Ohne IT-Sicherheit gelingt keine nachhaltige Digitalisierung

IT ist „der Motor“ und die Basis für das Wohlergehen unserer modernen und globalen Informations- und Wissensgesellschaft. Jedoch müssen wir feststellen, dass seit Beginn der IT die IT-Sicherheitsprobleme jedes Jahr größer und nicht kleiner werden. Eine wichtige Erkenntnis ist, dass die heutigen IT-Architekturen unserer Endgeräte, Server und Netzkomponenten nicht sicher genug konzipiert und aufgebaut sind, um den Fähigkeiten von intelligenten Hackern standzuhalten.
Täglich können wir den Medien entnehmen, wie sich kriminelle Hacker die unzureichende Qualität der Software für erfolgreiche Angriffe zu Nutze machen, Malware installieren, Passwörter sowie Identitäten stehlen und unsere Endgeräte ausspionieren. Ungesicherte IT-Systeme genießen zu viel Toleranz bei Nutzern und Unternehmen. Diese Einstellung wird sich in Zukunft mit der Bedeutung der IT in unserer Gesellschaft radikal ändern müssen.
Eine angemessene, sichere und vertrauenswürdige IT gemeinsam zu bewältigen, ist für die erfolgreiche Zukunft unserer Informations- und Wissensgesellschaft entscheidend. Letztlich muss die angestrebte Digitalisierung auch die Nachhaltigkeit als strategisches Ziel haben. Das gelingt nur, wenn die IT-Technologien und -Services sicher und vertrauenswürdig sind.

I. IT-Sicherheitsprobleme

Die Angriffsflächen der IT- und Internet-Technologie werden durch komplexere Software und kompliziertere Zusammenhänge zwischen Protokollen, Diensten und globalen Infrastrukturen vielfältiger und deutlich größer, was wir in der Berichterstattung von erfolgreich durchgeführten Angriffen jeden Tag erkennen müssen.
Die Angriffe auf unsere immer höheren Werte auf den IT-Systemen und deren Verfügbarkeit werden verteilter, raffinierter und professioneller ausgeführt, was Milliardenschäden verursacht. Die IT-Kriminalität erfährt eine zunehmende Industrialisierung und damit eine nicht zu unterschätzende und nie dagewesene professionalisierte Nachhaltigkeit, die sich in der Wahrscheinlichkeit von erfolgreichen Angriffen widerspiegelt.
Wir haben zurzeit ein starkes Ungleichgewicht zwischen Angreifern und Verteidigern. Bei der kritischen Beurteilung der aktuellen IT-Sicherheitssituation fallen einige IT-Sicherheitsprobleme besonders deutlich auf, die gelöst werden müssen, um mehr notwendige IT-Sicherheit und Vertrauenswürdigkeit aufzubauen /Pohl14/.

1. IT-Sicherheitsproblem: „Zu viele Schwachstellen in Software“

Die Software stellt in allen Branchen einen immer größeren Wertschöpfungsanteil dar. Wir nutzen Software in PCs, Notebooks, Smartphones, in sehr großen Rechenzentren, aber auch immer mehr in Autos, in Industrieanlagen, im Haus, beim Sport und zukünftig in allen Bereichen des privaten und beruflichen Lebens. Ein großes IT-Sicherheitsproblem ist, dass in der aktuell genutzten Software zu viele Schwachstellen vorhanden sind. Die **Software-Qualität** der Betriebssysteme und Anwendungen ist für die heutige Bedrohungslage nicht mehr ausreichend. Die Fehlerdichte, die Anzahl der **Softwarefehler** pro 1.000 Zeilen Code, ist bei qualitativ hochwertiger Software heute im Schnitt 0,3. Da gängige Betriebssysteme ca. 10. Mio. Zeilen Code haben, sind hier im Schnitt 3.000 Software-Fehler zu finden /Pohl11/. Teile von diesen Softwarefehlern sind Ziele für erfolgreiche Angriffe. Bei den großen Betriebssystemen und Anwendungen 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 professionellen Angreifer immer weniger **Software-Schwachstellen** professioneller für erfolgreiche Angriffe ausnutzen.

2. IT-Sicherheitsproblem: „Ungenügender Schutz vor Malware“

Malware ist der Oberbegriff für „**Schadsoftware**“ wie Viren, Würmer, Trojanische Pferde, usw. Angreifer (kriminelle Organisationen, politisch und wirtschaftlich orientierte Spione, Terroristen, usw.) nutzen Software-Schwachstellen und menschliche Unzulänglichkeiten aus, um Malware auf IT-Endgeräten zu installieren. Über E-Mail-Anhänge oder unsichere Webseiten mit Hilfe von sogenannten Drive-by Downloads wird hauptsächlich Malware in IT-Endgeräte unbemerkt eingeschleust. Das Institut für Internet-Sicherheit geht zurzeit davon aus, dass auf jedem 10. IT-Endgerät in Deutschland ungewollte intelligente Malware vorhanden ist, die über ein Botnetz gesteuert wird. Ein Botnetz ist eine Gruppe von IT-Endgeräten, die unter zentraler Kontrolle eines Angreifers stehen und von ihm für Angriffe genutzt werden. Dadurch können Angreifer Informationen von IT-Endgeräten auslesen (Keylogger, Trojaner), IT-Endgeräte für die Spam-Verteilung und DDoS-Angriffe nutzen sowie Daten verschlüsseln und Lösegeld für die Entschlüsselung verlangen, usw. Bei Lösegeldforderungen verschlüsseln die Angreifer mit Hilfe der Malware wichtige Daten auf dem IT-Endgerät und verlangen vom Besitzer z.B. 3.000 € für den Schüssel, mit dem die Daten wieder entschlüsselt werden können /Pohl13/.

