TeleTrusT Deutschland e.V.

Der IT-Sicherheitsverband.

Berlin, 08.02.2011

"Vertrauen 2.0"

Was braucht die Informations- und Wissensgesellschaft?

Situationsbericht

Prof. Dr. (TU NN) Norbert Pohlmann
TeleTrusT-Vorstandsvorsitzender
Leiter des Instituts für Internet-Sicherheit – if(is)

Motivation

Wir leben in einer vernetzten Informations- und Wissensgesellschaft, mit sehr vielen und sinnvollen und erfolgsverspechenden Möglichkeiten, in denen Vertrauen eine immer bedeutendere Rolle spielt. Die Werte, die als Bit und Bytes zur Verfügung stehen und die Abhängigkeit von den angebotenen IT-Dienstleistungen im Internet werden immer größer. Die Angriffsflächen der IT werden durch die komplexere Software und komplizierteren Zusammenhänge zwischen Protokollen, Diensten und Infrastrukturen größer und vielfältiger. Die Angriffe auf unsere Werte und die Verfügbarkeit der IT-Systeme werden immer verteilter, raffinierter und professioneller ausgeführt und die IT-Kriminalität erfährt eine zunehmende Industrialisierung und damit eine nicht zu unterschätzende und nie dagewesen Nachhaltigkeit.

Damit wir die vielen innovativen Möglichkeiten, die uns zur Verfügung stehen, positiv nutzen können, müssen wir Vertrauen in die neuen Technologien und Akteure aufbauen.

Vertrauen

Unter Vertrauen wird die Annahme verstanden, dass Entwicklungen einen positiven oder erwarteten Verlauf nehmen. Ein wichtiges Merkmal ist dabei das Vorhandensein einer Handlungsalternative. Dies unterscheidet Vertrauen von Hoffnung. Vertrauen beschreibt auch die Erwartung an Bezugspersonen oder Organisationen, dass deren künftige Handlungen sich im Rahmen von gemeinsamen Werten oder moralischen Vorstellungen bewegen werden. Vertrauen wird durch Glaubwürdigkeit, Verlässlichkeit und Authentizität begründet, wirkt sich in der Gegenwart aus, ist aber auf künftige Ereignisse gerichtet [Wikipedia].

Wo liegen die neuen Herausforderungen bezüglich des Vertrauens in unsere vernetzte Informations- und Wissensgesellschaft?

Was müssen wir tun, um Vertrauen aufzubauen, damit wir die innovativen Möglichkeiten, die die vernetzte Informations- und Wissensgesellschaft mit sich bringt, nutzen können und dabei nur ein kalkulierbares, minimales Risiko eingehen müssen? Klar ist, weniger Vertrauen bedeutet auch, dass die neuen Möglichkeiten weniger genutzt werden.

Vertrauen ist die Basis für Erfolg!

Verändernde Herausforderungen

Die schnellen Veränderungen im Internet und bei den IT-Endgeräten haben sehr viele Vorteile, aber erzeugen auch neue Herausforderungen im Bereich der IT-Sicherheit und der Vertrauenswürdigkeit auf sehr unterschiedlichen Ebenen. Im Folgenden werden einige Herausforderungen formuliert, denen wir angemessen und nachhaltig begegnen müssen.

Softwarequalität
Die Software stellt in allen Branchen einen immer größeren Wertschöpfungsanteil dar. Wir nutzen Software in PCs, Notebooks, SmartPhones, aber auch immer mehr in Autos, Industrieanlagen, Kühlschränken, usw.
Eine gute Software erreicht ein hohes Maß an Qualität, wenn sie eine hohe Funktionalität aufweist, alle Funktionen korrekt und zuverlässig arbeiten, eine einfache und verständliche Benutzerschnittstelle zur Verfügung gestellt wird und die Software kaum Schwachstellen aufweist. Eine schlechte Software hingegen hat viele Schwachstellen und ist damit einfach anzugreifen. Das Risiko für Schäden ist entsprechend gross.

