Ideen für eine IT-Sicherheitsstrategie in Deutschland

Klassenmodell für Security-Wirkung

Seit Edward Snowden ist klar geworden, dass wichtige IT-Technologien aus den USA und anderen Ländern absichtlich durch Anbieter und Geheimdienste manipuliert werden. Die Marktführer der meisten Technologien im Bereich der IT und IT-Sicherheit kommen vorherrschend aus den USA. Neben den klassischen IT-Sicherheitsbedrohungen (Malware, Phishing, Exploits) machen Manipulationen an weit verbreiteten Betriebssystemen, Routern, Verschlüsselungssystemen und Separationstechnologien die Bundesrepublik Deutschland sehr verwundbar für Cyberwar-Attacken sowie Industrie- und Wirtschaftsspionage. Die Kritischen Infrastrukturen („KRITIS") in Deutschland werden immer häufiger an das Internet angeschlossen und sind so theoretisch weltweit erreichbar. Dies sorgt für eine hohe Verwundbarkeit, da diese aus aller Welt angegriffen werden können. Diese veränderte Risikolage und der massive Verlust der Vertrauenswürdigkeit sind einige der Hauptmotive für die hier vorgestellten Ideen einer möglichen IT-Sicherheitsstrategie. Es gilt, die Schieflage der heutigen IT-Sicherheitssituation zu beseitigen, damit die Vertrauenswürdigkeit und damit eine angemessene Risikolage wiederhergestellt werden kann.

In nahezu allen Bereichen des menschlichen Lebens herrscht heute eine massive Abhängigkeit von IT-Systemen, die für den Nutzer fast immer eine Art „Black Box" darstellen. Es ist nicht feststellbar, ob ein IT-Gerät lediglich die gewünschte Funktionalität zur Verfügung stellt oder auch weitere Manipulationen und Backdoor-Erweiterungen enthält. So stellt sich die Frage nach einer möglichen absichtlichen Schwächung eines IT-Systems, welches nach außen hin sicher zu sein scheint.

Ein weiteres Problem besteht darin, dass viele Verantwortliche den Schutzbedarf erst gar nicht einschätzen und einordnen können. Mit der Frage nach der gewünschten und der tatsächlich erzielten Wirkung sind sie ebenfalls überfordert. Das gilt auch für die Sicherheitssysteme, welche die IT gegen unerwünschte „Nebenwirkungen" sichern soll. Höhe und Qualität der Wirkung von Schutzsystemen sind oft kaum klar bestimmbar. Das wäre jedoch notwendig und darf nicht vernachlässigt werden. Meist sind bei den Verantwortlichen obendrein das Maß der eigenen Verantwortung und die möglichen Konsequenzen unbestimmt. Tatsache ist, dass diesbezüglich bei jeder Sicht auf die großen IT-Sicherheitsfragen immer vom Schlimmsten ausgegangen werden muss.

Bewertung der IT-Technologien

Für die Einschätzung der aktuellen IT-Sicherheitslage und die Beurteilung des Zustands der IT-Sicherheitsindustrie war es notwendig, eine Analyse der zur Verfügung stehenden IT-Sicherheitstechnologien durchzuführen und diese zu bewerten. Die durchgeführte Technologieanalyse illustriert aus deutscher Sicht zahlreiche Defizite, denen in naher Zukunft auf angemessene Weise begegnet werden muss.

Dabei zeigt sich eines deutlich: Die Marktmacht der US-amerikanischen Unternehmen ist in vielen IT- und IT-Sicherheitsbereichen sehr groß. Natürlich könnte Europa beispielsweise unter enormem personellem und finanziellem Aufwand mögliche Alternativen im Sinne der nationalen technologischen Souveränität schaffen, aber der Preis wäre zu hoch. Ein völlig neues Betriebssystem vergleichbar zur Windows-Familie aus dem Nichts zu entwickeln oder konkurrenzfähige Routing-Produkte zu schaffen, wäre enorm teuer und würde lediglich die aktuellen IT-Technologien ohne großen technologischen Mehrwert substituieren. Diese Herausforderung lässt sich deutlich eleganter zur Zufriedenheit aller Beteiligten lösen.

