nicht.
Eine richtige Business-Strategie für Smartphones wäre: Es funktioniert erst mal gar nichts und der Benutzer muss Funktionen freischalten, die er unbedingt für die Erledigung seiner Aufgabenstellung braucht. Dadurch wird die Angriffsfläche auf mobile Geräte schon deutlich reduziert.

„Eine E-Mail ist offen wie eine Postkarte!“. Vom E-Mail-Dienst wird keine Vertraulichkeit garantiert! Passworte, Kreditkartennummern und weitere Bankdaten sowie vertrauliche Informationen werden im Klartext übertragen und stellen so ein großes Risiko dar. Denn die Möglichkeiten, eine E-Mail abzugreifen, sind sehr hoch. In einigen Ländern werden E-Mails analysiert, um zum Beispiel an das Know-how von Firmen aus anderen Ländern zu kommen. Das wussten wir eigentlich immer schon, aber Snowden hat es noch mal in unsere besondere Aufmerksamkeit gerückt. Damit sind E-Mails ein weiterer großer Risikofaktor. Wir wissen von Untersuchungen und Befragungen, dass heute weniger als vier Prozent aller E-Mails verschlüsselt werden. Wir wissen aber auch, dass mindesten 43 Prozent der E-Mails in Business-Prozessen verwendet werden (Dietrich und Pohlmann 2005). Aus diesem Grund sollten den Mitarbeitern im Unternehmen E-Mail-Verschlüsselungstechnologien zur Verfügung gestellt werden. Außerdem müssen die Mitarbeiter wissen, wie und - ganz wichtig - wann diese Verschlüsselungstechnologien für vertrauliche E-Mails verwendet werden sollen.

„Internet-Nutzer haben zu wenig Internet-Kompetenz“. Internet-Nutzer müssen die Gefahren des Internets kennen, sonst schaden sie sich und, über infizierte Malware, anderen. Laut einer BITKOM Umfrage von 2012 nutzt fast jeder fünfte Internet-Nutzer weder eine Personal-Firewall noch eine Anti-Malware-Lösung auf ihrem IT-Endgerät und sind damit nicht angemessen geschützt (BITKOM 2012). Hier müssen wir lernen, mit der Inkompetenz von viel zu vielen Nutzern umgehen zu können.

„Geschäftsmodel: Bezahlen mit persönlichen Daten“. Soziale Netzwerke wie Facebook, Partnerbörsen, YouTube, Xing, LinkedIn, Twitter und Co. bringen Nutzer aus verschiedenen Gesellschaftsgruppen zusammen und ermöglicht den Nutzern, sich darzustellen und sich real zu begegnen. Soziale Netzwerke schaffen auch neue Wege, Demokratie und Bürgerbeteiligungen zu gestalten, was eine neue und ungewohnte Herausforderung für alle Beteiligten darstellt.
Außerdem bringen Soziale Netzwerke die Diskussion über die informationelle Selbstbestimmung und den Datenschutz auf!
Eine Frage dazu ist, inwieweit Internet-Angebote zu tolerieren sind, bei denen wir nicht mit Geld, sondern mit unseren persönlichen Daten bezahlen. Wir lassen es mit der Akzeptanz der AGBs zu, dass die Anbieter über Profilbildungen indirekt Geldverdienen können. Aus den erhobenen persönlichen Daten der Nutzer erstellen Betreiber sozialer Netze Nutzerprofile, die für den Verkauf von Waren und Dienstleistungen genutzt werden, weil sie passgenaue, individualisierte Werbung ermöglichen. Zielgenaue Werbung lassen sich die Betreiber vieler sozialer Netzwerke durch das Schalten von individualisierten Anzeigen gut bezahlen. Dieses Prinzip „Bezahlen mit persönlichen Daten“ wird auch bei anderen Diensten wie Suchmaschinen, E-Mail-Diensten und Nachrichten-Diensten angewendet. Aber auch im Bereich von E-Commerce wie beispielsweise beim Online-Versandhaus Amazon werden personenbezogene Daten erhoben, gespeichert und ausgewertet, um den Kunden individuelle Angebote machen zu können (Pohlmann und Spogahn 2011). Hier werden unsere wichtigen und notwendigen Persönlichkeitsrechte sehr stark berührt. Die Herausforderung in diesem Bereich ist die Aufklärung der Nutzer über die Risiken und eine gemeinsame angemessene Lösung mit den Anbietern von sozialen Netzwerken zu finden und umzusetzen.

