TeleTrusT – Bundesverband IT-Sicherheit e.V.

Der IT-Sicherheitsverband.

TeleTrusT
Pioneers in IT security.

IT-Sicherheitsstrategie für Deutschland

Wirkungsklassen von IT-Sicherheitsmaßnahmen
für unterschiedliche Schutzbedarfe

Diese Publikation ist im Rahmen einer Abschlussarbeit an der Westfälischen Hochschule Gelsenkirchen am Institut für Internet-Sicherheit – if(is) entstanden.

Autor:

Sebastian Barchnicki

barchnicki@internet-sicherheit.de

Stand dieses Dokuments: 09.03.2015

Impressum

Herausgeber:

TeleTrusT – Bundesverband IT-Sicherheit e.V.
Chausseestraße 17
10115 Berlin
Tel.: +49 30 400 54 306
Fax: +49 30 400 54 311
E-Mail: info@ teletrust.de
https://www.TeleTrusT.de

Zusammenfassung

1. Veränderungen

Im Bereich der IT-Sicherheit gibt es eine steigende Anzahl an Herausforderungen. Neben den klassischen Bedrohungen gibt es insbesondere das Problem der zerstörten Vertrauenswürdigkeit. Es ist durch die bekannt gewordenen Unterlagen von Edward Snowden klar geworden, dass wichtige IT-Technologien aus den USA 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 vielen möglichen 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 ist einer der Hauptmotive für die hier vorgestellten Aspekte einer möglichen IT-Sicherheitsstrategie. Es muss eine Veränderung der heutigen IT-Sicherheitssituation herbeigeführt werden, damit die Vertrauenswürdigkeit und damit eine angemessene Risikolage wiederhergestellt werden kann.

2. Bewertung der IT-Technologien

Für die Einschätzung der aktuellen IT-Sicherheitslage und 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 aus deutscher Sicht illustriert 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 Technologien ohne großen technologischen Mehrwert substituieren. Diese Herausforderung lässt sich deutlich eleganter und zur Zufriedenheit aller Beteiligten lösen.

Ein wichtiges Handlungsfeld ist z. B. 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 werden. 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.

Mit Hilfe hochwertiger deutscher IT-Sicherheitstechnologien, passend und angemessen in Marktführenden IT-Technologien integriert, kann unser Risiko deutlich reduziert werden. Aus diesem Grund wird die Möglichkeit der "Austauschbarkeit" von IT-Sicherheitstechnologien gefordert.

3. Modelle

Eine besondere Herausforderung ist es also, mit Hilfe von eigenen IT-Sicherheitstechnologien, die Vertrauenswürdigkeit deutlich anzuheben und damit das Risiko eines Schadens zu minimieren.

Hierzu gibt es verschiedene Möglichkeiten und Wege. Da praktisch nicht ersetzbare IT-Technologien von ausländischen Marktführern existieren, wird die Alternative der "IT-Security-Replaceability" gefordert. Hierbei ist eine konstruktive Zusammenarbeit dieser Firmen notwendig. Die US-amerikanischen Marktführer sollen nicht generell substituiert werden, sondern dabei mitwirken, vertrauenswürdige IT-Sicherheitskomponenten aus Deutschland zu integrieren. Das hier gemachte 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 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.

4. Umsetzung

Für eine erfolgreiche nachhaltige Umsetzung eines angemessenen Sicherheitsniveaus mit einer notwendigen Vertrauenswürdigkeit müssen die Ziele exakt in einer gemeinsamen IT-Sicherheitsstrategie definiert werden. Ein gemeinsames Ziel sollte es sein, ein angemessenes IT-Sicherheitsrisiko für unsere Gesellschaft zu erreichen. Die gemeinsamen Ziele müssen mit allen Stakeholdern, wie Anwendern (große Firmen, KMUs, 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 ist. 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 dem 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.

» Wir werden nicht durch die Erinnerung an unsere Vergangenheit weise, sondern durch die Verantwortung für unsere Zukunft. «

George Bernard Shaw (1856-1950), ir. Schriftsteller

Inhaltsverzeichnis

1 Einleitung ... 1

1.1 Motivation ... 3

1.2 Ziele dieser Arbeit ... 4

1.3 Die Grenzen dieser Arbeit ... 5

1.4 Umsetzung ... 5

2 Vertrauenswürdigkeit, Standards und deren Grenzen ... 7

2.1 Etablierte Standards und Kataloge in der IT-Sicherheit ... 7

2.2 Definition: Vertrauenswürdigkeit ... 12

2.3 Wirkungsaspekte ohne Vertrauenswürdigkeit ... 15

3 IT-Sicherheitssituation und der Weg zu einem höheren IT-Sicherheitsniveau ... 17

3.1 Was ist IT-Sicherheit? ... 17

3.2 IT-Sicherheitsherausforderungen und Bedrohungen ... 17

3.3 Schwachstellen in Software ... 18

3.3.1 Schadsoftware-Erkennung und -Vermeidung ... 18

3.3.2 Komplexe zielgerichtete Angriffe (APT) ... 19

3.3.3 Identitätsdiebstahl ... 19

3.3.4 Messbarkeit von Gefahren- und Bedrohungspotenzial ... 19

3.3.5 Ineffektive IT-Sicherheitslösungen ... 19

3.4 Mindeststärke und Penetration von IT-Sicherheit ... 21

4 Die größten Stärken und Herausforderungen der IT-Sicherheit in Deutschland ... 23

4.1 "IT-Security made in Germany" ... 23

4.2 Verantwortung übernehmen ... 24

5 Analyse der wichtigsten und verfügbaren IT-Sicherheitstechnologien ... 26

5.1 Technologieanalyse der Anbieter im In- und Ausland ... 26

5.1.1 Bereich: Sichere Vernetzung ... 28

5.1.2 Bereich: Sicherer Internetzugang ... 30

5.1.3 Bereich: Digital Enterprise Security ... 31

5.1.4 Bereich: Client- und Serversicherheit ... 34

5.1.5 Bereich: Mobile Security ... 39

5.1.6 Gesamtauswertung nach Bewertungskriterien ... 44

5.1.7 Interpretation der Analyse ... 48

5.2 Besondere Kompetenzen in Deutschland ... 49

5.3 Handlungsempfehlungen ... 49

6 IT-Sicherheitsstrategie für Deutschland ... 51

7 Wirkungsklassen von IT-Sicherheitsmaßnahmen für unterschiedliche Schutzbedarfe ... 56

7.1 Unterschiedliche Wirkungsaspekte ... 56

7.2 Einteilung in Wirkungsklassen ... 60
7.2.1 Abgedeckte Schutzbedarfe ... 60
7.3 Voraussetzung für eine Einstufung in die Kernwirkungsklassen ... 61
7.3.1 Wirkungsklasse 0 ... 61
7.3.2 Wirkungsklasse 1 ... 61
7.3.3 Wirkungsklasse 2 ... 62
7.3.4 Wirkungsklasse 3 ... 62
7.3.5 Wirkungsklasse 4 ... 63
7.4 Definition: Wirkungsklassenmodell ... 65
7.5 Definition: Die Wirkungsklasse im Detail ... 68
7.5.1 Wirkungsklasse 0: Basis-IT-Sicherheit ... 68
7.5.2 Wirkungsklasse 1: Erweiterte IT-Sicherheit ... 68
7.5.3 Wirkungsklasse 2: Höherwertige IT-Sicherheit ... 69
7.5.4 Wirkungsklasse 3: Hochwertige IT-Sicherheit ... 70
7.5.5 Wirkungsklasse 4: Geheimschutz IT-Sicherheit ... 70
7.5.6 Verantwortung erkennen ... 70
7.5.7 Klasseneinstufung: Was sind die realen Kosten? ... 70
7.6 Rechtliche Aspekte ... 72
7.7 Kommendes IT Sicherheitsgesetz ... 73
7.8 Indikationen und mögliche Probleme ... 74
7.9 Kontinuierliches und angemessenes IT-Sicherheitsniveau ... 75
7.10 IT-Sicherheitsbedrohungen und -maßnahmen ... 77
7.11 Umgang mit Restrisiken ... 77
8 Die nächsten Aufgaben und Schritte ... 79
8.1 Die wichtigsten Stakeholder ... 80
8.1.1 Anwender ... 80
8.1.2 IT-Sicherheitsanbieter ... 80
8.1.3 Politik, Gesetzgeber ... 81
8.1.4 Wissenschaft und Forschung ... 81
8.2 Vorgehen: Der nächste Schritt zum Ziel ... 81
8.3 Umsetzungsvorschlag ... 83
9 Fazit und Ausblick ... 84
10 Literaturverzeichnis ... 87
11 Abbildungsverzeichnis ... 90
12 Tabellenverzeichnis ... 91

1 Einleitung

In unserem fast vollständig vernetzten Alltag ist es beinahe überall und zu jedem Zeitpunkt möglich, sich im Internet zu bewegen und persönliche Informationen zu teilen oder zu konsumieren. Vor einigen Jahren undenkbar, ist es heute nicht mehr notwendig aufgrund des Wechsels einer Örtlichkeit (z. B. von Zuhause zum Einkaufen) eine laufende Konversation unterbrechen zu müssen, egal ob diese als Videotelefonat oder vielleicht via Text geführt wird.

Die mobilen Geräte sind ebenfalls entsprechend leistungsfähig und übertreffen damalige Großrechner in Sachen Speicherkapazität und Rechenleistung bei Weitem. Die Formen und Gerätetypen werden dabei immer zahlreicher: Die Gerätelandschaft beinhaltet heute nicht nur Smartphones, sondern auch Tablets, "Wearables" (Smartwatches oder auch Kleidungsstücke und Schmuck), Haushaltsgeräte oder Komponenten in Fahrzeugen. Es ist bei der Entwicklung dieser Vielfalt noch lange kein Ende in Sicht.

Die persönlichen oder beruflich genutzten Geräte sind heute in jedem Fall wichtige Geheimnisträger und beherbergen die persönlichsten Daten ihres Besitzers oder aus wirtschaftlicher Sicht sehr wertvolle Informationen wie geistiges Eigentum, geschäftliche E-Mails, Konstruktionspläne, Absichten für wichtige strategische Entscheidungen eines Unternehmens uvm., die in den falschen Händen viel Schaden anrichten könnten.

So ist die Frage nach dem eigenen Schutzbedarf heute vermutlich anders zu beantworten als es noch vor den Enthüllungen von Edward J. Snowden im Juni 2013 der Fall gewesen ist. Bei vielen Verantwortlichen herrscht oft Unklarheit über den benötigten Schutz. Meist sind auch die Größe der eigenen Verantwortung und die möglichen Konsequenzen unbestimmt.

Es gab nach diesen Veröffentlichungen international und vor allem national viele Proteste sowie Empörung auf verschiedenen Seiten. Entrüstung herrschte auch darüber, dass Geheimdienste und Regierungen die theoretisch zur Verfügung stehenden Möglichkeiten auch praktisch voll und ganz ausschöpfen, ohne jegliche Rücksicht auf Selbstbestimmung und Datenschutz. Die Argumentation dabei ist meistens der "Schutz vor dem Terror" sowie "die Bewahrung des Friedens". Unter diesem Deckmantel wird in Wirklichkeit im großen Stil Industrie- und Wirtschaftsspionage betrieben.

Tatsache ist, dass diesbezüglich bei jeder Sicht auf die großen IT-Sicherheitsfragen immer vom Schlimmsten ausgegangen werden muss. Die Motivation ist häufig die Profilbildung möglichst aller Menschen für eine umfangreiche Auswertung oder wirtschaftliche Interessen.

Tatsächlich herrscht eine große Ohnmacht in Politik und Wirtschaft. Zwischenzeitlich wurde sogar der angeprangerte Spionageskandal durch die Politik sehr schnell für "beendet" erklärt. Dieser war natürlich längst nicht so beendet, wie von der Politik zunächst behauptet worden ist.

Diese Ohnmacht zeigt, dass wir aus dem Überwachungsskandal dazulernen müssen, um das Wissen und die Privatsphäre aller Internetteilnehmer in Deutschland zu schützen. Insbesondere ist es wichtig, neben wirtschaftlichem Know-how, auch die kritische Infrastruktur (wie z. B. Energie- und Wasserversorgung) auf keinen Fall zu vernachlässigen. Gerade dieser Punkt stellt eine sehr verwundbare Stelle unserer heutigen Gesellschaft dar und ist schützenswerter denn je. Ein großflächiger Ausfall der Stromversorgung oder ein ernster Störfall eines Atommeilers mitten im Bundesgebiet würde verheerende Folgen haben.

Die hiesigen Datenschutzbestimmungen sind weltweit einmalig und bilden ein Grundrecht für jeden Bundesbürger. Der Datenverkehr findet jedoch global statt und geht weit über die nationalen Landesgrenzen hinweg. Dies bedeutet gleichzeitig, dass in allen anderen Transitländern die dortigen Bestimmungen und Gesetze ganz anders sein können als die deutschen. Dies wird oft als Legitimation für das Mitlesen von Daten genutzt.

"Seit 2013 ist allgemein bekannt, dass die Geheimdienste praktisch den gesamten Internet-Datenverkehr ausspionieren – vornehmlich in Gestalt der ‚Five Eyes': Die Hauptakteure dieser

Allianz sind die National Security Agency (NSA) der USA und das britische Government Communications Headquarters (GCHQ), in zweiter Linie gesellen sich Australiens Defence Signals Directorate (DSD), das Communications Security Establishment Canada (CSEC) und Neuseelands Government Communications Security Bureau (GCSB) hinzu." [1, S.82] Die nationalen Nachrichtendienste sind hier ebenfalls involviert und richten ihre Ressourcen gegen die eigenen Bürger.

Als Resultat existiert mit jedem dieser Länder im Bereich der IT-Sicherheit ein riesiges Vertrauensproblem. Genau hier kann das in dieser Arbeit vorgestellte Konzept und insbesondere das Wirkungsklassenmodell nachhaltig helfen.

Um möglichst allen hier genannten Problemen entgegenzuwirken, ist in sehr enger Zusammenarbeit mit Experte aus der IT-Sicherheitsindustrie dieses Konzept als Vorschlag erarbeitet worden.

1.1 Motivation

In der heutigen Zeit sind Computersysteme ein integraler Bestandteil unserer Gesellschaft und erfüllen viele persönliche, private und zum Teil auch sehr kritische Aufgaben. Sie finden aus diesem Grund nicht nur einen sehr hohen Grad der Verbreitung, sondern es gibt kaum noch einen Bereich in unserem Alltag, egal ob privat, in der Wirtschaft oder dem öffentlichen Wesen, der ohne diese Technologien auskommen kann.

Es existiert demzufolge eine massive Abhängigkeit von IT-Systemen, die im Grunde genommen für den Nutzer fast immer eine Art "Black Box" darstellen. Es ist nicht feststellbar, ob ein 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 Systems, welches nach außen hin scheinbar sicher zu sein scheint.

Wird noch einen Schritt eher angesetzt, gibt es bereits bei der Einordnung große Probleme: Viele Verantwortliche können den Schutzbedarf erst gar nicht einschätzen und sind mit der Frage über die gewünschte und die tatsächlich erzielte Wirkung ebenfalls überfordert.

Der Zwiespalt, der heute existiert, stellt sich wie folgt dar: Einerseits gibt es für viele Bereiche nur sehr wenig Auswahl an möglichen IT Systemen, andererseits herrscht in vielen Bereichen der IT keine angemessene Vertrauenswürdigkeit. Die jährlich steigende Anzahl von IT-Sicherheitsvorfällen zeigt deutlich, dass das allgemeine Sicherheitsniveau zurzeit unzureichend ist. "Zwar wird die steigende Zahl gezielter Angriffe aus dem Netz von den meisten Unternehmen als Bedrohung erkannt und mit einer deutlichen Aufstockung der Budgets für Informationssicherheit beantwortet (im Vergleich zum Vorjahr durchschnittlich plus 51 Prozent). Gleichzeitig nahm aber auch die Zahl der Sicherheitsvorfälle um 25 Prozent zu. Sahen sich die Befragten in 2011/12 noch durchschnittlich 2.989 Attacken auf ihre IT-Infrastruktur ausgesetzt, waren es 2012/13 bereits 3.741 Angriffe." [2]

Auch ist die Wirksamkeit von IT-Sicherheitslösungen, die im Verlauf dieser Arbeit noch genauer erläutert wird, an vielen Stellen heute nicht ausreichend. Sie ist jedoch notwendig und darf nicht vernachlässigt werden.

Ein Beispiel hierzu sind gängige Verschlüsselungsverfahren: "US-Geheimdienste und die Standardisierungsbehörde NIST[1] haben dazu beigetragen, eigentlich sichere Kryptoverfahren zu unterminieren und die Anwender in trügerischer Sicherheit zu wiegen." [1, S.83]

Dies ist leider keine theoretische Annahme mehr, sondern Fakt und wurde zwischenzeitlich öffentlich zugegeben: "Im November 2013 musste ein NIST-Vertreter einräumen, dass die Behörde einen von der NSA entwickelten, absichtlich schwachen Pseudo-Zufallsgenerator standardisiert und sogar explizit zur Verwendung empfohlen hat. Die NSA dürfte somit Verschlüsselungen, die darauf basieren, deutlich leichter knacken können als öffentlich bekannt." [1, S.84]

[1] „National Institute of Standards and Technology“, Amerikanische Bundesbehörde für Standarisierungsprozesse mit etwa 2900 Mitarbeitern. - http://www.nist.gov/

1.2 Ziele dieser Arbeit

Überall dort, wo IT-Technologien eingesetzt werden, muss notwendigerweise die Frage gestellt werden, wie vertrauenswürdig diese eigentlich sind. Ist eine Komponente aus Fernost oder den Vereinigten Staaten mehr oder weniger vertrauenswürdig als ein Produkt aus Deutschland? Wie steht es um die Transparenz, die Verlässlichkeit und womöglich auch die Frage nach Haftung im Schadensfall?

In manchen Bereichen gibt es Marktführer oder dominierende Anbieter, welche sich im Ausland befinden und einige Kriterien wie Vertrauenswürdigkeit oder Transparenz ganz klar nicht erfüllen. Sie finden jedoch trotzdem breite Anwendung mangels Alternativen. Für diesen Fall werden verschiedene Lösungsansätze präsentiert, mit dem Ziel die Kritikpunkte entweder durch Nachweisbarkeit aus dem Weg zu räumen oder die kritischen Produktmodule so zu implementieren, dass sie durch nachweisbar vertrauenswürdige Technologien ausgetauscht werden können. Das Ziel sollte dabei klar definiert werden: Entweder die Hersteller sind bereit, einen Nachweis über die Vertrauenswürdigkeit ihrer Produkte zu liefern, oder sie müssen durch Wirtschaft und Politik motiviert werden, Schnittstellen für die Austauschbarkeit sicherheitskritischer Komponenten zu schaffen. Ein wichtiges Argument ist hierbei in Deutschland ebenfalls das Siegel "IT-Security made in Germany", welches bei schwierigen Entscheidungen behilflich sein kann.

Ein weiterer Kernaspekt dieser Arbeit soll es möglich machen, die Frage nach dem eigenen Schutzbedarf leichter zu beantworten. Die daraus zu schließenden Maßnahmen sollten sich dann in Form von "Wirkungsklassen" leicht ableiten lassen. Diese pragmatischen Wirkungsklassen berücksichtigen neben verschiedenen Bereichen und Nutzergruppen spezielle IT-Sicherheitsmaßnahmen für unterschiedliche Schutzbedarfe und werden im Kapitel "Wirkungsklassen von IT-Sicherheitsmaßnahmen für unterschiedliche Schutzbedarfe" auf Seite 56 genauer erläutert.

Im Prinzip soll es also möglich werden, die eigene Sicherheitslage für den Anwender/Entscheidungsträger leicht beurteilbar zu machen, damit mögliche Konsequenzen eingeschätzt werden können. Daraus sollen sich alle notwendigen IT-Sicherheitsmaßnahmen ableiten lassen, also im Prinzip eine Aussage darüber getroffen werden, wie viel Schutz ein bestimmtes IT-System benötigt.

Zudem soll auch eine Antwort auf die Frage der Umsetzung gegeben werden: Welche Personen und Gruppierungen sind hierbei bedeutsam? Wer sind die Stakeholder und wie lässt sich das hier vorgestellte Wirkungsklassenmodell oder das Prinzip der Austauschbarkeit für die IT-Sicherheitsstrategie wirkungsvoll umsetzen?

All dies wird im Kapitel "Die nächsten Aufgaben und Schritte" diskutiert und ein konkreter Umsetzungsvorschlag gemacht.

1.3 Die Grenzen dieser Arbeit

Wie der Titel dieser Arbeit bereits verdeutlicht, handelt es sich bei diesem Konzept lediglich um einen Teilaspekt einer notwendigen Gesamtlösung für eine effektive IT-Sicherheitsstrategie. Diese Arbeit sollte also keinesfalls als Gesamtlösung für die aktuellen Herausforderungen wahrgenommen werden. Sie soll vielmehr als mögliches zusätzliches Hilfsmittel gesehen werden, im Rahmen einer vollständigen IT-Sicherheitsstrategie für Deutschland.

Eine allgemeine Lösung für verschiedene komplexe sowie individuelle Anforderungen kann und soll hier nicht gegeben werden. Selbstverständlich sind die Facetten von IT-Sicherheitsanforderungen im Alltag sehr vielfältig. So kann beispielsweise ein Netzwerk je nach Bedarf in einem Unternehmen entweder vollkommen abgeschottet oder sehr offen gestaltet sein. Aus diesem Grund ist der Wert eines betrachteten IT-Systems sehr individuell und kann immer nur vom Benutzer und dem Verantwortlichen selbst zuverlässig eingeschätzt werden.

Diese Arbeit kann nicht einen Lösungsansatz für jedes einzelne Szenario liefern und ist als eine Art Grundsteinlegung für ein wirkungsvolles Gesamtkonzept zu sehen. Es ist aber möglich in komplexen Einzelfällen, in denen die IT-Landschaft sehr unterschiedlich zusammengesetzt ist, einen möglichen Weg zur Erarbeitung einer geeigneten Lösung aufzuzeigen.

Im Rahmen der Bewertungen werden keine neuen Standards definiert, sondern bereits verfügbare und etablierte IT-Sicherheitsstandards berücksichtigt und als Fundament für dieses Konzept verwendet.

1.4 Umsetzung

Die Methodik dieser Arbeit beruht auf einer Idee des Bundesverbandes für IT-Sicherheit - TeleTrusT, die sich damit beschäftigt hat, wie ein Konzept auszusehen hat, das als Teil einer Sicherheitsstrategie für Deutschland hilfreich und nützlich ist. Hierbei waren verschiedene Forschungsaspekte wichtig: Zum einen galt es den Fragen nachzugehen, wie die IT-Sicherheitsbranche im nationalen und internationalen Vergleich aufgestellt ist, in welchem Zustand sich die IT-Sicherheit befindet und welche Ziele für die kommende Dekade definiert werden könnten, an denen sich der erreichte Erfolg messen lässt. Zum anderen wurde ein Konzept benötigt, welches die auftretenden Defizite und Fragen angemessen beantworten und lösen kann.

Innerhalb dieser Fragestellung wurde das Wirkungsklassenmodell erarbeitet und definiert. Die Anforderung war es, die Bedürfnisse möglichst aller infrage kommenden Zielgruppen abzudecken. Es galt dabei ihnen ein Werkzeug an die Hand zu geben, mit dessen Hilfe sich der eigene Schutzbedarf effektiv und möglichst leicht ermitteln lässt.

Bei all diesen Aufgaben und Forschungsfragen war die Hilfe von Sicherheitsexperten erforderlich. Dankenswerterweise wurde diese Arbeit seitens der Wirtschaft und Industrie sowie der Behörden unterstützt, die Zwischenergebnisse kritisch hinterfragt und immer wieder optimiert. Es bestand die Gelegenheit, mit angesehenen Experten zu arbeiten, die viel nützliches Wissen zur Aufgabenstellung beitragen konnten und ihre kostbare Zeit für die Diskussion bestehender Problemlösungen und möglicher weiterer Schritte auf dem Weg zum Ziel zur Verfügung gestellt haben. Dies wurde in zahlreichen persönlichen Treffen und Telefonaten realisiert.

Involviert waren dabei insbesondere Ammar Alkassar (Sirrix AG), Michael Böffel und Christian Koob (secunet Security Networks AG), Dr. Guido von der Heidt (Siemens AG), Tobias Mikolasch (Bundesamt für Sicherheit in der Informationstechnik), Prof. Dr. Michael Waidner (Fraunhofer Institut SIT) und Prof. Dr. Norbert Pohlmann (Institut für Internet-Sicherheit).

Den zweiten Teil der Arbeit stellt die Technologieanalyse dar, welche gemeinsam mit den Experten der oben genannten Unternehmen und Institutionen aus der IT-Sicherheitsindustrie erarbeitet wurde.

Der Aufbau der Analyse ist hierbei nach Technologien und den dazugehörigen Produktbereichen gegliedert. Für jedes technologische Oberthema werden dabei jeweils relevante Unterpunkte als Produktbereiche betrachtet. Dabei wird eine Bewertung des jeweiligen Technologiebereiches hinsichtlich verschiedener Kriterien, wie beispielsweise seiner Bedeutung für die

Zukunft und der Marktstärke der deutschen Unternehmen, durchgeführt. Hierbei war es bedeutend darstellen zu können, wie die deutschen Unternehmen gegenüber den ausländischen positioniert sind und wo eine Nutzungslücke besteht, also der Abstand zwischen dem "Soll-Zustand" und dem "Ist-Zustand". Die Bewertungskategorie enthält hierbei farbliche Indikatoren (Abbildung 1), welche auf den ersten Blick erkennen lassen, wo es gut um die Position bestellt ist (grün) und an welcher Stelle noch reger Handlungsbedarf besteht (rot).

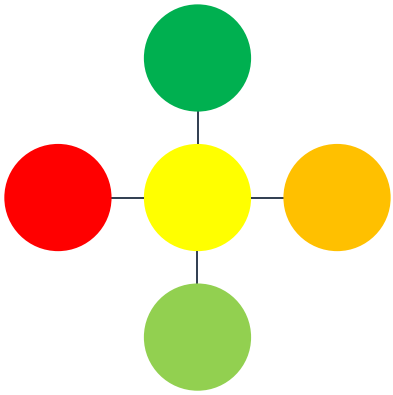


Abbildung 1 - Mögliche farbliche Indikationen

Dazwischen gibt es die Möglichkeit einer gelben und orangefarbenen Markierung für eine neutrale bis grenzwertig mittelmäßig geprägte Einstufung.

2 Vertrauenswürdigkeit, Standards und deren Grenzen

Informationstechnologie umfasst Aspekte der Vertrauenswürdigkeit. Hierfür wurden im Laufe der letzten Jahrzehnte, national und international, Standards, Richtlinien und Kataloge definiert. Der Erste entstand 1983 und ist damit heute bereits über 30 Jahre alt. Die wichtigsten von ihnen werden nachfolgend in chronologischer Form vorgestellt.