Die Ursachen für leicht angreifbare Software sind: Steigende Komplexität der Software, kein Sicherheitsbewusstsein der Entwickler, fehlende Expertisen der Entwickler (schlechter Programmierstil, mangelnde Informationen über eingesetzte Bibliotheken und Komponenten), fehlendes Wissen über aktuelle Sicherheitsbedrohungen, der Zeitdruck für der Fertigstellung der Software (Time-to-Market) und damit verbunden unzureichendes Testen und kurze Einführungsphasen. (Diese Liste ist nicht vollständig und erweiterbar). Der Softwareentwicklungsprozess verläuft deshalb häufig unsystematisch.

Die Hersteller arbeiten daran, die Anzahl der Schwachstellen in ihrer Software zu minimieren, aber die Angreifer machen zurzeit einen besseren "Job". Aus heutiger Sicht ist festzustellen, dass sich dieser Zustand nicht kurzfristig ändern wird, d.h. die Fehlerdichte von Software wird zwar kleiner, Fehlerfreiheit ist aber nicht erreichbar. Die kleiner werdende Anzahl der Software-Schwachstellen wird aber wegen ihrer professionellen Nutzung durch kriminelle Organisationen immer bedrohlicher..
Ein besonderes Risiko sind sogenannte Zero-Day-Attacks. Entdeckt jemand eine Sicherheitslücke und meldet diese nicht dem Software-Hersteller, so wird die Schwachstelle der Software erst nach dem ersten Angriff bekannt. Zero-Day-Attacken sind daher sehr effizient, weil sie großflächig neue Sicherheitslücken ausnutzen können, bevor Sicherheitsprodukte, wie z.B. Virenscanner die benötigten Signaturen zum Erkennen der Angriffscodes bereitstellen können. Hier brauchen wir innovative Ideen, wie diese Angriffsfläche insgesamt effektiv verkleinert werden kann.

Malware
Malware ist der Oberbegriff für "Schadsoftware" wie Viren, Würmer, Trojanische Pferde, usw. Angreifer (kriminelle Organisationen) nutzen Software-Schwachstellen aus, um Malware auf IT-Endgeräte zu installieren. Malware wird dann z.B. über E-Mail-Anhänge oder Webseiten mit Schadcode, auf denen die Nutzer surfen, auf die IT-Endgräten gebracht. Wir gehen zurzeit davon aus, dass auf jedem 25. IT-Endgerät ungewollte Malware vorhanden ist, die über ein Botnetz gesteuert wird. Dadurch können Angreifer Informationen von unseren IT-Endgeräten auslesen (Keylogger, Trojaner), unsere IT-Endgeräte für die Spam-Verteilung und DDoS-Angriffe nutzen, usw.

Zurzeit liegt die Erkennungsrate bei Anti-Malware-Produkten, bei nur 75 bis 90%! Das heißt, hier brauchen wir vertrauenswürdige Zusammenarbeitsformen zwischen den kompetenten Firmen und Organisationen, um die Wirkung der IT-Sicherheitsmechanismen zum Schutz gegen Malware deutlich zu erhöhen. Zurzeit gibt es viele Ideen, aber kein Businessmodell, das die Umsetzung dieses Weges einfach möglich macht.

Wir müssen die asymmetrische Bedrohungslage auflösen. Die meisten Angriffe mit Hilfe von Malware erfolgen global und ortsungebunden. Die Schutzmechanismen und die Reaktion auf einen erfolgreichen Angriff sind lokal. Der Aufwand des Schutzes multipliziert sich mit der Anzahl der Opfer, die alle für sich den gleichen Aufwand betreiben müssen, den Schaden zu begrenzen und zu beheben. Unser gemeinsames Ziel sollte sein, möglichst automatisiert, effektive Reaktionen auf Angriffe mit allen Beteiligten zu initiieren und damit die Wirkung gegen Angriffe deutlich zu erhöhen.