Ein wichtiges Handlungsfeld ist zum Beispiel eine verstärkte Nutzung von Verschlüsselung, wodurch bereits viele Angriffe und Schwachstellen ausgehebelt werden. Zudem sind innovative Konzepte notwendig, die eine höhere IT-Sicherheit und Vertrauenswürdigkeit bieten. Viele Angriffspunkte können mit Hilfe deutscher IT-Sicherheitstechnologien eliminiert wer-

den. Dies sind beispielsweise „Separierung und Isolierung", „sichere Plattformen" oder „Execution Prevention".

Ein hoher Grad der Vertrauenswürdigkeit eines IT-Systems gewährleistet einen höheren Schutz vor Cyberwar-Angriffen und Cyber-Attacken durch ausländische Behörden und Institutionen. Eine besondere Herausforderung ist es also, mit Hilfe von eigenen IT-Sicherheitstechnologien die Vertrauenswürdigkeit deutlich anzuheben und damit das Risiko eines Schadens zu minimieren.

IT-Security-Replaceability

Hierzu gibt es verschiedene Möglichkeiten und Wege. Der Ansatz der „IT-Security-Replaceability" (Austauschbarkeit) fordert eine konstruktive Zusammenarbeit aller Firmen. Die US-amerikanischen Marktführer sollen nicht generell substituiert werden, sondern dabei mitwirken, vertrauenswürdige IT-Sicherheitskomponenten aus Deutschland zu integrieren. Das Angebot einer Austauschbarkeit trägt massiv zu einem Vertrauensgewinn der Marktführer bei. Das Ziel ist es, mit geringstem Aufwand den höchsten Nutzen für alle Beteiligten zu erzielen. Hierbei soll auch das neue (im späteren Verlauf dieses Beitrags vorgestellte) Wirkungsklassen-modell helfen. Es ermöglicht eine pragmatische Vorgehensweise für die angemessene Nutzung von vertrauenswürdigen IT-Sicherheitslösungen, die den eigenen Schutzbedarf berücksichtigt und deren Umsetzung schnell und nachvollziehbar ist.

Die Idee der Austauschbarkeit beziehungsweise der „IT Security Replaceability" fordert die Austauschbarkeit von IT-Sicherheitsprodukten und IT-Sicherheitstechnologien innerhalb von Produkten, Betriebssystemen und Geräten. Dies sollte einfach und nachhaltig möglich sein. Ohne diesen Schritt lässt sich das verlorene Vertrauen aus der Vergangenheit in Betriebssysteme, absichtlich geschwächte Verschlüsselung und manipulierte Hardware nicht zurückgewinnen.

Dieses Prinzip würde IT-Marktführern ermöglichen, deutlich mehr Vertrauen zu schaffen. Der Kunde kann dabei entscheiden, welche IT-Technologie er einsetzen möchte (je nach Schutzbedarf und Wirkungsklassenmodell). Zudem könnte die Möglichkeit der Austauschbarkeit neue Perspektiven für die deutsche IT-Sicherheitsindustrie schaffen, da sie dann stärker weltweit tätig werden könnte. Dies wäre eine Win-Win-Situation für alle Beteiligten.

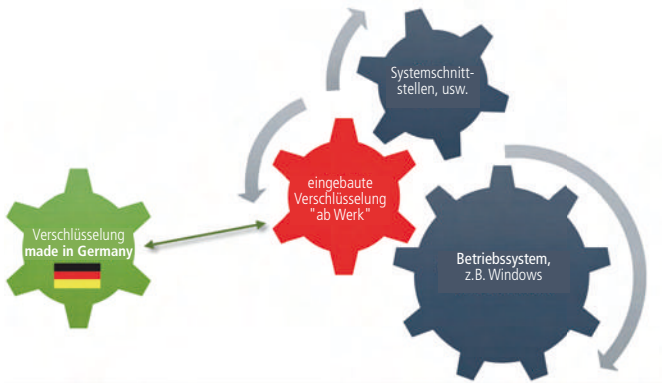

Bild 1: Beim Ansatz „IT-Security-Replaceability" sollen die US-amerikanischen Marktführer nicht generell substituiert werden, sondern dabei mitwirken, vertrauenswürdige IT-Sicherheitskomponenten aus Deutschland zu integrieren.