Des Weiteren wird auch der so elementare Begriff der Vertrauenswürdigkeit, der in der IT-Sicherheit eine sehr wichtige Rolle spielt, aufgegriffen und erläutert.

2.1 Etablierte Standards und Kataloge in der IT-Sicherheit

Über die vergangenen Jahrzehnte gab es immer wieder Entwicklungen, Standards und Definitionen von Kriterien und Modellen, welche bei der Bewertung der Sicherheit von Informationstechnologien (IT) helfen sollen. Die ersten Standards kommen aufgrund ihres Alters und dem fehlenden Bezug zu heutigen Herausforderungen nicht in Frage. Die neueren Standards sind zwar durchaus zeitgemäß, allerdings auch sehr umfangreich, komplex und deren Anwendung kann recht teuer ausfallen. Dies führt oft dazu, dass sie an eigentlich notwendiger Stelle keine Anwendung finden, weil ein Verantwortlicher den Aufwand und die Kosten scheut, sich mit diesen Kriterien und Standards auseinanderzusetzen.

Nachfolgend wird eine Übersicht der wichtigsten Bewertungskriterien ergänzend zum Wirkungsklassenmodell (siehe "Definition: Wirkungsklassenmodell", S. 65) vorgestellt.

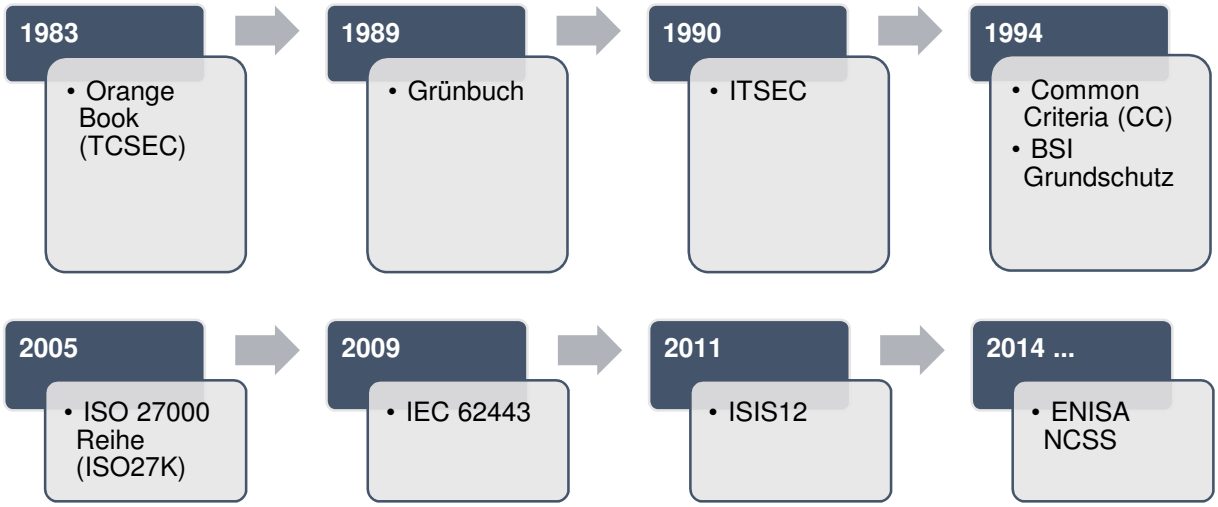


Abbildung 2 - Grafische Darstellung der zeitlichen Entwicklung von IT-Sicherheitsstandards

Die in Abbildung 2 berücksichtigten Zeitpunkte gehen von den Initialversionen der jeweiligen Standards aus bzw. deren Erstveröffentlichung. Sie bilden im Prinzip das Rückgrat der uns heute bekannten IT-Sicherheit.

Vollständigkeit und weitere Normen

Ein vollständiger Überblick würde den hier verfügbaren Rahmen sprengen und nur für kurze Zeit aktuell bleiben, da sich die diskutierten Normen in stetiger Weiterentwicklung befinden.

Die hier dargestellte chronologische Übersicht soll einen kleinen Überblick darüber geben, welche Standards, Normen und Richtlinien existieren. Es soll skizziert werden, wie komplex und umfangreich diese sind.

Zudem gibt es je nach Branche und Anforderung auch noch spezielle Regelwerke, die manchmal auf bereits etablierten Standards basieren, manchmal auch völlig neue Konzepte bilden.

1983

Den Anfang machte im Jahre 1983 das **Orange Book**[2] **(TCSEC-Kriterien)** als erstes und ältestes Modell seiner Art. Es wurde durch das US-amerikanische Department of Defense (DoD, Verteidigungsministerium der Vereinigten Staaten) entwickelt und stark auf Betriebssysteme ausgerichtet. Hierbei steht die Abkürzung TCSEC für "Trusted Computer System Evaluation Criteria", welches auch als Orange Book bekannt geworden ist und zum DoD Standard 5200.28-STD erhoben wurde. Dieser Standard fand vor allem in den USA Verwendung.

Die TCSEC-Kriterien sind auch wegen ihrer stark militärisch geprägten Ausrichtung und der dadurch entstandenen Vernachlässigung der Benutzer aus dem zivilen Sektor heute bei weitem nicht ausreichend. Die Anforderungen haben sich in den letzten Jahrzehnten stark verändert, daher sind diese Kriterien stark veraltet und finden heute keinerlei Anwendung mehr. Sie dienten jedoch als Fundament für weitere Standards und Kriterien, die in den nachfolgenden Jahren definiert worden sind.

1989

Zwischen 1989 und 1990 entstand als Kontrast zum amerikanischen Orange Book das **Grünbuch (ITSK)**. Es ist ein Kurzformbegriff für die "deutschen Sicherheitskriterien", welche eine Richtlinie für die Bewertung und Zertifizierung von IT-Systemen und Softwareprodukten darstellen. Dieses wurde von der damaligen "Zentrale für Sicherheit in der Informationstechnik" (ZSI) erarbeitet. Das ZSI ist aufgegangen im "Bundesamt für Sicherheit in der Informationstechnik" (BSI).

Das Grünbuch ist heute etwa 26 Jahren alt und erfüllt aufgrund des Alters und der rapiden technischen Weiterentwicklung nicht mehr alle Anforderungen, die an ein modernes IT-System gestellt werden. Obwohl es heute als veraltet gilt, bildete es die Grundlage für den ITSEC-Standard und das heute ebenfalls weitverbreitete Common Criteria (CC).

1990

Im Jahre 1990 wurde der **ITSEC-Standard** ("Information Technology Security Evaluation Criteria", Kriterien für die Bewertung der Sicherheit von Informationstechnologie) als europäischer Standard vorgestellt. Dieser Standard wurde gemeinsam in Frankreich, Deutschland, Großbritannien und den Niederlanden entwickelt und ist inhaltlich stark an das deutsche Grünbuch angelehnt. Zertifizierungen zum ITSEC können unter anderem durch das BSI oder die T-Systems GmbH durchgeführt werden. Die bereits zuvor erwähnten Standards ITSEC und TCSEC gingen gemeinsam im Common Criteria Standard auf.

1994

Im Jahre 1994 wurde der **Common Criteria for Information Technology Security Evaluation** (kurz: "Common Criteria", oder nur "CC") Standard vorgestellt mit dem Ziel, eine international einheitliche Basis zu schaffen, damit Sicherheitsprodukte nicht in verschiedenen Ländern wiederholt geprüft werden müssen und um existierende Standards zu vereinen. Die Urheber der ersten Version waren Deutschland, Niederlande, das Vereinigte Königreich, die Vereinigten Staaten, Frankreich und Kanada. Bis heute ist die Zahl der teilnehmenden Länder auf

[2] Seinen Namen bekam es aufgrund des orange-farbenen Einbandes.

insgesamt 26 angewachsen. Um eine breitere internationale Unterstützung zu erreichen, wurden die Common Criteria in ihrer damaligen Version 2.1 im Jahre 1999 in den ISO/IEC 15408 Standard überführt. Nach aktuellem Stand befindet sich der Standard in der Version 3.1 (Revision 4), welcher im Herbst 2012 veröffentlicht worden ist.

Der grundsätzliche Aufbau ist relativ überschaubar, die Umsetzung jedoch etwas anspruchsvoller. Die Common Criteria sind in drei Teile gegliedert und beginnen mit der Einführung und dem allgemeinen Modell, werden fortgesetzt mit den funktionalen Anforderungen und thematisieren im letzten Teil Anforderungen an die Vertrauenswürdigkeit.

Eine Beurteilung nach CC kann aufwendig und zeitintensiv sein.

1994

Der im Jahre 1994 entstandene **IT-Grundschutz** des Bundesamts für Sicherheit[3] in der Informationstechnik (BSI), auch bekannt als "IT-Grundschutzhandbuch" (GSHB), das seit 2005 unter dem Namen "IT-Grundschutz-Kataloge" bekannt ist, beinhaltet umfangreiche Informationen zu diversen Themen und Bereichen. Er wird seit Februar 2004 auf den Webseiten des BSI[4] kostenlos über das Internet zur Verfügung gestellt. Zuvor war es lediglich als Loseblattsammlung über den Bundesanzeiger Verlag erhältlich.

Die "IT-Grundschutz-Kataloge" des BSI beinhalten neben einer "Einführung in Grundschutzmethodik" und dessen Modellierung, verschiedene Bausteine wie "Übergreifende Aspekte", "Infrastruktur", "IT-Systeme", "Netze" und "Anwendungen" (B1 bis B5).

Als Beispiele sind hier auszugsweise das Notfallmanagement, Datenschutz, IT-Verkabelung, Schutzschränke, Server, Virtualisierung, VPNs und Webserver zu nennen, die berücksichtigt werden.

Zusätzlich gibt es spezielle "Gefährdungskataloge" für die Bereiche "Elementare Gefährdungen", "Höhere Gewalt", "Organisatorische Mängel" und einige weitere mehr (G0 bis G5). Hier werden Spezialfälle behandelt, die nur schwer vorhersehbar sind, aber trotzdem auftreten können und berücksichtigt werden müssen.

Dies wären im Detail beispielsweise Gefahren wie Feuer, Wasser, Diebstahl, Abhören, unerlaubte Ausübung von Rechten ("Zutritts-, Zugangs- und Zugriffsberechtigungen") aber auch mangelnde Kapazität von Archivdatenträgern und viele weitere mehr, gegliedert in die jeweiligen Kategorien.

Danach folgen inhaltlich die Maßnahmenkataloge für die Bereiche "Infrastruktur", "Organisation", "Personal" und weitere Kategorien (M1 bis M6). Hier werden unter anderem Maßnahmen thematisiert wie Einbruch- und Perimeterschutz, Einsatz von Einmalpasswörtern und sichere Nutzung von Browsern.

Zuletzt werden dem interessierten Verantwortlichen "Hilfsmittel" an die Hand gegeben. Darunter befinden sich Checklisten, Formulare, Dokumentationen, Studien und zahlreiche weitere Werkzeuge.

Als weiterer Baustein werden die IT-Grundschutz-Standards ("BSI-Standards") zur Verfügung gestellt, die vollkommen kompatibel zu der ISO 27000-Familie sind.

Der BSI-Standard gliedert sich im Kern in vier Bereiche. Diese sind der "BSI-Standard 100-1", welcher Standards hinsichtlich der "Managementsysteme für Informationssicherheit (ISMS)" definiert, und der "BSI-Standard 100-2", welcher die "IT-Grundschutz-Vorgehensweise" beschreibt und die Aufgaben und Anforderungen eines geeigneten Managementsystems hierfür.

[3] BSI-Jahresbericht 2003, 3.2 Grundlage der Risikovorsorge: IT-Grundschutz - https://www.bsi.bund.de/DE/Publikationen/Jahresberichte/jahresbericht_2003/32_IT-Grundschutz.html

[4] Webseite des BSI zu „IT-Grundschutz - die Basis für Informationssicherheit“ https://www.bsi.bund.de/IT-Grundschutz

Der "BSI-Standard 100-3" widmet sich der "Risikoanalyse auf Basis von IT-Grundschutz". Der vierte "BSI-Standard 100-4" beschreibt den Aufbau eines geeigneten "Notfallmanagements", "um die Kontinuität des Geschäftsbetriebs sicherzustellen"[5].

Das durch das BSI angebotene Material ist sehr umfangreich und deckt zahlreiche Möglichkeiten ab. Eine sehr große Informationsmenge birgt jedoch auch den Nachteil einer schwierigen Entscheidungsfindung. Umfangreiche Kataloge und Standards erfordern besondere Aufmerksamkeit. Die Planung und Umsetzung kann dementsprechend sehr umfassend sein.

Dieser Abschnitt soll einen Überblick über die bedeutendsten Aspekte der BSI-Standards und Kataloge sein. Eine vollständige Darstellung würde den Rahmen dieser Arbeit sprengen, da der Katalog über 4.400 Seiten stark ist. Interessierte seien hier auf die Webseiten des BSI[6] verwiesen.

2005

Die **ISO 27000**-Reihe ist eine Sammlung von Standards für die IT-Sicherheit und wurde erstmals am 15. Oktober 2005 veröffentlicht. Diese Norm wird von der "Internationalen Organisation für Normung" ("International Organization for Standardization", kurz ISO) herausgegeben.

Die aktuellste "stabile" Version stammt aus dem Jahr 2013. Eine neuere Version befindet sich in Vorbereitung und liegt in einer Entwurfsfassung vom Februar 2014 vor.

Die Normen sind sehr weitläufig und umfangreich und werden stetig weiterentwickelt. Mitte 2013 waren es über 20 Standards und über 30 weitere Normen befanden sich zu diesem Zeitpunkt in der Planung. Es gibt neben dem eigentlichen ISO-Norm-Dokument, welches kostenpflichtig angeboten wird, auch verschiedene andere Quellen[7], aus denen die dazugehörigen Informationen – meist in englischer Sprache – bezogen werden können.

2009

IEC 62443 ist Teil einer internationalen Normenreihe über die "IT-Sicherheit für industrielle Leitsysteme – Netz- und Systemschutz"[8] und entstand im Jahr 2009.

Diese Normen spielen innerhalb von industriellen Kommunikationsnetzwerken eine Rolle und beschreiben die Netzwerk- und Systemsicherheit für industrielle Prozess- und Messsysteme.

2011

Die **Norm ISIS12** ist die Kurzform für "Informations-Sicherheitsmanagement System in 12 Schritten". Dieses Modell wurde vom "Bayerischen IT-Sicherheitscluster e.V." entwickelt und beschreibt ein "einfach einzuführendes Sicherheitsmanagementsystem". Nach den Angaben der Verfasser kann dieses Verfahren "als mögliche Vorstufe zur ISO/IEC 27001- bzw. BSI IT-Grundschutz-Zertifizierung verwendet werden." [9]

Nach einer Umsetzung kann diese durch den "Exklusivpartner DQS" zertifiziert werden und ist dann drei Jahre lang gültig. ISIS12 wird nach den Angaben des Bayerischen IT-Sicherheitscluster e.V. als "ein Dienstleistungsprodukt (…) vermarktet". Weitere interessierte Partner für die Vermarktung können den Verein kontaktieren und sich über die "Beitrittskonditionen und Möglichkeiten" informieren[10].

---

[5] IT-Grundschutz-Standards - https://www.bsi.bund.de/DE/Publikationen/BSI_Standard/it_grundschutzstandards.html

[6] Übersicht der BSI-Themen im Internet - https://www.bsi.bund.de/DE/Themen/themen_node.html

[7] "The ISO 27000 Directory" - http://www.27000.org/

[8] "Normenreihe IEC 62443 Industrial communication networks – Network and system security" - IT-Sicherheit für Netze und Systeme - https://de.wikipedia.org/wiki/IEC_62443

[9] „ISIS12 – Informationssicherheit für den Mittelstand und Organisationen" - http://www.it-sicherheit-bayern.de/itsecurity/120678-669,1,0.html

[10] „ISIS12: Zertifizierungsmöglichkeit & ISIS12-Lizenznehmer" - http://www.it-sicherheit-bayern.de/kompetenz/112268-662-isis12_zertifizierungsmoeglichkeit___aufnahme_neuer_isis12_dienstleister,1,0.html

2014

Im November 2014 hat die ENISA ("European Union Agency for Network and Information Security") ein **Bewertungsrahmenwerk zur nationalen Cyber-Sicherheitsstrategie (NCSS)** veröffentlicht.

Die Zielgruppe für dieses Bewertungsrahmenwerk ist sehr speziell. Es sind genauer gesagt Regelwerkexperten und Regierungsbeamte, die eine eigene NCSS "entwerfen, implementieren und evaluieren müssen".[11]

Technische Richtlinien und Themen des BSI

Wird ein bestimmtes IT-System entwickelt und dabei ein Anspruch auf Sicherheit erhoben, gibt es für den Aufbau und die Absicherung dieser IT-Systeme vom BSI zur Verfügung gestellte technische Richtlinien. Sie sind als eine Ergänzung zu den technischen Prüfvorschriften des BSI zu sehen "(…) und liefern Kriterien und Methoden für Konformitätsprüfungen sowohl der Interoperabilität von IT-Sicherheitskomponenten als auch der umgesetzten IT-Sicherheitsanforderungen"[14]. Die technischen Richtlinien haben zwar Empfehlungscharakter, allerdings entsteht ihre eigentliche Verbindlichkeit erst durch "(…) individuelle Vorgabe des Bedarfsträgers" [14]. Das bedeutet, es ist im Einzelfall stark davon abhängig, für welchen Technologiebereich das IT-System entwickelt wird und was dieses später leisten soll. Ist hier beispielsweise eine Ankopplung oder der Einsatz im Bereich der kritischen Infrastrukturen (z. B. Energiesystem) vorgesehen, dann stellt sich nicht die Frage nach dem Richtliniencharakter, sondern die Richtlinie muss Anwendung finden und sich dann auch einer Prüfung unterziehen, in der die Umsetzung durch eine Zertifizierung nachzuweisen ist.

Konformitätsnachweise einer technischen Richtlinie (TR) des BSI erfolgen durch beim BSI anerkannte Prüfstellen. Besteht die Notwendigkeit oder das Interesse einer Anerkennung, berät das BSI innerhalb eines kostenfreien Beratungsgesprächs.

Die technische Richtlinie "BSI TR-03109 - Technische Vorgaben für intelligente Messsysteme und deren sicherer Betrieb" ist beispielsweise eine sehr wichtige Richtlinie, da sie die Grundlage für die sichere Entwicklung und den Betrieb von "Smart Meter Gateways"[12] ebnen soll.

Zusätzlich zu diesem Aufwand muss auch das "Schutzprofil für ein Smart Meter Gateway (BSI-CC-PP-0073)" nach Common Criteria beachtet werden, welches auf 93 Seiten im Detail beschreibt, wie ein "Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen" aussieht. Darüber hinaus muss hier auch das "Schutzprofil für das Sicherheitsmodul eines Smart Meter Gateways (BSI-CC-PP-0077)" berücksichtigt werden, das sich nochmals auf 87 Seiten mit einem "Schutzprofil für das Sicherheitsmodul der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen" beschäftigt.

In diesem Fall sind die Dokumente als verbindlich anzusehen, denn der Hinweis auf der Webseite des BSI sagt unmissverständlich: "Diese Verordnung regelt technische Mindestanforderungen an den Einsatz von Messsystemen im Sinne von § 21d Absatz 1 des Energiewirtschaftsgesetzes."[13]

Vom Umfang her sind das insgesamt einige hundert Seiten Vorgaben und Richtlinien, die hier im Detail von den Verantwortlichen durchgearbeitet, verstanden und umgesetzt werden müssen, um einer Überprüfung für eine Zertifizierung bei der Abnahme standhalten zu können.

---

[11] „Bewertung nationaler Cyber-Sicherheitsstrategien“ - http://www.datensicherheit.de/aktuelles/bewertung-nationaler-cyber-sicherheitsstrategien-24504

[12] Smart Meter sind intelligente Strom-, Wasser- oder Wärmezähler. Gateway steht dabei als Synonym für die Datenübertragung der Verbrauchswerte vom Verbraucher zum Energieversorger. - http://www.itwissen.info/definition/lexikon/smart-meter-Intelligenter-Zaehler.html

[13] „Schutzprofil für ein Smart Meter Gateway (BSI-CC-PP-0073)“ - https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Gateway/schutzprofil_smart_meter_gateway_node.html

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet eine Vielzahl weiterer Themen und Publikationen an, welche sich mit aktuellen Themen auseinandersetzen und laufend erweitert werden.

Hierbei gibt es zum einen die technischen Richtlinien (z. B. BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen), welche das Ziel haben "angemessene Sicherheitsstandards zu verbreiten"[14]. In diesem Fall beschäftigt sich die Richtlinie TR-02102 mit ausgewählten kryptografischen Verfahren und nimmt dabei auch eine Bewertung der Sicherheit vor. Zwar erheben die Dokumente "keinen Anspruch auf Vollständigkeit", allerdings bedeutet dies nicht, dass "die nicht aufgeführten Verfahren als unsicher beurteilt werden".[15]

Diese Richtlinie gliedert sich beispielsweise im Detail nochmals in "BSI TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen", "BSI TR-02102-2 – Verwendung von Transport Layer Security (TLS)" und "BSI TR-02102-3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2)".

Sofern notwendig, werden diese Richtlinien zeitnah überarbeitet und den sich verändernden Gegebenheiten und Rahmenbedingungen angepasst.

Diese Richtlinien sind sehr detailliert ausgearbeitet, umfangreich und dienen als eine Orientierungshilfe und Nachschlagewerk für Verantwortliche und Interessierte. Sie sind für viele weitere Themen und Bereiche verfügbar und kostenlos über die Webseiten des BSI zu beziehen.

Das BSI bietet zusätzlich einen "Themen"-Bereich[16] auf den eigenen Webseiten an, welcher sehr viele hilfreiche Informationen rund um verschiedene Fragestellungen liefern soll. Hierbei werden Themen behandelt wie beispielsweise "Biometrie", "Sicheres E-Government", "Smart Metering"[17], und "Elektronische Ausweise". Die "Themen-Dokumente" vermitteln Wissen auf vielen Ebenen und sind technisch weniger tief greifend als die Richtlinien selbst, beziehen diese aber an den relevanten Stellen mit ein.

Eine sehr wichtige und aktuelle Fragestellung ist beispielsweise das erwähnte Thema "Smart Metering Systems" im Bereich intelligenter Stromnetze. Auf 36 Seiten behandelt das BSI hier alles rund um die Sicherheit für intelligente Stromnetze und richtet sich damit in erster Linie an die Entwickler solcher Systeme aber auch an interessierte Anwender und Verantwortliche. Es sind derzeit insgesamt 56 Themen-Dokumente verfügbar und das Angebot wird laufend erweitert.

Beide Bereiche (Themen und Richtlinien) bieten einen sehr wertvollen Fundus an Informationen und Wissen für viele Bereiche und Zielgruppen in der IT-Sicherheit.

2.2 Definition: Vertrauenswürdigkeit

Vertrauen und Vertrauenswürdigkeit sind sehr essentielle Begriffe, die in allen Lebensbereichen eine tragende Rolle spielen. Im nachfolgenden sollen diese näher erläutert werden.

"Vertrauen"

Nach [RoSiBuCa98, Luhm1979, Cole1990] ist es ein "komplexer Begriff, der in verschiedensten Bereichen durchdacht und untersucht worden ist (Sozialwissenschaften, Philosophie, Psychologie, Informatik, ...)".

Also: "Ein Begriff, der in Zusammenhang mit dem Vertrauen in die Ehrlichkeit, Aufrichtigkeit, Kompetenz und Zuverlässigkeit einer vertrauenswürdigen Einheit gesetzt wird." [3, S.8]

---

[14] „Technische Richtlinien des BSI (BSI-TR)“ - https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html

[15] Kryptographische Verfahren: Empfehlungen und Schlüssellängen, S. 13
- https://www.bsi.bund.de/cae/servlet/contentblob/477256/publicationFile/30924/BSI-TR-02102_V1_0_pdf.pdf

[16] „Übersicht BSI-Themen“ - https://www.bsi.bund.de/DE/Themen/themen_node.html

[17] Smart Meter sind intelligente Strom-, Wasser- oder Wärmezähler. - http://www.itwissen.info/definition/lexikon/smart-meter-Intelligenter-Zaehler.html

Aus gesellschaftlicher Sicht wird Vertrauen folgendermaßen definiert: "Soziales Vertrauen - Das Vertrauen in die Sicherheit oder der Güte von etwas, aus Gründen der Reputation, einer Vorstellung, einer Empfehlung oder des wahrgenommenen Nutzens." [3, S.8]

Im Sinne der Wirtschaft könnte also auch tituliert werden: "Vertrauen ist ein individuelles Gefühl und eine Vorbedingung für die Aufnahme von Geschäftsbeziehungen. Es ergänzt bei wenigen sachkundigen Nutzern vorhandenes und bei vielen unkundigen Nutzern fehlendes Wissen um differenzierte Sicherheitsmechanismen." [3, S.8]

"Vertrauen kann bei positiven Anwendungserfahrungen wachsen und bleibt solange erhalten, bis es erschüttert wird." [3, S.8]

Die Trusted Computing Group (TCG) definiert ein System als vertrauenswürdig, "wenn es sich immer in einer erwarteten Weise zu einem beabsichtigten Zweck verhält."[18]

Die Realität

Unabhängig vom Umfeld muss beim Einsatz von IT-Technologien sichergestellt werden, dass Informationen nicht heimlich durch Unbefugte entwendet oder manipuliert werden. Um dies zu verhindern, werden z. B. Firewalls oder VPN-Gateways eingesetzt, aber auch Verschlüsselungssoftware oder besonders sichere Betriebssysteme. Sind diese auf dem neusten technischen Stand und korrekt konfiguriert, ist die prinzipielle maximal erreichbare und wahrnehmbare Sicherheit zwar gegeben, allerdings ist die konkrete Sicherheit nur bedingt tatsächlich vorhanden, obwohl sie eine wichtige Rolle spielt: "In einer perfekten Welt würden Vertrauen, gegenseitige Rücksichtnahme und Freundlichkeit regieren. Dort wären alle Informationen für jeden frei zugänglich, niemand würde sich zulasten anderer bereichern (...)." [4, S.25]

Wir leben in keiner perfekten Welt und: "die reale Welt sieht leider anders aus: Einfluss, Informationen und Wissen - und damit Macht - sind ungleich verteilt. Einbruch und Diebstahl gefährden Eigentum. Betrug, Verrat und Übervorteilung gehören zum Geschäftsleben." [4, S.25]

Fakt ist, dass in der Vergangenheit vermehrt Informationen veröffentlicht worden sind, die belegen, dass Geräte absichtlich von Werk aus oder auf dem Weg zum Empfänger vorsätzlich mit Hintertüren ausgestattet worden sind, um sich später unbemerkt Zugriff auf die angeschlossene Infrastruktur verschaffen zu können.