Wir müssen kritisch feststellen, dass die **Anti-Malware-Produkte** heute bei Massen-Angriffen mit 75% bis 95% eine zu schwache Erkennungsrate haben. Bei gezielten und direkten Angriffen auf ein IT-System ist die Erkennungsrate im Schnitt sogar nur 27 %.

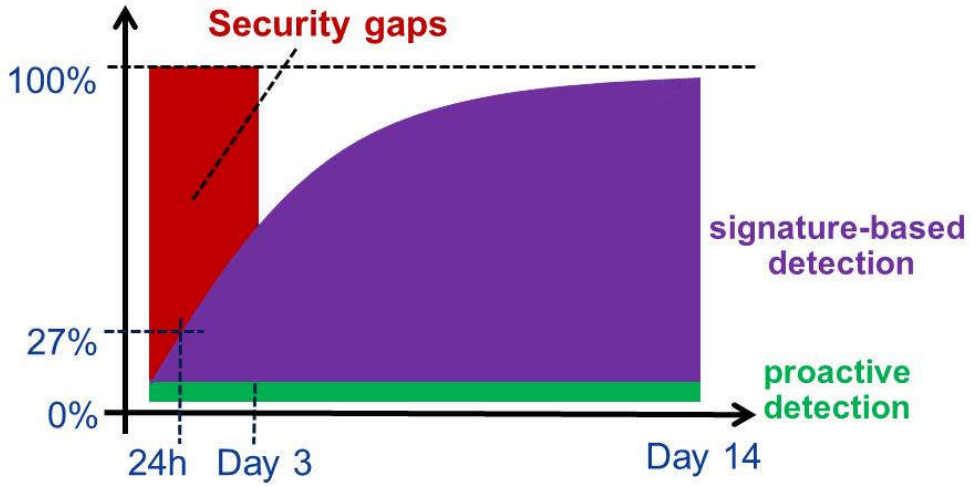

Abb. 1: Erkennungsrate von Malware

Advanced Persistent Threat (APT) ist die Begrifflichkeit, die sich für intelligente Malware wie Stuxnet und Flame international etabliert hat. Advanced Persistent Threat (APT) wird 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 Angreifer einen großen Aufwand auf sich (Advanced), um erfolgreich auf ein Opfer-IT-System zuzugreifen und möglichst lange (Persistent) unentdeckt zu bleiben. So kann es über einen längeren Zeitraum Informationen ausspähen oder Schaden anrichten.

Symantec als größter Hersteller von Anti-Malware-Lösungen hat sich zu Wort gemeldet und mitgeteilt, dass sie nur noch 45 % der Malware erkennen. Diese Zahl

spiegelt sicherlich das neue Verhältnis zwischen gezielten und Massen-Angriffen wider.

3. IT-Sicherheitsproblem: „Keine internationalen Lösungen für Identifikation und Authentifikation“

Im Jahr 2018 nutzen wir immer noch Passworte für die Authentifikation im Internet. Wir alle kennen die Probleme: Verwendung von schlechten Passwörtern oder ein gutes Passwort, das für viele Anwendungen verwendet wird. Passworte werden z.B. im Klartext in E-Mails durch das Internet übertragen. Viele Internet-Nutzer fallen immer noch auf **Phishing-E-Mails** herein, die Passworte abgreifen. Auch das Abgreifen von Passwörtern mit Hilfe von sogenannten **Keyloggern** ist ein großes IT-Sicherheitsproblem /BSI14/. Durch die Nutzung dieser unsicheren Authentifikation-Technologien entstehen jährlich hohe Schäden von 1,9 Milliarden Euro (Verisign Fraud Barometer, 2009). Sehr gute Identifikations- und Authentifikationslösungen sind vorhanden, wie z.B. die ID-Funktion des neuen Personalausweises in Deutschland, nur werden diese kaum angeboten oder genutzt und haben international wenig Bedeutung.

4. IT-Sicherheitsproblem: „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 ca. 2.5 % Malware direkt oder indirekt vorhanden sind, die dafür sorgen können, dass die Nutzer der Webseiten mit Malware infiziert werden.

Hintergrund ist, dass die Unternehmen Webseiten im Internet zur Verfügung stellen, die nicht sicher genug erstellt worden sind und dadurch Angreifer die Webseiten mit Malware verseuchen können. Die eigenen Kunden infizieren sich so mit Malware auf den Webseiten des Unternehmens. Das Problem bei Webseiten ist, dass zu viele Unternehmen und Behörden nur Wert auf Benutzerführung, Farbgestaltung sowie ihre eigene Darstellung legen und nicht auf die IT-Sicherheit, die aber für die Nutzer der Webseite wichtig ist. Das ist so, als wenn ein Logistikunternehmen LKW ohne Bremsen im Straßenverkehr nutzt. Die Unternehmen übernehmen keine Verantwortung für die IT-Sicherheit ihrer eigenen Webseiten. Große Firmen wie Sony wurden sogar mehrmals hintereinander gehackt, weil sie es nicht für nötig hielten, sich und ihre Kunden angemessen zu schützen. Aber auch Regierungsorganisationen zeigen, dass sie nicht in der Lage sind, geheime Informationen oder datenschutzrelevante Bürgerinformationen angemessen zu schützen.