IT-Sicherheit als Konzept

Überall, wo sich informationsverarbeitende Systeme befinden, gibt es auch eine Notwendigkeit, Informationen, die in jeglicher Form verarbeitet und gespeichert werden, vor dem Zugriff durch Unbefugte zu schützen. Dies sind insbesondere Gefahren wie Diebstahl, Manipulation oder gar die absichtliche Vernichtung und Sabotage.

Der Begriff der IT-Sicherheit ist ein facettenreicher Oberbegriff, der sehr viele Bereiche abdeckt und nicht einfach als einziger Punkt auf einer To-do-Liste eines Verantwortlichen abgehakt werden kann. Neben den grundlegenden Dingen wie Netzwerksicherheit und Zugangssicherheit sind auch andere Faktoren bedeutsam wie beispielsweise die Fragen nach der IT-Sicherheit der eingesetzten Software- und Hardwareprodukte: Weisen die eingesetzten Anwendungen oder Hardwarekomponenten Sicherheitslücken auf? Falls ja, lassen sich diese beheben? Falls sie sich aufgrund mangelnder Unterstützung durch den Hersteller nicht beheben lassen, was ist zu unternehmen?

Wirkungsklassenmodell

Das in Abbildung 2 vorgestellte „Wirkungsklassenmodell" ist in fünf sogenannte Wirkungsklassen unterteilt (0 bis 4). Diese Wirkungsklassen bauen aufeinander auf. Jede Klasse enthält neben den zusätzlichen eigenen Objekten auch jene aus der darüberliegenden Klasse. So deckt beispielsweise die Wirkungsklasse 0 als Gefahren die Angriffe auf die Privatsphäre von Bürgern und durch Cybercrime ab, wohingegen die Wirkungsklasse 1 zusätzlich zu den Elementen der Klasse 0 auch Cybercrime mit höherem Gefahrengrad und den gesetzlichen Datenschutz von Unternehmen, Organisationen und Behörden berücksichtigt.

Die Beschreibung unmittelbar rechts neben dem farblichen Reiter für die Angabe der Klasse beschreibt die Zielgruppe, für welche sie den Schutzbedarf deckt. Die betitelten Kosten für jede Wirkungsklasse ergeben sich in den einzelnen Fällen aus dem Grundpreis für die Anschaffung eines IT-Systems (zum Beispiel PC). Diese sind hier als prozentuale Kosten des „Grundbetrags" veranschlagt, um das IT-System dem Bedarf entsprechend schützen zu können. Siehe Bild 2.

Eine Einordnung in die Wirkungsklasse soll die Umsetzung des eigenen Schutzbedarfs vereinfachen. Hier besteht die Idee, dass Sicherheitsanbieter passende Lösungen und Produkte anbieten, die mit den Wirkungsklassen harmonieren. Der Nutzer kann nach Einstufung der einzelnen IT-Systeme innerhalb der Organisation diese relativ einfach und effektiv mit dem notwendigen Schutz ausstatten.

Technologieanalyse

Im Rahmen der Ausarbeitung für die Aspekte der IT-Sicherheitsstrategie wurde eine Technologieanalyse erstellt. Diese soll einen Überblick über das Angebot und den Zustand der IT-Sicherheitsbranche in Deutschland geben. Nachfolgend wird nur eine zusammenfassende Darstellung von Teilergebnissen diskutiert, da die gesamte