Hat eine Institution mit derartigen Absichten sehr viel Geld zur Verfügung und womöglich auch noch gesetzliche Handhabe gegenüber nationalen Herstellern (wie z. B. in den USA), lassen sich fast immer Fehler in Produkten finden, und eben diese zum eigenen Vorteil ausnutzen. Hier sind neue Konzepte notwendig, die dies wirkungsvoll verhindern. Berichte aus jüngster Vergangenheit zeigen, dass enorme finanzielle Aufwendungen zur Beschaffung von Sicherheitslücken getätigt werden: "Ein Vertrag ist an die Öffentlichkeit gekommen, laut dem der amerikanische Geheimdienst NSA Informationen über Schwachstellen bei der französischen Sicherheitsfirma Vupen[19] einkauft." [5] Dies bedeutet gleichzeitig, dass erworbene Schwachstellen nicht sofort bzw. teilweise überhaupt nicht den Weg an die Öffentlichkeit finden. So können die betroffenen Systeme, die mit hoher Wahrscheinlichkeit in allen Ländern auf allen Ebenen im Einsatz sind, nicht gehärtet werden. Leider bleibt der Verbleib und Zweck der gekauften Schwachstellen verborgen und wird nicht veröffentlicht. Dies sorgt auf der einen Seite für die bestehende Gefährdung der Öffentlichkeit durch offenbleibende Sicherheitslücken und fördert auf der anderen Seite den Markt für ein solches Angebot immer weiter.

Solche Risiken und Praktiken sind heute allgegenwärtig und lassen sich nur durch verschiedene Maßnahmen vermeiden. So ist es denkbar, eine Evaluierung von Technologien durchzuführen, in der nachgewiesen werden muss, dass von der Herstellung bis zur Inbetriebnahme keinerlei Manipulation stattfindet und z. B. keine gewollten Hintertüren eingebaut worden sind.

[18] US-amerikanische Standardisierungs-Organisation der Computerindustrie - http://www.trustedcomputinggroup.org/
[19] "VUPEN is the leading provider of defensive and offensive cyber security intelligence and advanced vulnerability research." - http://www.vupen.com/english/

In diesem Fall wäre die Beweiserbringung bereits sehr schwierig. Bei bewusst integrierten Hintertüren gestaltet sich dies umso schwieriger.

Vertrauen ist also wichtiger denn je: "Die Vertraulichkeit eines IT-Dienstes ist der Grad der Nichtausforschbarkeit der zu schützenden Daten." [4]

Einem Produkt könnte beispielsweise eine höhere Vertraulichkeit attestiert werden, wenn es in seiner Gesamtheit in Deutschland entwickelt und produziert worden ist, die Firma ihren Hauptsitz in Deutschland hat, niemand von außen mit dem Ziel der Schwächung oder Manipulation der Produkte Einwirkung genommen hat und die Lieferkette ebenfalls gesichert ist – und all dies nachgewiesen werden kann.

Der Preis für einmal verlorenes Vertrauen ist sehr hoch. Eine Möglichkeit verlorenes Vertrauen in Teilen zurückzugewinnen, wäre es die Austauschbarkeit zu ermöglichen und Transparenz zu fördern. Dies wird detailliert im Kapitel "IT Security Replaceability" auf Seite 51 diskutiert.

2.3 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 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.

Mangels Alternativen muss sichergestellt werden, dass in solch einem Fall die Integration einer weniger vertrauenswürdigen Komponente in ein vertrauenswürdiges Netzwerk mit Bedacht geschieht und falls technisch möglich, alle notwendigen Maßnahmen getroffen werden. Dies bedeutet im Detail, dass es aufgrund fehlender Alternativen keine Ausweichmöglichkeiten gibt und dies entsprechend bei der Planung und Umsetzung Berücksichtigung finden muss.

Abhängigkeit zum Ausland

In den meisten Technologiebereichen kommen die Marktführer aus dem Ausland, wie die spätere genauere Betrachtung im Kapitel "Analyse der wichtigen und verfügbaren IT-Sicherheitstechnologien" noch genauer zeigt. Dies wird zwar bisher offenbar mangels Alternativen hingenommen, allerdings wird dabei eines deutlich: 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.

Nationale Souveränität

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 Transparenz, Vertrauen und andere Werkzeuge und Prozesse erreicht.

Dies kann beispielsweise durch das Konzept der "Austauschbarkeit" erreicht werden, welches im weiteren Verlauf dieser Arbeit genauer erläutert wird. Die Idee der "IT Security Replaceability” fordert die Austauschbarkeit von IT-Sicherheitsprodukten und IT-Sicherheitstechnologien innerhalb von Produkten, Betriebssystemen und Geräten von den großen und wichtigen IT-Marktführern. 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.

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", Frage: **Wirkungsvoller Schutz von Informationen?**

⇔

"konkrete Wirkung", Frage: **Angewendeter Schutz verlässlich und sicher genug?**

⇔

"gewollte Wirkung" , Frage: **Durchgeführte Schutzmaßnahmen frei von Hintertüren?**

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.

Wie sich die drei hier gestellten Fragen nach der Wirkung im Detail beantworten lassen und welche Schritte notwendig sind, um eine verändernde und positive Wirkung zu erreichen, wird im Kapitel "Unterschiedliche Wirkungsaspekte" noch einmal im Detail beleuchtet.

3 IT-Sicherheitssituation und der Weg zu einem höheren IT-Sicherheitsniveau

Dieses Kapitel widmet sich einigen Aspekten, aus denen sich hauptsächlich IT-Sicherheitsprobleme ergeben und beleuchtet, welche Defizite es in Deutschland hinsichtlich Sicherheit und IT-Sicherheitslösungen gibt - vorbereitend für den Weg zu möglichen Lösungen zugunsten eines angemessenen IT-Sicherheitsniveaus.

3.1 Was ist IT-Sicherheit?

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 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?

Das Einspielen von Sicherheitsupdates ist dabei nur das absolute Minimum dessen, was getan werden sollte, um dieser Herausforderung gerecht zu werden. Es stellt sich auch die Frage nach absichtlichen Hintertüren in der eingesetzten Hardware, die trotz eingespielter Updates den jederzeitigen unbefugten Zugriff durch "Freunde und Partner" aus dem Ausland erlaubt. Hier spielt die Vertrauenswürdigkeit eine entscheidende Rolle, die bereits im Kapitel "Definition: Vertrauenswürdigkeit" diskutiert wurde.

Der Begriff IT-Sicherheit hat viele Aspekte und ist mehr ein Konzept als eine Plug-and-Play Lösung innerhalb einer übergeordneten Business Strategie zu sehen. IT-Sicherheit lässt sich nicht einfach erwerben und die an die eigene IT-Infrastruktur "drangesteckt", um alle Probleme zu lösen. Der Faktor Mensch ist hierbei erheblich und muss durch regelmäßige und qualitative Schulungen berücksichtigt werden.

Die Frage nach der richtigen und möglichst vollständigen Realisierung eines IT-Sicherheitskonzeptes im Unternehmen ist komplex und scheitert schon oft an der Frage nach dem eigenen Schutzbedarf oder der Beurteilung der eigenen Risiken und Rolle: Was wird an Schutzmaßnahmen benötigt? Von welcher Wichtigkeit sind die betrachteten IT-Systeme? Handelt es sich um bedeutsame Basisdienste für die Gesellschaft (KRITIS[20], Stichwort: z. B. Wasser- und Stromversorgung)?

All diese Fragen sind nicht trivial und können nicht im Rahmen dieses Dokuments beantwortet werden. Das sollen sie auch gar nicht. Das Ziel ist es, hier ein universelles Werkzeug zur Verfügung zu stellen, damit Verantwortliche herausfinden können, wie sie zielführend zur richtigen Antwort finden.

3.2 IT-Sicherheitsherausforderungen und Bedrohungen

In beinahe allen Bereichen der IT-Sicherheit und den IT-Sicherheitsanforderungen herrscht ein dringender Nachholbedarf. Es existiert somit viel Raum für notwendige Verbesserungen.

[20] Kritische Infrastrukturen; Definition und Übersicht: http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html

In einigen Bereichen existieren bereits passende Lösungen, in anderen gibt es wiederum Potential zu Verbesserungen wie beispielsweise im Bereich der "Firewalls" oder "Device & Portkontrolle" und der Notwendigkeit für neue Problemlösungen und weitere vertrauenswürdige und sichere Produkte.

"IT-Systeme benötigen einen ihrer Bedeutung angemessenen wirksamen Schutz. Besteht bei Ausfall des Systems oder erfolgreichem Angriff auf das IT-System Gefahr für Leib und Leben von Menschen, so sind höchstmögliche Sicherheitsniveaus anzustreben und auf Dauer auch zu gewährleisten." [4, S.80]

Die Anforderungen an die IT-Sicherheit sind klar definierbar und können in verschiedene Bereiche, aus denen Gefahr droht, eingeteilt werden. Problematisch sind Schwachstellen in Softwareprodukten, mangelhafte und unvollständige Schadsoftware- und Malware-Erkennung. Des Weiteren sind komplexe zielgerichtete Angriffe, welche eine besondere Herausforderung darstellen, Gefahren eines Identitätsdiebstahls, Messbarkeit von Gefahren- und dem Bedrohungspotenzial sowie allgemein ineffektive IT-Sicherheitslösungen ebenfalls sehr wichtige Themen, die nachfolgend im Detail näher erläutert werden.

3.3 Schwachstellen in Software

Die Kernprobleme, die für dieses Konzept eine gewichtige Rolle spielen, sind beispielsweise die Existenz zahlreicher Schwachstellen in Software. Dabei ist bereits jede einzelne Schwachstelle zu viel. Softwareentwicklung ist eine sehr komplexe Herausforderung und bietet sehr viel Raum für Fehler.

"Mit der steigenden Komplexität der IT-Systeme und der in ihnen eingesetzten Hard- und Softwarekomponenten wächst die Fehlerhäufigkeit exorbitant. Diese Fehlerrate zeigt sich besonders schmerzlich in den Schwachstellen, die Angreifer ausnutzen." [4, S.84]

Jede Software besteht aus sehr vielen Zeilen Programmcode. Jede Zeile Quelltext birgt die Gefahr, dass sie nicht einwandfrei und damit fehlerbehaftet ist. In der Masse betrachtet münden also im Prinzip sehr viele Zeilen Programmcode in sehr vielen möglichen Schwachstellen. Dies wird die "Fehlerdichte in der Informatik" genannt. [6]

Diese Fehler könnten durch verschiedene Angriffsvektoren genutzt werden, wie am Beispiel von Betriebssystemen, welche mit ca. 10 Mio. Programmzeilen im besten Fall auf etwa 3.000 Fehler kommen. Diese ließen sich in den meisten Fällen aktiv dazu nutzen in ein IT-System einzubrechen, es zu manipulieren, zu übernehmen oder Daten zu stehlen. (Klassifikation der Fehlerdichte siehe nachfolgende Tabelle 1)

Fehlerdichte (Anzahl)	Klassifizierung der Programme
weniger als 0,5	stabile Programme
0,5 bis 3	reifende Programme
3 bis 6	labile Programme
6 bis 10	fehleranfällige Programme
mehr als 10	unbrauchbare Programme

Tabelle 1 – Fehlerdichte pro 1000 Zeilen Code und Klassifizierung von Programmen [6]

3.3.1 Schadsoftware-Erkennung und -Vermeidung

Ein weiterer Punkt, bei dem ein Nachholbedarf besteht, ist der Bereich der Schadsoftware-Erkennung und -Vermeidung. Schadsoftware wird immer komplexer und die Anzahl der Bedrohungen (Malwarefamilien und Arten von Schadsoftware) steigt rasant an. So entdeckte

Kaspersky 2014 nach eigenen Angaben täglich 315.000 neue Schädlinge, im Jahr 2013 waren es noch 200.000. [7]

Das Dilemma für den Nutzer ist die Erkennungsrate von lediglich ca. 45% [8], zumal die Antiviren-Software selbst keinerlei Schutz gegen zielgerichtete Hackerangriffe bietet. Die Gefahr ist jedoch groß: "Viren, Trojaner und andere Schadsoftware stellen nach ihrem wirtschaftlichen Schaden bereits heute die größte Sicherheitsgefahr bei stationären Rechnern dar." [9]

Erschwerend hinzu kommt die Tatsache, dass die Software, die den Anwender schützen soll, selbst Fehler enthalten kann. Dies trägt wiederum dazu bei, dass sich die verwundbare Fläche eines Systems vergrößert.

3.3.2 Komplexe zielgerichtete Angriffe (APT)

Die sogenannten "Advanced Persistent Threats" (APT, fortgeschrittene, andauernde Bedrohungen) spielen im Bereich der Cyber-Attacken eine zunehmend wichtige Rolle und stehen als Synonym für einen sehr komplexen zielgerichteten Angriff auf kritische IT-Infrastrukturen (nicht nur KRITIS) bzw. in erster Linie deren Mitarbeiter oder elementare wirtschaftliche Ziele. So könnte der Angriff auf die iranischen Uran-Aufbereitungsanlagen aus der Vergangenheit dieser Kategorie zugeordnet werden. Solch eine Attacke (hier mit Hilfe einer hoch spezialisierten Schadsoftware mit dem Namen "Stuxnet"[21]) lässt sich nur mit einem beträchtlichen Aufwand an personellen und finanziellen Mitteln realisieren und dient am Ende einem genau definierten Ziel, wie in diesem Fall iranische Zentrifugen, die im Rahmen des iranischen Atomprogramms verwendet werden. So wurde mit dem Ziel der Sabotage unbemerkt und ohne den klassischen militärischen Einsatz von Soldaten, Panzern, Flugzeugträgern, und Menschenleben das iranische Atomprogramm deutlich ausgebremst.

Auch in diesem Bereich ist die Abwehr einer Bedrohung sehr komplex und zum jetzigen Zeitpunkt gibt es an dieser Stelle einen großen Nachholbedarf.

Statt Zentrifugen könnte es in naher Zukunft kritische Infrastruktur treffen, wie Energie- und Wasserversorgung oder Krankenhäuser.

3.3.3 Identitätsdiebstahl

Ein großes Problem im Internet ist der Diebstahl von Identitäten. Zum einen ist es für den Nutzer selbst schwierig mit probaten Mitteln die eigene Identität effektiv zu schützen und zum anderen ist das Aufdecken eines durchgeführten Missbrauchs für einen Betroffenen beinahe unmöglich. Sieht er sich mit den Auswirkungen konfrontiert, ist es meistens bereits zu spät, um die daraus entstehenden Folgen vermeiden zu können. Hier besteht ebenfalls viel Raum für Verbesserungen.

3.3.4 Messbarkeit von Gefahren- und Bedrohungspotenzial

Oft ist nicht klar, wie schwerwiegend eine existierende Gefahr ist und welche Konsequenzen eine Bedrohung haben kann. Es ist notwendig, neue Methoden für die Messbarkeit von Gefahren und einer Bewertung des Bedrohungspotenzials zu entwickeln. Hier kann die Wissenschaft und Forschung behilflich sein, neue Denkweisen und Konzepte zu erarbeiten oder bestehende neue Technologien mit Hilfe der Industrie zur Marktreife zu führen.

3.3.5 Ineffektive IT-Sicherheitslösungen

In vielen Fällen werden jedoch IT-Sicherheitslösungen eingesetzt, welche sowohl absichtlich als auch unabsichtlich für die vorgesehenen Zwecke ineffektiv und teilweise völlig ungeeignet sind. Ein Beispiel ist der Einsatz einer Antivirensoftware unter Windows XP als Schutzmaßnahme und der Rechtfertigung eines weiteren Einsatzes dieses Betriebssystems. Der Support wurde im April 2014 eingestellt. Seit diesem Zeitpunkt gibt es keinerlei Sicherheitsupdates seitens des Herstellers. Eine Ausnahme bildet hier ein Angebot für Unternehmen und Behörden, welche die Möglichkeit haben einen verlängerten Updatesupport zu erwerben. Dies ist

[21] *Stuxnet* ist eine sehr hochspezialisierte Schadsoftware (originaler Name: *RootkitTmphider*) und wurde zur Überwachung und Manipulation technischer Prozesse von SCADA-Systemen der Firma Siemens entwickelt.

jedoch nur bedingt sinnvoll, da dies zum einen sehr teuer ist und zum anderen den notwendigen Wechsel auf ein aktuelleres System nur verzögert, ihn jedoch nicht verhindert. Details zu den ausgehandelten Konditionen sind nur schwer zu benennen, da die Verhandlungen hinter verschlossenen Türen stattfinden. Für die britische Regierung ging es hierbei im Rahmen eines Vertrages für das erste Jahr um siebstellige Beträge: "Microsoft erhält von der britischen Regierung etwa 6,5 Millionen Euro (5,48 Millionen britische Pfund) für den verlängerten Support von Windows XP. Die Vereinbarung gilt zunächst für ein Jahr." [10] Deutsche Behörden haben indes ebenfalls ähnliche Verträge geschlossen.

Es gab Nutzer ohne Kapital für solche Verträge, die das Problem mit der Installation von Sicherheitssoftware umgehen wollten. Der Verlass einzig auf eine "Sicherheitssuite" als Softwareprodukt für Windows XP ist nicht ratsam und mündet in einer ineffektiven Sicherheitsstrategie, von der unbedingt abzuraten ist.

Im Bereich der Hardwareprodukte gibt es ebenfalls vergleichbare Probleme. Dort gibt es immer wieder schwerwiegende Sicherheitslücken, die manchmal sogar Millionen von Nutzern auf einen Schlag betreffen. So traf es in jüngster Vergangenheit DSL-Router: "Millionen DSL-Router durch TR-069-Fernwartung kompromittierbar." [11]

Falls in solch einem Fall das eigene Gerät betroffen ist, bleibt oft nur die Hoffnung, dass der Internetserviceprovider schnell reagiert und die Updates vom Hersteller freigibt, falls dieser überhaupt welche liefert. Der Grund ist oftmals ein spezifisches Gerät eines einzigen Herstellers vom Anbieter, bei dem es oft keine Möglichkeit gibt, das Gerät gegen Produkte anderer Firmen auszutauschen. Die Reichweite dieser Sicherheitslücke war enorm: "Einer Statistik aus dem Jahr 2011 zufolge sind zirka 150 Millionen Breitband-Router für TR-069 ausgelegt." [11]

Im Klartext bedeutet dies den Besitz eines verwundbaren IT-Systems, ohne die Möglichkeit eine Alternative einsetzen zu können oder das Problem auf andere Weise selbst lösen zu können. Die einzige Möglichkeit wäre es, das verwundbare Gerät bewusst vom Netz zu nehmen, inklusive dem Verzicht auf einen Internetzugriff. Dies ist in der Realität natürlich nicht praktikabel und somit realitätsfern.

3.4 Mindeststärke und Penetration von IT-Sicherheit

Jede IT-Sicherheitslösung muss Penetrationen, also aktiven Angriffen, standhalten. Die Frage nach ihrer Wirksamkeit und der Schwachstellenanalyse solcher Systeme sollte stets berücksichtigen, dass jeder Angreifer prinzipiell immer über genügend Zeit verfügt sich einen Punkt zu suchen, an dem er angreifen will. 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.

Jede Organisation hat Werte, die sie schützen möchte und sollte. Diese Werte können in verschiedenen Gestalten auftreten, sind aber in diesem Fall immer in digitaler Form vorhanden und im nachfolgenden Beispiel durch den "Geldsack" ("Assets") in Abbildung 3 dargestellt.

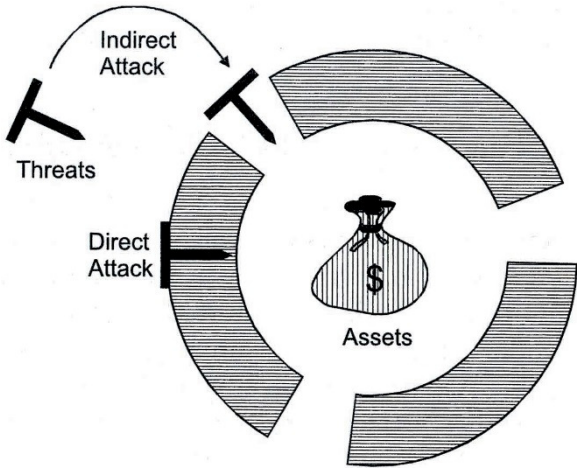


Abbildung 3 - Wirksamkeit von IT-Sicherheit [12, S.405]

Wie hier ersichtlich, bietet die Sicherheitslösung in dieser Skizze eine dicke Schutzwand, die gegen den Angriff (Nagel mit einer bestimmten Länge) gewappnet zu sein scheint. Gegen direkt gerichtete Angriffe ist der Schutz ausreichend, da der Nagel die Schutzschicht nicht durchdringen kann. Allerdings ist diese Schutzschicht nie durchgängig und rundum geschlossen. In der Realität gilt es Konzepte umzusetzen, die immer Vor- und auch Nachteile haben – beides geht immer Hand in Hand. So ist es also möglich, durch einen indirekten Angriff einen Weg für eine erfolgreiche Attacke zu finden und die Sicherheitsmaßnahmen zu umgehen. Dies kann ein geschickt gewählter Angriff sein aber auch eine zuvor eingebaute Hintertür und die absichtliche Schwächung des IT-Sicherheitssystems. [12]

An dieser Skizze werden zwei Dinge deutlich: Zum einen muss immer ein passendes IT-Sicherheitskonzept mit möglichst mehrstufiger Sicherheit gewählt werden. Es darf sich dabei nicht auf nur eine bestimmte Technologie gestützt werden. Zum anderen spielt die Vertrauenswürdigkeit eine große Rolle, denn das sicherste System ist absolut nutzlos, wenn der Angreifer eine Hintertür kennt.

Als Beispiel einer Veranschaulichung eines gelungenen IT-Sicherheitskonzeptes dient die nachfolgende Abbildung 4. Hierbei wurde mit Hilfe mehrerer Schichten (Basic, Medium und High) erfolgreich versucht, wirksame Gegenmaßnahmen zu treffen, die keine Lücken offen lassen, um einen alternativen Weg zu finden.

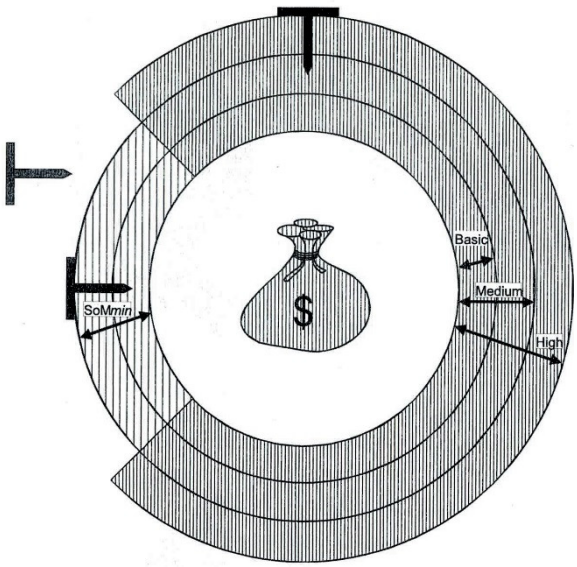


Abbildung 4 - Penetration von IT-Systemen und Mindeststärke [12, S.406]

Zudem ist die gewählte Mindeststärke hier ausreichend und bietet genügend Schutz, um allen kalkulierbaren Angriffen entgegenzuwirken.

Durch die hier erreichte Mindeststärke, ist es möglich ein angemessenes Sicherheitsniveau zu erreichen. Auf diesem Wege lassen sich die eigenen Werte effektiv schützen.

Der Grund für die ausreichende Sicherheit liegt in den verschiedenen Schichten. Es ist keine singuläre Lösung, sondern eine Kombination verschiedener Technologien.

Natürlich stellt die Veranschaulichung in Abbildung 4 den optimalen Weg dar. In der Realität kann das Sicherheitsniveau zwar nie perfekt und undurchdringlich sein, allerdings kann es mit Hilfe von Konzepten, Regelwerken und Planung angemessen ausfallen. So kann zumindest die Wahrscheinlichkeit verkleinert werden, Lücken in der Infrastruktur offenzulassen.

4 Die größten Stärken und Herausforderungen der IT-Sicherheit in Deutschland

Die IT-Sicherheit in Deutschland hat besondere Stärken, durch die sie sich im internationalen Vergleich von den Mitbewerbern hervorheben kann. Hierzulande gibt es eine sehr hohe Kompetenz im Bereich des Datenschutzes und dem Bestreben die Privatsphäre jedes Einzelnen adäquat zu schützen. Wiederkehrende Verstöße und auftretende Probleme in diesem Bereich werden zur Lösungsfindung konstruktiv in der Öffentlichkeit diskutiert.

"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." [13]

4.1 "IT-Security made in Germany"

Wie bereits angesprochen, setzen ausländische Institutionen und Firmen sehr vieles daran, Sicherheitskonzepte und Architekturen von IT-Produkten durch unzulässige Praktiken zu ihrem Vorteil zu beeinflussen. Dies geschieht beispielsweise in Form von Manipulationen von Netzwerkhardware auf dem Postweg, Einbau von Hintertüren oder indirektem Einfluss beim Erarbeiten von vermeintlich sicheren Standards, um die darauf basierenden Komponenten leichter brechen zu können.

Beim Einsatz solcher illegal manipulierten Technologien und Geräten muss erst einmal grundsätzlich davon ausgegangen werden, dass Schwachstellen vorhanden sind und auch ausgenutzt werden können. Dies kann direkt oder indirekt eine ernsthafte Bedrohung darstellen. Zum einen ist dies problematisch im Hinblick auf unsere eigene Infrastruktur in Deutschland und die Versorgung in Form von Wasser oder Energie. Zum anderen aber auch im Bereich der Behörden und Unternehmen, wo es um viele wesentliche persönliche Daten von Bürgern geht oder der Sicherung des nationalen Know-hows innerhalb von Forschung und Entwicklung.

Selbst Institutionen wie die Büros des EU-Parlaments und der Bundesregierung stellen hier keine Ausnahme dar. "Wirtschaft, Verwaltung und Gesellschaft sind auf sichere und vertrauenswürdige Informationsinfrastrukturen angewiesen. Dies erfordert Sicherheitsmaßnahmen und IT-Sicherheitsprodukte, die adäquaten Schutz auf hohem Niveau bieten und der Bedeutung der zu schützenden Güter angemessen sind." [14]

Die IT-Sicherheitsindustrie aus Deutschland genießt hier ein hohes Maß an Vertrauen, denn sowohl national als auch international hat "made in Germany" in sehr vielen Bereichen ein sehr großes Gewicht. "Gerade wir in Deutschland haben kulturell und gesetzlich, aber auch in der IT-Sicherheitsforschung und in der IT-Sicherheitsindustrie, die idealen Voraussetzungen hier einen wichtigen Beitrag zu einem sicheren und vertrauenswürdigen Internet zu leisten." [13]

Die nationale Sicherheitsindustrie ist sehr mittelstandsgeprägt und auf zahlreichen Gebieten der IT-Sicherheitsforschung aktiv. Sie besitzt in manchen Bereichen eine einmalige und weltweit geschätzte Sicherheitsevaluierung (z. B. BSI oder TÜV). Auch gibt es keinerlei Reglementierung im Bereich der Kryptografie in Deutschland, im Gegensatz zu den USA. Dementsprechend ist also die Kryptopolitik in Deutschland eine sehr offene, was ebenfalls große Vorteile mit sich bringt und einen Pluspunkt im Bereich der Vertrauenswürdigkeit darstellt.