5. IT-Sicherheitsproblem: „Neue Gefahren durch die Nutzung mobiler Geräte“

Die Vorteile von mobilen Geräten, wie Smartphones und Tablets sind bestechend. Über die vielfältigen Kommunikationsschnittstellen (UMTS/LTE, WLAN, Bluetooth, NFC, …) ist das Internet mit seinen Diensten stets und überall verfügbar. Sehr leistungsstarke Endgeräte sind immer und fast überall nutzbar, sowie einfach und schnell über Touchscreens zu bedienen. Mobile Geräte sind multifunktional: Handy, Navi, Musik/TV-Gerät, Medizin-/Gesundheitsgerät …, Zugang zum Unternehmen, Internet-Dienste …, universeller Computer/Apps – alles in einem mobilen 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 der mobilen Geräte, auf denen zunehmend wertevolle Daten

gespeichert werden. Die Gefahr einer Bewegungsprofilbildung und die einfache Möglichkeit der Einsichtnahme in der Öffentlichkeit, sind nicht zu unterschätzen. Die Nutzung von „bösen“ Apps, d.h. Malware auf unseren mobilen Geräten, die unsere Daten auslesen, wird durch das Prinzip „**Masse statt Klasse**“ und nicht vertrauenswürdige App-Stores wahrscheinlicher /AcPo12/. Aber auch die Nutzung von falschen oder manipulierten Hotspots wird durch „mal schnell E-Mails checken“ immer häufiger zum Angriffspunkt auf unsere Werte. Eine weitere Gefahrenquelle für Unternehmen ist die parallele Nutzung von mobilen Geräten für private und berufliche Zwecke (z.B. **Bring Your Own Device**). Ein großes Problem dabei ist, dass die meisten mobilen Geräte für den Konsumer-Markt erstellt werden. Hier wird von den Anbietern die Strategie verfolgt: Die mobilen Geräte, wie z.B. das iPhone, müssen für den unerfahrendsten anzunehmenden Benutzer erstellt werden und praktisch intuitiv bedient werden können. Erst einmal funktioniert alles, wenn der Benutzer mehr Sicherheit möchte, dann müsste er Einschränkungen vornehmen, was er meistens gar nicht kann. Eine Business-Strategie mit dem Fokus auf Sicherheit hingegen wäre: Es funktioniert erst einmal gar nichts und der Benutzer muss Funktionen freischalten, die er unbedingt für die Erledigung seiner Aufgabenstellung braucht.Dadurch würde die Angriffsfläche auf mobilen Geräten schon deutlich reduziert.

6. IT-Sicherheitsproblem: „Eine E-Mail ist wie eine Postkarte!“

Es wird vom E-Mail-Dienst keine Vertraulichkeit garantiert! Passworte, Kreditkartennummern und weitere Bankdaten sowie vertrauliche Informationen werden im Klartext übertragen und stellen so ein großes Risiko dar! Die Möglichkeiten, eine E-Mail abzugreifen sind sehr hoch. In einigen Ländern werden alle E-Mails analysiert, um z.B. an das Knowhow von Firmen anderer Länder zu kommen. Damit sind E-Mails gegenwärtig ein weiterer großer Risikofaktor.

Wir wissen von Untersuchungen und Befragungen, dass zurzeit zu wenig E-Mails (wahrscheinlich 5 %) verschlüsselt werden /PePo14/. Wir wissen aber auch, dass mindesten 43 % der E-Mails in Business-Prozessen verwendet werden. Aus diesem Grund sollten den Mitarbeitern im Unternehmen E-Mail-Verschlüsselungstechnologien zur Verfügung gestellt werden. Typischerweise kommen in der Regel zwei verschiedenen Standards zum Einsatz. Dies ist zum einen S/MIME, der vermehrt in größeren Unternehmen verwendet wird, und zum anderen OpenPGP, der schnell und unabhängig ohne Unternehmensserver auf den IT-Endgeräten des Anwenders betrieben werden kann. Außerdem müssen die Mitarbeiter wissen, wie und – ganz wichtig – wann diese Verschlüsselungstechnologien für vertrauliche E-Mails verwendet werden sollen. Hier muss der Arbeitgeber für mehr Sensibilisierung seiner Angestellten sorgen, den Mitarbeitern muss bewusst sein, dass Kunden- und Firmendaten besonders sensibel und schützenswert sind.

7. IT-Sicherheitsproblem: „Geschäftsmodel: Bezahlen mit persönlichen Daten“

Soziale Netzwerke wie Facebook, Partnerbörsen, YouTube, XING, LinkedIn, Twitter und Co. bringen Nutzer aus verschiedenen Gesellschaftsgruppen zusammen und ermöglichen 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 AGB zu, dass die Anbieter und deren Partner über Profilbildungen

indirekt Geld verdienen 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 /PoSp11/. 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.
Nur eine klare Übersicht über die eigenen persönlichen Daten, die bei den Internet-Dienstanbietern gespeichert sind, hilft, sich selbstbestimmt im Internet zu bewegen. Der Online Privacy Service (OPS) stellt einen zukunftsweisenden Lösungsvorschlag für die Anbieter von Internet-Diensten dar und ist eine pragmatische Umsetzungsmöglichkeit des Rechtes, vergessen zu werden (neue EU-Verordnung für Datenschutz im Internet). OPS zeigt auf, wie eine aktive informationelle Selbstbestimmung im Internet umgesetzt werden kann, die die Wahrung der Grundrechte der Nutzer gewährleistet und damit das Internet vertrauenswürdiger macht /HePo12/.