Für Abonnenten ist dieser Artikel auch digital auf www.datakontext.com verfügbar

Wirkungsklasse 0	**Bürger mit privater Nutzung**
Gefahren:	Privatsphäre, Cybercrime
Kosten:	Grundbetrag +5%
Wirkungsklasse 1	**Unternehmen, Organisation, Behörden**
Gefahren:	Privatsphäre, Cybercrime mit höherem Gefährdungsgrad, gesetzlicher Datenschutz
Schutzbedarf:	mittel
Kosten:	Grundbetrag +10%
Wirkungsklasse 2	**Unternehmen, Organisation, Behörden, Infrastruktur**
Gefahren:	Industriespionage, gezielte Angriffe auf Werte des Unternehmens, Cybercrime
Schutzbedarf:	hoch
Kosten:	Grundbetrag +20%
Wirkungsklasse 3	**Unternehmen, Organisation, Behörden, Infrastruktur**
Gefahren:	Wirtschaftsspionage (Nachrichtendienste) und Cyberattacken, Cyberwar (Sabotagen)
Schutzbedarf:	sehr hoch, inkl. VS-NfD
Kosten:	Grundbetrag +50%
Wirkungsklasse 4	**Verschlusssachen**
Nationale Sicherheit	
Schutzbedarf:	gemäß Geheimschutzordnung GSO, ab VS/V
Kosten:	Grundbetrag +400%

Bild 2: Wirkungsklassenmodell

Technologieanalyse ausführlich durchgeführt wurde und jeder Technologiebereich einzeln betrachtet worden ist.

Die in der Tabelle in Bild 3 gewählten Farben sollen ein Ampel-ähnliches Farbschema repräsentieren. Die Farbcodierung soll die Erfassung durch den Leser auf den ersten Blick erleichtern und den Vergleich mit anderen Elementen vereinfachen. Farblich sind die Ampelfarben Grün, Gelb und Rot berücksichtigt worden, wobei es jeweils eine Abstufung im grünen und roten Bereich gibt, wie im oberen Bereich der Tabelle zu sehen ist. Siehe Bild 3.

Eine genauere Betrachtung der Tabelle zeigt, welche Bereiche in naher Zukunft unbedingt bearbeitet und gefördert werden müssen. Es wird deutlich, dass insbesondere die Bereiche E-Mail-Verschlüsselung, Secure Instant Messaging und die Basistechnologien große Aufmerksamkeit der deutschen IT-Sicherheitsindustrie und Förderungsmaßnahmen des Staates benötigen.

Die Bereiche, in denen die Defizite besonders stark ausgeprägt sind, lassen den Schluss auf fehlende Basistechnologien und eine Know-how-Lücke zu. Dies ist insbesondere in den Technologiebereichen sichtbar, bei denen es wenige Lösungen gibt, also weder Marktstärke noch ein Vorsprung der deutschen Unternehmen vorherrscht. Offenbar ist es hier bis heute nicht gelungen, mit den üblichen Mitteln und der eigenen Kraft der Unternehmen konkurrenzfähige Produkte zu entwickeln. Dies wären Bereiche wie IPS/IDS, Data Leakage Prevention und vor allem im Bereich der Basistechnologien. In all diesen Bereichen muss also nach neuen Wegen, Lösungen und Innovationen geforscht werden.

Besonders ins Auge sticht hier über alle Technologiebereiche hinweg der Abstand und die herrschende Lücke zwischen dem Soll-Ist-Vergleich der einzelnen IT-Sicherheitstechnologien. Die Zeile „Abstand zwischen Soll- und Ist-Zustand (Δ)" beschreibt den Unterschied zwischen der Notwendigkeit der IT-Sicherheitstechnologien in deutschen Unternehmen und den sich tatsächlich im Einsatz befindenden IT-Sicherheitstechnologien.

Positiv ist hier, dass alle betrachteten Bereiche mit ihrer dunkelgrünen Markierung klar zeigen, dass sie allesamt ohne Ausnahme bedeutend für die Zukunft sind. Dies ist als ein positives Signal zu werten, denn es unterstreicht, dass sich die IT-Sicherheitsindustrie in den richtigen Bereichen bewegt. Es wird aber auch offensichtlich, dass in vielen Bereichen noch großer Handlungsbedarf besteht.

Wirkungsaspekte ohne Vertrauenswürdigkeit

In manchen Fällen ist ein hohes Maß an Vertrauenswürdigkeit nicht ohne Weiteres erreichbar. Dies kann beispielsweise dann der Fall sein, wenn der Zwang besteht, mangels Alternativen auf ein bestimmtes Produkt setzen zu müssen, diese IT-Technologie aus dem Ausland stammt und keine nachgewiesene Vertrauenswürdigkeit besitzt. In diesem Fall gilt es, aufgrund der weltweit sehr verschiedenen Ansichten über Datenschutz und Gesetze, einen Nachweis zu erbringen. Es könnte aber auch ein europäisches Produkt sein, welches in der Vergangenheit durch Sicherheitslücken und Probleme negativ aufgefallen ist.