Eine weitere Herausforderung in diesem Bereich ist, dass zunehmend Malware gezielt für Personen und deren IT-Endgeräte geschrieben und genutzt wird. Mit solchen "Targeted Attacks" sollen typischerweise Informationen wie Strategiepläne von Vorständen/Politikern, Entwicklungsdaten von neuen Produkten, usw. entwenden werden. Da bei solchen gezielten Angriffen die Anti-Malware-Produkte konzeptionell schlechter wirken, muss hier nach neuen wirkungsvollen Sicherheitskonzepten gesucht werden.

CyberWar (Stuxnet)
CyberWar wird eine immer realere Bedrohung in Form von gezielten Angriffen auf kritische Infrastrukturen. Neben den DDOS-Angriffen, wie die auf Estland, ist Stuxnet damit eine weitere potentielle Bedrohung von des Staates. 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. Es wird spekuliert, dass diese Malware mit dem Ziel geschrieben wurde, 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.

Unser gemeinsames Ziel muss sein, vertrauenswürdige Industrieanlagen und kritische Infrastruktursysteme zu entwickeln, die robust gegen intelligente Malware sind.

Sicherheit von Informationen
Die Menge an Informationen in Organisationen wächst gewaltig und gleichzeitig werden immer mehr Informationen zwischen Organisationen ausgetauscht. WikiLeaks hat die Diskussion über die Sicherheit von Informationen auf eine neue Ebene gebracht. Die Frage ist, sind wir überhaupt in der Lage, Informationen in einer vernetzten Informations- und Wissensgesellschaft geheim zu halten?

Die Herausforderung in diesem Bereich ist, IT-Sicherheitslösungen zur Verfügung zu stellen, die den neuen Anforderungen gerecht werden. Enterprise-Right- und Information-Right-Systems oder Information-Centric Security sind einige Schlagworte für Lösungen, die dazu verwendet werden können. Trusted Computing ist z.B. eine Sicherheitstechnologie, die sehr vielversprechend ist, um bei vertrauenswürdigen Instanzen in verteilten und komplexen IT-Infrastrukturen Informationen zu schützen. Der Trend geht sehr stark von der "Perimeter-Sicherheit" hin zu einer offenen "Objekt-Sicherheit".

Mobility ("Mobiles Internet")
Die Vorteile von mobilen Geräten, wie z.B. SmartPhones und SmartPADs sind bestechend. Das Internet mit seinen Diensten ist über die vielfältigen Kommunikationsschnittstellen (WLAN, UMST…LTE, usw.) stets verfügbar. Sehr leistungsstarke Endgeräte sind immer und fast überall nutzbar sowie einfach und schnell über Touchscreens zu bedienen. Mobile Geräte sind multifunktional, d.h. Handy, Computer, Navi, Musik/TV-Gerät, Zugang zum Unternehmen - alles in einem Gerät. Mit "Local Based Service" kommen nützliche und innovative Dienste hinzu.

Aber auch die Gefährdungen für mobile Geräte sind nicht zu unterschätzen. Ständig wechselnde unsichere Umgebungen (Flughäfen, Bahnhöfen, Cafés) erhöhen die Wahrscheinlichkeit des unabsichtlichen Verlustes und des gezielten Diebstahls! Immer wertvollere Daten und Dienste stehen auf mobilen Geräten zur Verfügung. Die Gefahr einer Bewegungsprofilbildung muss berücksichtigt werden, und die einfache Möglichkeit der öffentlichen Einsicht ist in unsicheren Umgebungen nicht zu unterschätzen.

Die Verbreitung und Nutzung von mobilen Geräten und das Mobilfunknetz als Internet-Zugang schreitet sehr schnell voran. Laut Gartner werden 2013 mehr als die Hälfte der Internet-Nutzer auch mit mobilen Geräten über Mobilfunknetze ins Internet gehen. Laut Facebook werden heute schon täglich mehr als die Hälfte der Inhalte mit mobilen Geräten eingestellt. Auch in Unternehmen werden mobile Geräte in die Businessprozesse eingebunden.

Die Herausforderung in diesem Bereich ist, eine passende Nutzung und angemessene Schutzmechanismen für mobile Geräte zu finden, die die Risiken kalkulierbar werden lassen.