Deutschlands IT-Sicherheitsindustrie kann in vielen Bereichen eine traditionell verlässliche IT-Sicherheit vorweisen. Vor dem kulturellen Hintergrund gibt es in Deutschland ein hohes Verständnis für die IT-Sicherheit und den Datenschutz.

Hierzulande kann auf sehr viel Erfahrung zurückblickt werden, sowohl im Hinblick auf die Lösungsfindung für verschiedene Problemstellungen, als auch der Umsetzung von IT-Sicherheitslösungen.

Abbildung 5 - TeleTrusT-Initiative "IT Security made in Germany" Siegel

Zusammengenommen ist die IT-Sicherheit als Marke aus Deutschland also aus all diesen verschiedenen Gründen ein starkes Argument.

"ITSMIG" ("IT Security made in Germany") wurde 2005 auf Initiative des Bundesministeriums des Innern (BMI), des Bundesministeriums für Wirtschaft und Technologie (BMWi) sowie Vertretern der deutschen IT-Sicherheitswirtschaft etabliert und 2008 in einen eingetragenen Verein überführt. Sowohl BMI als auch BMWi haben eine Schirmherrschaft übernommen.

Nach intensiven Erörterungen kamen TeleTrusT und ITSMIG 2011 überein, dass sich auf ihren Handlungsfeldern Synergien erschließen lassen. Seitdem werden die ITSMIG-Aktivitäten unter dem Dach von TeleTrusT als TeleTrusT-Arbeitsgruppe "ITSMIG" fortgeführt.

Die Arbeitsgruppe "ITSMIG" verfolgt das Ziel der gemeinsamen Außendarstellung der mitwirkenden Unternehmen und Institutionen gegenüber Politik, Wirtschaft, Wissenschaft und Öffentlichkeit auf deutscher, europäischer bzw. globaler Ebene. BMWi und BMI sind im Beirat der Arbeitsgruppe vertreten.

Die Verwendung des markenrechtlich geschützten TeleTrusT-Qualitätszeichens "IT Security made in Germany" wird interessierten Anbietern auf Antrag und bei Erfüllung der nachstehenden Kriterien zeitlich befristet gestattet:

1. Der Unternehmenshauptsitz muss in Deutschland sein.
2. Das Unternehmen muss vertrauenswürdige IT-Sicherheitslösungen anbieten.
3. Die angebotenen Produkte dürfen keine versteckten Zugänge enthalten (keine "Backdoors").
4. Die IT-Sicherheitsforschung und -entwicklung des Unternehmens muss in Deutschland stattfinden.
5. Das Unternehmen muss sich verpflichten, den Anforderungen des deutschen Datenschutzrechtes zu genügen.

[15]

Dies stellt sicher, dass die Vergabe des Siegels auf der einen Seite die Souveränität der nationalen Unternehmen stärkt und auf der anderen Seite dem Kunden, der eine Entscheidung treffen möchte, Hilfestellung hinsichtlich der Fragen nach Qualität und Vertrauenswürdigkeit bieten kann.

Aktuell gibt es über 100 Unternehmen, die als Zeicheninhaber eingetragen sind und über die Erlaubnis verfügen, dieses Siegel zu verwenden.

4.2 Verantwortung übernehmen

Das gemeinsame Ziel der Industrie und Politik ist klar definiert: Deutschland muss Verantwortung übernehmen und ein sicheres und vertrauenswürdiges globales Internet für die Zukunft entscheidend mitgestalten.

Es gibt viele Wege, die parallel beschritten werden müssen, um das gemeinsame Ziel zu erreichen. Insbesondere die Austauschbarkeit und die Nachweisbarkeit der Vertrauenswürdigkeit von IT-Systemen und IT-Sicherheitsprodukten ist hier ein wichtiges Ziel.

Die notwendige Verantwortung zu übernehmen, bedeutet wohlüberlegt zu handeln und gemeinsam am Erfolg dieses Konzeptes mitzuarbeiten. Gemeinsam bedeutet, dass jeder Stakeholder (Anwender, Industrie, Forschung, Politik) hierfür berücksichtigt werden muss. Ganz besonders sind hier sowohl die Politik als auch die IT-Sicherheitsindustrie gefragt.

Nur wenn sich alle gemeinsam entscheiden Verantwortung zu übernehmen, wird genug Energie freigesetzt um das Ziel auch zu erreichen. Es ist substanziell bedeutend, dass alle Interessensgruppen Hand in Hand zielstrebig, durch klare Definitionen und eine gemeinsame konsequente Umsetzung, an der Lösungsfindung arbeiten.

5 Analyse der wichtigsten und verfügbaren IT-Sicherheitstechnologien

Um einen Eindruck davon zu erhalten, wie die nationale IT-Sicherheitsindustrie gegenüber der internationalen Konkurrenz aufgestellt ist und welche Stärken sowie Defizite die IT-Sicherheitsfirmen in den wichtigsten Kategorien haben, wurde die nachfolgende Analyse ausgearbeitet.

5.1 Technologieanalyse der Anbieter im In- und Ausland

In diesem Unterkapitel werden die Ergebnisse einer Analyse der bedeutendsten und verfügbaren IT-Sicherheitstechnologien dargestellt. Hierbei werden "Bewertungen der Lage" bezüglich der eigentlichen IT-Sicherheitstechnologie, der "Bedeutung für die Zukunft" sowie die "Marktstärke der deutschen IT-Sicherheitsunternehmen" in den entsprechenden IT-Sicherheitsbereichen vorgenommen.

Zusätzlich wird der "Abstand zwischen Soll- und Ist-Zustand" (Lücke) betrachtet und abgeschätzt. Dieser Abstand soll im Prinzip eine Indikation in Form eines realen Abstandes zwischen dem aktuellen Zustand und dem eigentlich notwendigen Stand (nachfolgend auch als Delta bezeichnet) liefern. Realer Abstand ergibt sich aus in der Technologieanalyse ersichtlichen Defiziten zwischen dem Optimum und der tatsächlichen Alltagssituation: Beispielsweise sollte der Einsatz der "Virtuellen Schleuse" im Alltag oft Verwendung finden, was leider nicht der Fall ist.

In der Kategorie Bedrohungen werden exemplarisch Fälle von möglichen Angriffsszenarien und Bedrohungen dargestellt.

Zusätzlich werden in der Kategorie der Anbieter die Standorte berücksichtigt, um die geografische Aufteilung im Ausland aufzuzeigen, welche hinsichtlich Vertrauenswürdigkeit und IT-Sicherheit eine Rolle spielen kann. Die nachfolgende Tabelle 2 zeigt den Aufbau eines tabellarischen Elementes innerhalb der Analyse und soll verdeutlichen, wie dieser zu interpretieren ist.

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
Bewertung der Technologie nach verschiedenen Aspekten (siehe Legende in Tabelle 3)	*Angabe, ab welcher Wirkungsklasse diese Technologie eingesetzt wird.*	*Beschreibung einer möglichen Bedrohung als Beispielszenario, vor der hier Schutz geboten wird.*	*Dieser Bereich enthält eine Übersicht wichtiger Anbieter im In- und Ausland aus dieser Kategorie.*

Tabelle 2 - Erläuterung des Aufbaus der Tabellen innerhalb der Analyse

Legenden

Jede Technologie innerhalb jedes Bereiches besitzt, wie bereits angedeutet, eine Bewertung, die nachfolgend definiert wird. Hierbei werden sowohl kleine Symbole als auch Buchstaben (A bis D) verwendet. Jeder dieser Buchstaben repräsentiert eine spezielle Kategorie und einen Farbcode, der eine Bewertung repräsentiert.

	**A**	Bedeutung für die Zukunft
	**B**	Technologischer Vorsprung in Deutschland
	**C**	Marktstärke der dt. Unternehmen
	**D**	Abstand zwischen "Soll und Ist-Zustand" (Lücke / Δ Delta / "GAP")

Tabelle 3 - Legende für die Bewertungskriterien und deren Interpretation

Die nachfolgend in Tabelle 4 dargestellten gewählten Farben sollen ein Ampel-ähnliches Farbschema repräsentieren, anstatt der ursprünglichen Bewertungsversion mit Hilfe von ("--" bis "++"). 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 4 zu sehen ist.

Die für die Bewertungselemente notwendige Farbskala besitzt zwei Ebenen, d. h. für die Bewertung von A, B und C gibt es fünf verschiedene Farbcodes – also die vollständige Bandbreite. Für die Kategorie D (Abstand) werden sinnvollerweise nur drei Farbmarkierungen verwendet: Minimale bis keine Lücke ("GAP"/Delta) vorhanden. In diesem Fall wäre dies durch eine hellgrüne Färbung im Bewertungselement gekennzeichnet. Im Falle einer kleinen bis normalen Lücke wäre der Indikator orange und bei einem großen Defizit dunkelrot. Dies ist im unteren Bereich der Tabelle 4 dargestellt.

++	+	0	-	--
	Neutral, Δ minimal		Kleines bis normales Δ	Großes Δ

Tabelle 4 - Legende der farblichen Bewertungsskala für die Eigenschaften A, B, C und D

Für die eigentliche Bewertung der jeweiligen Technologie wurde hier, wie bereits erwähnt, ein vereinfachtes Schema verwendet, das als grafisches Bewertungselement daherkommt und die Buchstaben A bis D farblich bewertet. Dieses Schema ist nachfolgend in der Abbildung 6 dargestellt.

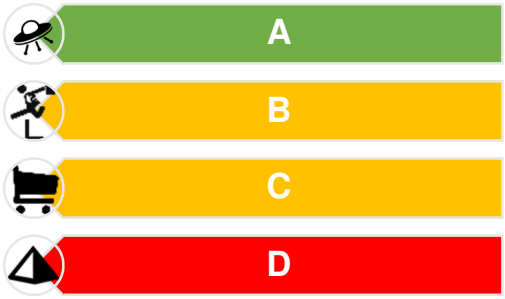


Abbildung 6 - Bewertungselement zur visuellen Darstellung von A bis D

Sind im Bereich "In- und Ausländische Anbieter" in der Kategorie "Deutschland" Firmennamen geklammert, kann dies verschiedene Ursachen haben. Die Klammerung dient hierbei als Kennzeichnung für den Einsatz ausländischer Technologien innerhalb der angebotenen Produkte, oder ist ein Hinweis auf eine substanzielle finanzielle Beteiligung durch externe ausländische Investoren.

Zu jeder der nun folgenden Technologietabellen wird eine kurze Erläuterung gegeben, ggf. eine Abgrenzung definiert oder, falls notwendig, weiterführende Informationen gegeben.

5.1.1 Bereich: Sichere Vernetzung

Nachfolgend wird der Bereich der sicheren Vernetzung dargestellt und in die wichtigsten Bestandteile aufgeschlüsselt. Hierzu gehören die sichere Anbindung von Benutzern, Layer3-VPN, die Layer2-Verschlüsselung und die Datendiode.

Sichere Anbindung mobiler User / Telearbeiter

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
A B C D	alle ab Klasse 1	Abfangen sensibler Informationen und Abhören von Kommunikation	**Ausland:** Cisco (USA), Juniper (USA), Fortinet (USA) **Deutschland:** secunet, genua, NCP, gateprotect, Sirrix, HOB, Innominate, LANCOM

Tabelle 5 - Technologiebetrachtung sichere Anbindung mobiler User / Telearbeiter

Der Bereich "Sichere Anbindung" betrifft Nutzer, die aus entfernten Örtlichkeiten eine Verbindung zum Unternehmen aufbauen möchten. Die Verbindung kann dabei sowohl aus einer öffentlichen als auch privaten Netzumgebung von Unterwegs hergestellt werden. Dies kann ein privates Netzwerk sein, oder das WLAN an einem beliebigen Punkt auf der Welt.

Layer3-VPN

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
A B C D	alle ab Klasse 3	Mitschneiden und Abfluss von Daten durch Hintertüren und Sicherheitslücken in Netzwerkhardware	**Ausland:** Cisco (USA), Fortinet (USA), Juniper (USA), Check Point (Israel) **Deutschland:** secunet, genua, gateprotect, Sirrix, Lancom, HOB, Innominate

Tabelle 6 - Technologiebetrachtung Layer3 Virtual Private Network (L3VPN)

Das "Layer3-VPN" ist notwendig, um die Kommunikation zwischen verschiedenen Endpunkten zu schützen. Virtual Private Networks (VPN) garantieren Authentizität, Vertraulichkeit und Integrität. Diese Technologie eignet sich hervorragend vor allem dazu, Standorte miteinander zu verbinden oder Mitarbeiter von unterwegs oder daheim aus sicher an das Firmennetzwerk anzubinden.

Layer2-Encryption

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 3	Mitschneiden und Abfluss von Daten durch Hintertüren und Sicherheitslücken in Netzwerkhardware	**Ausland:** SafeNet (USA), Crypto AG (Schweiz) **Deutschland:** secunet, Rohde & Schwarz, atmedia

Tabelle 7 - Technologiebetrachtung Layer2-Encryption

Layer2-Verschlüsselung ist eine hoch performante Sicherheitslösung, welche durchaus als Alternative mit einigen Vorteilen zu Layer3-VPNs gesehen werden kann. Insbesondere wenn es um hohe Bandbreiten geht, ist die Layer2-Verschlüsselung im Vorteil. Der Schutzfaktor steht und fällt jedoch mit der Vertrauenswürdigkeit der eingesetzten Produkte in diesem Bereich.

Datendiode

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 4	Angriff auf Übermittlung und Empfang von Daten, die in eine Richtung an einen festen Empfänger transportiert werden	**Ausland:** - **Deutschland:** genua, secunet

Tabelle 8 - Technologiebetrachtung Datendiode

Diese Technologie ist für abgeschottete Netze gedacht, die zwar Daten empfangen sollen aber keinesfalls auf dem Rückkanal Daten preisgeben sollen. Hierfür werden verschiedene Technologien wie Firewalls und spezielle Software (Mikrokernel) miteinander kombiniert, um eine unidirektionale Kommunikation zu erreichen. [16]

In diesem Bereich sind die Deutschen Technologieführer. Im Ausland gibt es keine nennenswerte Konkurrenz in diesem Bereich.

5.1.2 Bereich: Sicherer Internetzugang

Nachfolgend wird das Gebiet "Sicherer Internetzugang" dargestellt und in seine wesentlichen Bereiche eingeteilt. Hierbei werden die Technologien "Firewalls", "Intrusion-Detection-Systeme/Intrusion-Prevention-Systeme", "Remote-Controlled Browsers Systeme/ReCoBS" und "virtuelle Schleuse" berücksichtigt.

Firewall

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 1	Angriffe von außen, Portscans, ungewollte Kommunikation von Diensten und Anwendungen nach außen	**Ausland:** Sourcefire/Cisco (USA), ISS/IBM (USA), Extreme Networks (USA), Symantec (USA), McAfee (Intel, USA), Hewlett-Packard (USA), Palo Alto Networks (USA) **Deutschland:** genua, gateprotect, Innominate

Tabelle 9 - Technologiebetrachtung Firewall-Systeme

Der Begriff der Firewall betrifft hier die Perimeter-Sicherheit in Unternehmensnetzwerken. Der Schutz, gegen offensichtliche und weniger offensichtliche Angriffe von außen, soll damit gegeben werden. In diesem Bereich stehen die mittelständischen deutschen Anbieter einer sehr starken Konkurrenz aus dem Ausland gegenüber. Alleine der Marktführer Cisco aus den USA hat schätzungsweise 75.000 Mitarbeiter und einen Umsatz von ca. 40 Mrd. Euro im Jahr 2013. IBM, Intel und die anderen "Schwergewichte" sind personell und finanziell ähnlich aufgestellt.

IPS/IDS

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 3	Angriffe von außen, die unmittelbar auf die Infrastruktur einer Organisation durchgeführt werden	**Ausland:** Sourcefire/Cisco (USA), ISS/IBM (USA), Extreme Networks (USA), Symantec (USA) **Deutschland:** Institut für Internet-Sicherheit

Tabelle 10 - Technologiebetrachtung IPS/IDS

Die Intrusion-Prevention-Systeme/Intrusion-Detection-Systeme (IPS/IDS) bilden eine sehr wesentliche Technologie und werden durch immer komplexere Angriffe und größere, sich verändernde Netzwerke immer bedeutender. Eigentlich sollte die Einstufung an dieser Stelle die Wirkungsklasse 2 sein, denn bereits dort ist eine Notwendigkeit gegeben. Leider finden diese Systeme in der Realität erst ab der Klasse 3 Anwendung. Hier muss zukünftig in allen betroffenen Unternehmen ein Umdenken stattfinden.

Sicherer Browser/ReCoBS

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 3	Einbruch in Systeme durch infizierte Webseiten	**Ausland:** FireEye (USA), Bromium (USA), Invincea (USA) **Deutschland:** Sirrix, secunet, m-privacy, itWatch

Tabelle 11 - Technologiebetrachtung Remote-Controlled Browsers System (ReCoBS)

"Unter einem Remote-Controlled Browsers System (ReCoBS) versteht das BSI den Webzugang mit Hilfe von speziell gesicherten Terminalserver-Systemen als modularen Bestandteil von Sicherheitsgateways. Dabei laufen die Browser nicht auf den Arbeitsplatz-PCs, sondern auf einem Terminalserver außerhalb des lokalen Netzwerks (LAN) und werden von den Arbeitsplätzen aus ferngesteuert. Im Browser auf dem Terminalserver werden alle Webinhalte ausgeführt, sodass bei Einhaltung entsprechender Sicherheitsanforderungen aktive Inhalte nicht ins LAN gelangen können." [17, S.3]

Die Technologie ist zwar vorhanden und der deutsche Markt hat ein breites Angebot in diesem Sektor, dennoch ist die Diskrepanz zwischen dem notwendigen und dem realen Einsatz bedauerlicherweise "größer". Dies zeigt auch in der farblichen Markierung des Indikators in der Kategorie D. Hier sollten Überlegungen angestellt werden, wie der Einsatz von ReCoBs-Systemen gefördert werden könnte, um einen höheren Stand der Sicherheit zu erreichen.

Virtuelle Schleuse

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 2	Einschleusen von Schadcode in beliebige Umgebungen mit Hilfe von Dokumenten, Dateien und anderen Trägersystemen	**Ausland:** FireEye (USA) **Deutschland:** itWatch

Tabelle 12 - Technologiebetrachtung Virtuelle Schleuse

Die sogenannte "Virtuelle Schleuse" bildet eine Art Quarantäne-System, um das Einschleusen von Schadcode zu verhindern. Auch die Schäden, die durch reine Unaufmerksamkeit entstehen können, lassen sich mit hoher Wahrscheinlichkeit verhindern. [18]

Die auf diesem Feld aktive Firma aus Deutschland ist ein mittelständisches Unternehmen, das einem Konzern aus den USA gegenüber steht. Die amerikanische Firma FireEye[22] hat etwa 1.000 Mitarbeiter, also etwa zehnmal so viele wie die deutsche Konkurrenz in diesem Bereich. Zu den Geldgebern von FireEye zählt unter anderem Juniper Networks[23]. Obwohl die Bedrohung durch Schadsoftware sehr groß ist, findet diese Technologie in zu wenigen Bereichen Anwendung.

5.1.3 Bereich: Digital Enterprise Security

Dieser Abschnitt behandelt Technologien, die für die Unternehmenssicherheit elementar sind. Hierbei gibt es verschiedene Bereiche, die von Bedeutung sind und deshalb hier berücksichtigt werden.

[22] http://de.wikipedia.org/wiki/FireEye
[23] http://de.wikipedia.org/wiki/Juniper_Networks

Authentifikation

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 1	Identitätsdiebstahl, Missbrauch fremder Identitäten	**Ausland:** RSA (USA), gemalto/SafeNet (USA), Verisign (USA), Atos (Frankreich), Comodo (Großbritannien), GlobalSign (Großbritannien) **Deutschland:** Bundesdruckerei, secunet, Giesecke & Devrient, D-Trust, Deutsche Telekom, Kobil Systems, bremen online services

Tabelle 13 - Technologiebetrachtung Authentifikation

In diesem Bereich sind Technologien gemeint, die eine zuverlässige Authentifikation des Gegenübers ermöglichen. Als Beispiel wäre die Webseite des eigenen E-Mail-Anbieters oder der Bank anzuführen. Es muss bei einem Aufruf eines Dienstes oder einer Webseite für den Nutzer möglich sein zu überprüfen, ob es sich tatsächlich um die erwartete Webseite respektive Dienst handelt oder um eine gefährliche Fälschung. Hierzu gibt es spezielle kryptografische Verfahren und Signierungsmöglichkeiten, die das ermöglichen. Auch der Schutz von Identitäten spielt hier eine Rolle.

Sichere Anbindung zwischen Anbieter und Anwender

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 2	Mitlesen und Auswerten von vertraulichen Daten	**Ausland:** Cisco (USA), Juniper (USA) **Deutschland:** secunet, genua, Sirrix, gateprotect, Innominate, LANCOM

Tabelle 14 - Technologiebetrachtung sichere Anbindung zwischen Anbieter und Anwender

Basierend auf der Authentifikation, welche die Grundlage für diese Kategorie bildet, muss auch die Technologie vorhanden sein, um die sichere Kommunikation vom Anbieter zum Nutzer zu gewährleisten. Diese Kategorie wird abgegrenzt zur VPN-Technologie.

Hardware-Sicherheitsmodul (HSM)

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 3	Angriff auf vermeintlich sichere kryptografische Programmmodule	**Ausland:** gemalto/SafeNet (USA), Thales (Frankreich) **Deutschland:** Utimaco (CryptoServer, bis Kl. 3) secunet (SINA Core, Kl. 4)

Tabelle 15 - Technologiebetrachtung Hardware-Sicherheitsmodul (HSM)

Im Bereich der Hardware-Sicherheitsmodule ist neben einer starken Bedeutung auch das Angebot in Deutschland ausbaufähig. Die Konkurrenz aus dem Ausland ist schlagkräftig. Die Firma gemalto[24] aus den USA hat beispielsweise mehr als 10.000 Mitarbeiter und ist in mehr als 100 Ländern aktiv. Die Firma Thales[25] aus Frankreich mit insgesamt 65.000 Mitarbeitern, wovon alleine in Deutschland 4.500 tätig sind, ist ebenfalls ein "Schwergewicht" und verfügt

[24] https://de.wikipedia.org/wiki/Gemalto
[25] https://de.wikipedia.org/wiki/Thales_Group

auch über gigantische personelle und finanzielle Ressourcen. Natürlich sind die HSM-Produkte nur ein Bereich aus den breiten Produktpaletten der Anbieter, aber diese Zahlen geben trotzdem ein Gefühl für die herrschenden Relationen auf dem Markt. Die deutschen Firmen aus diesem Bereich sind aus der Kategorie Mittelstand und damit deutlich kleiner.

Public-Key-Infrastruktur (PKI)

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
A B C D	alle ab Klasse 2	Fälschen von Identitäten, um sich als Bank oder Institution auszugeben, um das Vertrauen von Anwendern zu erschleichen	**Ausland:** Microsoft (USA), Verizon (USA), OpenTrust (Frankreich), neXus (Schweden), Comodo (Großbritannien), GlobalSign (Großbritannien) **Deutschland:** secunet, zertificon, Bundesdruckerei/D-TRUST, T-Systems/TeleSec, Sirrix, secardeo

Tabelle 16 - Technologiebetrachtung Public-Key-Infrastruktur (PKI)

Die sogenannte Public-Key-Infrastruktur ermöglicht eine sichere und vertrauenswürdige Kommunikation im Internet. Mit Hilfe von PKI können Dokumente und Nachrichten sowohl signiert als auch verschlüsselt werden. Hierbei ist klar ersichtlich, dass die Umstände in Deutschland technologisch fortgeschritten und günstig sind. Die Nutzung von Verschlüsselung ist allerdings viel zu gering und muss in naher Zukunft unbedingt ausgebaut werden.

5.1.4 Bereich: Client- und Serversicherheit

Der nachfolgende Abschnitt beschreibt den Bereich der Client- und Serversicherheit. Hierbei gibt es verschiedene Technologien, die je nach Anforderung und Schutzbedarf unterschiedlich ausfallen können.

Antivirus und Personal Firewall

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
A B C D	alle ab Klasse 0	Schadsoftware-Infektionen, ungewollte Verbindungen nach außen	**Ausland:** Symantec (USA), Kaspersky (Russland), AVG (Niederlande), Panda (Spanien), F-Secure (Finnland), AVAST (Tschechien), Trend Micro (Japan), McAfee/Intel (USA), BullGuard (Großbritannien), Eset (Slowakei), Bitdefender (Rumänien), Ikarus (Österreich), Sophos (Großbritannien) **Deutschland:** Avira, (GData)

Tabelle 17 - Technologiebetrachtung Antivirus und Personal Firewall

Dieses Segment widmet sich den Antivirus-Lösungen und Personal Firewalls. Diese bilden einen heute immer noch wichtigen Faktor auf der Client- und Serverseite.

Die Bedeutung von Antiviren-Software ist für die Zukunft schwächer geworden, da nach Meinung der führenden Antiviren-Hersteller die Erkennungsraten heutzutage unbefriedigend sind. Neue effektivere Technologien sollen dort zukünftig Abhilfe schaffen.

Die zukünftige Bedeutung des klassischen Antiviren-Schutzes ist relativ eingeschränkt. Dieser sollte in den meisten Fällen trotzdem nicht vernachlässigt werden, da er heute und mittelfristig einen bedeutenden Baustein innerhalb eines IT-Sicherheitskonzeptes bilden wird.

In dieser Kategorie dominieren die ausländischen Anbieter den Markt. Innovationen aus Deutschland sind hier im Moment nur wenige in Sicht. Hinzu kommt, dass beispielsweise Antivirenhersteller für eine bessere Erkennung Technologien aus dem Ausland lizenzieren, um diese dann in die eigenen deutschen Produkte zu integrieren (z. B. GData).

Exploit Protection / Sicherer Browser

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
A B C D	alle ab Klasse 1	Angriffe durch infizierte Webseiten, Diebstahl lokaler persönlicher Daten	**Ausland:** Bromium (USA), Invincea (USA) **Deutschland:** Sirrix, secunet

Tabelle 18 - Technologiebetrachtung Exploit Protection / Sicherer Browser

Softwareprodukte mit "Exploit Protection", wie beispielsweise spezielle Browser, sind in der Lage einen Teil der Angriffe aus dem Internet abzuwehren. Dazu gehören zum Beispiel Schadsoftware, in Teilen auch APTs und Zero-Day-Exploits. Sie können dabei helfen den realen Schutz enorm zu steigern.

Natürlich sind Softwareprodukte mit Exploit Protection nicht immun gegen Angriffe jeglicher Art, können aber das Risiko erheblich senken.