8. IT-Sicherheitsproblem: „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 haben 30 % der Internet-Nutzer keine Personal Firewall und 28 % keine Anti-Malware Lösung auf ihrem IT-Endgerät und sind damit nicht angemessen geschützt. Es besteht noch ein sehr großer Nachholbedarf die Internet-Nutzer so auszubilden, dass sie in der Lage sind, sich selbst angemessen zu schützen /Ein-Mal-Eins/.
Auf der anderen Seite verlangen wir zurzeit sehr viel von den Nutzern. Wenn wir die Situation mit dem Kauf eines Autos vergleichen, würde das bedeuten, dass der Verkäufer beim Rausgehen zum Käufer sagt, nehmen sie sich ein paar Airbags, Sicherheitsgurte und Bremsschläuche. Bitte denken Sie daran, dass sie dies einbauen müssen, bevor sie los fahren. Wir würden uns heute kein Auto kaufen. In der IT akzeptieren wir diesen Zustand und müssen ihn mit viel Kompetenz kompensieren.
Hier muss noch viel Aufklärungsarbeit in einfacher, zugänglicher Form geleistet werden. Ein gutes Beispiel dafür ist die Initiative „Cyberschutzraum“: Ein Netzwerk von Experten erstellt Videos zum Umgang mit und Handeln im Internet sowie mit mobilen Endgeräten. Angelehnt an die Stilistik der 70er-Jahre TV-Reihe „Der 7. Sinn“, möchten die kurzweiligen Videoclips auf Gefahren und Hindernisse im digitalen Alltag aufmerksam machen und den Zuschauern zeigen, wie sie selbst etwas für ihre eigene Sicherheit tun können. Die Videos sind kostenlos verfügbar unter: https://cyberschutzraum.de/

9. IT-Sicherheitsproblem: „Manipulierte IT und IT-Sicherheitstechnologien“
Die NSA fügt in IT-Sicherheitsprodukte Hintertüren ein, manipuliert IT-Sicherheits-Standards und -Technologien und macht daher unser Geschäftsleben und unsere

Internet-Aktivitäten unsicher. Schlechte Zufallszahlen in IT-Sicherheitsprodukten machen z.B. die Verschlüsselung nutzlos! Wir zahlen viel Geld für Verschlüsselungsprodukte, die keinen Nutzen für uns haben. Nicht nur die NSA nutzt diese Schwachstelle, um Zugriff auf unsere Daten zu haben, sondern auch kriminelle Organisationen und Wirtschaftsspione. Die NSA gibt jährlich 75 Milliarden Dollar für **Spionage** aus, und einen großen Teil davon verwendet sie dafür, die Sicherheit des Internets zu kompromittieren und unsere Werte angreifbar zu machen! Das ist eine wirklich schlechte Situation für uns alle. Hier müssen wir handeln, um als Gesellschaft eine angemessene Cyber Security für unsere Werte zu erreichen!

10. IT-Sicherheitsproblem: „Unsichere IoT-Geräte“

Die Hersteller von IT-Geräten aus dem Bereich des Internet der Dinge, wie z.B. Internet-Videokameras, stellen heute IT-Technologie zur Verfügung, die bei weitem nicht die IT-Sicherheitsanforderungen erfüllen, die wir heute und für die Zukunft brauchen.

Wo liegt das Problem?

Wenn einfache Internet-Videokameras gehackt werden können, ist das erst mal ein Problem des Anwenders. Wenn Angreifer mein Wohnzimmer beobachten können, verletzt das meine Persönlichkeitsrechte und erhöht die Wahrscheinlichkeit eines Einbruches, wenn ich nicht zu Hause bin.

Das weit größere Problem haben wir vor einigen Monaten kennengelernt. Angreifer haben sehr viele Internet-Videokameras und weitere IT-Geräte, die mit dem Internet verbunden sind, wie Drucker, Föne, Kaffeemaschinen, usw. fremdgenutzt, um die Infrastruktur des Internets insgesamt erfolgreich anzugreifen. Dies ist ein sehr großes Problem und macht das Internet sehr verletzlich und damit nicht verlässlich. Dieser Zustand sorgt dafür, dass viele wichtige IT-Sicherheitsexperten eine generelle Zulassung von IT-Geräten für das Internet als Lösung verlangen.

Was können wir tun?

Die IT-Hersteller müssen eine besondere Verantwortung übernehmen und nur noch sichere und vertrauenswürdige IT-Geräte im Internet zu Verfügung zu stellen, die den Stand der Technik im Bereich der IT-Sicherheit berücksichtigen. Außerdem müssen wir die Produkthaftung deutlich schärfer umsetzen, damit die IT-Hersteller und Anbieter ihr Interesse an sicheren Lösungen erhöhen. Ohne eine höhere Verantwortung der wichtigen Player im Internet, sind „der Motor“ und die Basis für das Wohlergehen unserer modernen und globalen Gesellschaft in Gefahr. Aber auch wir als Endnutzer müssen verantwortungsvoll handeln und die Konsequenzen unseres Tuns tragen: Wie viele smarte Lösungen brauche ich wirklich in meinen eigenen vier Wänden? Muss mein privates Laufpensum samt Puls ins Internet gespeist werden? Je gläserner wir uns machen, desto angreifbarer werden wir und unsere Werte.

11. IT-Sicherheitsproblem: „Fake News“

Eine weitere Herausforderung liegt im Bereich von Fake News, rechtswidrige Inhalte, Hasskommentare, Cyber-Mobbing, Wahlmanipulation, Gewaltvideos …

Wir wollen Nutzer-generierte Inhalte haben, aber wenn sich die Nutzer nicht an Regeln halten haben wir ein Problem.