Cloud Computing
Cloud Computing umfasst die Idee, IT-Infrastrukturen (Rechenkapazität, Datenspeicher-, fertige Software- und Programmierumgebungen) und Softwareanwendungen (E-Mail, Office-Systeme, SAP) dynamisch an den Bedarf angepasst über das Internet den Nutzern als Dienst zur Verfügung zu stellen. Doch die Verlagerung von Daten und IT-Diensten in die "Cloud" geht mit einem Kontrollverlust einher.

Insbesondere bei Privatpersonen und mittelständischen Unternehmen wird Cloud Computing eine besondere Rolle spielen, besonders auch in Verbindung mit der Mobilität (Anywhere Application Architecture). Für den Mittelstand sind die größeren Compliance-Anforderungen selber kaum noch umzusetzen.

Die Herausforderung bei Cloud Computing ist, wie die Sicherheit und Vertrauenswürdigkeit von Anbietern geschaffen, gemessen und aufrecht erhalten werden kann. Hier spielen besonders auch die unterschiedlichen Werte und Vorstellungen der Anbieter der unterschiedlichen Länder eine Rolle.

Robustheit und Verfügbarkeit des Internets
Wir brauchen für das Internet eine sehr hohe Robustheit, um die Verfügbarkeit auf allen Ebenen zu stärken. Herausforderungen in diesem Bereich sind: Die Einführung DNSSEC, Secure BGP und IPv6. Außerdem müssen wir geeignete Sicherheitsmechanismen gegen DDoS-Angriffe einführen.

Die DDoS-Angriffe als Reaktion auf die Sperrung von Konten von WikiLeaks, haben gezeigt, wie anfällig sehr große Organisationen gegenüber solchen Angriffen im Internet sind.

Mit der zunehmenden Wertschöpfung durch das Internet oder mit Hilfe des Internets wird eine immer größere Abhängigkeit entstehen, die für Bürger, Firmen, Regierungen sowie Staaten existenziell bedeutsam ist.

Soziale Netzwerke
Soziale Netzwerke wie Facebook, YouTube, Xing, LinkedIn, Twitter & Co. bringen Nutzer aus verschiedenen Gesellschaftsgruppen zusammen und ermöglichen den Nutzern, sich darzustellen. Soziale Netzwerke schaffen auch neue Wege, Demokratie und Bürgerbeteiligungen zu gestalten, was eine neue und ungewohnte Herausforderung für alle Beteiligten darstellt.

Außerdem rufen soziale Netzwerke die Diskussion über die informationelle Selbstbestimmung und den Datenschutz hervor! Eine Frage dazu ist, inwieweit Internet-Angebote zu tolerieren sind, bei denen wir nicht über das direkte Bezahlen des Angebotes, sondern über das Zulassen von Profilbildungen, den Anbietern das indirekte Geldverdienen ermöglichen. Die Herausforderungen in diesem Bereich sind die Aufklärung der Nutzer über die Risiken und die Suche und Umsetzung einer gemeinsamen angemessenen Lösung mit den Anbietern von Sozialen Netzwerken.

Internet der Dinge
Die Digitalisierung von Technologien, Geräten und Maschinen durch alle Lebensbereiche hindurch hilft uns viele Aufgabenstellungen zu lösen und unsere Leben einfacher zu gestalten. Dies bedeutet aber auch, dass kritische Infrastrukturen wie Stromnetze, Verkehrssysteme, Lieferketten im Handel und Bankensysteme immer intelligenter, aber auch immer anfälliger gegen Angriffe werden.

Am "Internet der Dinge", nehmen zunehmend eigenständige Geräte teil, die ihrerseits schnell komplexe Zusammenhänge bewerten und eigenständig reagieren müssen. Beispiele sind die Entscheidungen für den Nachkauf von Lebensmitteln und Gerätefunktionskontrollen im SmartHome, Energiemanagement in Gebäuden und Green IT.