Radikale Veränderung der Rahmenbedingungen

Weitere aktuelle Herausforderungen ergeben sich auch durch die radikalen Veränderungen der Rahmenbedingungen im Internet. Das Internet geht über alle Grenzen und Kulturen hinaus. Die Auffassungen darüber, was richtig und was falsch ist, sind unterschiedlich. Die Chinesen haben z.B. eine andere Einstellung zum Schutz von Patenten als der Rest der Welt. Auch die Unsicherheiten bei verschiedenen Rechtssystemen müssen im e-Commerce berücksichtigt werden. In vielen Ländern ist noch keine Strafverfolgung bei Missbrauch möglich, was den professionellen Angreifer die einfache Möglichkeit bietet, unentdeckt Straftaten zu begehen.

Außerdem erleben wir gerade eine radikale Entwicklung und Veränderung in der IT und im Internet sowohl durch Soziale Netzte wie Facebook und Twitter, wie auch durch Cloud Computing und den Betrieb von kritischen Infrastrukturen, wie die Stromversorgung per Internet. Wir haben durch neue Betriebssysteme, wie z.B. Android, neue IT-Konzepte, neue intelligente Angriffsstrategien und neue Player im IT-Markt veränderte Bedingungen, auf die wir uns sehr schnell einstellen müssen. Der Atomausstieg sorgt zum Beispiel für mehr Risiko in der Energieversorgung, da jetzt die intelligenten Stromnetze und deren Komponenten vernetzt werden, um intelligenter, also effizienter zu werden. Dadurch werden bekannte Angriffe im Internet auch auf Stromnetze anwendbar und damit steigen unter den heutigen Voraussetzungen das Risiko einer Unterbrechung der Stromversorgung und damit die Funktionsfähigkeit unserer Gesellschaft durch Internet-Angriffe erheblich (González Robles, Pohlmann, Riedel und Urban 2013). Dies macht uns als Gesellschaft für einen Cyber War sehr anfällig.

Kritische Beurteilung der aktuellen IT-Sicherheitssituation des Internets

Professionelle Hacker greifen alles und weltweit erfolgreich an! Professionelle Hacker haben in den letzten Jahren sogar amerikanische IT-Firmen, wie z.B. Google und RSA Security erfolgreich gehackt. Auch die großen US-Zeitschriften wie New York Times und Washington Post waren für die professionellen Hacker leichte Beute und fast alle US-Behörden waren für die Eindringlinge wie ein Schweizer Käse. Wir müssen realisieren, dass unsere heutigen IT-Sicherheitslösungen weder Geheimdienste, noch professionelle Hacker stoppen können. Das ist kein rein deutsches Problem, sondern ein weltweites. Wenn die professionellen Hacker dieser Welt das richtige Wissen haben und über genug Geld verfügen, können sie jede Organisation erfolgreich hacken.

Aber auch die Enthüllungen von Edward Snowden zeigen uns, dass wir ein großes IT-Sicherheitsproblem haben. Und das betrifft nicht nur das Handy von Bundeskanzlerin Angela Merkel. Natürlich wussten wir, dass die NSA und Co. uns ausspionieren. Aber der Umfang und die Tiefe, sowie das viele Geld, das dafür ausgegeben wird, haben die Grenzen unserer Vorstellungskraft deutlich überschritten. NSA und Co. sorgen dafür, dass unsere IT und IT-Sicherheitsmechanismen manipuliert werden und machen damit unsere Geschäfte unsicher und unsere Leben unwürdig. Wir haben ein sehr großes Vertrauensproblem! Wem können wir noch trauen? Internet-Firmen, IT-Sicherheitsanbietern, Staaten, usw.? Die Freiheit des Internets, aber auch die Freiheit der Bürger sind in Gefahr.

Wer ist für die Balance zwischen Freiheit und Sicherheit im Internet verantwortlich?

