IT-Sicherheitsherausforderungen im 21. Jahrhundert

Die Schäden durch Angriffe im Internet zeigen, dass wir uns zurzeit nicht angemessen schützen.

Das Internet mit seinen vielfältigen innovativen Möglichkeiten hat eine hohe Relevanz in unserer modernen Gesellschaft erreicht, die noch weiter steigen wird.
Die Angriffsflächen der IT- und Internet-Technologie werden durch komplexere Software und kompliziertere Zusammenhänge zwischen Protokollen, Diensten und Infrastrukturen vielfältiger und deutlich größer, was wir in der Berichterstattung von erfolgreich durchgeführten Angriffen lernen können.
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 dagewesen professionalisierte Nachhaltigkeit, die sich in der Wahrscheinlichkeit von Angriffen widerspiegelt.
Seit dem Beginn des Internets beobachten wir, dass die IT-Sicherheitsprobleme immer größer und größer werden, nicht kleiner. Die IT-Sicherheitsprobleme sind mit der NSA-Affäre nochmals stärker geworden. Das heißt, wir haben ein starkes Ungleichgewicht zwischen Angreifern und Verteidigern. Bei der kritischen Beurteilung der aktuellen IT-Sicherheitssituation fallen einige Sicherheitsprobleme besonders deutlich auf, die berücksichtigt werden sollten, um mehr IT-Sicherheit und Vertrauenswürdigkeit aufzubauen.

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 Rechnerzentren, aber auch immer mehr in Autos, in Industrieanlagen, im Haus, usw. Ein großes 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 an Softwarefehlern 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 10 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 ausnutzen. Die Hersteller von Software müssen ihre Softwareentwicklungsprozesse optimieren, um eine höher Qualität zu erreichen und die Nutzer sollten proaktive Sicherheitssysteme verwenden, damit ihre IT-Systeme robuster und vertrauenswürdiger werden.

Sicherheitsproblem: „Ungenügender Schutz vor Malware". Malware ist der Oberbegriff für "Schadsoftware" wie Viren, Würmer, Trojanische Pferde, usw. Angreifer (kriminelle Organisationen, Spione, Terroristen, …) nutzen Software-Schwachstellen 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 20. 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. 1.000 € 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 direkten Angriffen auf ein IT-System ist die Erkennungsrate im Schnitt sogar nur 27 %.

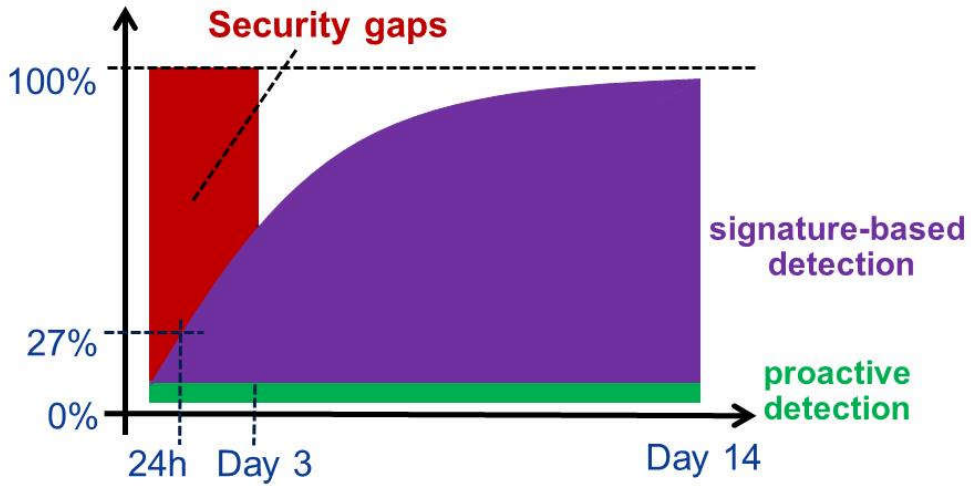

Abb. 1: Erkennungsrate von Malware

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 auszuspähen oder Schaden anzurichten.
Vor einigen Wochen hat sich Symantec als größter Hersteller von Anti-Malware Lösungen zu Wort gemeldet und hat mitgeteilt, dass sie nur noch 45 % der Malware erkennen. Diese Zahl spiegelt sicherlich das neue Verhältnis zwischen gezielten und Massen-Angriffen wider.