In diesem Bereich gibt es eine überschaubare Zahl von Anbietern, die sich gegenüberstehen. Dadurch, dass herkömmliche Softwarelösungen aufgrund von neuen Bedrohungsarten an Effektivität einbüßen, wird diese Art der Lösungen in Zukunft eine immer wichtigere Rolle spielen.

In diesem Bereich besteht eine größere Lücke zwischen Soll- und Ist-Zustand.

Device- und Portkontrolle

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 2	Kopie vertraulicher Dokumente auf beliebige externe Datenträger	**Ausland:** Symantec (USA), McAfee/Intel (USA), DeviceLock (USA), Sophos (Großbritannien), **Deutschland:** itWatch, digitronic, (CenterTools)

Tabelle 19 - Technologiebetrachtung Device- und Portkontrolle

Die "Device- und Portkontrolle" ist heute und in naher Zukunft ein immer größer werdendes Thema, da externe Datenträger zunehmend als Werkzeug für Angriffe und Spionage verwendet werden können.

Dies könnten bösartige Peripheriegeräte sein, welche neben ihrer eigentlichen Tätigkeit als Maus, USB-Stick oder Webcam auch Schadroutinen beherbergen, Stichwort: "BadUSB: Wenn USB-Geräte böse werden"[26]. Solch ein Gerät kann ohne Portkontrolle nach dem Einstecken in einen USB-Port sofort aktiv werden und Schadsoftware auf dem betroffenen IT-System installieren. Ab diesem Zeitpunkt gilt das System als kompromittiert und ist nicht mehr vertrauenswürdig.

Auch der Datendiebstahl ist hier ein Thema: Mit Hilfe von kleinen externen Datenträgern lassen sich leicht Daten in großen Mengen kopieren.

[26] „BadUSB: Wenn USB-Geräte böse werden“ - http://heise.de/-2281098

Full Disk Encryption

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 1	Einsehen von Daten auf verlorenen oder gestohlenen Geräten durch Unbefugte	**Ausland:** Microsoft (USA), McAffee/Intel (USA), Sophos (Großbritannien), Winmagic (Kanada), EgoSecure/Kaspersky (Russland) **Deutschland:** Sirrix, secunet, (CE Infosys), (CenterTools)

Tabelle 20 - Technologiebetrachtung Festplattenvollverschlüsselung

Mit der "Full Disk Encryption" ist die Festplattenvollverschlüsselung gemeint, welche alle verbauten Datenträger in einem System betrifft. Hierbei soll der unbefugte Zugriff durch Dritte unterbunden werden. Diese Technologie bietet Schutz bei Verlust von Geräten durch Unaufmerksamkeit oder Diebstahl. Der sogenannte "Evil Maid Angriff"[27], bezieht sich auf Geräte, die unbeaufsichtigt bleiben, beispielsweise in einem Hotelzimmer.

Hier herrscht nach wie vor noch ein großer Nachholbedarf. Zum einen ist die Verbreitung entsprechender Software "made in Germany" in diesem Segment viel zu gering, zum anderen ist die Möglichkeit die weniger sichere und nicht vertrauenswürdige Alternative "Bitlocker" durch ein höherwertiges Produkt auszutauschen bisher leider nicht gegeben.

File & Folder Encryption

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 1	Diebstahl von Wechseldatenträgern und Extraktion sensibler Daten	**Ausland:** Microsoft (USA), Symantec (USA), Cryptzone (Schweden), Cypherix (Süd-Afrika), DESlock (Großbritannien), Sophos (Großbritannien) **Deutschland:** apsec, itWatch, Sirrix, Secomba, digitronic, Brainloop, ContentPro

Tabelle 21 - Technologiebetrachtung File & Folder Encryption (Objektverschlüsselung)

Die folgende Kategorie beschreibt ebenfalls Verschlüsselung, jedoch mit dem Fokus auf einzelne Objekte. Das könnten einzelne Dokumente oder Container sein, die sicher weitergegeben und ausgetauscht werden sollen. Hier muss sichergestellt werden, dass niemand außer den autorisierten Personen Zugriff auf die geschützten Informationen erhält. Dies kann je nach Wirkungsklasse persönliche Daten von Bürgern gefährden oder im schlimmsten Fall die nationale Sicherheit betreffen.

[27] „(…) evil maid attack concisely describes the scenario: if the owner leaves a computer unattended in a hotel room“ - http://testlab.sit.fraunhofer.de/content/output/project_results/bitlocker_skimming/

Voll-Virtualisierung / Trusted Computing, Separation

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 2	Infektion oder Angriffe auf einen Rechner kompromittieren das gesamte System	**Ausland:** oklabs/General Dynamics (USA), Oracle (USA), Lynx Software Technologies (USA), Bromium (USA), Microsoft (USA), Intel (USA), BlackBerry (Kanada), Sysgo/Thales (Frankreich), **Deutschland:** secunet, Sirrix, genua, Telekom

Tabelle 22 - Technologiebetrachtung Voll-Virtualisierung/Trusted Computing, Separation

Diese Technologie ist dazu bestimmt, sichere Betriebssysteme zu entwerfen und zu betreiben. Zusätzlich ermöglicht sie es, hochgradig sichere Virtualisierungslösungen zu konzipieren. Innerhalb von Systemen, die auf dieser Technologie basieren, spielen oft kritische Dienste eine Rolle. Sie verhindern eine übergreifende Kompromittierung von Systemen, die gemeinsam auf der gleichen Hardwarebasis ihren Dienst verrichten. In Zukunft wird diese Technologie innerhalb der Architektur von Betriebssystemen eine wesentlichere Rolle spielen. Mit Hilfe der Separation lassen sich Anwendungen getrennt voneinander sicher betreiben. Wird eine Anwendung innerhalb eines separierten Teils durch einen erfolgreichen Angriff kompromittiert, hat dies keinerlei Auswirkungen auf alle anderen Anwendungen und Routinen auf dem gleichen IT-System.

Diese Technologie ist in vielen Bereichen bereits heute erfolgreich im Einsatz. Dabei handelt es sich um eine wesentliche Schlüsseltechnologie, bei der vor allen die USA eine führende Rolle spielen.

Data Leakage Prevention

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 2	Abfluss hochsensibler Daten nach außen	**Ausland:** Symantec (USA), RSA (USA), Websense (USA), Verdasys (USA) **Deutschland:** itWatch, iT-Cube Systems, genua, Brainloop, ContentPro

Tabelle 23 - Technologiebetrachtung Data Leakage Prevention

Die Data Leakage Prevention verhindert den Abfluss sensibler Daten nach außen. Sie ist auch als "Data Loss Prevention" bekannt. Dadurch soll der Datendiebstahl effektiv verhindert werden.
Neben der Schulung und Sensibilisierung der eigenen Mitarbeiter werden technische Sicherheitsmaßnahmen getroffen, welche Datenträger, verschiedene Ausgabesysteme und die bekannte Copy & Paste Funktion reglementieren können.

Wie die Tabelle aufzeigt, kommt die Konkurrenz hier größtenteils aus den USA.

E-Mail-Verschlüsselung

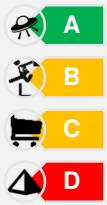
Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 0	Abfangen, Mitlesen und Manipulieren von E-Mail-Korrespondenz	**Ausland:** Microsoft (USA), Symantec (USA) **Deutschland:** Telekom/Telesec, Sirrix, Giegerich & Partner, cryptovision, secardeo, zertificon

Tabelle 24 - Technologiebetrachtung E-Mail-Verschlüsselung

Anzumerken ist, dass De-Mail hierbei keine Rolle spielt und keine Berücksichtigung findet, da bei der De-Mail zwar eine Transportverschlüsselung verwendet wird, der Inhalt jedoch im Klartext auf dem Server des Betreibers vorliegt und an jeder Stelle, an der die E-Mail gespeichert wird, von Dritten eingesehen und gelesen werden kann. Sie ist also per Definition unsicher. Hinzu kommt, dass die De-Mail inkompatibel zum etablierten E-Mail-System ist und Nutzer beider Systeme technisch nicht in der Lage sind, untereinander zu kommunizieren.

Vielmehr ist die hier bewertete Technologie für eine vertrauliche und sichere E-Mail-Kommunikation zwischen Kommunikationspartnern maßgeblich. Dabei wird der Inhalt der Korrespondenz erst beim Verfasser verschlüsselt und dann übertragen. Nur der Adressat ist in der Lage, die Nachricht zu entschlüsseln und sie zu lesen. Die Metadaten werden dabei jedoch nicht geschützt.

Die Sicherheit eines solchen Systems hängt von vielen Faktoren ab. Zum einen ist der für die Verschlüsselung verwendete Algorithmus wesentlich, zum anderen natürlich auch die Vertrauenswürdigkeit der Umgebung, auf der sich die für die Verschlüsselung notwendigen geheimen Schlüssel befinden. Lassen sich die Schlüssel durch eingebaute Hintertüren entwenden, kann die gesamte stattfindende Korrespondenz entschlüsselt und gelesen werden. Dies lässt sich durch eine mehrstufige Authentifikation effektiv vermeiden.

Die Analyse zeigt deutlich, dass hier in allen Bereichen ein großer Nachholbedarf besteht.

Sicheres Logon (Smartcard etc.)

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 1	Nicht autorisierte Nutzung von Geräten	**Ausland:** RSA (USA), gemalto/SafeNet (USA), gemalto (Niederlande), Atos (Frankreich) **Deutschland:** Telesec, secunet, Giesecke & Devrient, Bundesdruckerei/D-TRUST, Sirrix, digitronic, itWatch

Tabelle 25 - Technologiebetrachtung Sicheres Logon (Smartcard etc.)

Im Bereich des sicheren Logons sind insbesondere Lösungen wie Smartcards gemeint, mit Hilfe derer sich die Identität einer Person und gleichzeitig die Befugnis für die Nutzung eines Gerätes oder das Betreten einer Räumlichkeit feststellen lassen.

Remote Access / Secure VPN

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 2	Belauschen der Kommunikation zwischen Host und entfernter Maschine	**Ausland:** Cisco (USA), Juniper (USA) **Deutschland:** NCP, secunet, HOB, genua, Innominate, LANCOM

Tabelle 26 - Technologiebetrachtung Remote Access / Secured VPN

Die VPN-Technologie bzw. der "Remote Access" ist notwendig, um eine vorübergehende und sichere Verbindung zwischen zwei Endpunkten zu etablieren.

Im Gegensatz zu normalen VPN-Technologien für gesicherte Netzwerktunnel sind die Remote Access Lösungen darauf optimiert, unabhängig von Standort und Übertragungstechnik beispielsweise gesicherte Fernwartungskanäle für Industrieanlagen zu ermöglichen. Hierbei sind insbesondere Industrieroboter und Windräder als mögliche Einsatzorte zu nennen.

Da es sich bei diesen Punkten meist um Übergänge zwischen den eigenen Netzwerken und dem Internet handelt, sind hier vertrauenswürdige Technologien sehr essenziell. Die ausländischen Konzerne aus diesem Bereich sind meist US-Firmen.

5.1.5 Bereich: Mobile Security

Dieser Bereich betrifft die mobile Sicherheit, bei der alle möglichen Geräte aus dieser Kategorie betroffen sein können. Hierzu zählen Smartphones, Tablets, Notebooks und demnächst auch neue Geräteklassen wie zum Beispiel Smartwatches und im allgemeinen "Wearables".

App Security / Secure Marketplace

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 2	Einschleusen von bösartigen Apps, um Daten auf mobilen Geräten auszuspähen	**Ausland:** Bitdefender (Rumänien), Sophos (Großbritannien), Samsung (Südkorea) **Deutschland:** Avira

Tabelle 27 - Technologiebetrachtung App Security / Secure Marketplace

Aufgrund immer größerer Verbreitung von Smartphones nimmt auch die Relevanz dieser Geräte im Businessumfeld deutlich zu. Die verhältnismäßig kleinen Geräte, die den Nutzer immer und überall begleiten, sind gleichzeitig auch Geheimnisträger geworden und beinhalten sehr viele persönliche und geschäftliche Daten.

Durch nachträglich installierte Applikationen (Apps) werden mobile Endgeräte personalisiert und den Bedürfnissen ihrer Nutzer angepasst Dadurch steigt aber die Gefahr an, denn das Personalisieren ist nur durch die Installation von Apps möglich. "Vor dem Herunterladen einer App (…) muss der Nutzer entscheiden, ob er der App den Zugriff auf weitere Daten wie Kontakte, E-Mails, Fotos, Anmeldedaten (…) erlaubt. Dies ist problematisch, da die Nutzer nicht über Weiterverarbeitung der gesammelten Daten informiert werden und keinerlei Kontrolle darüber haben, welche Daten wie oft abgerufen, übertragen und verarbeitet werden." [19, S.10–11]

In solch einem Fall stellt sich die Frage nach einer möglichen vertrauenswürdigen Quelle für Apps.

Ein Verbot von mobilen Geräten wird dabei nicht als sinnvoll erachtet: "Gerade Unternehmen sollten ihren Mitarbeitern für die erhöhte Produktivität Smart Mobile Devices (SMDs), aber mit den nötigen Schutzfunktionen, zur Verfügung stellen." [19, S.14]

Für diesen Zweck bietet es sich an, mit Hilfe von Secure Marketplaces, App-Security-Mechanismen, starker Eingrenzung der verfügbaren Apps oder der Prüfung von Apps auf Vertrauenswürdigkeit das Risiko sich eine schädliche App "einzufangen", zu minimieren. Die Szenarien sind oft sehr komplex und die Problematik erfordert viel Aufwand.

Die Analyse offenbart in Deutschland deutliche Defizite. Die Anbieter aus dem Ausland sind hier in größerer Zahl vorhanden und treten sogar als Produzenten von Hardware auf. So können sie ihre Produkte perfekt aufeinander abstimmen (z. B. Samsung).

Sichere Plattform

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
A B C D	alle ab Klasse 2	Angriffe auf qualitativ mangelhafte Softwarekomponenten eines Systems	**Ausland:** Secusmart/Blackberry (Kanada), Blackphone (Schweiz), Thales (Frankreich) **Deutschland:** Telekom, Sirrix

Tabelle 28 - Technologiebetrachtung Sichere Plattform

Die Kategorie "Sichere Plattform" beschreibt Basistechnologien, die in verschiedenen Bereichen zum Zuge kommen. Dies können beispielsweise vertrauenswürdige Sicherheitsplattformen für Smartphones sein, ohne die keine vollständig sicheren und vertrauenswürdigen Smartphones für sicherheitsrelevante Umgebungen und Geheimnisträger denkbar wären. Durch die Akquisition des deutschen Anbieters Secusmart durch das kanadische Unternehmen Blackberry, ist die nationale Souveränität in diesem Bereich deutlich geschwächt worden.

Cloud Encryption

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
A B C D	alle ab Klasse 0	Ausspähen von Daten und Diebstahl geistigen Eigentums durch Dritte (Firmen, Mitarbeiter, Geheimdienste)	**Ausland:** Spideroak (USA), CipherCloud (USA), Trend Micro (Japan) **Deutschland:** Sirrix, Telekom, itWatch, Secomba, digitronic, Brainloop, ContentPro, secardeo

Tabelle 29 - Technologiebetrachtung Cloud Encryption (Cloud Verschlüsselung)

Viele Unternehmen und Privatpersonen nutzen Cloud-Dienste oft und gerne. Die Vorteile sind dabei offensichtlich: Die Handhabung ist einfach, die Verfügbarkeit der Daten erhöht sich, auf allen Geräten sind die Dokumente vorhanden und im Falle eines Hardwareausfalls bleiben die Daten bestehen und lassen sich im Notfall sogar ohne eigenes Endgerät über einen beliebigen Browser abrufen.

Die Server dieser Cloud-Anbieter befinden sich oftmals an nicht genau nachvollziehbaren Standorten. Bei genauerer Betrachtung aller Cloud-Dienste weltweit, lässt sich feststellen, dass schätzungsweise 90% aller Server in den USA zu finden sind. Dadurch drängt sich natürlich die Frage auf, was mit den dort abgelegten Daten tatsächlich passiert.

Dies ist vor allem dann genau zu prüfen, wenn es sich um kritische Daten aus Industrie und Wirtschaft handelt. Hierbei ist vollkommen klar, dass Nachrichtendienste und Regierungen Zugriff haben und mitlesen können – offiziell oder inoffiziell.

Abhilfe kann mit eigenen lokal verwalteten Cloud-Diensten oder der "Zero-Knowledge-Technik" geschaffen werden, bei der mit Hilfe von Kryptografie und passenden Werkzeugen die Daten erst verschlüsselt und dann in die Cloud hochgeladen werden. Der Anbieter hat dabei jedoch aufgrund der Verschlüsselung beim Client keinerlei Einsicht in die Daten und sieht im Zweifelsfall nur "Datenmüll". In diesem Bereich gibt es zahlreiche Anbieter aus Deutschland, die sich auf diese Art der Verschlüsselung spezialisiert haben.

In den USA gibt es keinen mit Deutschland vergleichbaren Datenschutz. Dies hat zur Folge, dass personenbezogene Daten eigentlich nicht dorthin übertragen werden dürften. Unter diesem Vorbehalt wäre die Nutzung US-amerikanischer Cloud-Dienste nicht möglich. Um dem entgegenzuwirken und die Übermittlung von personenbezogenen Daten in die USA zu ermöglichen, hat die EU speziell für diesen Zweck den sogenannten "Safe-Harbor-Pakt" beschlossen.

Alle daran teilnehmen Unternehmen verpflichten sich, den dort geforderten Richtlinien zum Datenschutz zu genügen. Allerdings ist das Safe-Harbor-Abkommen[28] hier offenbar eher als ein Papiertiger zu sehen: "(…) zum Safe-Harbor-Abkommen kam eine Untersuchung im Auftrag des Unabhängigen Landeszentrums für Datenschutz in Schleswig-Holstein Anfang des Jahres zu dem Ergebnis, dass diese Vorschriften das Papier nicht wert sind, auf dem sie gedruckt wurden." [20]

Das Safe-Harbor-Abkommen selbst bietet demnach keinen nennenswerten Schutz. Zudem herrscht oftmals Unklarheit über die Zugriffsmöglichkeiten unbefugter Personen auf die Daten in der Cloud. Aus diesem Grund sollte die Nutzung zusätzlicher Verschlüsselungstechnologien breitere Anwendung finden.

Voice Encryption

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
A B C D	alle ab Klasse 0	Ausspähen von Gesprächen	**Ausland:** Whisper Systems (USA), BlackBerry/Secusmart (Kanada), Sectra (Schweden), Skype/Microsoft (USA) **Deutschland:** GSMK, Rohde & Schwarz, Sirrix, HOB

Tabelle 30 - Technologiebetrachtung Voice Encryption (Sprachverschlüsselung)

Im Bereich der Sprachverschlüsselung gibt es verschiedene Anbieter aus dem In- und Ausland. Durch den Verlust von Secusmart ist der deutsche Markt bedeutend geschwächt worden. Es wäre wünschenswert, wenn hier weitere sichere und qualitativ hochwertige Lösungen entstehen würden, denn aus dem Ausland stammende Produkte in diesem Bereich sind per Definition als nicht vertrauenswürdig einzustufen und für Geheimnisträger nicht geeignet.

[28] http://www.faz.net/aktuell/feuilleton/medien/safe-harbor-ein-versprechen-ohne-wert-13100247.html

Secure Instant Messaging

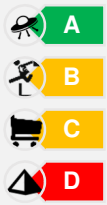
Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 0	Mitschneiden und Auswerten aller Inhalte textueller Kommunikation	**Ausland:** Open Whisper Systems (USA), BlackBerry (Kanada), Threema (Schweiz), Brosix (Bulgarien), Facebook (USA) **Deutschland:** GSMK, Sirrix, Chiffry, shape.ag

Tabelle 31 - Technologiebetrachtung Secure Instant Messaging

Der Bereich des Secure Instant Messaging spielt heute eine sehr große Rolle und hat für einen deutlichen Rückgang der sonst sehr starken Nutzung von SMS gesorgt. Die Messenger-Tools wie WhatsApp und Co. sind unkompliziert, schnell und zuverlässig und vor allem größtenteils kostenlos. Leider haben die meisten von ihnen auch ein Vertrauenswürdigkeitsproblem, denn die Nachrichten werden entweder unzureichend oder überhaupt nicht verschlüsselt und die Server stehen zumeist in den USA.

In diese Kerbe schlagen seit einiger Zeit die Secure Messenger, welche zwar das gleiche Prinzip anbieten wie ihre Vorgänger, jedoch kommen hier starke Verschlüsselungsverfahren zum Einsatz, die es ermöglichen eine vertrauenswürdige und sichere Kommunikation zu betreiben, ohne die Einsicht durch Dritte zu riskieren.

Die größten Vertreter stammen hier jedoch aus dem Ausland und die Marktanteile der deutschen Anbieter sind noch verhältnismäßig gering. Zudem findet diese Technik leider noch zu wenig Einsatz durch die Anwender.

Mobile Device Management

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 2	Angriffe auf mobile Geräte aufgrund von Schwachstellen durch mangelnde Wartung oder Diebstahl	**Ausland:** Airwatch/VMWare (USA), MobileIron (USA), Good Technology (USA), Fiberlink/IBM (USA), Citrix (USA), Symantec (USA), Sophos (Großbritannien), Soti (Kanada), EgoSecure/Kaspersky (Russland) **Deutschland:** Sirrix, Seven Principles, HOB

Tabelle 32 - Technologiebetrachtung Mobile Device Management

"Mobile Device Management-Anwendungen (MDM) greifen auf Schnittstellen, die das Betriebssystem bereitstellt, zu, um SMDs zentralisiert administrieren und konfigurieren zu können." [19, S.13]

Mobile Endgeräte beinhalten die Gefahr, dass ihre Nutzung innerhalb eines Unternehmers mangels Überblick durch den Verantwortlichen, außer Kontrolle gerät. Gefahren und Stolperfallen bei der Nutzung wären beispielsweise: Geräte gehen verloren, es wird versucht bedenkliche Apps zu installieren und Geräte werden teilweise weder verschlüsselt noch wird eine Bildschirmsperre verwendet. So kann der einfache Mitarbeiter durch die falsche Nutzung seines mobilen Endgerätes eine Gefährdung für die Datensicherheit des gesamten Unternehmens darstellen.

Um diesem Problem zu begegnen, bieten sich MDM-Lösungen an: "Im Bereich der sicherheitsrelevanten Konfigurationseinstellungen gewährleisten MDM-Lösungen insbesondere die einheitliche Sicherheitskonfiguration und helfen, die freie Konfigurier- und Erweiterbarkeit in gewissen Rahmenbedingungen einzuschränken." [19, S.13]

Basistechnologie (Secure Execution Environment)

Bewertung	erforderlich ab	Bedrohungen	In- und Ausländische Anbieter
	alle ab Klasse 3	Angriff auf Systemebene und Ausspähen von Daten durch Unbefugte	**Ausland:** Samsung (Südkorea), Trustonic (Großbritannien), SecuSmart/Blackberry (Kanada) **Deutschland:** Giesecke & Devrient

Tabelle 33 - Technologiebetrachtung Basistechnologie (Secure Execution Environment)

Die Kategorie "Secure Execution Enviroment" ist als grundsätzliche Basistechnologie zu sehen, die in verschiedenen Produkten und Lösungen zum Einsatz kommt und als Fundament dient, um diese sicher und vertrauenswürdig gestalten zu können. Sie ermöglicht es beispielsweise vertrauenswürdige Umgebungen auf mobilen Endgeräten zu schaffen und den unautorisierten Zugriff durch Unbefugte im Verlustfall zu verhindern. Die Sicherheit der Information auf solch einem IT-System hängt maßgeblich von der Qualität der eingesetzten Basistechnologie ab.

Damit wird auch die Wichtigkeit und Relevanz klar: Ist beispielsweise ein IT-Sicherheitsprodukt aus Deutschland mit Hilfe einer ausländischen Basistechnologie entwickelt worden, könnte hier eine Hintertür offenstehen, die so nicht gewollt ist und eine große Gefahr darstellt. In diesem Fall würde in einem Worst-Case-Szenario das darauf aufbauende IT-Sicherheitsprodukt ad absurdum geführt.

5.1.6 Gesamtauswertung nach Bewertungskriterien

Nachfolgend wurde über alle einzelnen Kategorien hinweg eine Durchschnittsbewertung für jeden einzelnen Bereich akkumuliert und ein Durchschnitt gebildet. Hierbei war das Ziel über alle Bereiche hinweg ein zusammenfassendes Ergebnis zu erhalten, welches möglichst die reale Situation abbilden soll. Das Ziel dabei ist es, sichtbar zu machen, an welcher Stelle Handlungsbedarf besteht und wie schwerwiegend Defizite und Probleme sind.

Durchschnitt: Sichere Vernetzung

Nachfolgend ist in Abbildung 7 der Durchschnitt für den Bereich der **sicheren Vernetzung** zu finden.

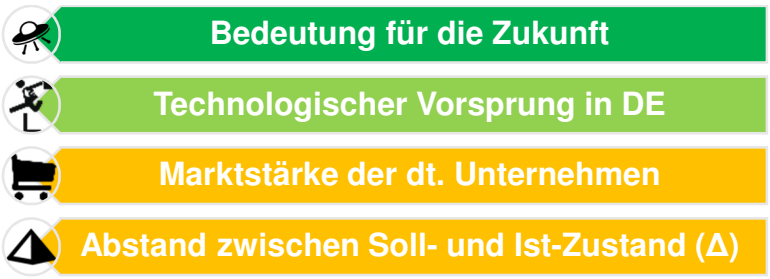


Abbildung 7 - Durchschnitt für den Bereich: Sichere Vernetzung

Hierbei wird deutlich, dass die Bereiche der Marktstärke und der des Soll- und Ist-Zustands in jedem Fall noch Aufmerksamkeit benötigen.

Durchschnitt: Sicherer Internetzugang

In der nachfolgenden Abbildung 8 befindet sich der Durchschnitt für den Bereich **sicherer Internetzugang**.

Abbildung 8 - Durchschnitt für den Bereich: Sicherer Internetzugang

In dieser Kategorie wird deutlich, dass starke Defizite in allen praktischen Bereichen herrschen. Insbesondere die Marktstärke der ausländischen Unternehmen übertrifft die der Deutschen bei Weitem. Hier besteht sehr starker Handlungsbedarf, um diese Defizite mittelfristig zu beheben. Insbesondere in diesen Bereichen sind innovative Lösungen bedeutend, bei denen die Forschung aus Deutschland einen wertvollen Beitrag leisten kann.

Durchschnitt: Digital Enterprise Security

Die nachfolgende Abbildung 9 zeigt den Durchschnitt für **Digital Enterprise Security**.

Abbildung 9 - Durchschnitt für den Bereich: Digital Enterprise Security

Die deutschen Unternehmen sind hier nicht schlecht aufgestellt. Die zur Verfügung stehenden Technologien finden jedoch nicht im ausreichenden Maße den Weg zu den betroffenen Anwendern.

Durchschnitt: Client- und Serversicherheit

Die Abbildung 10 stellt den Durchschnitt für die **Client- und Serversicherheit** dar.