Wie können wir Dinge erkennen?

Wie schnelle können die Dienstanbieter die Inhalte löschen? Ohne, dass sie zu viel löschen? Welchen Institutionen können wir diese Verantwortung übertragen? Eine überwachende Instanz ist zwingend nötig, um die Persönlichkeitsrechte von Opfern zu schützen. Aber wie kann Kontrolle bei dieser Schnelllebigkeit und den unvorstellbaren Mengen an Daten (bei Facebook allein 60 Millionen Bilder pro Tag, die gepostet werden, Statistik Socialmedia-Institute.com 7/2016) überhaupt funktionieren und

Zensur verhindert werden? Auch hier würden aufgeklärte und selbstbestimmte Nutzer für ehebliche Erleichterung sorgen. Eine sensible Eigenverantwortlichkeit hinweg durch alle Altersklassen und sozialen Schichten, kombiniert mit empfindlichen Strafen für Zuwiderhandlungen wäre ein Schritt in die richtige Richtung.

II. Problematische Rahmenbedingungen

Weitere Herausforderungen resultieren auch aus den Veränderungen der Rahmenbedingungen. Das Internet ist global und geht über alle Grenzen und Kulturen hinaus. Es gibt insbesondere im E-Commence unterschiedliche Auffassungen darüber, was richtig und was falsch ist. Die Unsicherheiten bei verschiedenen Rechtssystemen müssen berücksichtigt werden. Es gibt noch zu viele Länder, in denen keine **Strafverfolgung** möglich ist. Außerdem erleben wir gerade eine radikale Entwicklung und Veränderung in der IT und im Internet z.B. durch mobile Geräte, Soziale Netze wie Facebook und Twitter oder durch Cloud Computing sowie die Internetfizierung von Kritischen Infrastrukturen. Wir haben durch neue Betriebssysteme, neue IT-Konzepte, neue Angriffsstrategien und neue Player im IT-Markt neue Gegebenheiten und Rahmenbedingungen, auf die wir uns immer wieder sehr schnell einstellen müssen.

III. Wie sieht eine gesellschaftliche Sichtweise auf die unterschiedlichen IT-Sicherheitsprobleme aus?

Privatsphäre und Datenschutz

Der Aspekt Privatsphäre spielt für jeden Bürger eine sehr wichtige Rolle. Eine Gesellschaft, die wirtschaftlich und politisch auf die Eigenverantwortlichkeit des Einzelnen setzt, muss umgekehrt das schützen, was den einzelnen als Sozialwesen und als Wirtschaftsfaktor ausmacht: Einerseits, seine persönliche Integrität und andererseits, seinen materiellen Besitz. Wenn wir als Gesellschaft nicht mehr in der Lage sind, diese Anforderungen zu erfüllen, dann verlieren wir einen Teil der Demokratie und geben unsere Freiheit auf. Unsere gesellschaftlichen Reaktionen in der Summe sind, bezogen auf die Schwere des Angriffes auf unsere Privatsphäre, der überwiegend durch die NSA und die unterstützenden US-Internet-Marktführer durchgeführt wird, lächerlich, bezogen auf die Schäden für unsere Gesellschaft. Eine offene und aktive Diskussion darüber, wie der Datenschutz und die Privatsphäre in der Zukunft gestaltet werden können und muss sowie welche Rolle sie spielen sollen, wird intransparent eher hinter geschlossenen Türen von einigen wenigen Fachleuten geführt.

Selbstbestimmung und Autonomie

Internet-Dienste machen Handlungsvorschläge für uns Nutzer auf der Basis verschiedener Arten von Sensoren, wie Wearables, Smartphones, Internet-Dienste, usw. Intelligente Algorithmen nutzen diese vielen privaten Sensordaten, bewerten diese, vergleichen sie mit privaten Daten von anderen Menschen und nutzen allgemeines Wissen und Erfahrungen, um Handlungsempfehlungen für uns Nutzer zu berechnen. Das kann für uns sehr nützlich sein, bezogen auf eine gute Entscheidung für eine Handlung. Der individuelle Mensch mit seinem persönlichen Wissen, Erfahrungen und seine Intuition sowie zusätzlich intelligente Algorithmen mit sehr vielen Daten und fast unbegrenzter Rechnerpower sind ein optimale Ergänzung.
Wenn die Internet-Dienste das für uns transparent machen, sind gut berechnete Handlungsempfehlungen für unsere optimale Handlungsentscheidung sehr hilfreich.

Wenn die Internet-Dienste aber mit solchen Diensten indirekt Geld verdienen, wird die berechnete Handlungsempfehlung eher im Interesse des Internet-Dienstes und dessen Kunden liegen, als im Interesse der Nutzer. Jeder Nutzer wird zwangsläufig zum Produkt. Das Problem dabei ist, dass wir unsere Selbstbestimmung verlieren und Marionetten der Internet-Dienste werden. Das können wir als moderne Gesellschaft nicht wollen.