Sicherheitsproblem: „Keine internationalen Lösungen für Identifikation und Authentifikation“. Im Jahr 2014 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. 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.

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, das auf den deutschen gemessen Webseiten zurzeit ca. 2.5 % Malware direkt oder indirekt vorhanden sind, die dafür sorgen können, dass die Nutzer der Webseiten mit Malware infiziert werden (https://iks.internet-sicherheit.de/kennzahlen/bedrohung/#c289).
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. 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 LKWs 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 halten, sich und ihre Kunden angemessen zu schützen. Aber auch Regierungsorganisationen zeigen, dass sie nicht in der Lage sind, geheime Informationen oder datenschutz-relevante Bürgerinformationen angemessen zu schützen.

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/AppsHandy - 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, Bahnhöfen, Cafés) erhöhen die Wahrscheinlichkeit des unabsichtlichen Verlustes und des gezielten Diebstahls. Die Gefahr einer Bewegungsprofilbildung und die einfache Möglichkeit der Einsichtnahme in der Öffentlichkeit, 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 /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. 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 dümmsten anzunehmenden Benutzer erstellt werden. Erst mal funktioniert alles, wenn der Benutzer mehr Sicherheit möchte, dann muss er Einschränkungen vornehmen, was er meistens nicht kann. Eine richtige Business-Strategie wäre: Es funktioniert erst mal gar nichts und der Benutzer muss Funktionen

freischalten, die er unbedingt für die Erledigung seiner Aufgabenstellung braucht! Dadurch würde die Angriffsfläche auf mobile Geräte schon deutlich reduziert.

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 andere Länder zu kommen. Damit sind E-Mails ein weiterer großer Risikofaktor zurzeit. Wir wissen von Untersuchungen und Befragungen, dass zurzeit zu wenig E-Mails (wahrscheinlich zwischen 4 und 8 %)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 meist 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 können. Außerdem müssen die Mitarbeiter wissen, wie und - ganz wichtig - wann diese Verschlüsselungstechnologien für vertrauliche E-Mail verwendet werden sollen.

Sicherheitsproblem: „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 /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, aus der neuen EU-Verordnung für Datenschutz im Internet. Er 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/.

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.

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 Internet zu kompromittieren und unsere Werte angreifbar zu machen! Das ist eine wirklich schlechte Situation für uns alle. Hier müssen wir schnell und aktiv handeln, um als Gesellschaft eine angemessene IT-Sicherheit für unsere Werte zu erreichen!

Weitere aktuelle Herausforderungen: Weitere aktuelle Herausforderungen resultieren auch durch die Veränderungen der Rahmenbedingung. Das Internet geht über alle Grenzen und Kulturen hinaus. Es gibt 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 Soziale Netzte 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 Gegebenheit und Randbedingungen, auf die wir uns sehr schnell einstellen müssen.

Wie sieht eine Gesellschaftliche Sichtweise auf die unterschiedlichen IT-Sicherheitsprobleme aus?

Betrachten wir als erstes die Wirtschaftsspionage. 50 Milliarden Euro Schaden im Jahr laut den Aussagen aus dem Bundesinnenministerium. Dies können wir uns als Wissensgesellschaft nicht leisten! Die Angreifbarkeit unserer IT wird zurzeit immer höher und unsere Werte damit immer risikobehafteter. Hier müssen wir sofort aktiv werden und mit den Stakeholdern zusammen geeignete IT-Sicherheitsmaßnahmen einleiten, um unsere Werte als Wissensgesellschaft deutliche wirkungsvoller zu schützen.