Abbildung 10 - Durchschnitt für den Bereich: Client- und Serversicherheit

In diesem Bereich sind die deutschen Unternehmen ebenfalls nicht so stark positioniert, wie die Konkurrenz aus dem Ausland. Zudem müssen auch hier die Technologien und Produkte den Weg zum Anwender finden.

Durchschnitt: Mobile Security

Die Abbildung 11 zeigt als letzte den Durchschnitt für die **mobile Sicherheit.**

Abbildung 11 - Durchschnitt für den Bereich: Mobile Security

Die mobile Sicherheit ist ein relativ junges Feld und hat eine extrem starke Bedeutung für die Zukunft. Nach einigen Konsolidierungen des Marktes und Innovationen aus dem Ausland, ist hier in Zukunft der Handlungsbedarf in jedem Fall groß. Zum einen muss vermieden werden, dass hier in den beiden "gelben" Bereichen die Farbe "rot" sichtbar wird und zum anderen ist die Akzeptanz der Nutzer für die aktuellen Produkte relativ gering. Dies liegt oft an der Komplexität und dem dadurch erzeugten Aufwand oder der Unklarheit, was das Richtige für den Anwender ist.

Durch die starke Verbreitung mobiler Geräte und der immer weiter steigenden Anzahl an Diensten, Geräten und Bandbreiten, steht die IT-Sicherheitsindustrie in diesem Bereich noch am Anfang der Entwicklung.

Komplettübersicht als Gesamtmatrix

Die Nachfolgende Tabelle 34 zeigt in einer möglichst kompakten Darstellung die Gegenüberstellung aller Technologiebereiche in einer Matrix und ermöglicht eine direkte Vergleichbarkeit untereinander. Sie greift dabei noch einmal die zuvor gebildeten Durchschnittsergebnisse auf. Insbesondere soll sie durch diese Kompakte Darstellung möglichst übersichtlich Defizite aufdecken und dabei behilflich sein, herauszufinden an welcher Stelle noch Handlungsbedarf für die einzelnen Gruppen und die umsetzenden Verantwortlichen besteht.

	Sichere Vernetzung	Sicherer Internet-zugang	Digital Enterprise Security	Client- und Serversicherheit	Mobile Security
Bedeutung für die Zukunft					
Technologischer Vorsprung in DE					
Marktstärke der dt. Unternehmen					
Abstand zwischen Soll- und Ist-Zustand (Δ)					

Tabelle 34 - Übersicht aller Ergebnisse im Durchschnitt als Gesamtmatrix

Zusätzlich zur Gesamtmatrixdarstellung des Durchschnitts wurde in der Tabelle 35 eine detaillierte Gesamtübersicht zusammengestellt, welche alle Technologien, unabhängig von ihrem Bereich, noch einmal gegenüberstellt. Dies bietet eine kompakte Gesamtsicht auf die Gebiete der IT-Sicherheitsindustrie.

	Bedeutung für die Zukunft	Technologischer Vorsprung in DE	Marktstärke der dt. Unternehmen	Abstand zwischen Soll- und Ist-Zustand (Δ)
Sichere Anbindung mobiler User / Telearbeiter				
Layer3-VPN				
Layer2-Encryption				
Datendiode				
Firewall				
IPS/IDS				
Sicherer Browser/ReCoBS				
Virtuelle Schleuse				
Authentifikation				
Sichere Anbindung zwischen Anbieter und Anwender				
Hardware-Sicherheitsmodul (HSM)				
Public-Key-Infrastruktur (PKI)				
AV und Personal Firewall				
Exploit Protection / Sicherer Browser				
Device und Portkontrolle				
Full Disk Encryption				
File & Folder Encryption				
Voll-Virtualisierung / Trusted Computing, Seperation				
Data Leakage Prevention				
E-Mail-Verschlüsselung				
Sicheres Logon (Smartcard etc.)				
Remote Access / Secured VPN				
App Security / Secure Marketplace				
Sichere Plattform				
Cloud Encryption				
Voice Encryption				
Secure Instant Messaging				
Mobile Device Management				
Basistechnologie (Secure Execution Environment)				

Tabelle 35 - Übersicht aller Einzelergebnisse im Detail als Gesamtmatrix

Wie diese Tabelle ebenfalls deutlich aufzeigt, spielen beinahe alle betrachteten Bereiche eine wichtige Rolle für die Zukunft, doch gibt es trotzdem viele Lücken und Probleme.

Eine genauere Betrachtung der Tabelle zeigt, welche Bereiche in naher Zukunft unbedingt gefördert werden müssen. Es wird deutlich, dass insbesondere die Bereiche E-Mail-Verschlüsselung, Secure Instant Messaging und die Basistechnologien große Aufmerksamkeit und Förderungsmaßnahmen 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 stechen hier über alle Technologiebereich hinweg der Abstand und die herrschende Lücke zwischen dem Soll-Ist-Vergleich der einzelnen IT-Sicherheitstechnologien.

Positiv ist hier, dass alle betrachteten Bereiche mit ihrer dunkelgrünen Markierung klar aufzeigen, dass sie allesamt ohne Ausnahme bedeutend für die Zukunft sind. Dies ist als ein positives Signal zu werten und zeigt, dass sich die IT-Sicherheitsindustrie in den richtigen Bereichen bewegt.

5.1.7 Interpretation der Analyse

Die Technologieanalyse zeigt in jedem Fall einige Stärken der deutschen IT-Sicherheitsindustrie, jedoch auch viele Schwächen. Vor allem aber zeigt sie eines: Die ausgesprochen starke Dominanz der amerikanischen Firmen in vielen Bereichen, in denen vertrauenswürdige Technologien essenziell wichtig sind. Es sollte klar sein, dass grundsätzlich jeder Technologie aus den USA misstraut werden muss. Dieser Umstand unterstreicht nochmals die Wichtigkeit der IT-Sicherheitsstrategie und den notwendigen sichtbar gewordenen Handlungsbedarf der IT-Sicherheitsindustrie.

Auf der einen Seite muss sich jeder, der ausländische Technologien nutzt, darüber im Klaren sein, dass es dort ein riesiges Vertrauensproblem gibt – auf der anderen Seite zeigt die Analyse ganz deutlich, dass die dortige Konkurrenz nach wie vor finanziell und personell über gigantische Ressourcen verfügt, die nicht nur in die Produktsicherheit investiert werden, sondern die auch in Marketing und die Lobbyarbeit fließen.

Die Konsequenz daraus ist: Neben der geforderten Austauschbarkeit von Produktfunktionalitäten als gestecktes Ziel, sollte das jetzige Ergebnis der Technologieanalyse durch weitere strategische Überlegungen massiv verbessert und ausgebaut werden.

5.2 Besondere Kompetenzen in Deutschland

Aus der tabellarischen Technologieanalyse lassen sich neben offenkundigen Defiziten auch Stärken und besondere Kompetenzen ableiten. Die deutsche IT-Sicherheitsindustrie hat ihre Stärken in den Bereichen Sicherheitskerne, welche z. B. für sicheres Booten oder Separierungstechnologien benötigt werden. Auch Security Token in Form von Smartcards oder Hardware-Sicherheitsmodule sind eine besondere Kompetenz, sowie auch Verschlüsselungstechnologien für Kryptohardware, Kommunikations- und Objektverschlüsselung.

Die Stärke der deutschen Unternehmen, wie in der Abschlussbetrachtung der Technologieanalyse ersichtlich, ist jedoch noch nicht dort, wo sie sein sollte. Der technologische Vorsprung an sich, spiegelt nicht die hohen Kompetenzen in Form eines hohen Verbreitungsgrades der Produkte und einem großen Angebot wieder.

An dieser Stelle könnte jedoch die später noch diskutierte Idee des "IT Security Replaceability" helfen, die beiden Kategorien B und C der Technologieanalyse auf ein besseres Maß anzuheben.

Zudem gibt es mittlerweile auch proaktive IT-Sicherheitstechnologien zur Exploitbekämpfung und Technologien zur Abwehr von Schadsoftware, Firewall-Technologien für Perimeter-Sicherheit für Infrastrukturen und Netzwerke verschiedener Größen.

Ein weiterer Bereich in dem es wesentliche Kompetenzen gibt, sind Technologien für sichere Identitäten, die die Grundlage für Vertrauen im Internet bilden. Diese gibt es beispielsweise in Form von PKI (Public Key Infrastruktur), TrustCentern und Frühwarnsystemen, die eine neue Form von Angriffserkennung und Lagebildgenerierung bieten.

Die besonderen Kompetenzen dürfen nicht darüber hinwegtäuschen, dass auch weiterhin in den meisten Bereichen der IT-Sicherheitsbranche dringender Handlungsbedarf besteht. So muss auch weiterhin in Forschung investiert werden, um Innovationen zu schaffen.

Die ausländische Konkurrenz ist in vielen Bereichen auf dem Vormarsch. Dort fehlende Innovationen oder fehlendes Know-how werden durch Firmenübernahmen kompensiert. Das unterstreicht der folgende Punkt noch einmal: "Deutsche IT-Sicherheitsunternehmen sind weltweit führend bei der Herstellung von Produkten, die höchsten Ansprüchen im Hinblick auf Vertrauenswürdigkeit und Informationssicherheit genügen." [14]

Ein positives Beispiel und einmalig auf dem Markt sind Technologien zur Kommunikationslagebildgenerierung, die sich im Institut für Internet-Sicherheit[29] seit etwa sieben Jahren an der Westfälischen Hochschule in Gelsenkirchen in der Entwicklung befinden und auf breites Interesse in der Industrie und bei Behörden stoßen. Hiermit ist es beispielsweise möglich, für ein Netzwerk beliebiger Größe mit Hilfe von Sonden ein Lagebild zu erstellen, das dabei hilft sowohl Gefahren und Anomalien zu erkennen als auch verschiedene Zeitpunkte miteinander vergleichbar zu machen. Auch ist es möglich, die eigene Lage für eine bessere Beurteilung anonym mit anderen Lagebildern von anderen Teilnehmern zu vergleichen. Es ist dabei unmöglich auf Inhaltsdaten zuzugreifen oder diese zu analysieren.

Hierbei wurde auch der Landes- und Bundesdatenschutzbeauftragte hinzugezogen. Dieses System ist in Deutschland entstanden und optimal auf den in Deutschland sehr hohen Datenschutzmaßstab ausgelegt.

5.3 Handlungsempfehlungen

Es ist vollkommen offensichtlich, dass die bisher aufgezeigten Herausforderungen Handlungen erfordern. Dabei sind die Adressaten klar zu benennen. Die Ohnmacht der Politik und die Defizite in der IT-Sicherheitsindustrie sprechen eine deutliche Sprache: Wir befinden uns offenkundig in einer Krise.

29 Das Institut für Internet-Sicherheit - if(is) ist eine Innovative, unabhängige und wissenschaftliche Einrichtung der Westfälischen Hochschule - https://www.internet-sicherheit.de/

"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." [13]

Nun gilt es also einen Pfad aus dieser Krise zu finden.

Neben allen anderen in Frage kommenden Ministerien sind die Adressaten insbesondere:

- Bundesministerium für Wirtschaft und Energie (BMWi)
- Bundesministerium des Inneren (BMI)

Natürlich aber auch:

- Industrie
- Anwender

Hierbei müssen die unterschiedlichen Anforderungen der einzelnen Länder berücksichtigt werden. Unabkömmlich ist dabei, dass sich alle Ministerien und Gruppen auf ein klares Ziel einigen und dieses dann gleichzeitig und gemeinsam angehen. Nur in diesem Fall können die hier gemachten Vorschläge und Ideen effektiv umgesetzt werden. Details zur Zielführung finden sich im Kapitel "Umsetzungsvorschlag", in dem eine konkrete Strategie zur Lösungsfindung gegeben wird.

6 IT-Sicherheitsstrategie für Deutschland

Für die Erhöhung des IT-Sicherheitsniveaus in nachhaltiger Art und Weise auf einen jeweils angemessenen Stand wird eine ausgearbeitete Strategie benötigt, die nachfolgend vorgestellt werden soll. Hierbei wird auf vorhandene IT-Sicherheitsprozesse und -technologien zurückgegriffen und im Bedarfsfall IT-Sicherheitslösungen für neue Problemstellungen erarbeitet. Dabei ist der Fokus jedoch auf einen wichtigen Punkt zu legen: Es müssen in erster Linie aus Deutschland stammende, hochwertige und wirkungsvolle IT-Sicherheitstechnologien und -prozesse berücksichtigt werden. Die Gründe hierfür sind vielfältig und werden später nochmals im Detail aufgegriffen und diskutiert. Hierbei werden die etablierten IT-Systeme und -Lösungen der jeweiligen internationalen Hersteller konstruktiv in die IT-Sicherheitsstrategie eingebunden.

Hierbei spielt die Idee "**IT Security Replaceability**" im Sinne der Austauschbarkeit für die Zukunft eine gewichtige Rolle. Denn herstellereigene Komplettlösungen erfüllen in mancher Hinsicht nicht die notwendigen Kriterien. Die Vertrauenswürdigkeit ist zum heutigen Zeitpunkt nicht immer gegeben respektive überprüfbar. Darauf wird im Kapitel Unterschiedliche Wirkungsaspekte näher eingegangen.

Wie in der nachfolgenden Abbildung 12 dargestellt, bleibt die Frage nach der Vertrauenswürdigkeit heutzutage fast immer unbeantwortet.

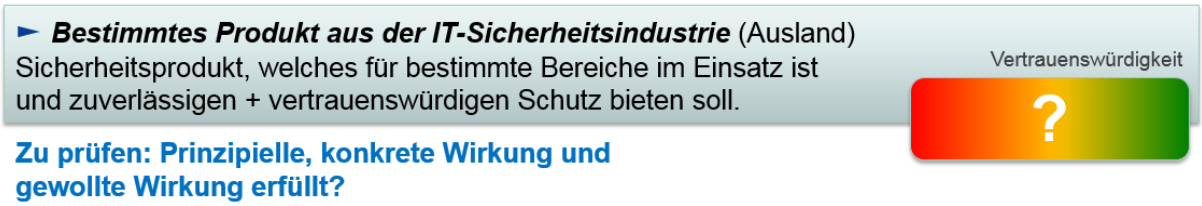


Abbildung 12 - Prinzipielle Einstufung der Vertrauenswürdigkeit und Wirkung

Hersteller aus dem Ausland sind selten bereit, die Wirkung ihrer Produkte überprüfbar zu machen oder sie so transparent und austauschbar zu gestalten, dass der Nutzer sich selbst ein Bild machen kann, um sich im Zweifelsfall für ein deutsches Produkt zu entscheiden.

IT Security Replaceability

Die Idee der "IT Security Replaceability" fordert die Ersetzbarkeit und Austauschbarkeit von IT-Sicherheitsprodukten und IT-Sicherheitstechnologien von den großen und wichtigen IT-Marktführern. Dabei sollte dies einfach und nachhaltig möglich sein.

Beispiele wären hier Krypto-Technologien (Algorithmen, Zufallszahlengeneratoren, …) und weitere Sicherheitslösungen wie Verschlüsselungsprodukte (z. B. Festplattenverschlüsselung wie Bitlocker), Abschottungstechnologien wie virtuelle Maschinen und IT-Sicherheitstoken wie SmartCards oder HSMs.

Dabei hätte eine Austauschbarkeit, also die **IT Security Replaceability** enorme Vorteile!

Zum jetzigen Zeitpunkt ist ein IT-Produkt in sich geschlossen und in den seltensten Fällen erlaubt der Hersteller neben der Einsicht in die Arbeitsweise, den Austausch bestimmter (insbesondere kritischer) Elemente. Dies ist in der heutigen Zeit jedoch inakzeptabel und muss sich in Zukunft ändern.

Die nachfolgende Abbildung 13 stellt beispielhaft dar, wie solch eine Austauschbarkeit anhand eines Betriebssystems aussehen würde. Die Zahnräder stellen in diesem Fall eine kleine Auswahl an grundlegenden Elementen eines Betriebssystems dar. Das auszutauschende Element wäre dabei die "eingebaute Verschlüsselung ab Werk", welche einen potenziellen Schwachpunkt darstellt, da sie oft weder zur Revision der Sicherheit offen steht, noch unklar ist, welche kryptografische Algorithmen tatsächlich zum Einsatz kommen und wie gut und ausreichend diese umgesetzt worden sind. In diesem Fall ist dann auch unklar, ob absichtliche Schwächungen in Form von Hintertüren im Design existieren, die ein "Aufbrechen" eines verschlüsselten Systems mit sehr wenig Aufwand erlauben. Ein deutsches Produkt ("grünes Zahnrad") hingegen würde durch einen Austausch die Möglichkeit bieten, durch nachgewiesene Vertrauenswürdigkeit und zertifiziert starke Algorithmen und sichere Schlüssel ein deutlich höheres IT-Sicherheitslevel zu erreichen.

Ein offenes IT-Sicherheitssystem und die freie Wahl von kritischen Bausteinen eines IT-Sicherheitsproduktes hätten viele Vorteile. Alle kritischen Teile wie Verschlüsselungsalgorithmen, der für Verschlüsselungen immanent wichtige Zufallszahlengenerator oder das Verschlüsselungsprogramm des Betriebssystems könnten gegen geprüfte deutsche Produkte und Technologien ausgetauscht werden. Dies wäre ein enormer Sicherheitsgewinn – für den Anwender und die Wirtschaft, da die Wirksamkeit und die Vertrauenswürdigkeit besser eingeschätzt werden könnte.

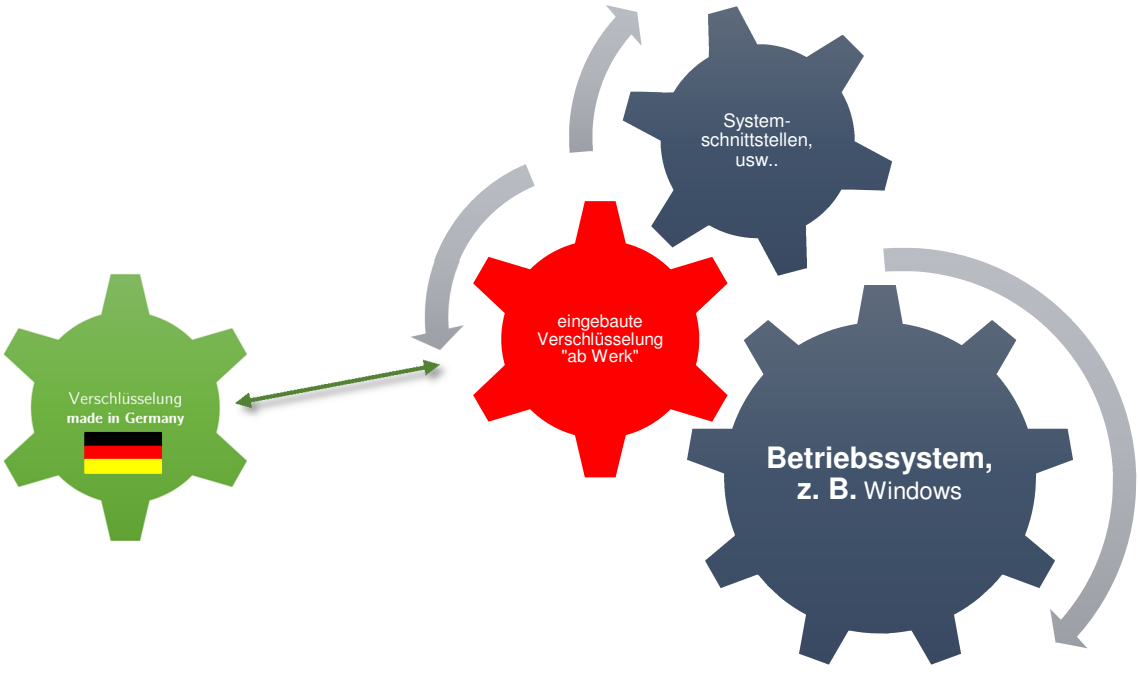


Abbildung 13 - IT Security Replaceability innerhalb eines Betriebssystems (Schema)

In Deutschland gibt es sehr viel Expertise im Bereich der Überprüfung und Zertifizierung. Neben dem BSI gibt es weitere weltweit sehr angesehene Prüforganisationen wie den Technischen Überwachungsverein (TÜV). Dieses Know-how könnte ebenfalls mit einfließen und dazu beitragen, dass durch weitere Prüfungen, Prüfverfahren und Zertifizierungen, die Qualität der IT-Sicherheit aus Deutschland steigt und dabei Vertrauenswürdigkeit und Zuverlässigkeit bescheinigt bekommt. Dies wäre ein weiterer positiver Aspekt: Ein austauschbares Produkt

aus Deutschland für den Ersatz eines ausländischen Produktteils mit einem TÜV- und BSI-Siegel hat national und international ein enormes Gewicht.

Die Konsequenz daraus wäre: IT-Marktführer in den einzelnen Bereichen schaffen deutlich mehr Vertrauenswürdigkeit für ihre IT-Sicherheitslösungen und könnten auch verlorenes Vertrauen zurückgewinnen.

Würde diese Möglichkeit zur Verfügung stehen, könnten die Kunden entscheiden, welche IT-Sicherheitstechnologien sie einsetzen wollen, z. B. abhängig vom eigenen Schutzbedarf und der notwendigen Wirkungsklasse. Zudem besitzt die deutsche IT-Sicherheitsindustrie einen einfachen Zugang zum globalen Markt und genießt weltweit ein hohes Ansehen in den verschiedenen Bereichen.

Sobald die Nutzer diese Möglichkeit geschlossen fordern, wird die IT- und IT-Sicherheitsindustrie im Zugzwang sein und für die Nachfrage ein Angebot bieten.

Die Vorteile wären zusammengefasst:

- Die **IT-Marktführer** schaffen deutlich mehr **Vertrauenswürdigkeit** für ihre IT-Lösungen.
- Die **Kunden können selbst entscheiden**, welche IT-Sicherheitstechnologien sie einsetzen wollen. (in Abhängigkeit zum Schutzbedarf → Wirkungsklassenmodell)
- Die **Produkte der deutschen IT-Sicherheitsindustrie** können in Zukunft auch **von ausländischen Kunden adaptiert werden**, wo sie einen sehr guten Ruf genießen.
- Nur überprüfte und zertifizierte Produkte würden zum Einsatz kommen, falls nötig und gewünscht.

Dies wäre eine echte "Win-win-Situation" für alle Beteiligten und schafft durch eine stärkere Kooperation und Transparenz mehr Vertrauen.

Wünschenswerte Teilziele

Das Ziel ist es, mit Hilfe der Stakeholder (Anwender, Hersteller, Politik, Forschung) die erforderlichen IT-Sicherheitsmaßnahmen zu identifizieren und mit einzubeziehen, um das gesteckte Ziel nachhaltig und erfolgreich umzusetzen. Hierzu wird die Roadmap den jeweiligen erforderlichen Anforderungen angepasst und umgesetzt.

Es gibt eine Reihe von wünschenswerten Zielen, wie in Abbildung 14 dargestellt, von denen die Meisten sofort klar auf der Hand liegen. Hierzu gehören die stärkere Verschlüsselung von Kommunikation via E-Mail und Web-Datenverkehr, um einen höheren Grad der Privatsphäre zu erreichen und zu verhindern, dass Dritte Informationen mitlesen und missbrauchen können. "Während Anfang 2011 nur etwa 5% des gesamten Web-Datenverkehrs verschlüsselt waren (HTTPS), stieg der Anteil bis Anfang 2013 auf 12%. Kurz vor den Snowden-Enthüllungen im Juni 2013 waren fast 20% des Web-Verkehrs verschlüsselt, derzeit sind es rund 23%." [1, S.86] Eine deutliche Steigerung bis zum Jahr 2020 wäre hier wünschenswert.

E-Mailverschlüsselung im Sinne der "Ende-zu-Ende-Verschlüsselung" findet zum heutigen Zeitpunkt immer noch sehr wenig Akzeptanz. Wenn über E-Mailverschlüsselung gesprochen wird, dann ist damit der Schutz von vertraulichen Inhalten innerhalb einer E-Mail gemeint. Hierbei ist jedoch nicht die SSL/TLS-Transportverschlüsselung/Transportsicherung zwischen Sender und Empfänger gemeint, welche auch in Werbespots von E-Mail-Providern als "Verschlüsselung" betitelt werden, denn hiermit werden die Nachrichten trotzdem im Klartext übertragen und sind durch dritte (Mitarbeiter, Behörden, Angreifer) einsehbar. Die eigentlich relevante und einzusetzende Technologie soll die Möglichkeit der inhaltlichen Verschlüsselung bei der E-Mail-Korrespondenz bieten. Hierbei kann beispielsweise als Standard S/MIME (Secure / Multipurpose Internet Mail Extensions) oder PGP (Pretty Good Privacy) zum Einsatz kommen. Wird beim Einsatz dieser Systeme auf entsprechend sichere Verfahren gesetzt, gibt es keinerlei Möglichkeiten die verschlüsselten Nachrichten selbst mit Hilfe enormer Rechenkapazitäten "aufzubrechen".

Auch hier wäre eine entsprechende Steigerung ein gewünschtes Ziel.

Ebenfalls ist ein wichtiges Ziel die Malware-Infektionen für die Zukunft zu senken, denn jeder betroffene Rechner kann als Werkzeug missbraucht werden, um mittelbar oder unmittelbar Schaden anzurichten. Dabei sind diese Infektionen weit verbreitet: "60 Prozent der kleinen und mittleren Unternehmen beklagen Malware-Infektionen." [21] Die Bedrohung, die von Schadsoftware ausgeht, ist also groß: "Kaspersky Lab entdeckte täglich 315.000 neue Schädlinge; im Vorjahr waren es noch 200.000." [7] Hier besteht ebenfalls für die kommenden Jahre großer Handlungsbedarf, um dieser Entwicklung Herr zu werden.

Erklärtes Ziel

Das erklärte Gesamtziel ist es mittel- bis langfristig ein deutlich höheres IT-Sicherheitsniveau zu erreichen, als es heute der Fall ist. Hierbei wäre als ein sinnvolles mögliches Zwischenziel das Jahr 2020 zu nennen.

Natürlich ist die Herausforderung, dieses Zwischenziel im Jahre 2020 zu erreichen, groß. Bis zum jetzigen Zeitpunkt gibt es zwar Werkzeuge, wie beispielsweise die bereits genannten Sicherheitskriterien (Common Criteria, ITSEC, ...), allerdings sind diese nur dann anwendbar, wenn dem Nutzer sein Sicherheitsbedarf klar geworden ist. Es mangelt zudem an der Möglichkeit einer Klassifikation von Gefahren und Schutzbedarfen, welche auch die Vertrauenswürdigkeit mitberücksichtigen.

Für das Erreichen des Ziels, das IT-Sicherheitsniveau signifikant zu erhöhen, wird nachfolgend ein Konzeptvorschlag gemacht, welcher auf einer Einteilung von IT-Systemen in leicht verständliche Wirkungsklassen beruht. Als Hilfe für die Umsetzung steht zu Beginn die Identifikation und eine darauf basierende Empfehlung angemessener IT-Sicherheitsmaßnahmen für jede Wirkungsklasse, jedoch immer unter Berücksichtigung herausragender nationaler, vertrauenswürdiger Technologien und Standards.