Wirtschaftsspionage

Die Wirtschaftsspionage ist eine weitere gesellschaftliche Herausforderung. 100 Milliarden Euro Schaden im Bereich der Wirtschaftsspionage im Jahr laut dem Verein Deutscher Ingenieure (VDI). Die Schäden beinhalten insbesondere Umsatzeinbußen von 23 Milliarden Euro durch Plagiate, Kosten von 18,8 Milliarden Euro durch Patentrechtsverletzungen und Verluste durch Ausfall, Diebstahl oder Beeinträchtigen von IT-Systemen sowie Produktions- und Betriebsabläufen von 13 Milliarden Euro.
Diesen hohen Betrag an Schaden können wir uns als Wissensgesellschaft nicht leisten! Die Angreifbarkeit unserer IT wird immer größer und unsere Werte, die als Bits und Bytes zur Verfügung stehen, werden immer risikobehafteter. Hier müssen wir umgehend aktiv werden und mit den unterschiedlichen Stakeholdern zusammen geeignete, gemeinsame IT-Sicherheitsmaßnahmen einleiten, um unsere Werte als Wissensgesellschaft deutlich wirkungsvoller zu schützen. Diese Angelegenheit muss auf allen Ebenen zur Chefsache werden.
Der Bereich Internet-Kriminalität mit z.B. erfolgreichen Angriffe auf Online Banking und Distributed Denial of Service (DDoS) Angriffen, verursacht jährlich einen Schaden von ca. 100 Mio. Zusätzlich sollten wir hier beachten, dass die Dunkelziffer in diesem Bereich sehr hoch sein wird. Insbesondere der Bereich DDoS und Erpressungen mit der Androhung von DDoS, ist zurzeit ein lukrativer Bereich für kriminelle Organisationen].

Cyber War

Eine weitere und immer bedeutsamere Herausforderung ist Cyber War. Angriffe auf Kritische Infrastrukturen, wie die Energieversorgung, stellen eine prinzipiell höhere Angreifbarkeit unserer Gesellschaft dar und bilden eine neue Ebene der existenziellen Bedrohung.
Mit Stuxnet haben wir lernen müssen, dass mit einem Kostenaufwand von rund 9 Mio. US Dollar für eine intelligente Malware politische Ziele einfach und sehr erfolgreich umgesetzt werden können. Mit der intelligenten Malware Stuxnet haben die Amerikaner und Israelis zusammen die Uran-Aufbereitung im Iran um zwei Jahre verzögern können.
Die schreckliche Alternative dieses politischen Zieles wäre gewesen, dass über 200.000 Soldaten in den Iran einmarschiert wären, was nicht nur Kosten von mehreren Milliarden US Dollar verursacht, sondern auch Menschenleben aufs Spiel gesetzt hätte. Wir müssen uns auf diese neue Wirklichkeit von Cyber War professionell einstellen.
Dieser erfolgreiche Angriff im Iran ist im Grunde genommen auch auf Deutschland übertragbar, denn mit dem Ausstieg aus der Atomenergie haben wir als Gesellschaft einen mutigen Weg eingeschlagen. Der Atomausstieg sorgt hier z.B. für mehr Risiko in der Energieversorgung, da jetzt die Stromnetze und deren Komponenten vernetzt werden, um intelligenter, d.h. effizienter zu werden. Dadurch steigen das Risiko einer Unterbrechung der Stromversorgung und damit die Funktionsfähigkeit unserer Gesellschaft durch Internet-Angriffe erheblich. D.h. wir müssen dafür sorgen, dass

unsere Energieversorgung und die anderen Kritischen Infrastrukturen für unsere Gesellschaft sicher und robust gegen Cyber-Angriffe werden.

IV. Die Herausforderungen

Wir kennen die IT-Sicherheitsprobleme, doch die heute vorhandenen und genutzten IT und IT-Sicherheitsmaßnahmen reduzieren das IT-Sicherheitsrisiko nicht ausreichend! Wir brauchen Paradigmenwechsel in der IT und IT-Sicherheit, um das Risiko für unsere Gesellschaft auf ein angemessenes Maß zu reduzieren.
Wir müssen realisieren, dass unsere Herausforderungen nicht trivial sind, und wenn wir jetzt nicht mit allen Stakeholdern zusammen eine gemeinsame **IT-Sicherheitsstrategie** definieren und passende Maßnahmen einleiten, wird die Nutzung des Internets mit all seinen Diensten immer problematischer. Im Folgenden werden ein paar innovative Ideen aufgezeigt, die wir gemeinsam umsetzen müssen.

1. Paradigmenwechsel „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 IT-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, uns gegenüber die volle Verantwortung. Auch die Automobilhersteller arbeiten mit mehreren hundert Zulieferern zusammen. Und doch gibt es für uns 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 werden.

2. Paradigmenwechsel „Proaktive versus reaktive IT-Sicherheitslösungen“

Bei den heutigen reaktiven IT-Sicherheitssystemen, 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 (sichere Betriebssysteme) und Virtualisierung, können Software messbar machen und mit einer starken Isolation Anwendungen mit ihren Daten separieren und so nachhaltige und angemessene IT-Sicherheit bieten /PoSp13/.

Abb. 2: Modere und wirkungsvolle IT-Sicherheitsarchitekturen

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 /HLP08/. 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.

3. Paradigmenwechsel „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 mit Rechten versehen, die definiert, 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.

4. Paradigmenwechsel „Zusammenarbeit versus Isolierung“
Die grundsätzlich unsichere und schlecht umgesetzte 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, den 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 reduziert und der Zugang zu qualifizierten IT-Sicherheitsexperten optimiert. Aus diesem Grund brauchen wir ein Business-Modell und **Vertrauenskonzepte,** die eine Zusammenarbeit motivieren. Ein Business-Modell welches insgesamt weniger Geld für IT-Sicherheitsmaßnahmen erfordert und als Resultat ein gemeinsames geringeres Schadensrisiko für alle kooperierenden Firmen erzielt.