Im "Internet der Dinge" werden sehr viele Dinge miteinander interagieren. Die Herausforderung ist: Wie kann dies sicher umgesetzt werden, damit wir Vertrauen in unsere Geräte und Maschinen haben können?

Beim Thema SmartGrid geht es um eine effiziente, zuverlässige und intelligente Stromversorgung, mit dem Ziel der Energieverbrauchsoptimierung. In diesem Bereich müssen viele Aufgabenstellungen mit der Kompetenz der IT-Sicherheit gelöst werden, da eine Vernetzung und Steuerung von Stromerzeugern, Speichern, elektrischen Verbrauchern und Netzbetriebsmitteln in Energieübertragungs- und -verteilungsnetzen der Elektrizitätsversorgung, vertrauenswürdig umgesetzt werden muss.

Internet-Kompetenz
Internet-Kompetenz ist das Wissen und die Erfahrung, die ein Internet-Nutzer braucht, um sicher und vertrauenswürdig Dienste im Internet nutzen zu können.

Dazu müssen die Nutzer für einen richtigen, bewussten Umgang mit IT-Endgeräten und dem Internet geschult werden, das heißt, sie müssen die Regeln und richtigen Verhaltensweisen verinnerlichen, um die Risiken und Gefahren erkennen und abschätzen zu können.

Da die IT-Technologien und -Diensten alleine keine vollständige Sicherheit erbringen können, ist das richtige Verhalten des Nutzers unabdingbar für die sichere Nutzung und den Aufbau von Vertrauen.

Unterschiedliche Kulturen, Werte und Gesetze
Das Internet ist global und geht über alle Grenzen und Kulturen hinaus. Ein Problem, das dabei auftaucht ist, dass in vielen Ländern keine Strafverfolgung möglich ist. Kriminelle Organisatione finden hier sehr effektive Handlungsräume. Es gibt auch Unterschiede bei den Werten und moralischen Vorstellungen, über das, was richtig und was falsch ist! Einige Länder schützen geistiges Eigentum, andere nicht. Viele Länder betreiben aktive Wirtschaftsspionage, andere nicht. Cyber Warfare ist heute eine ernst zu nehmende Bedrohung.

Unterschiedliche Rechtssysteme und -auffassungen erzeugen Probleme bei grenzüberscheitenden und verteilten Anwendungen (Cloud Computing). Aber auch die kulturellen Unterschiede bezüglich der Bedürfnisse von Sicherheit und Vertrauen sind zu beachten.

Vertrauen in dies Technologie- und Dienstanbieter
Die Technologie- und Dienstanbieter haben eine sehr hohe Verantwortung für die Dinge, die sie uns anbieten. In der IT- und Internet-Branche ist diese Verantwortung noch nicht so stark ausgeprägt. Fehlende Strukturen von Produkt- und anderen Haftungen sowie das Auf-den-Markt-bringen von Lösungen, die gegen Gesetze und Wertvorstellungen verstoßen, kennzeichnen das Problem deutlich.

Hier ist es entscheidend, dass die Technologie- und Dienstanbieter Vertrauen aufbauen, damit die Entwicklung positiv weiter gehen kann.

Weitere Herausforderungen sind die Netzneutralität des Internets, organisationsübergreifendes Identifikationsmanagement, internationale E-Mail-Sicherheit, höhere Webserver-Sicherheit, globale Privatheit, usw.

Zusammenfassung
Die Herausforderungen der IT-Sicherheit und Vertrauenswürdigkeit werden immer größer, internationaler und sehr viel komplexer. Da aber nur bei einer angemessenen IT-Sicherheit und Vertrauenswürdigkeit der IT-Systeme und -Dienste diese auch genutzt werden, müssen wir uns den Herausforderungen stellen, passende innovative IT-Sicherheitslösungen entwickeln und zur Verfügung stellen. Nur so können wir unseren Platz in der vernetzten Informations- und Wissensgesellschaft finden.

TeleTrusT lädt dazu ein, sich zu beteiligen und gemeinsam Verantwortung für unsere digitale Zukunft zu übernehmen.