Ein weiterer dringlicher Punkt ist die Austauschbarkeit von Technologien innerhalb der marktbeherrschenden Produkte als möglicher und notwendiger Lösungsweg aus der Vertrauenswürdigkeitsmisere der Vergangenheit. Eine Austauschbarkeit von 30% bis 2020 wäre ein wünschenswertes Ziel.

Hierbei ist es erforderlich anzumerken, dass auch die Vertrauenswürdigkeit der umliegenden Komponenten nachgewiesen werden muss. Es genügt nicht einen Teil einer Software austauschbar zu machen, um ihre Vertrauenswürdigkeit zu erhöhen und die restlichen Komponenten dabei außer Acht zu lassen.

Weitere mögliche Ziele wären, wie in Abbildung 14 schematisch dargestellt, beispielsweise die deutlich weitere Verbreitung kollektiver IT-Sicherheitsbilder. Auch die Minderung von Sabotagevorfällen im Bereich der Infrastruktur von häufigem Auftreten (x Vorfälle) zu einem definierten niedrigeren Niveau (y Vorfälle).

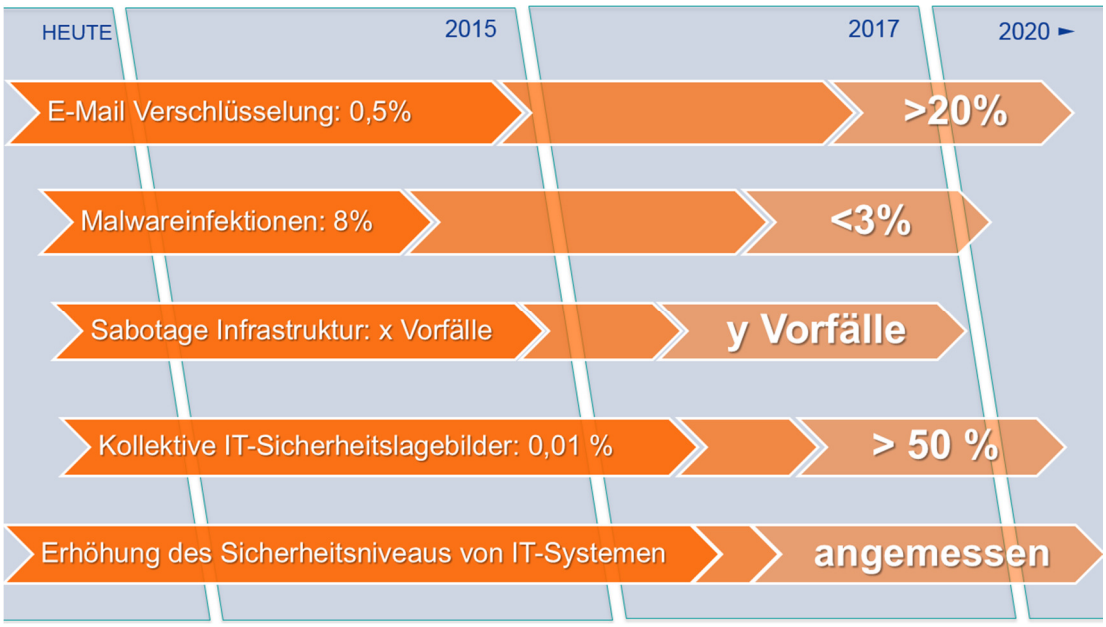


Abbildung 14 - Beispiele möglicher Ziele

Insgesamt sollte das heute herrschende Sicherheitsniveau von IT-Systemen in naher Zukunft auf ein angemessenes Maß erhöht werden. Dies kann aber nur erreicht werden, wenn alle Teilgebiete, in denen Defizite herrschen, schrittweise Verbesserungen erfahren. Angefangen bei der E-Mail-Verschlüsselung, über die Senkung der Malware-Infektionen bis hin zu den erwähnten kollektiven IT-Sicherheitslagebildern.

7 Wirkungsklassen von IT-Sicherheitsmaßnahmen für unterschiedliche Schutzbedarfe

In diesem Kapitel werden nachfolgend neben den unterschiedlichen Wirkungsaspekten und der Einführung der Wirkungsklassen, welche das Schlüsselelement bilden, auch die Inpflichtnahme der internationalen Anbieter in Verbindung mit den Herausforderungen und notwendigen Maßnahmen diskutiert.

7.1 Unterschiedliche Wirkungsaspekte

Wie bereits diskutiert, gibt es heute viele Bedrohungen mit zahlreichen Gefahren und in den kommenden Jahren werden diese noch weiter anwachsen. "Angesichts der vielfältigen, potenziellen Bedrohungen, die Schwachstellen zum Schaden der Organisation ausnutzen, bestehen daher immer Risiken in der Informationssicherheit." [22, S.6]

Der Begriff der "Wirkung" oder auch "wirkungsvolle Informationssicherheit", der für die unterschiedlichen Wirkungsaspekte notwendig ist, wird nach DIN ISO/IEC 27002:2014-02 folgendermaßen erläutert: "Eine wirkungsvolle Informationssicherheit verringert (…) Risiken durch Schutz der Organisation vor Bedrohungen und Schwachstellen und vermindert dadurch die Auswirkungen auf organisationseigene Werte." [22, S.6]

Der ITSEC-Standard sagt zur Wirksamkeit: "Bei der Evaluation der Wirksamkeit wird beurteilt, ob die sicherheitsspezifischen Funktionen und Mechanismen, die durch den Evaluierungsgegenstand zur Verfügung gestellt werden, wirklich die vorgegebenen Sicherheitsziele erreichen."

Zusätzlich muss berücksichtigt werden: "Der Evaluierungsgegenstand wird hinsichtlich der Eignung der Funktionalität, des Zusammenwirkens der Funktionen (…), der Konsequenzen von bekannten und entdeckten Schwachstellen (…) und der Einfachheit der Anwendung beurteilt."

Bei der Betrachtung konkreter Bedrohungen gilt laut ITSEC-Standard: "Zusätzlich wird bei der Bewertung der Wirksamkeit die Fähigkeit der Sicherheitsmechanismen des Evaluierungsgegenstands, Widerstand gegen einen direkten Angriff zu leisten, bewertet (Stärke des Mechanismus). Für die Stärke der Mechanismen sind drei Stufen definiert - niedrig, mittel und hoch - die ein Maß für das Vertrauen sind, inwieweit die Sicherheitsmechanismen des Evaluierungsgegenstands in der Lage sind, direkten Angriffen zu widerstehen."[30]

Dies bedeutet aber auch, dass aus der Herausforderung heraus unterschiedliche Ergebnisse erzielt werden können, je nach Sichtweise und der Analyse des Problems.

Der hier vorgestellte Vorschlag stützt sich dabei auf genau drei Sichtweisen, mit Hilfe derer die maximale Wirkung erzielt werden kann. Die Wirkungsarten werden nachfolgend tabellarisch dargestellt. Die notwendigen Anforderungen hierbei sind der Wirkungsaspekt, also welche Art der Wirkung wird gegen eine konkrete Bedrohung erzielt und welche Anforderungen dies an die nachfolgende Maßnahme stellt, die schließlich dabei helfen soll die gewünschte Wirkung zu erzielen. "Wenn es um Ressourcen geht, über die Internetattacken erfolgen, landet Deutschland auf Platz vier – 12,51 Prozent der Attacken weltweit gingen von Deutschland aus, hinter den USA (25,54%), Russland (19,44%) und den Niederlanden (12,80%)." [7]

IT-Sicherheit ist natürlich ein Kostenfaktor und "IT-Sicherheitsmaßnahmen sind Investitionen. Ihre Kosten setzen sich aus Hard- und Softwarekosten, Installations- und Betriebsaufwänden zusammen. Ihre Erträge summieren sich aus der Minderung des IT-Risikos, der Aufwandsreduzierung (…)" [4, S.79]. Ein geeignetes Konzept zu finden mag keine triviale Aufgabe sein, aber mit Hilfe der Wirkungsklassen und der Klarheit über Anforderungen sowie den eigenen Schutzbedarf stellt dies keine große Hürde mehr dar. Wichtig ist auch: "IT-Sicherheit ist ein

[30] „IT-Sicherheitskriterien (ITSEC), Abschnitt 1.14, Seite 9“ - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-dt_pdf.pdf?__blob=publicationFile

kontinuierlich zu verfolgendes Ziel. Ein Sicherheitsniveau ist nur dann wirksam, wenn es sowohl zeitliche als auch örtliche Konstanz und damit Verlässlichkeit aufweist.". [4, S.37] Aus diesem Grund müssen der Wirkungsaspekt, die Anforderung und die Maßnahme immer wieder hinterfragt und neu ausgerichtet werden. Vor allem die Frage nach der Abgrenzung ist dabei notwendig: "Welche Technologie setze ich genau ein und welche sollte gemieden werden?"

Belangvoll ist auch die Frage nach der richtigen Verschlüsselung: Einige Verfahren sind heute bereits wirkungslos und andere sind gerade noch in Ordnung um einen Schutz der Vertraulichkeit zu gewährleisten. Auch Firewall-Systeme alleine sind in aller Regel nicht genug und reichen selbst nicht aus um ein Sicherheitskonzept als ausreichend zu beurteilen und eine sinnvolle Wirkung zu erzielen.

Die nachfolgenden Tabellen (Tabelle 36 bis Tabelle 38) geben ein Beispiel für die Definition und den Unterschied von prinzipieller, konkreter und gewollter Wirkung.

Prinzipielle Wirkung

Wirkungsaspekt: prinzipielle Wirkung gegen konkrete Bedrohungen
Anforderung: z. B. Verschlüsselung gegen das Lesen von Klartext
Maßnahme: Darstellung der Wirkung von Kryptoverfahren Kryptografische Verfahren gibt es in zahlreicher Form. Neben sehr guten und starken, gibt es auch sehr schwache und veraltete. Beim Einsatz eines Kryptoverfahrens, also einer Verschlüsselung als Teil eines IT-Sicherheitsprodukts ist es daher fundamental, sowohl eine sichere Variante zu wählen als auch dessen Umsetzung (z. B. die Programmierung selbst) ordentlich durchzuführen. Dabei ist auch zu beachten, dass das sicherste kryptografische System unwirksam wird, wenn es Unbefugten gelingt (z. B. Nachrichtendienste), durch Ausnutzen absichtlich eingebauter Schwächen und Hintertüren, Zugriff auf die Daten zu erhalten. 〉 Die deutsche Bundesnetzagentur beschreibt beispielsweise in ihrem "Algorithmenkatalog" geeignete und ungeeignete kryptografische Verfahren: z. B. "Abschnitt 3.1., RSA-Verfahren: (…) Geeignete Schlüssellängen für RSA-Verfahren: 2048 (Empfehlung) bis Ende 2019" [23, S.7] ➔ Demnächst sollte also möglichst flächendeckend RSA 4096 zum Einsatz kommen.

Tabelle 36 - Darstellung: Prinzipielle Wirkung

Konkrete Wirkung

Wirkungsaspekt: konkrete Wirkung gegen konkrete Bedrohungen

Anforderung: richtige Implementierung von Verschlüsselungstechnologien; Zufallszahlen, Algorithmen, Einbindung, …

Maßnahme: Evaluierung von IT-Sicherheitslösungen

IT-Sicherheitslösungen sollten in bestimmten Bereichen gewisse Kriterien erfüllen. Dafür gibt s die bereits erwähnten Schutzprofile (z. B. nach Common Criteria) und technischen Richtlinien des BSI (BSI-TR), die umgesetzt werden müssen. Die Berücksichtigung dieser Kriterien ist notwendig um Zertifizierungen zu bekommen und gesetzliche Vorgaben zu erfüllen.

〉 Common Criteria findet hier heute flächendeckend Anwendung und beinhaltet:

Funktionale Sicherheitsanforderungsklassen [24, S.66]
- Klasse FAU: Sicherheitsprotokollierung
- Klasse FCO: Kommunikation
- Klasse FCS: Kryptographische Unterstützung
- Klasse FDP: Schutz der Benutzerdaten
- Klasse FIA: Identifikation und Authentisierung
- Klasse FMT: Sicherheitsmanagement
- Klasse FPR: Privatsphäre
- Klasse FPT: Schutz der EVG-Sicherheitsfunktionen
- Klasse FRU: Betriebsmittelnutzung
- Klasse FTA: EVG-Zugriff
- Klasse FTP: Vertrauenswürdiger Pfad/Kanal

Klassen von Anforderungen an die Vertrauenswürdigkeit [24, S.66–67]
- Klasse ACM: Konfigurationsmanagement
- Klasse ADO: Auslieferung und Betrieb
- Klasse ADV: Entwicklung
- Klasse AGD: Handbücher
- Klasse ALC: Lebenszyklus-Unterstützung
- Klasse ATE: Testen
- Klasse AVA: Schwachstellenbewertung
- Klasse AMA: Erhaltung der Vertrauenswürdigkeit

Die CC unterscheiden nicht nach der Korrektheit der Implementierung und der Wirksamkeit der Mechanismen, sondern führen sieben Vertrauenswürdigkeitsstufen (EAL1 - EAL7) ein. (…) Spezielle Pakete von Vertrauenswürdigkeitskomponenten bilden die EAL, von EAL 1 – "funktionell getestet", bis EAL 7 – "formal verifizierter Entwurf und getestet". [24, S.66–67]

Tabelle 37 - Darstellung: Konkrete Wirkung

Gewollte Wirkung

Wirkungsaspekt: gewollte Wirkung gegen konkrete Bedrohungen
Anforderung: sind z. B. Hintertüren oder gewollte Schwächen eingebaut
Maßnahme: Qualitätssiegel "*IT Security made in Germany*" IT-Sicherheitsprodukte und Firmen aus dem Ausland unterliegen an erster Stelle den dortigen Gesetzen und finden dann einen Weg auf den deutschen Markt. Dabei sind Gesetze im Bereich des Datenschutzes in keinem Land der Welt mit der Qualität in Deutschland vergleichbar. Zudem gibt es in vielen Ländern künstlich eingeschränkte Sicherheit und Vertrauenswürdigkeit, damit dortige Behörden und Organisationen nicht ins Hintertreffen geraten, wenn sie Zugriff auf diese Systeme nehmen wollen. Der Export dieser IT-Systeme ins Ausland ist dabei überhaupt kein Thema. 〉 Das Erhalten dieses Qualitätssiegels, setzt spezielle Kriterien voraus, um Transparenz zu gewährleisten und Vertrauenswürdigkeit zu ermöglichen: ▪ Der Unternehmenshauptsitz muss in Deutschland sein. ▪ Das Unternehmen muss vertrauenswürdige IT-Sicherheitslösungen anbieten. ▪ Die angebotenen Produkte dürfen keine versteckten Zugänge enthalten (keine Backdoors). ▪ Die IT-Sicherheitsforschung und – Entwicklung des Unternehmens muss in Deutschland stattfinden. ▪ Das Unternehmen muss sich verpflichten, den Anforderungen des deutschen Datenschutzrechtes zu genügen. Daraus resultieren zahlreiche Vorteile, die Software aus dem Ausland zum jetzigen Zeitpunkt nicht bieten kann.

Tabelle 38 - Darstellung: Gewollte Wirkung

Marktführende IT-Technologien kommen in vielen Bereichen aus dem Ausland wie ein Betriebssystem mit integrierter Festplattenverschlüsselung (z. B. Windows mit Bitlocker), welche als ein Gesamtprodukt erworben und eingesetzt werden können. Die Verschlüsselungssoftware Bitlocker ist ein fester Bestandteil der Windows-Betriebssysteme von Microsoft und lässt sich zum jetzigen Zeitpunkt nicht einfach durch eine andere Software ersetzen.

Als Alternative bietet sich lediglich der Einsatz einer zusätzlichen Software an, die zur Koexistenz mit Bitlocker gezwungen ist, inklusive der daraus entstehenden Nachteile für den Kunden und dem deutlich höheren Aufwand für eine benutzerfreundliche Integration für den Hersteller, sofern diese überhaupt möglich ist. Nachfolgend wird ein Beispiel auf Basis der oben genannten Kombination aus Betriebssystem und eingebauter Verschlüsselung aufgezeigt.

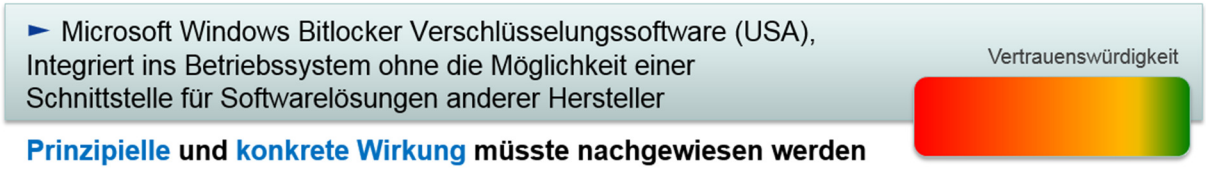


Abbildung 15 - Notwendigkeit der Erbringung von Nachweisen

Die vollständige Vertrauenswürdigkeit kann also an dieser Stelle nicht gewährleistet werden (Abbildung 15). Die Gründe sind vielfältig: Der Hauptsitz der Firma befindet sich in den USA, also unterliegt sie den US-amerikanischen Gesetzen. Eine geforderte eingebaute Abschwächung von Sicherheit ist somit möglich. Es ist unklar, inwiefern die Erfüllung der prinzipiellen und konkreten Wirkung gegeben ist. Die Software Bitlocker befindet sich, mangels Alternativen, trotzdem großflächig im Einsatz.

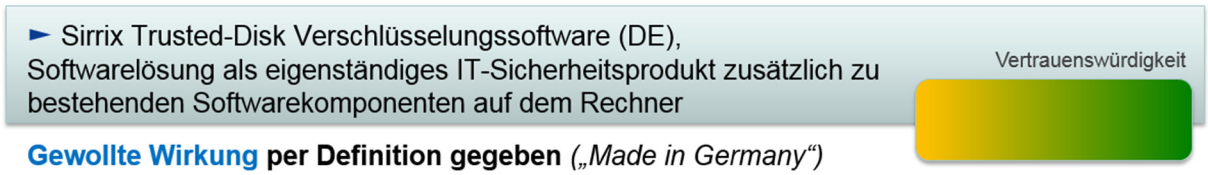


Abbildung 16 - Wirkung per Definition gegeben

Ein Beispiel einer deutschen IT-Sicherheitslösung ist die in Abbildung 16 aufgeführte Verschlüsselungssoftware *Trusted-Disk* der Firma *Sirrix AG* mit dem Hauptsitz in Deutschland. Hierbei ergibt sich aus der Gesamtheit der wichtigsten Kriterien (deutsche Firma, Hauptsitz in Deutschland, in Deutschland entwickelte und zertifizierte Software, …) eine maximale Vertrauenswürdigkeit, welche im Hinblick auf die gewollte Wirkung per Definition gegeben ist: "Made in Germany".

Eine mögliche und hier geforderte Lösung besteht also darin, eine Schnittstelle von Seiten der großen Hersteller anzubieten, um bestimmte Komponenten partiell durch deutsche Lösungen für eine höhere Wirkung der IT-Sicherheit ersetzbar zu machen.

7.2 Einteilung in Wirkungsklassen

Eine Einstufung des eigenen Schutzbedarfs ist schwierig. Je nach Umfang und Verantwortungsbereich können die Konsequenzen bei einer Fehleinschätzung verheerend sein. Wenn sich ein Kraftwerksbetreiber im Bereich IT-Sicherheit wissend oder unwissend Versäumnisse eingestehen muss und diese womöglich auch noch von einem Angreifer vorher entdeckt worden sind, kann das im schlimmsten Fall zu einer ernsten Bedrohung werden – für das Kraftwerk und alle darauf angewiesenen Teilnehmer, in diesem Fall die gesamte Bevölkerung.

Die auf diesem Problem basierende Idee war es, eine Klassifikation zu entwickeln, die sowohl eine Einstufung des eigenen Bedarfs ermöglicht, als auch eine rudimentäre Aussage über die dadurch zu erwartenden Kosten zulässt.

7.2.1 Abgedeckte Schutzbedarfe

Es wurden also insgesamt fünf Wirkungsklassen definiert, welche jede für sich gesehen einen bestimmten Schutzbedarf abdeckt und bestimmte Gefahren abwehren soll. Die Kosten wurden jeweils unter dem Aspekt der Komplexität innerhalb der Zielgruppe für diese abgeschätzt.

Nachfolgend wird in Abbildung 17 eine Übersicht der Wirkungsklassen aus der Perspektive der IT-Sicherheitsbedrohungen dargestellt: Welche Wirkungsklassen gibt es und welcher Schutzbedarf wird in den verschiedenen Wirkungsklassen gedeckt?

Wirkungsklasse 0 Basis-IT-Sicherheit	Infektionen durch Schadsoftware (Viren, PC-Geiselnahme, Keylogger, Trojaner)
	Angriffe auf das heimische Netzwerk, Abfischen von Banking Daten
Wirkungsklasse 1 Schutzbedarf: mittel	Angriff auf den Datenbestand (Kunden-, Mandanten-, Patient-, und Unternehmensdaten)
	Infektionen durch Schadsoftware und Mitschneiden von Kommunikation
Wirkungsklasse 2 Schutzbedarf: hoch	Diebstahl von Plänen und Dokumenten mit Hilfe von Schadsoftware
	Kopieren von sensiblen Daten auf externe Datenträger
Wirkungsklasse 3 Schutzbedarf: sehr hoch	Sabotage von kritischer Infrastruktur (Wasserwerke, Energieversorger, Finanzdienstleister)
	Gezielte Attacke gegen einzelne Wissensträger in Industrie und Politik

Wirkungsklasse 4 Verschlusssachen bis streng geheim	Angriff auf Informationen und Kommunikation
	Eindringen in staatliche oder wirtschaftlich extrem kritische Systeme

Abbildung 17 - Wirkungsklassen aus der Perspektive von IT-Sicherheitsbedrohungen

7.3 Voraussetzung für eine Einstufung in die Kernwirkungsklassen

Die Einstufung in die geeigneten Wirkungsklassen geschieht in erster Linie anhand des Schutzbedarfes. Zwar besteht das Klassenmodell aus insgesamt fünf Wirkungsklassen, jedoch haben die Klassen 0 und 4 einen besonderen Stellenwert. Dies wird nachfolgend für alle Klassen im Detail erläutert. Die Klassen 1, 2 und 3 bilden dabei die Kernwirkungsklassen, innerhalb dieser sich die meisten Systeme wiederfinden.

Die Einstufung in die Wirkungsklassen muss differenziert durchgeführt werden. Allem voran sollte nach einer sorgfältigen Prüfung der IT-Landschaft erst einmal erfasst werden, welche Gruppen von IT-Systemen es im Unternehmen gibt und welchen Schutzbedarf diese haben, um ihn dann effektiv abdecken zu können. Hierbei ist zu berücksichtigen, dass nicht einfach die gesamte Organisation oder das Unternehmen aufgrund einiger weniger Systeme mit sehr hohem Schutzbedarf komplett in die Wirkungsklasse 3 fällt. Ein mögliches Szenario ist dabei, dass völlig unterschiedliche Gewichtungen hinsichtlich des Schutzbedarfes entstehen können.

Es kann beispielsweise ein kleiner Anteil von 5% einen sehr hohen Schutzbedarf aufweisen, rund 15% einen hohen und 35% einen mittleren Schutzbedarf. In diesem Fall müssen dann gleich mehrere Wirkungsklassen berücksichtigt werden. Alle restlichen IT-Systeme, die aufgrund eines niedrigen Schutzbedarfes in keine der drei Schutzklassen fallen, werden automatisch in die Wirkungsklasse 0 eingeordnet.

7.3.1 Wirkungsklasse 0

Die Wirkungsklasse 0 deckt im Prinzip den Grundschutz von IT-Systemen ab und bildet eine Basis für alle anderen Klassen. Die abgedeckten Gefahren sind hierbei die Bedrohung der Privatsphäre und Cybercrime im klassischen Sinne. Zu den Abwehrmaßnahmen gehören Anti-Malware Tools und Personal Firewalls.

Der prozentuale Anteil, aus Sicht der Gesamtmenge aller IT-Systeme in Deutschland, liegt in dieser Wirkungsklasse bei 100%, d. h. hierbei wird der Grundschutz als solcher berücksichtigt und sollte in jedem Fall als Mindestmaß Berücksichtigung finden.

Die Kosten für diese Wirkungsklasse belaufen sich auf lediglich ca. 5% vom regulären Anschaffungspreis des IT-Systems.

Ein Beispiel für die Wirkungsklasse 0 sind im Prinzip alle IT-Systeme innerhalb der eigenen Nutzung durch den Anwender im privaten Bereich.

7.3.2 Wirkungsklasse 1

Diese Wirkungsklasse richtet sich an Unternehmen, Organisationen und Behörden, welche einen mittleren Schutzbedarf haben. Die Gefahren liegen hier beispielsweise bei Verstößen gegen die Privatsphäre respektive den gesetzlichen Datenschutz, und betreffen daher alle Unternehmen. Zudem ist hier auch Cybercrime mit höherem Gefährdungsgrad relevant, was im Detail bedeutet, dass ein Angriff auf diese Gruppe womöglich interessanter sein kann, als auf den Bürger mit privater Nutzung aus der Wirkungsklasse 0.

Es liegt auf der Hand, dass Unternehmen und Behörden aus Sicht eines Angreifers mit hoher Wahrscheinlichkeit deutlich interessantere und wertvollere Daten haben, als der Bürger in seinem kleinen Büro daheim.

In der Wirkungsklasse 1 finden sich also alle IT-Systeme eines Unternehmens oder einer Organisation, die zwar eine positive Relevanz haben, denen jedoch keine existenzielle Bedeutung zukommt. In jeder IT-Landschaft gibt es Systeme, die keine wichtige Rolle spielen, wie beispielsweise ein PC auf dem eine Elster-Software für die kommende Steuererklärung genutzt wird. Eine Gefährdung dieses Systems ist in der Tat kritisch, allerdings würde sich ein Ausfall nicht unmittelbar im Geschäftsbetrieb niederschlagen und die Existenz des Unternehmens gefährden.

Dies bedeutet im Detail, dass ein Ausfall hingenommen werden kann, ohne größere Schäden und Konsequenzen für die Gesellschaft, Leib und Leben und den Unternehmer.

Der prozentuale Anteil aus Sicht der Gesamtmenge aller IT-Systeme in Deutschland liegt in dieser Wirkungsklasse schätzungsweise bei etwa 70%.

Die Kosten für diese Wirkungsklasse belaufen sich auf ca. 10% vom regulären Anschaffungspreis des IT-Systems.

Ein Beispiel für die Wirkungsklasse 1 wären alle Unternehmen.