Wer sind die eigentlichen Player im Internet? Alle Regierungen der Welt haben die neuen Themen des Internets für ihre Bürger zu behandeln. Die Herausforderung dabei ist, welche Themen muss eine Regierung zusammen mit den mehr als 190 anderen Regierungen weltweit bearbeiten und welche nicht. Dann haben wir die IT-Firmen, die für die IT-Technologien, -Produkte und -Dienstleistungen verantwortlich sind. Hier kommen die wichtigsten Softwarefirmen, wie Google, Apple, Microsoft, Facebook, etc. aus den USA. Viele wichtige Hardwarefirmen kommen aus Asien. Einige wichtige Industrietechnologien kommen aus Deutschland.
Zurzeit haben wir mehr als 2 Milliarden Nutzer im Internet, die darüber potenziell alle miteinander verbunden sind. Aber in den nächsten Jahren werden eine Menge weiterer Menschen und vor allen 50 Milliarden Dinge, wie Kühlschränke, Autos, Staubsauger, usw. dazukommen. Zusätzlich gibt es noch die Anwendungsfirmen, die das Internet für ihre Zwecke nutzen, z.B. Repräsentieren der Firmen über Webseiten, Austausch von E-Mails, das Anbieten von Internet-Diensten, usw.

Wenn wir in die Zukunft schauen, stellt sich die Frage: Welche möglichen Szenarien können sich für das Internet entwickeln? Ein Szenario ist eine weiterhin sehr erfolgreiche Entwicklung des Internets. Die verschiedenen Player im Internet finden Lösungen, wie erfolgreich zusammengearbeitet werden kann und stellen sicher, dass das Internet vertrauenswürdig und sicher genug ist, damit sich die Nutzer (Bürger und Kunden) gut fühlen und das Internet frei nutzen.
Ein zweites Szenario, das wir uns nach den Abhörenthüllungen gerade sehr gut vorstellen können, ist, dass wir eine erfolglose Entwicklung des Internets erleben werden. Die Nutzer fühlen sich im Internet nicht mehr wohl, weil die Sicherheit unzureichend ist, kein Vertrauen vorhanden ist, es an Verantwortung der IT-Firmen fehlt, die Regierungen sich unangemessen verhalten, usw.
Ein drittes Szenario für das Internet könnte ein Regierungs-dominiertes Internet sein. Das Internet besteht aus vielen Regierungs-Dörfern, die verschiedene wirtschaftliche und politische Gruppen repräsentieren. Das könnten z.B. die USA mit Kanada sein, die Europäische Union, BRICS mit oder ohne China, China alleine, die OPEC, usw. Die einzelnen unterschiedlichen Regierungs-Dörfer arbeiten zusammen oder auch nicht. Auf jeden Fall haben wir nicht mehr das offene und globale Internet. Die verschiedenen Regierungs-Dörfer haben dann z.B. verschiedene Regeln in den Bereichen Datenschutz, Abhörschnittstellen, Sicherheit und Informationspolitik. Die Regierungen bestimmen, was ihre Bürger unter welchen Randbedingungen tun dürfen.
Ein viertes Szenario könnte ein IT-Firmen-dominiertes Internet sein. Die verschiedenen IT-Firmen-Dörfer werden durch die Marktführer in den verschiedenen Bereichen oder Regionen repräsentiert. Beispiele sind IT-Firmen wie Google, Apple, Deutsche Telekom, Amazon oder Facebook. Auch in diesem Szenario würden die IT-Firmen-Dörfer möglicherweise zusammenarbeiten oder auch nicht, auf jeden Fall gäbe es das offene globale Internet nicht mehr. Die Telekom hat mit ihrer Ankündigung der Veränderung der Flatrate schon einen Hinweis gegeben, in welche Richtung sich das für die Kunden unerfreulich entwickeln kann. Auch die Idee eines Deutschen Internets kann nicht das Ziel einer globalen und modernen Gesellschaft sein.

Wo liegt das eigentliche Problem, das wir in der Veränderung zu einer immer globaleren Gesellschaft Internet lösen müssen?
Die grundsätzlichen Überlegungen von David Loy könnten helfen, das Problem zu verstehen. Wir haben es ist hier mit einem alten soziologischen Paradox zu tun, das besagt: Menschen kreieren Gesellschaften, aber Gesellschaften kreieren auch Menschen.
Dieses Paradox beschreibt den Aspekt, dass wirtschaftliche und politische Systeme nicht neutral sind. Die amerikanische Regierung hat z.B. mit der NSA ein Abhörsystem geschaffen, das die Menschen auf der Welt nicht haben wollen, auch nicht in den USA. Durch die Einstufung dieser Aktivitäten zu Staatsgeheimnissen hat die Bevölkerung keine klaren Informationen darüber erhalten. Sogar die Firmenleiter der großen IT-Firmen haben keinen klaren Überblick über die Geschehnisse, da sie keinen Zugriff auf die Staatsgeheimnisse haben dürfen. Eine solche Entwicklung ist nie gut für eine Gesellschaft und deren Bürger. Die IT-Firmen haben zwar nur zum Zweck der individuellen Werbung unsere persönlichen Daten gesammelt, aber schaffen damit Möglichkeiten für die Regierungen, darauf zuzugreifen.
Aus diesem Grund wird es für uns heute sehr wichtig sein, dass wir uns daran erinnern, dass wir Bürger für die Ziele und deren Umsetzungen in einer Gesellschaft verantwortlich sind. Wir haben zwar ein politisches System geschaffen, das das im vorgegebenen Rahmen für uns tun soll, aber es hat sich leider zu stark von der notwendigen Freiheit der Bürger entfernt. Die wichtigste Frage wird langfristig sein, wie die internationale Gesellschaft mit ihren Bürgern ein wirtschaftliches und politisches System etabliert, das zukünftig eine sehr gute Balance zwischen Freiheit des Einzelnen und der Sicherheit aller Bürger kreiert. Das Internet ist dabei eine internationale Infrastruktur, die neue Randbedingungen für die Regierungen, für die globalen IT-Firmen, aber auch für die Nutzer notwendig macht.

Wir Menschen müssen uns unserer Verantwortung bewusst sein und unseren Beitrag in den unterschiedlichen Rollen leisten.
Als Internet-Nutzer sollten wir wissen, wie wir uns im Internet bewegen können, ohne dass wir direkt Fehler machen oder angegriffen werden. Dazu gehört auch, dass wir unsere IT-Geräte sicher machen und richtig nutzen.
Als verantwortliche Politiker müssen wir in der Lage sein, den neuen veränderten internationalen Anforderungen gerecht zu werden. Wir müssen in einem globalen Internet-Zeitalter herausfinden, welche Teile der Verantwortungen von Regierungen global und welche Teile lokal sind. Globale Aspekte sind z.B. die Etablierung von internationalen IT-Sicherheitsinfrastrukturen für die Identifikation, Authentifikation, E-Mail-Sicherheit, usw. sowie die Umsetzung von einer internationalen Strafverfolgung.
Als Mitarbeiter einer IT-Firmen müssen vertrauenswürdige und sichere IT-Technologien und -Dienste zur Verfügung stellen. Dazu gehört auch der richtige Umgang mit den persönlichen, datenschutzrelevanten und vertrauenswürdigen Daten. Hierzu muss ein zukunftsorientiertes Geschäftsmodell entwickelt werden, wie mit den vielfältigen Nutzerdaten angemessen umgegangen werden kann. Vorschläge, wie der Online Privacy Service für eine zukunftsweisende aktive informationelle Selbstbestimmung der Nutzer im Internet liegen schon seit einiger Zeit auf dem Tisch und müssen nur noch standardisiert und flächendeckend eingeführt werden (Heidisch und Pohlmann 2012).
Genau diese Verantwortung gibt uns die Möglichkeit, eine neue und angemessene Balance zwischen Freiheit und Sicherheit umzusetzen. Diese Gelegenheit sollten wir nicht verpassen.

Innovative Internet-Sicherheitsstrategien und -Sicherheitslösungen, um die Sicherheit und Vertrauenswürdigkeit im Internet zu erhöhen.

Die professionellen Hacker und Snowden haben uns gezeigt, dass wir eine Menge unterschiedlicher Probleme und Herausforderungen im Internet haben. Aber wir haben auch sehr viele positive Möglichkeiten mit der Hilfe von innovativer Internet-Sicherheitsstrategie und -Sicherheitslösungen das Internet sicherer und vertrauenswürdiger zu gestallten.
Deutschland sollte Verantwortung übernehmen und ein sicheres und vertrauenswürdiges globales Internet für die Zukunft entscheidend mit kreieren.
Gerade wir in Deutschland haben kulturell und gesetzlich, aber auch in der IT-Sicherheitsforschung und in der IT-Sicherheitsindustrie, die idealen Voraussetzungen einen wichtigen Beitrag zu einem sicheren und vertrauenswürdigen Internet zu leisten. Die schon vorhandenen innovativen und wirkungsvollen IT-Sicherheitsmechanismen aus Deutschland müssen in der Industrie und bei den Behörden konsequent eingesetzt werden. Anreize für die Wirtschaft müssen geschaffen und die Internet Sicherheitsforschung muss noch stärker gefördert werden. Nur so können wir die vielen positiven Möglichkeiten in Zukunft vertrauenswürdig nutzen.
Im Folgenden werden einige Internet-Sicherheitsstrategien und -Sicherheitslösungen aufgezeigt, die uns helfen können, das Internet sicherer und vertrauenswürdiger zu gestallten.

Verantwortung versus Gleichgültigkeit: Zurzeit bestimmen die großen Technologiehersteller und Dienste-Anbieter wie Google, Apple, Facebook und Microsoft was wir als Nutzer brauchen. Doch die Verantwortung für ihre Lösungen übernehmen sie nicht. Was wir allerdings dringend benötigen, ist eine Herstellerverantwortung wie in der Automobilbranche! Wenn wir heute ein Auto kaufen, übernimmt der Hersteller, bei dem wir das Auto kaufen, gegenüber uns, die volle Verantwortung. Aber auch die Automobilhersteller arbeiten mit mehreren hundert Zulieferern zusammen. Doch gibt es für die Kunden immer nur einen Ansprechpartner. Die Hersteller lassen die Autos überprüfen und wenn sie einen Fehler erkennen, werden große Rückrufaktionen gestartet, um Fehler zu beheben, bevor die eigentlichen Probleme auftreten. Dies hat ein sehr großes Vertrauen zu den Herstellern aufgebaut. Wer übernimmt die Verantwortung für IT-Systeme? Am Ende keiner! Wenn die IT-Hersteller beginnen würden, die Gesamtverantwortung zu übernehmen, dann würden die heutigen IT-Sicherheitsprobleme deutlich geringer. Alle Softwareprogramme und die Hardware wären besser aufeinander abgestimmt und Fehler würden einfacher gefunden und behoben.

Proaktive versus reaktive IT-Sicherheitslösungen: Bei den heutigen reaktiven IT-Sicherheitssystemen im Internet, wie Anti-Spam-, Anti-Malware-, Intrusion-Detection-Systemen rennen wir den IT-Angriffen hinterher. Das bedeutet, wenn die IT-Sicherheitslösungen einen Angriff durch eine entsprechende Angriffssignatur oder eine Anomalie erkennen, dann versuchen sie uns so schnell wie möglich zu schützen, um den Schaden zu reduzieren. Die zunehmende Vielfalt und Komplexität unserer IT-Endgeräte und IT-Infrastrukturen brauchen aber deutlich verlässlichere, robustere und wirkungsvollere IT-Sicherheitskonzepte. Wir müssen weg von ausschließlich reaktiven hin zu modernen proaktiven IT-Sicherheitssystemen, die eine Ausführung von intelligenter Malware, eines der größten Probleme zurzeit,

verhindern können. Solche proaktiven IT-Sicherheitssysteme arbeiten mit einem kleinen Sicherheitskern und Virtualisierung, können Software messbar machen und mit einer starken Isolation, Anwendungen mit ihren Daten separieren und nachhaltige und angemessene IT-Sicherheit bieten. Für proaktive IT-Sicherheitssysteme muss die Softwarearchitektur der IT-Endgeräte allerdings grundlegend anders aufgebaut sein als bisher. Außerdem müssen Sicherheits-Infrastrukturkomponenten gemeinsam umgesetzt werden, damit diese IT-Sicherheits- und Vertrauenstechnologien organisationsübergreifend genutzt werden können. Auf der Forschungsebene wurden die Vorteile der proaktiven IT-Sicherheitssysteme schon längst dargestellt und nachgewiesen. Die ersten IT-Sicherheitsunternehmen bieten heute bereits ausgereifte Lösungen. Jetzt wird es Zeit, dass diese von der Industrie und den Behörden eingeführt werden, damit eine notwendige höhere Sicherheit und Vertrauenswürdigkeit der IT-Endgeräte und IT-Infrastrukturen erzielt werden kann.