5. Paradigmenwechsel „Verantwortung der Staaten“

Mit Edward Snowden haben wir lernen müssen, dass die NSA unter dem Vorwand, terroristische Aktivitäten im Internet zu identifizieren, das ganze Internet umfänglich abhört und IT-Sicherheitstechnologien zum Schaden von Unternehmen und Bürgern schwächen. Sogar das Abhören von Staatsträgern, wie die deutsche Bundeskanzlerin Merkel, gehört dazu.
Mit den neuen Enthüllungen der CIA-Aktivitäten in Deutschland (Generalkonsulat der USA in Frankfurt a. M.)wissen wir jetzt, dass sogar Fernseher als Abhörinstrumente genutzt werden, um in unserer Privatsphäre zu schnüffeln. WhatsApp-Kommunikation kann, trotz Verschlüsselung, durch die Strafverfolgungsbehörden mitgelesenen werden. Die Liste der spionierenden und manipulierenden Aktivitäten, auch anderer Länder, wie China und Russland, ist sehr lang.
Alles was machbar ist, wird auch gemacht!
Leider stimmt das, wenn wir in die Unterlagen von NSA und CIA rein schauen und die täglichen News verfolgen. Aber wohin führt uns das? In den nächsten Jahren werden z.B. im Internet der Dinge sehr viele Innovationen kommen, die unsere Lebensräume verbessern werden. Im Bereich der Gesundheitsversorgung werden wir aktuelle medizinische Werte messen und überwachen lassen, um das Risiko von kritischen Situationen von Menschen deutlich zu minimieren. Autonomes Fahren wird den Straßenverkehr in der Summe sehr viel sicherer machen und den Komfort der Mobilität deutlich erhöhen.
Für die Geheimdienste dieser Welt wird es dann aber auch möglich sein, aus der Ferne Herzschrittmacher für bestimmte Personen auszuschalten, oder mit autonomen Fahrzeugen Unfälle zu produzieren, wenn die Fahrgäste „unerwünscht“ sind.
Cyberwaffen, die in fremden Staaten Wahlen manipulieren, Wirtschaftsspionage durchführen, Angriffe auf kritischen Infrastrukturen umsetzen, usw. verursachen finanzielle Schäden und schwächen das gesamte Internet als Motor unserer globalen Gesellschaft.
Wie kann diese ungünstige Entwicklung verhindert werden?
Nur wenn die Staaten dieser Welt sich gemeinsam darauf einigen, das Internet mit den vielen Möglichkeiten nicht für die eigenen Interessen zu missbrauchen, wird das Internet sich positiv weiterentwickeln können.
Ähnlich dem Atomwaffensperrvertrag brauchen wir einen internationalen Cyberwaffensperrvertrag, der die Staaten verpflichtet, das Internet nicht für eigene Interessen zu missbrauchen und Cyberwaffen nicht zu nutzen sowie das Recht auf die „friedliche Nutzung“ des Internets zum Gegenstand hat.
Wenn die Staaten dieser Welt sich nicht darauf einigen können, das Internet nicht für Cyberwar zu missbrauchen, wird sich das Internet über kurz oder lang nicht weiter entwickeln können.

V. Basis in Deutschland und der der Weg zu mehr IT-Sicherheit

Die Voraussetzungen in Deutschland bezüglich wichtiger und verfügbarer IT-Sicherheitstechnologien sind sehr gut. Für die Umsetzung brauchen wir aber pragmatische Wirkungsklassen von IT-Sicherheitsmaßnahmen für unterschiedliche Schutzbedarfe. Vertrauenswürdige und sichere IT-Sicherheit aus Deutschland kann nur in enger Zusammenarbeit mit den internationalen IT-Marktführern umgesetzt werden. Dazu müssen neue Ideen und Konzepte wie „**IT Security Replaceability**“ für alle gewinnbringend umgesetzt werden. Die Idee der „IT Security Replaceability” fordert die Ersetzbarkeit, Austauschbarkeit von IT-Sicherheitsprodukten und IT-Sicherheitstechnologien von den großen und wichtigen IT-Marktführern. Dabei sollte dies einfach und nachhaltig möglich sein. Beispiele wären hier Krypto-Technologien (Algorithmen, Zufallszahlengeneratoren, …) und weitere Sicherheitslösungen wie Verschlüsselungsprodukte (z.B. Festplattenverschlüsselung wie Bitlocker), Abschottungstechnologien wie Virtuelle Maschinen und IT-Sicherheitstoken wie SmartCards oder HSMs (siehe auch /TeleT14/).
Um diese Ideen realistisch umsetzen zu können müssen wir eine gemeinsame IT-Sicherheit Strategie mit passenden Zielen definieren und zusammen umsetzen. Dies wird dann erfolgreich umgesetzt werden können, wenn Anwender (große Firmen, KMUs, Berater, usw.), IT-Sicherheitsindustrie, IT-Sicherheitsforschung und Politik eng zusammenarbeiten.

Schwachstellen aufzeigen, Lösungen anbieten: Das Manifest zur IT-Sicherheit

Das Manifest zur IT-Sicherheit ist eine öffentliche Erklärung der beiden Bundesverbände für IT-Anwender – VOICE und IT-Sicherheit – TeleTrusT, die aufzeigt, wie gemeinsam eine angemessene Risikolage in der IT erreicht werden kann. Dazu haben sich die IT-Sicherheitsexperten aus beiden Verbänden zusammengetan, um die vorhandenen IT-Sicherheitsprobleme zu analysieren und Auswege aufzuzeigen, wie wir gemeinsam zu mehr IT-Sicherheit kommen können.
Das Ergebnis sind sechs Thesen, die Aufzeigen welche Herausforderung wir haben und wie diese gemeinsam und erfolgreich bewältigt werden können.