Der Wunsch nach „nationaler Souveränität" bei der IT-Sicherheit ist sehr groß und wächst stetig an. Dabei wird das Verlangen nach Aspekten wie Transparenz, Sicherheit, Vertrauenswürdigkeit und der Beseitigung und Vermeidung von Hintertüren laut.

Die Marktführung ausländischer Unternehmen in wichtigen Bereichen der IT mündet in der fehlenden und nicht angemessenen Vertrauenswürdigkeit. Die „nationale Souveränität" bedeutet in diesem Fall, die vollständige Kontrolle über Bereiche zu behalten, die sich durch Vertrauenswürdigkeit innerhalb der IT-Sicherheit erreichen lässt. Diese wiederum wird selbst durch Transpa-

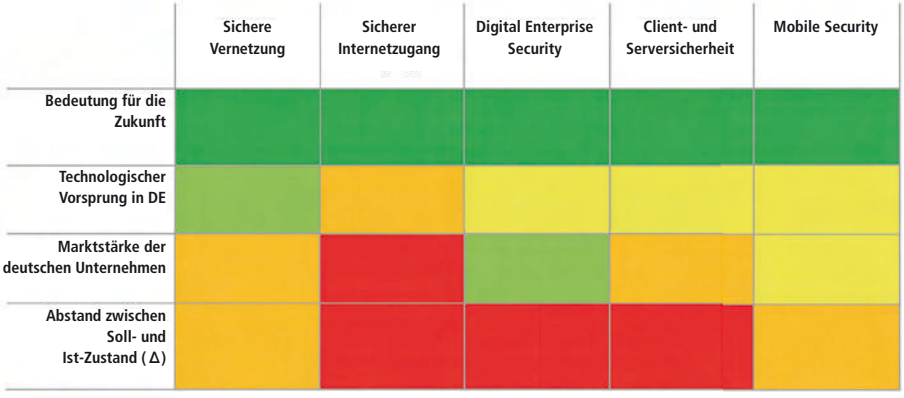

Bild 3: Übersicht aller Ergebnisse der Technologieanalyse

renz, Vertrauen und andere Werkzeuge und Prozesse erzielt. Dies kann beispielsweise durch das Konzept der „Austauschbarkeit" umgesetzt werden.

Wirkungsaspekte

Es gibt unterschiedliche IT-Sicherheitsmaßnahmen und Aspekte, wie eine maximale Wirkung zu erzielen ist. Daraus leitet sich der Begriff „Wirkungsaspekt" ab. Hierbei gibt es die Möglichkeit der Unterscheidung in drei verschiedene Bereiche, die sich jedes Mal jeweils gegen eine konkrete Bedrohung richten:

- „prinzipielle Wirkung", zum Beispiel Verschlüsselung gegen das Lesen von Klartext
- „konkrete Wirkung", zum Beispiel richtige Implementierung von Verschlüsselungstechnologien; Zufallszahlen, Algorithmus, Einbindung …
- „gewollte Wirkung", zum Beispiel Hintertüren oder zielgerichtete Schwächen eingebaut

Bei all diesen Fragen und Aspekten spielen, neben den Fragen der IT-Sicherheit im Allgemeinen, insbesondere auch der Datenschutz und die informationelle Selbstbestimmung als ein Grundrecht in Deutschland eine wesentliche Rolle.

Umsetzung

Für eine erfolgreiche nachhaltige Umsetzung eines angemessenen IT-Sicherheitsniveaus mit der notwendigen Vertrauenswürdigkeit müssen die Ziele exakt in einer gemeinsamen IT-Sicherheitsstrategie definiert werden. Ein gemeinsames Ziel sollte es sein, ein angemessenes IT-Sicherheitsrisiko für die Gesellschaft zu erreichen. Die gemeinsamen Ziele müssen mit allen Stakeholdern wie Anwendern (Unternehmen, Bürger …), der IT-Sicherheitsindustrie, der IT-Sicherheitsforschung sowie Politik und Verwaltung umgesetzt werden.