Als zweiten und sehr wichtigen Aspekt sollten wir den Wert der Privatsphäre diskutieren, der für jeden Bürger eine sehr wichtige Rolle spielt. 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 Anforderung zu erfüllen, dann verlieren wir einen Teil der Demokratie, unsere Freiheit. Unsere Reaktionen sind bezogen auf die Schwere des Angriffes auf unsere Privatsphäre, die durch NSA und die unterstützenden US-Internet-Firmen durchgeführt wird, lächerlich.
Ein weiterer wichtiger Aspekt ist Cyber War. Angriffe auf Kritische Infrastrukturen, der Umstieg auf alternative Energien und damit prinzipielle höhere Angreifbarkeit unserer Gesellschaft sind weiter wichtige Herausforderungen,
Mit Stuxnet haben wir lernen müssen, dass mit einem Kostenaufwand für eine intelligente Malware von rund 9 Mio. US Dollar politische Ziele einfach und sehr erfolgreich umgesetzt werden können. Die schreckliche Alternative 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 CyberWar professionell einstellen.
Mit dem Ausstieg aus der Atomenergie haben wir als Gesellschaft einen mutigen Weg eingeschlagen. Der Atomausstieg sorgt 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 steigt 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 sein werden.

Die Herausforderungen
Wir kennen die IT-Sicherheitsprobleme, doch die heute vorhandenen und genutzten 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 zwei bis drei Gänge hoch schalten, haben wir eine Situation, bei der unsere Optionen sehr viel geringer sind!

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 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. 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.

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 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/.

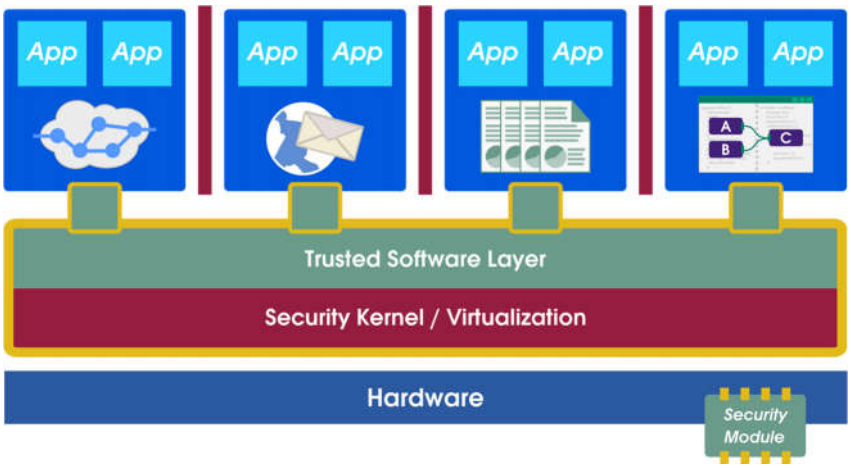

Abb. 2: Modere und wirkungsvolle Sicherheitsarchitekturen

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 /PoRe08/. 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.

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 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.

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, 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 reduziert und der Zugang zu qualifizierten IT-Sicherheitsexperten optimiert.

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 beschriebenen Paradigmenwechsel für das Erreichen einer höheren IT-Sicherheit und Vertrauenswürdigkeit einleiten. Die Paradigmenwechsel werden aufwendig sein, und es bedarf einer Koordinierung. Eine moderne Gesellschaft sollte diese notwendigen Schritte erkennen und zügig umsetzen.

Literatur

/PoRe08/ N. Pohlmann, H. Reimer: "Trusted Computing - Ein Weg zu neuen IT-Sicherheitsarchitekturen", Vieweg-Verlag, Wiesbaden 2008

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

/PoSp11/ N. Pohlmann, N. Spogahn: „Bauchladen – Wie man Googles Dienste umsichtig nutzt", iX - Magazin für professionelle Informationstechnik, Heise-Verlag, 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, 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, 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, 5/2013

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

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

Norbert Pohlmann ist Informatikprofessor für Verteilte Systeme und Informationssicherheit im Fachbereich Informatik und geschäftsführender Direktor des Instituts für Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen.
Vorher war er von 1988 bis 1999 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.
Prof. Pohlmann ist Mitinitiator und Vorsitzender des Programmkomitees der "Information Security Solutions Europe"-Konferenz (ISSE), die jährlich in unterschiedlichen europäischen Städten (Berlin, Barcelona, London, Paris, Wien, Berlin, Budapest, Rom, Warschau, Madrid, Den Haag, Berlin, Prag, Brüssel) stattfindet.
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