1.These:
Ohne IT-Sicherheit gelingt keine nachhaltige Digitalisierung!
Die Gesellschaft muss intolerant gegenüber unsicheren IT-Lösungen werden und Gemeinsam für mehr IT-Sicherheit sorgen!

2.These:
Gemeinsam mehr wirkungsvollere IT-Sicherheitslösungen nutzen!
Die IT-Marktführerschaft der USA, die stark fragmentierten Sicherheitsprodukte und ein fehlendes gemeinsames Vorgehen macht es für Unternehmen schwer, die passenden sicheren und vertrauenswürdigen IT-Lösungen zu finden und einzusetzen.

3.These:
Verschlüsselung und Vertrauen sind die digitalen Werkzeuge für die informationelle Selbstbestimmung!
Um digitale Werte umfänglich zu schützen, müssen sie sicher verschlüsselt werden und die IT-Sicherheitslösungen müssen transparent und vertrauenswürdig sein!

4.These:

Security-by-Design, Privacy-by-Design und nachvollziehbare Qualitätssicherung sind unabdingbar!
Wie die unsicheren IoT-Geräte gezeigt haben, brauchen wir IT-Sicherheit und Datenschutz direkt in den IT-Geräten und in den Internet-Diensten eingebunden. Die IT-Hersteller müssen mehr Verantwortung für die IT-Sicherheit ihrer Produkte übernehmen.

5.These:
Wir brauchen eigene Souveränität von IT-Sicherheitsinfrastrukturen!
Der technologische Stand in Europa muss gesichert, stark ausgebaut und umfänglich gefördert werden, um die eigene Souveränität für wichtige IT-Infrastrukturen langfristig sicherzustellen!

6.These:
Cyber-War, Cyber-Sabotage und Cyber-Spionage werden immer bedrohlicher!
Das bedeutet, wenn eine IT-Lösung das Potenzial bietet, negative Auswirkungen auf die kritische Infrastrukturen auszuüben, so muss sie besonders sorgfältig geprüft und regelmäßig kontrolliert werden!

Eine enge Zusammenarbeit zwischen den Herstellern und Anwendern ist nötig, um angemessene, wirkungsvolle, sichere und vertrauenswürdige IT-Lösungen in den operativen Einsatz zu bringen und umfangreiche und übergreifende IT-Konzepte erfolgreich umzusetzen.

VI. Zusammenfassung

Wenn wir die positiven Möglichkeiten der modernen IT und des Internets strategisch nutzen wollen, dann müssen wir sehr kurzfristig neue Wege einschlagen und die z.B. die beschriebenen Paradigmenwechsel für das Erreichen einer höheren IT-Sicherheit und Vertrauenswürdigkeit einleiten.
Die Umsetzung einer **IT-Sicherheitsstrategie** für eine angemessene IT-Sicherheit wird aufwendig sein, muss mit allen Stakeholdern gemeinsam erfolgen, sollte schnell umgesetzt werden und bedarf einer starken Koordinierung. Eine moderne Gesellschaft sollte diese notwendigen Schritte erkennen und zügig umsetzen.

Literatur

/HLP08/ N. Heibel, M. Linnemann, N. Pohlmann: „Mehr Vertrauenswürdigkeit für Anwendungen durch eine Sicherheitsplattform", in "Trusted Computing - Ein Weg zu neuen IT-Sicherheitsarchitekturen", Hrsg.: N. Pohlmann, H. Reimer; Vieweg-Verlag, S. 73-85, Wiesbaden 2008

/Pohl11/ *N. Pohlmann:* „Bugs, die Nahrung für Malware – Von guter, schlechter und böser Software", IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, S. 32-34, 4/2011

/PoSp11/ *N. Pohlmann, N. Spogahn:* „Bauchladen – Wie man Googles Dienste umsichtig nutzt", iX - Magazin für professionelle Informationstechnik, Heise-Verlag, S. 98-101, 07/2011

/AcPo12/ *O. Achten, N. Pohlmann:* "Sichere Apps – Vision oder Realität? ", DuD Datenschutz und Datensicherheit – Recht und Sicherheit in

Informationsverarbeitung und Kommunikation, Springer Fachmedien, Wiesbaden, S. 161-164, 03/2012

/HePo13/ *M. Heidisch, N. Pohlmann:* „Aktive informationelle Selbstbestimmung in der Online-Welt – Privacy Service macht das Internet vertrauenswürdiger". IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, S. 64-67, 1/2013

/Pohl13/ *N. Pohlmann:* „Daten gegen Diebstahl sichern“, Wirtschaftsspiegel, IHK Münster, 2/2013

/PoSp13/ *N. Pohlmann, A. Speier:* „Eine Diskussion über Trusted Computing – Sicherheitsgewinn durch vertrauenswürdige IT-Systeme“. IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, S. 55-58, 5/2013

/PePo14/ *D. Petersen, N. Pohlmann:* „Wiederaufbau - Verschlüsselung als Mittel gegen die Überwachung“, iX - Magazin für professionelle Informationstechnik, Heise-Verlag, S. 82-86, 05/2014

/Pohl14/ N. Pohlmann; „IT-Sicherheitsherausforderungen im 21. Jahrhundert“. Die Polizei - Fachzeitschrift für die öffentliche Sicherheit mit Beiträgen aus der Deutschen Hochschule der Polizei. Carl Heymanns Verlag Köln, S. 255-260, 9/2014