Anwender können der IT-Sicherheitsindustrie klar beschreiben, welche IT-Technologien sie zur Verfügung stellen soll, damit sie zielführend und benutzbar sind. Natürlich müssen die Anwender das Geforderte auch einsetzen. Ein zentraler Punkt ist die problemlose Interoperabilität der Produkte untereinander. Dies bedeutet, dass unterschiedliche IT-Sicherheitstechnologien und -produkte aus Deutschland stimmig zusammenarbeiten müssen.

Bei der Umsetzung muss die IT-Sicherheitsindustrie eng mit den ausländischen IT-Marktführen zusammenarbeiten, damit das Ergebnis optimal für den Anwender nutzbar gemacht werden kann. Werden genügend qualitativ hochwertige IT-Sicherheitstechnologien aus Deutschland auch auf dem internationalen Markt angeboten, können durch einen größeren Absatzmarkt die Preise dementsprechend niedriger ausfallen. Die Aufgabe der Politik ist es, hier entsprechende Rahmenbedingungen zu schaffen, um das gemeinsame Ziel zu begünstigen.

Die Forschung muss in Zukunft stärker in die Weiterentwicklung bestehender und das Finden neuer und notwendiger IT-Sicherheitstechnologien eingebunden werden. Nur durch Innovationen lässt sich in Zukunft ein angemessenes IT-Sicherheitsrisiko erreichen und halten. Hierbei muss der Technologietransfer zwischen Forschung und Industrie gefördert und durchgeführt werden.

Fazit

Jede IT-Sicherheitslösung muss modernen Angriffs- und Manipulationsmethoden standhalten. Die Frage nach ihrer Wirksamkeit und der Schwachstellenanalyse solcher IT-Systeme sollte stets berücksichtigen, dass jeder Angreifer prinzipiell immer über genügend Zeit verfügt, sich eine Schwachstelle zu suchen. Dies liegt daran, dass der Angreifer die investierte Zeit und den Zeitpunkt des Angriffs selbst bestimmen kann. Der IT-Sicherheitsverantwortliche muss auf der Seite des Angriffsziels die Entscheidung treffen, an welchen Stellen welcher Schutz angebracht ist.

Wurde nach aller Planung und Umsetzung ein angemessenes IT-Sicherheitsniveau erreicht, ist es von Bedeutung, dieses auch dauerhaft zu halten. Manche Bedrohungen flachen möglicherweise irgendwann wieder ab, andere neue Gefährdungsszenarien entstehen und müssen dann berücksichtigt werden.

Die Herausforderung, der Deutschland im Bereich der angemessenen IT-Sicherheit und Vertrauenswürdigkeit in einer sich immer schneller verändernden Bedrohungslage begegnen muss, ist groß, aber lösbar. Im Hinblick auf die „Industrie 4.0" müssen gemeinsam konkrete Schritte unternommen werden, um die in vielen Bereichen kritische IT-Sicherheitslage im Land zu verbessern und auf ein angemessenes Maß anzuheben. Der Gedanke, dass die Energieversorgung durch einen Cyberwar-Angriff für längere Zeit unterbrochen werden könnte oder die wichtigsten Unternehmen in Deutschland Opfer von Industriespionage werden und ihre Existenzbasis verlieren, ist düster.

Ausblick

Der Preis für einmal verlorenes Vertrauen ist sehr hoch. Eine Möglichkeit, verlorenes Vertrauen in Teilen zurückzugewinnen, wäre die Austauschbarkeit zu ermöglichen und Transparenz zu fördern. Die Wirkungsklassen können helfen, diese Idee pragmatisch umsetzen. Es ist wichtig, dass für eine erfolgreiche Umsetzung alle unterschiedlichen Verantwortlichen gemeinsam daran arbeiten, dieses Ziel zu erreichen. ■

Die vollständige Version der Arbeit, die diesem Artikel zugrunde liegt, finden Sie unter: https://www.teletrust.de/it-sicherheitsstrategie/
oder
https://www.internet-sicherheit.de/it-sicherheitsstrategie/.

SEBASTIAN BARCHNICKI ist wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen und im Forschungsbereich der IT-Sicherheitsstrategie tätig.

NORBERT POHLMANN ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT.