Norbert Pohlmann

Lehren aus der IT-Sicherheitskrise ziehen!

Die Enthüllungen über die Aktivitäten der NSA bieten die Chance, zu lernen wie Spione und professionelle Hacker unsere IT-Schutzmaßnahmen umgehen und darauf aufbauend IT-Sicherheitstechnologien zu verbessern.

Die Enthüllungen von Edward Snowden haben den IT-Sicherheitsexperten gezeigt, dass – trotz aller IT-Sicherheitsversprechen – nahezu alle Internet-Infrastrukturen; IT-Systeme und -Anwendungen erfolgreich angegriffen werden können. Und das betrifft nicht nur das Handy von Bundeskanzlerin Angela Merkel. Auch die USA haben massive Sicherheitsprobleme. Chinesische Hacker haben in den letzten Jahren amerikanische IT-Firmen wie Google und RSA Security erfolgreich gehackt. Auch große US-Zeitschriften wie die New York Times oder die Washington Post waren für die professionellen Hacker leichte Beute. Die Sicherheitsmaßnahmen von US-Behörden waren für die Eindringlinge löchrig wie ein Schweizer Käse.

Wir müssen realisieren, dass unsere heutigen IT-Sicherheitslösungen weder Geheimdienst noch professionelle Hacker stoppen können. Das ist kein rein deutsches Sicherheitsproblem, sondern ein weltweites. Wenn die professionellen Hacker dieser Welt das richtige Wissen haben und über genug Geld verfügen, können sie jede Organisation erfolgreich hacken.

Natürlich wussten wir, dass NSA und Co. uns ausspionieren. Aber der Umfang und die Tiefe, sowie das viele Geld, das dafür ausgegeben wird, haben die Grenzen unserer Vorstellungskraft deutlich überschritten. NSA und Co. sorgen dafür, dass unsere IT und IT-Sicherheitsmechanismen manipuliert werden und machen damit unsere Geschäfte unsicher und unsere Leben unwürdig.

Was sind die richtigen Schlussfolgerungen?

Wir sollten die Krise als Chance begreifen und nicht im Bereich der Spionage aufrüsten! Statt die USA anzuklagen, sollten wir auf sie zugehen und gemeinsam über verbesserte IT und IT-Sicherheitstechnologien sprechen. Wir können von der NSA lernen: Wie gelang es ihnen, unseren Schutz zu umgehen? Wie können wir uns mit diesem Wissen in Zukunft besser schützen? Welche Schwachstellen nutzen die erfolgreichen Hacker dieser Welt, um uns so erfolgreich zu hacken? Was können wir von den erfolgreichen Hackern lernen, um uns gegen Wirtschaftsspionage und Terrorismus zu schützen?

Wir sind in Deutschland gerade dabei als Vorreiter aus der Atomenergie auszusteigen und auf alternative Energien umzusteigen. Dazu brauchen wir intelligente Stromnetze, die an das Internet angeschlossen sind. Das heißt, alle bekannt gewordenen Angriffe im Internet sind auch auf unsere Stromversorgung anwendbar. Die Elektromobilität mit all ihren Vorteilen macht unsere Fahrzeuge und Verkehrsinfrastrukturen angreifbar, weil diese miteinander und im Internet verbunden sind. Industrie 4.0 bedeutet für die deutsche Leitindustrie viele positive Perspektiven für die Zukunft, aber auch neue IT-Sicherheitsrisiken, denen wir angemessen entgegenwirken müssen.

Zukünftige Angriffe können zu höheren Schäden und zum Verlust des Vertrauens in das Internet führen!

Die chinesischen Hacker und Snowden haben uns gezeigt, dass wir eine Menge unterschiedlicher Sicherheitsprobleme und Herausforderungen im Internet haben. Aber wir haben auch sehr viele positive Möglichkeiten, mit Hilfe der innovativen IT-Technologien und Lösungen, die auf uns warten. Also sollten wir die Krise als Chance begreifen und besser in die Internet-Sicherheit investieren, statt gegenseitiges Misstrauen zu schüren. Deutschland sollte Verantwortung übernehmen und ein sicheres und vertrauenswürdiges, globales Internet für die Zukunft entscheidend mit kreieren.

Gerade wir in Deutschland haben kulturell und gesetzlich, aber auch in der IT-Sicherheitsforschung und in der IT-Sicherheitsindustrie, die idealen Voraussetzungen einen wichtigen Beitrag zu einem sicheren und vertrauenswürdigen Internet zu leisten. Die schon vorhandenen, innovativen und wirkungsvollen IT-Sicherheitsmechanismen aus Deutschland müssen in der Industrie und bei den Behörden konsequent eingesetzt werden. Anreize für die Wirtschaft müssen geschaffen und die Internet Sicherheitsforschung muss noch stärker gefördert werden. Nur so können wir die vielen positiven Möglichkeiten in Zukunft vertrauenswürdig und sicher nutzen.

Norbert Pohlmann

Professor für Informationssicherheit und geschäftsführender Direktor des Instituts für Internet-Sicherheit an der Westfälische Hochschule Gelsenkirchen sowie Vorstandsvorsitzender des TeleTrusT – Bundesverband IT-Sicherheit.
E-Mail: pohlmann@internet-sicherheit.de