Objekt-Sicherheit versus Perimeter-Sicherheit: Perimeter-Sicherheit soll z.B. mit Hilfe von Firewall- und VPN-Systemen verhindern, dass Fremde aus dem Internet auf das eigene Unternehmensnetz zugreifen können (Abschottung) und dass die ausgetauschten Daten nicht von anderen gelesen und manipuliert werden können. Da aber immer mehr mobile Geräte über alternative Kommunikationswege, wie Mobilfunknetze und Hotspots vorbei an zentralen Unternehmens-Firewall ins Internet gehen, verliert die Perimeter-Sicherheit an Wirkung und Bedeutung. Bei Objekt-Sicherheit, Informationsflusskontrolle werden die Objekte geschützt und mit Rechten versehen, die definieren, wer sie in welcher IT-Umgebung wie nutzen darf. Die Objekte werden dadurch über ihren ganzen Lebenszyklus vertrauenswürdig gesichert. Voraussetzung ist, dass mit Hilfe von proaktiven IT-Sicherheitssystemen die Umsetzung von Policies auch auf fremden IT-Systemen durchgeführt werden kann. Auch hier brauchen wir internationale IT-Sicherheitsinfrastrukturen, damit im Prinzip jeder mit jedem sicher und vertrauenswürdig Objekte austauschen kann.

Zusammenarbeit versus Isolierung: Wir müssen erkennen, dass wir zurzeit ein Ungleichgewicht bei Angreifern und Verteidigern im Internet haben. Die Angreifer sind die besten Internet-Spezialisten der Welt und haben sehr erfolgreiche Geschäftsprozesse. Die Angreifer brauchen nur eine Sicherheitslücke zu finden, um erfolgreich zu sein. Die Verteidiger finden keine Internet-Sicherheitsspezialisten und entsprechende Budgets, um sich angemessen schützen zu können. Die Verteidiger müssen jedes Loch stopfen, um sicher zu sein und das sind zurzeit sehr viele.
Die grundsätzlich unsichere und schlecht umgesetzte IT und Internet-Technologie sowie die unzureichende Internet-Kompetenz der Nutzer sorgen dafür, dass Angriffe Schaden verursachen. Ist eine Firma Opfer eines Angriffes geworden, versucht sie in der Regel das Problem alleine und isoliert zu lösen. Die Informationen über erfolgte Angriffe, die Vorgehensweise der Angreifer, der Umfang von Schäden und die Wirkung von Gegenmaßnahmen bleiben somit für die Gesellschaft ungenutzt. Durch eine geordnete und vertrauenswürdige Zusammenarbeit von Firmen und Behörden würde eine deutlich höhere gesamt Internet-Sicherheit erreicht werden können. Dann wäre z.B. die Sicherheitslage besser einschätzbar, die kritischen Schwachstellen würden gemeinsam identifiziert, die Widerstandsfähigkeit zusammen erhöht, die Verteidigungskosten in der Gesamtheit reduziert und der Zugang zu qualifizierten IT-Sicherheitsexperten optimiert.

Ausblick

Wenn wir die positiven Möglichkeiten der modernen IT und des Internets strategisch und langfristig nutzen wollen, dann müssen wir sehr kurzfristig neue Wege einschlagen und die beschriebenen Strategiewechsel für das Erreichen einer höheren Internet-Sicherheit und Vertrauenswürdigkeit einleiten. Die Strategiewechsel werden aufwendig sein, und es bedarf einer Koordinierung. Eine moderne Gesellschaft sollte diese notwendigen Schritte erkennen und zügig umsetzen.

