Statement: Prof. Norbert Pohlmann (2016)

Wir brauchen in der Zukunft deutlich sicherere und vertrauenswürdigere IT

Der Trend ist deutlich: Immer mehr Menschen nutzen IT und das Internet. Die IT-Sicherheit weist jedoch drastische Lücken auf, sodass kriminelle Hacker im Prinzip alles angreifen können. Lösungsansätze für IT-Sicherheitsprobleme gibt es genügend, allerdings fehlt eine einheitliche, nachhaltige Strategie für die Umsetzung von mehr IT-Sicherheit.

Die IT und das Internet sind „der Motor" und die Basis für das Wohlergehen unserer modernen und globalen Gesellschaft. Leider müssen wir feststellen, dass seit Beginn der IT und des Internets die IT-Sicherheitsprobleme jedes Jahr größer und nicht kleiner werden. Der Schaden im Bereich der Wirtschaftsspionage wird zurzeit mit 51 Mrd. Euro pro Jahr beziffert. Weitere gesellschaftliche Herausforderungen, neben der Wirtschaftsspionage, liegen in den Bereichen Privatheit und Autonomie sowie im Bereich Cyberwar, der die Qualität und Quantität von Angriffen durch andere Staaten sowie Terroristen erhöhen und damit den gesellschaftlichen Schaden deutlich vergrößern wird.

Die heutigen IT-Architekturen unserer Endgeräte und Server sind nicht so konzipiert und aufgebaut, um den Fähigkeiten von intelligenten Hackern angemessen entgegenzuwirken. Wir können es täglich den Medien entnehmen, wie kriminelle Hacker die schlechte Qualität der Software für erfolgreiche Angriffe ausnutzen, Malware installieren, Passwörter sowie Identitäten stehlen, unsere Endgeräte ausspionieren, usw.

Die Bundesregierung hat jetzt einen Notfallplan zum zivilen Selbstschutz entwickelt. Die Bevölkerung soll Vorräte für den Katastrophenfall anlegen. Nahrung für zehn Tage, Trinkwasser für fünf. Auslöser des Katastrophenfalls können insbesondere Cyber-Angriffe auf unsere Strom- und Wasserversorgung sein. Das heißt, die Bevölkerung soll sich berechtigt darauf einstellen, dass Cyber-Angriffe auf unsere Gesellschaft stattfinden werden. Aber eine gemeinsame Strategie, die für eine nachhaltige Verbesserung der IT und IT-Sicherheit sorgt, entwickelt die Bundesregierung seit Jahren nicht.

Apple gibt sehr viel Geld für das eigene Image aus, das Unternehmen betont stetig, dass seine Produkte besonders sicher sein sollen. Aber die Spionagesoftware Pegasus, die neue unbekannte Schwachstellen ausgenutzt hat, zeigt, dass real viel zu wenig getan wird! Die Firma, die diese Schwachstellen für die Geheimdienste mit ihren Experten gefunden hat, macht im Jahr einen Umsatz von 75 Mio. Dollar. Hauptarbeitsfeld ist das Finden von Schwachstellen in vielen Betriebssystemen und Anwendungen. Apple dagegen hat im Jahr 2015 allein einen Gewinn von 53 Mrd. Dollar erwirtschaftet. Wenn Apple nur ein Promille des Jahresgewinns in das Finden von vorhandenen Schwachstellen stecken würde, wäre ihr Image deutlich authentischer!

Wir brauchen in Zukunft sichere und robuste IT-Architekturen für unsere Endgeräte (Notebook, Smartphone, Tablets, Smartwatchs, …) und Server, die z.B. mit Hilfe von intelligenten kryptographischen Verfahren sowie Separierung- und Isolierungstechnologien dafür sorgen, ein angemessenes Level an IT-Sicherheit zu erreichen, um die Höhe des Schadens zu reduzieren. Durch eine vermehrte Nutzung von Verschlüsselungstechnologie für die Übertragung und Speicherung von Daten könnte eine Vielzahl von Angriffsflächen eliminiert werden. Dazu brauchen wir integrierte, einfach zu bedienende Verschlüsselungslösungen, die einen optimalen Schutz gewährleisten. Eine Produkthaftung der IT-Hersteller und -Dienstanbieter würde die notwendige Verantwortung positiv motivieren und für mehr IT-Sicherheit zu sorgen.

Cloud-Dienste liegen eindeutig im Trend. Hier ist die Nutzung von professionellen Rechenzentren - im Gegensatz zu Servern im Keller - für eine Vielzahl von Mittelständlern ein sofortiger

Sicherheitsgewinn bezüglich der Verfügbarkeit von wichtigen Informationen und IT-Diensten. Die Integration von widerstandsfähigen IT-Sicherheitsdiensten, die für die Nutzenden einfach zu bedienen sind sowie die vertrauenswürdige zur Verfügungsstellung der Dienste der Cloud-Betreiber sind Herausforderungen in diesem Bereich. Hier könnten sich insbesondere die deutschen Anbieter profilieren.

Trotz der manchmal beängstigenden Risiken des digitalen Wandels sollten wir vorrangig den Chancen der Digitalisierung unser Hauptaugenmerk schenken: Moderne und sichere IT-Sicherheitslösungen stehen bereit! Wir brauchen nur noch eine gemeinsame Strategie und den festen Willen, um diese flächendeckend einzusetzen und so die Vorzüge des Fortschritts mit einem angemessenen Risiko auszukosten.