Statement: Prof. Norbert Pohlmann (2012)

Das Risiko von unsicheren Internet-Technologien

Die Schäden durch Angriffe im Internet zeigen, dass wir uns zurzeit nicht angemessen schützen (können). Wir brauchen Paradigmenwechsel!

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. Die Angriffe auf unsere immer höheren Werte auf den IT-Systemen und deren Verfügbarkeit werden verteilter, raffinierter und professioneller ausgeführt. Die IT-Kriminalität erfährt eine zunehmende Industrialisierung und damit eine nicht zu unterschätzende und nie dagewesen professionalisierte Nachhaltigkeit.
Bei der kritischen Beurteilung der aktuellen IT-Sicherheitssituation fallen einige Sicherheitsprobleme besonders deutlich auf, die durch einen Paradigmenwechsel gelöst werden könnten.

Erstes 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 3.000 Software-Fehler zu finden. 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 Angreifer immer weniger Software-Schwachstellen professioneller ausnutzen. Es müssen passende IT-Sicherheitssysteme geplant werden, da ein sehr hohes Bedrohungspotential durch Software-Schwachstellen vorhanden ist.

Zweites 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 25. IT-Endgerät in Deutschland ungewollte Malware vorhanden ist, die über ein Botnetz gesteuert wird. 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. Wir müssen kritisch feststellen, dass die Anti-Malware-Produkte heute mit 75% bis 95%

eine zu schwache Erkennungsrate haben. Bei direkten Angriffen auf ein IT-System ist die Erkennungsrate im Schnitt sogar nur 27 %. 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, um über einen längeren Zeitraum Informationen auszuspähen oder Schaden anzurichten. Gegen diese Art von hochentwickelten Angriffen mit intelligenter Malware haben wir im Prinzip heute keine passenden Abwehrtechnologien!

Drittes Sicherheitsproblem: „Keine internationalen Lösungen für Identifikation und Authentifikation". Im Jahr 2012 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. 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 keine Bedeutung.

Viertes Sicherheitsproblem: „Unsichere Webseiten im Internet". Heute wird Malware hauptsächlich über unsichere Webseiten im Internet verteilt. Hintergrund ist, dass die Unternehmen Webseiten im Internet zur Verfügung stellen, die nicht sicher genug sind. 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. 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.

Fünftes Sicherheitsproblem: „Neue Gefahren durch die Nutzung mobiler Geräte". Die Vorteile von mobilen Geräten, wie Smartphones und Tablets sind bestechend. Über die vielfältigen Kommunikationsschnittstellen (WLAN, UMST … LTE, usw.) 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, Computer, Navi, Musik/TV-Gerät, Zugang zum Unternehmen - alles in einem Gerät. Mit "Local Based Service" kommen nützliche und innovative Dienste 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. Eine

weitere Gefahrenquelle für Unternehmen ist die parallele Nutzung von mobilen Geräten für private und berufliche Zwecke.

Sechstes 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.

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 Internet-fizierung 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. 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.
Die grundsätzlich unsichere und schlecht umgesetzte Technologie, kombiniert mit einer ungenügenden Internet-Kompetenz der Nutzer, zeigt auf, dass wir Paradigmenwechsel brauchen, um zukünftig die moderneren Internet-Technologien und -Dienste risikoärmer nutzen zu können.

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 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.

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 - 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 - 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.

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.