Literarturverzeichnis

C. Dietrich, N. Pohlmann: „eMail-Verlässlichkeit – Verbreitung und Evaluation". In Proceedings der DACH Security Konferenz 2005, Hrsg.: Patrick Horster, syssec Verlag, 2005

N. Pohlmann, N. Spogahn: „Bauchladen – Wie man Googles Dienste umsichtig nutzt“, iX - Magazin für professionelle Informationstechnik, Heise-Verlag, 07/2011

S. Feld, N. Pohlmann, M. Sparenberg, B. Wichmann: „Analyzing G-20´Key Autonomous Systems and their Intermeshing using AS-Analyzer”. In Proceedings of the ISSE 2012 - Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe 2012 Conference, Eds.: N. Pohlmann, H. Reimer, W. Schneider; Springer Vieweg Verlag, Wiesbaden 2012

O. Achten, N. Pohlmann: "Sichere Apps – Vision oder Realität? ", DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Springer Fachmedien, Wiesbaden, 03/2012

M. Heidisch, N. Pohlmann: „Elektronischer Datenbrief – eine aktive informationelle Selbstbestimmung im Internet“, Website Boosting, Nürnberg, 03-04/2012

N. Pohlmann: „Daten gegen Diebstahl sichern“, Wirtschaftsspiegel, IHK Münster, 2/2013

A. González Robles, N. Pohlmann, R. Riedel, T. Urban: „Anforderungen an IT-Systeme in kritischen Infrastrukturen – Gefahrenpotenzial intelligenter Stromnetze aus der Sicht der IT-Sicherheit“. IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 4/2013

BITKOM: Fast jeder fünfte Surfer nutzt weder Virenschutz noch Firewall
http://www.bitkom.org/de/markt_statistik/64026_72211.aspx
Zugegriffen: 17.11.13

Friedrich: 50-Milliarden-Schaden durch Wirtschaftsspionage (2013)
http://www.lvz-online.de/nachrichten/wirtschaft-nachrichten/friedrich-50-milliarden-schaden-durch-wirtschaftsspionage/r-wirtschaft-nachrichten-b-366571.html
Zugegriffen: 15.11.13

Verisign: 15 Prozent der Deutschen sind Opfer von Online-Kriminalität (2009)
http://www.symantec.com/about/news/release/article.jsp?prid=20090916_03&company=verisign
Zugegriffen: 15.11.13

Kurzlebenslauf: Prof. Dr. (TU NN) Norbert Pohlmann

Norbert Pohlmann ist Informatikprofessor für Verteilte Systeme und Informationssicherheit, Direktor des Instituts für Internet-Sicherheit und Leiter des Master-Studiengangs Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen. Von 1988 bis 1999 war er geschäftsführender Gesellschafter der Firma KryptoKom, Gesellschaft für kryptographische Informationssicherheit und Kommunikationstechnologie mbH. Nach der Fusion der KryptoKom mit der Utimaco Safeware war er von 1999 bis 2003 Mitglied des Vorstandes der Utimaco Safeware AG. Seit April 1997 ist Prof. Pohlmann Vorstandsvorsitzender des Bundesverbands für IT-Sicherheit TeleTrusT, der sich zur Aufgabe die Etablierung von vertrauenswürdigen IT-Systemen gemacht hat.

Außerdem ist Prof. Pohlmann Mitglied des wissenschaftlichen Beirates der GDD (Gesellschaft für Datenschutz und Datensicherung e.V.), Mitglied des Beirates des eco (Verband der deutschen Internetwirtschaft e.V.) und Mitglied im Lenkungskreis „Taskforce IT-Sicherheit“ (Bundesministeriums für Wirtschaft und Technologie).

Er war fünf Jahre Mitglied der "Permanent Stakeholders' Group" der ENISA (European Network and Information Security Agency), die Sicherheitsagentur der europäischen Gemeinschaft (www.enisa.europa.eu).

Zahlreiche Fachartikel und mehrere Bücher, Vorträge und Seminare auf dem Gebiet der Informationssicherheit dokumentieren seine Fachkompetenz und sein Engagement auf dem Gebiet IT-Sicherheit.

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule Gelsenkirchen
Neidenburger Str. 43
45877 Gelsenkirchen
Tel.: +49 / 209 / 9596 515
Handy: +49 / 173 / 3021 838
E-Mail: pohlmann@internet-sicherheit.de
URL: http://www.internet-sicherheit.de