7.3.3 Wirkungsklasse 2

Diese Wirkungsklasse richtet sich zwar ebenfalls an Unternehmen, Organisationen und Behörden, zusätzlich werden hier aber auch Infrastrukturen berücksichtigt, die insgesamt alle einen hohen Schutzbedarf aufweisen. All die Aspekte aus der vorherigen Wirkungsklasse 1 finden auch hier mindestens Anwendung. Neben den dort geltenden Bedrohungen, gibt es hier jedoch eine Steigerung des Gefahrenpotenzials. Innerhalb dieser Klasse werden neben Cybercrime auch Punkte wie Industriespionage und gezielte Angriffe auf die Werte des Unternehmens berücksichtigt. Diese Punkte sind besonders kritisch, da sich dahinter oft die Existenzfrage verbirgt.

Durch Industriespionage betroffene Unternehmen könnten im schlimmsten Fall um ihre Geschäftsgrundlage gebracht werden. Gezielte Angriffe auf IT-Infrastrukturen in Unternehmen und eine herbeigeführte Störung zwischen diesen, würde die Steuerung von Industrieanlagen und den Warenfluss innerhalb der Wirtschaft negativ beeinflussen oder sogar zum Stillstand bringen, was verheerende finanzielle Folgen haben kann.

In der Wirkungsklasse 2 finden sich also IT-Systeme wieder, die absolut relevant für eine Organisation sind und ein Ausfall oder ein erfolgreicher Einbruch in diese Systeme, neben extrem hohen Kosten, auch die Existenz dieses Unternehmens bedrohen kann.

Der prozentuale Anteil, aus Sicht der Gesamtmenge aller IT-Systeme in Deutschland, liegt in dieser Wirkungsklasse nach Expertenschätzungen bei etwa 27%.

Die Kosten für diese Wirkungsklasse belaufen sich auf 20% vom regulären Anschaffungspreis des IT-Systems.

Ein Beispiel für die Wirkungsklasse 2 sind alle Rechner bei Warenproduzenten oder in Forschungsinstituten, die einen Wert für das Unternehmen darstellen.

7.3.4 Wirkungsklasse 3

Diese Wirkungsklasse richtet sich zwar, wie die vorherige Klasse 2, auch an Unternehmen, Organisationen, Behörden und Infrastrukturen, allerdings ist hier in jeder der Kategorien der "kritische Aspekt" zu berücksichtigen. Aus diesem Grund berücksichtigt die Klasse 3 alle "kritischen Infrastrukturen", die für das tägliche Leben von großer Bedeutung sind.

Der Schutzbedarf in dieser Klasse ist als sehr hoch einzustufen, wobei hier ebenfalls die Geheimhaltungsstufe VS-NfD ("VERSCHLUSSSACHE – NUR FÜR DEN DIENSTGEBRAUCH") zu berücksichtigen ist. Die Einsicht in Informationen dieser Stufe durch nicht befugte Personen, kann sich nachteilig auf die nationalen Interessen und die der Partner der Bundesrepublik Deutschland auswirken.

In Klasse 3 ist mit erhöhter Gefahr in verschiedenen Bereichen zu rechnen, welche als Steigerungen zu der vorangegangenen Wirkungsklasse 2 zu sehen.

Hier spielen vor allem Faktoren eine Rolle, die eine sehr große Bedrohung darstellen. Dies sind im Detail Wirtschaftsspionage durch Nachrichtendienste aus dem Ausland, Cyberattacken auf kritische Punkte innerhalb der Bundesrepublik und Cyberwar (Cyberkrieg) als Sabotageakt, welcher heute bereits von einigen Staaten erfolgreich durchgeführt wird und in der Vergangenheit Finanzsysteme, Parlamente oder Forschungseinrichtungen dauerhaft zu Fall gebracht hat. Ein Beispiel dafür findet sich im Jahre 2007 in Estland. "Die Internet-Angriffe hatten zu einer vorübergehenden Schließung von estnischen Regierungsseiten geführt und die Geschäfte führender Unternehmen behindert." [25]

Die Ausmaße eines solchen Angriffs auf essenzielle Institutionen und Infrastrukturen eines Landes sind nur schwer abzuschätzen und hatten in diesem Fall verheerende Folgen: "Es war jedenfalls ein Angriff, bei dem es auch um Leben und Tod ging. Die Angriffe richteten sich nicht nur gegen Banken, Behörden, die Regierung, sondern auch gegen unsere Notrufnummer." [26]

Sind Angriffe auf Organisationen, (kritische) Infrastrukturen und Behörden bzw. derer Systeme mit einer Zugehörigkeit zu dieser Wirkungsklasse erfolgreich, ist nicht nur die Existenz und der Betrieb dieser gefährdet, sondern betrifft auch Dritte.

Der prozentuale Anteil, aus Sicht der Gesamtmenge aller IT-Systeme in Deutschland, liegt in dieser Wirkungsklasse schätzungsweise bei etwa 3%.

Die Kosten für diese Wirkungsklasse belaufen sich auf ca. 50% vom regulären Anschaffungspreis des IT-Systems, wobei hier zusätzliche Kosten für die zu verwendende Infrastruktur berücksichtigt werden müssen.

Ein Beispiel für die Wirkungsklasse 3 wären IT-Systeme im Bereich von kritischen Infrastrukturen wie Wasserwerke, (Atom)Kraftwerke, Stromnetze und Krankenhäuser.

Die Konsequenzen eines möglichen Impacts (Einschlags) auf diesem Niveau wäre katastrophal: "Die Unterbrechung der Energieversorgung hat ganz anders gelagerte Folgen. Die Störung des Betriebs einer Chemieanlage mit giftigen Chemikalien, einer Kernkraftanlage oder einer Fernlenkwaffe können zu übelsten Folgen führen." [4, S.80]

7.3.5 Wirkungsklasse 4

Diese Klasse stellt die schärfste Version aller Wirkungsklassen innerhalb des Modells dar und deckt einen Schutzbedarf gemäß Geheimschutzordnung (GSO) ab "VERSCHLUSSSACHE-VERTRAULICH" (VS/V) über "GEHEIM" bis hin zu "STRENG GEHEIM".

Alle IT-Systeme innerhalb dieser Klasse betreffen die nationale Sicherheit und sind dementsprechend von extrem kritischer Natur. Angriffe und Einsichtnahme innerhalb dieser Systeme durch unbefugte Personen, können für die nationalen Interessen der Bundesrepublik mindestens schädlich sein. Ein Sicherheitsverstoßes in der Stufe "GEHEIM" kann schwere Schäden nach sich ziehen in der Stufe "GEHEIM" und lebenswichtige Interessen auf nationaler Ebene oder internationale Partner gefährden.

In dieser Klasse werden die notwendigen Maßnahmen zur Sicherung der IT-Systeme durch speziell hierfür definierte Gesetze und Vorschriften geregelt. Alle Gesetze und Vorschriften, die hier zu berücksichtigen sind, müssen zwingend Anwendung finden und ohne jeglichen Spielraum umgesetzt werden.

Der prozentuale Anteil, aus Sicht der Gesamtmenge aller IT-Systeme in Deutschland, liegt in dieser Wirkungsklasse nach Expertenschätzungen insgesamt bei etwa 0,01% und fällt damit im Vergleich zu den vorher beschriebenen Klassen relativ gering aus.

Die Kosten für diese Wirkungsklasse belaufen sich auf etwa 400% vom regulären Anschaffungspreis des IT-Systems.

Ein Beispiel für die Wirkungsklasse 4 sind IT-Systeme im militärischen Einsatz, Bereiche innerhalb von Rechenzentren des Geheimdienstes, des Verfassungsschutzes und des Bundeskriminalamts.

7.4 Definition: Wirkungsklassenmodell

Das in diesem Kapitel in Abbildung 18 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 darüber liegenden Klasse. So deckt beispielsweise die Wirkungsklasse 0 als Gefahren die Angriffe auf die Privatsphäre und Cybercrime ab, wohingegen die Wirkungsklasse 1 zusätzlich zu den Elementen der Klasse 0 auch Cybercrime mit höherem Gefahrengrad und den gesetzlichen Datenschutz 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 (z. B. PC). Diese sind hier als prozentuale Kosten des "Grundbetrags" veranschlagt, um das IT-System dem Bedarf entsprechend schützen zu können.

Wirkungsklasse 0 — **Bürger mit privater Nutzung**

- Gefahren: Privatsphäre, Cybercrime
- Kosten: Grundbetrag +5%

Wirkungsklasse 1 — **Unternehmen, Organisationen, Behörden**

- Gefahren: Privatsphäre, Cybercrime mit höherem Gefährdungsgrad, gesetzlicher Datenschutz
- Schutzbedarf: mittel
- Kosten: Grundbetrag +10%

Wirkungsklasse 2 — **Unternehmen, Organisationen, Behörden, Infrastruktur**

- Gefahren: Industriespionage, gezielte Angriffe auf Werte des Unternehmens, Cybercrime
- Schutzbedarf: hoch
- Kosten: Grundbetrag +20%

Wirkungsklasse 3 — **Unternehmen, Organisationen, 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%

Abbildung 18 - Das Wirkungsklassenmodell

Definition der Begrifflichkeiten

Nachfolgend werden die im Wirkungsklassenmodell verwendeten Begrifflichkeiten näher definiert, um Missverständnissen vorzubeugen und Klarheit hinsichtlich der einzelnen Grundbegriffe zu schaffen. In der ersten Kategorie wird in Tabelle 39 die Anwendersicht berücksichtigt.

Anwendersicht

Wirkungsklasse	Grad/Stufe welche eine bestimmte Wirkung definiert. Abhängig von der Stufe deckt eine Klasse einen bestimmten Schutzbedarf ab und berücksichtigt dabei bestimmte Zielgruppen. Es gibt verschiedene Prinzipien von Wirkungen, mit deren Hilfe sich eine bestimmte Bedrohungsart abwehren lässt. Die Hierarchie ist aufeinander aufbauend als Vererbung zu sehen, die nächst größere Klasse beinhaltet immer die Aspekte der nächst kleineren Klasse.
Schutzbedarf	Definiert den Umfang und die Stufe der Notwendigkeit an Sicherheitsmaßnahmen, die ein Anwender benötigt.
Privatsphäre	Berücksichtigt den eigenen höchst privaten Raum eines Anwenders.
Kosten	Definiert die prozentual geschätzten Zusatzkosten, die zusätzlich zur Anschaffung eines IT-Systems entstehen.
Bürger mit privater Nutzung	Juristische Person als Arbeitnehmer oder Selbstständiger und dem Einsatz der IT "Zuhause".
Unternehmen	Alle Unternehmen
Organisation	Repräsentiert einen Konzern oder einen gemeinsamen Verbund von verschiedenen Unternehmen.
Behörde	Staatliches Verwaltungsorgan bzw. Dienststelle.
(kritische) Infrastruktur	"Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden." [27] Laut dem Bundesministerium des Innern (BMI) und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe werden folgende Bereiche als "kritische Infrastrukturen" angesehen: ▪ Energie (Elektrizität, Gas, Mineralöl) ▪ Informationstechnik und Telekommunikation (Telekommunikation, Informationstechnik) ▪ Transport und Verkehr (Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik) ▪ Gesundheit (Medizinische Versorgung, Arzneimittel und Impfstoffe Labore) ▪ Wasser (Öffentliche Wasserversorgung, Öffentliche Abwasserbeseitigung) ▪ Ernährung (Ernährungswirtschaft, Lebensmittelhandel) ▪ Finanz- und Versicherungswesen (Banken, Börsen, Versicherungen, Finanzdienstleister) ▪ Staat und Verwaltung (Regierung und Verwaltung, Parlament, Justizeinrichtungen, Notfall-/ Rettungswesen einschließlich, Katastrophenschutz) ▪ Medien und Kultur (Rundfunk (Fernsehen und Radio), gedruckte und elektronische Presse, Kulturgut, symbolträchtige Bauwerke) Aber auch ein Verbund von IT-Systemen, die für den Austausch von Informationen elementar sind.
Nationale Sicherheit	Gewissheit der Gesellschaft geschützt zu sein vor der Gefährdung des Staates und seiner Bürger, wie z. B. vor Übergriffen durch Kriminelle, Terrorismus und andere Staaten.
Verschlusssache	Der Geheimhaltung unterliegende Information oder Dokument. Unterschiedliche Stufen möglich.

VS-NfD	Geheimhaltungsstufe: "VERSCHLUSSSACHE – NUR FÜR DEN DIENSTGEBRAUCH"
GSO	Geheimschutzordnung, Gesetz zum Geheimschutz als Vorschrift für die zu treffenden Vorkehrungen.
VS/V	Geheimhaltungsstufe: "VERSCHLUSSSACHE – VERTRAULICH"

Tabelle 39 - Definition von Begriffen aus Sicht der Anwender

In der nun folgenden Tabelle 40 werden die Begriffe der Bedrohungen bzw. der Gefährdungen definiert.

Bedrohungen und Gefährdungen

Cybercrime	Computerkriminalität (z. B. Betrug, Phishing)
Cybercrime mit höherem Gefährdungsgrad	Computerkriminalität mit erhöhtem Schadenspotenzial (z. B. Sabotage, digitale Erpressung)
Gesetzlicher Datenschutz	Beinhaltet das Grundrecht auf informationelle Selbstbestimmung und den Schutz vor Missbrauch persönlich relevanter Daten. (Gehaltsdaten, Krankheitsdaten, Personaldaten, …)
Industriespionage	Gezielter Diebstahl von wichtigen Daten aus der Industrie wie Know-how, Pläne und Programmcode durch Konkurrenzunternehmen.
Gezielte Angriffe auf Werte des Unternehmens	Komplexe zielgerichtete Bedrohungen, die sehr punktuell durchgeführt werden und dadurch sehr schwer zu identifizieren sind.
Wirtschaftsspionage	Angriff und illegale Erbeutung von Informationen aus der Wirtschaft durch ausländische Nachrichtendienste.
Cyberattacken	Cyberangriff auf spezifische Bereiche einer Infrastruktur größeren Ausmaßes.
Cyberwar (Sabotage)	Cyberkrieg als alternatives Mittel zum Einsatz von Truppen, enormen finanziellen Mitteln und Waffen zur Durchsetzung von Zielen einer Regierung.

Tabelle 40 - Definition von Begriffen aus Bedrohungssicht

Insbesondere die Begriffe von Cybercrime und Cyberwar sowie Industriespionage spielen bei den Bedrohungen eine wesentliche Rolle. Die bereits angesprochene Cyberwaffe Stuxnet aus dem Jahr 2010 ist hierbei ein gutes Beispiel bei dem mit vergleichsweise niedrigem monetären Einsatz (schätzungsweise 9 Mio. Euro) eine hohe Wirkung erzielt werden konnte. In diesem Fall wurden beispielsweise wichtige Anlagen im Iran zerstört, ohne den klassischen Einsatz von Soldaten, Kriegsgerät und Menschenleben.

Aus Sicht der Angreifer war solch ein Vorgehen also deutlich günstiger. Der Angriff war vollkommen ohne Blutvergießen durchführbar und erzielt meist trotzdem die gewünschte Wirkung, in diesem Fall nämlich das iranische Atomprogramm deutlich auszubremsen respektive lahmzulegen.

7.5 Definition: Die Wirkungsklasse im Detail

Nachfolgend werden die Wirkungsklassen im Detail diskutiert. Beleuchtet werden dabei sowohl die zu den jeweiligen Klassen gehörenden IT-Sicherheitsmaßnahmen als auch die notwendigen personellen Maßnahmen.

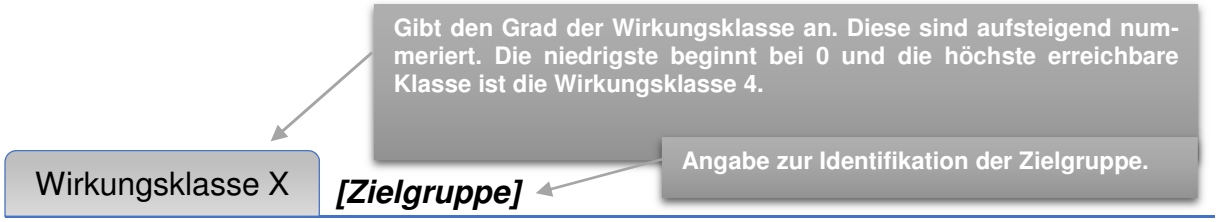


Abbildung 19 - Definition einer Wirkungsklasse und ihrer Elemente

7.5.1 Wirkungsklasse 0: Basis-IT-Sicherheit

IT-Sicherheitsmaßnahmen: Hier der Einsatz von Technologien zur Abwehr von Schadsoftware notwendig, sowie die Nutzung von Software zum Schutz der Privatsphäre.

Sollte die Nutzung einer Cloud in Erwägung gezogen werden, so sind die Daten in dieser unbedingt verschlüsselt abzulegen. Empfohlen wird dies bei einem Anbieter, der nach dem "Zero-Knowledge" Prinzip arbeitet. Hierbei erfolgt die Verschlüsselung clientseitig und die generierten Schlüssel für die Entschlüsselung der Daten verbleiben immer beim Nutzer und finden niemals den Weg zum Anbieter. Andernfalls könnten Dritte trotz Verschlüsselung mit geringem Aufwand die dort abgelegten und persönlichen Daten einsehen.

Bei all diesen Maßnahmen ist es erforderlich, dass möglichst besonders vertrauenswürdige Technologien aus Deutschland zum Einsatz kommen.

Personelle Sicherheitsmaßnahmen: Nutzer innerhalb dieser Klasse sollten über ein solides Basiswissen über den Umgang mit IT und IT-Sicherheitsrisiken verfügen, also ein Mindestmaß an Verständnis über die Wirkung und mögliche Konsequenzen aufgrund von Fehlverhalten.

Kompetenzen in der Ergreifung notwendiger Maßnahmen bei Problemfällen sind ebenfalls notwendig.

7.5.2 Wirkungsklasse 1: Erweiterte IT-Sicherheit

IT-Sicherheitsmaßnahmen: Neben der Basis-IT-Sicherheit, die hierbei inkludiert werden muss, sind zwingend sichere Anwendungen bzw. sichere Browser vorausgesetzt. Wenn möglich, sollten hier weder Java- noch Flash-Technologien zum Einsatz kommen, da diese in der Vergangenheit immer wieder als Angriffsvektoren genutzt wurden. Ebenfalls ist es essenziell, neben dem Betriebssystem auch die genutzten Softwareprodukte in der neusten Version zu benutzen und im Falle von Sicherheitsproblemen auf Alternativen auszuweichen.

Fiktives Beispiel: Stellt ein Autoproduzent einen Fehler bei einem häufig verkauften Fahrzeug fest (z. B. die Bremsen versagen), wird bei Kraftfahrzeugen ebenso wie in der IT-Sicherheit von der Nutzung abgeraten, bis eine Lösung gefunden ist und eine Reparatur durchgeführt werden kann. Eine Weiternutzung könnte andernfalls schwerwiegende Konsequenzen für den Fahrer und seine Umwelt nach sich ziehen.

Der Lösungsweg in IT-Sicherheitsfragen ist also ähnlich.

Des Weiteren muss für die Sicherung und Aufbewahrung der anfallenden Daten ein geeignetes Backup-System genutzt werden. Eine sichere Verwahrung der Backup-Medien muss dabei gewährleistet sein.

Die Nutzung von Cloud-Diensten darf nicht optional, sondern ausschließlich verschlüsselt, nach dem bereits vorher erläuterten "Zero-Knowledge" Prinzip, geschehen.

"Anwälte, Journalisten, Ärzte und Priester müssten die Vertraulichkeit ihrer Kommunikation schützen, sagte Snowden in einem Interview mit Guardian-Chefredakteur Alan Rusbrigder und dem Journalisten Ewen MacAskill in einem Moskauer Hotel unweit des Roten Platzes." [8]

Die Wichtigkeit und Notwendigkeit erschließt sich aus den in jüngster Vergangenheit, durch Edward Snowden veröffentlichten Dokumenten. Sie zeigen die Bedrohung durch Nachrichtendienste, sowohl für die Privatsphäre als auch das Wissen in jeglicher digitaler Form – weltweit.

Personelle Sicherheitsmaßnahmen: Nutzer innerhalb dieser Klassifikation müssen, neben dem Basiswissen, ein erweitertes Wissen über den Umgang und die Gefahren in Verbindung mit IT-Systemen vorweisen können. Zudem ist es notwendig, einen umfangreichen Fundus an Wissen über Datenschutzaspekte und den Umgang mit persönlichen Daten vorzuweisen.

Vertrauliche respektive persönliche Daten, die in falsche Hände fallen, sind eine Gefahr für die Betroffenen und können auch Konsequenzen nach sich ziehen, die im ersten Augenblick vielleicht gar nicht vermutet werden, Stichwort: Die heute stattfindende Aggregation von Daten und "Big Data".

7.5.3 Wirkungsklasse 2: Höherwertige IT-Sicherheit

IT-Sicherheitsmaßnahmen: Zu der bereits erwähnten erweiterten IT-Sicherheit, müssen zusätzlich weitere Technologien zum Einsatz kommen, welche eine höhere Stufe der Sicherheit ermöglichen. Dies sind Sicherheitskerne, bei denen es sich um eine Zusammenfassung von sicherheitsrelevanten Diensten im Sinne der Softwarekomponenten handelt, die vom Rest isoliert werden.

Die Verschlüsselung ist ein wichtiger Eckpfeiler. Hiermit ist sowohl die System- als auch die Objektverschlüsselung gemeint.

Um den Missbrauch von Diensten und Sicherheitsschleusen (z. B. Zugangsberechtigungen zu Räumlichkeiten und Gebäuden) durch Unbefugte zu verhindern ist ein sicheres Identitätsmanagement erforderlich.

Zudem sind Frühwarnsysteme ein essenzielles Werkzeug, mit dessen Hilfe die Verwundbarkeit einer Infrastruktur aufgedeckt oder Angriffe erkannt und abgewehrt werden können. Das Spektrum der Einsatzmöglichkeiten solch eines Systems ist groß, denn es existieren bereits Konzepte für ein globales Internet-Frühwarnsystem. [28]

Bei der Nutzung dieser Sicherheitsmechanismen ist es nötig, möglichst besonders vertrauenswürdige Technologien aus Deutschland zu verwenden.

Personelle Sicherheitsmaßnahmen: Zum bereits erwähnten erweiterten Wissen, sind weitere Kenntnisse über intelligente Social Engineering Angriffe notwendig. Hierbei gilt es Angriffe auf "sozialer Ebene" zu erkennen und abzuwehren. Solche Angriffe basieren auf zwischenmenschlicher Manipulation, mit dessen Hilfe sich der Angreifer gezielt Informationen über ein System verschaffen möchte. Diese erbeuteten Informationen können einem Angreifer entweder ein System und dessen Aufbau inkl. dessen Schwachstellen beschreiben oder es gelingt ihm sogar unmittelbaren Zugriff, mit Hilfe des Opfers, zu erlangen (Diebstahl von Zugangsdaten/Credentials[31]).

Um solche und andere Angriffsmethoden kennenzulernen und darauf effektiv reagieren zu können, muss ein Sicherheitstraining durchgeführt werden, bei dem großer Wert auf die Verantwortung gelegt wird, um sich darüber klar zu werden, welche Risiken eventuelle Angriffe mit sich bringen.

[31] *Credentials* stellen im Bereich der Identifikation einen *Berechtigungsnachweis* dar.

7.5.4 Wirkungsklasse 3: Hochwertige IT-Sicherheit

IT-Sicherheitsmaßnahmen: Neben dem Einsatz der höherwertigen IT-Sicherheit, müssen hier für die besonderen Umstände (z. B. kritische Infrastrukturen) auch proaktive IT-Sicherheitstechnologien zum Einsatz kommen. Bei diesen ist es ebenfalls bedeutend, möglichst besonders vertrauenswürdige Technologien aus Deutschland zu verwenden.

Personelle Sicherheitsmaßnahmen: Neben dem erweiterten Wissen sind tiefgehendes Sicherheitstraining und Awareness notwendig, bei dem aufgezeigt werden muss, welche Verantwortung diese Sicherheitsklasse mit sich bringt. Zudem muss dargestellt werden, welche Risiken vorhanden sind und welche Konsequenzen möglich sind, die es zu vermeiden gilt.

Auch ist eine Aufklärung darüber notwendig, wie eventuell herrschende Unklarheiten beseitigt werden können und wo externe kompetente Hilfe zu finden ist, falls die eigene Kompetenz die Grenzen erreicht hat.

7.5.5 Wirkungsklasse 4: Geheimschutz IT-Sicherheit

IT-Sicherheitsmaßnahmen: In dieser Kategorie ist ausschließlich hochwertige IT-Sicherheit inklusive erweiterter Sicherheitsmaßnahmen einzusetzen. Hierbei gilt es die strengen gesetzlichen Vorgaben gemäß der Geheimschutzordnung (VS/GSO) zur Wahrung der nationalen Sicherheit zu erfüllen.

Hierbei ist es von fundamentaler Bedeutung, ausschließlich möglichst besonders vertrauenswürdige Technologien aus Deutschland zu verwenden.

Personelle Sicherheitsmaßnahmen: Elementar sind zum einen ein umfassendes Sicherheitstraining und ausführliche Awareness-Maßnahmen, zum anderen besonders umfangreiches Wissen über zielgerichtete Angriffe jeglicher Art.

Zusätzlich ist es eminent Kenntnisse über die notwendigen Vorschriften zu haben, welche in höchstem Maße im Dienste der nationalen Sicherheit und der internationalen Partner eine Rolle spielen.

7.5.6 Verantwortung erkennen

Die Übersicht der Wirkungsklassen und die sich daraus ergebenden Fragen und Antworten müssen in jedem Fall gestellt und auch beantwortet werden - genau hierbei sollen die bereits besprochenen Elemente helfen.

Jeder Verantwortliche muss sich der herrschenden Situation klar werden: Menschen mit kriminellem Antrieb, zwielichtige Organisationen und ausländische Geheimdienste sind nur ein Teil der Bedrohungen, denen unsere IT-Systeme ausgesetzt sind. Es geht nicht um Terrorismusabwehr oder Gefahrenvermeidung, wie es die ausländischen Geheimdienste immer wieder beteuern, um ihre Tätigkeiten zu rechtfertigen. In erster Linie ist heutzutage jeder Internetnutzer grundsätzlich ein Verdächtiger und jede wirtschaftlich gut aufgestellte Kraft ein lohnenswertes Ziel, bei dem sich Werte abschöpfen und ins Ausland transferieren lassen. Die sich daraus ergebenen Konsequenzen liegen auf der Hand: Verantwortung muss übernommen werden und die Ohnmacht, in der sich die Gesellschaft innerhalb dieser Themen befindet, beendet werden.

7.5.7 Klasseneinstufung: Was sind die realen Kosten?

Wurde der Schutzbedarf ermittelt, stellt sich natürlich die Gesamtkostenfrage. Die entstehenden Gesamtkosten beim Einsatz höherer Wirkungsklassen sind dabei meist nur unwesentlich höher als im ersten Augenblick vermutet. Dies hat verschiedene Gründe.

Es kann durchaus vorkommen, dass nur kleinere Teile innerhalb einer Institution einen sehr hohen Schutzbedarf haben und die restlichen Bereiche mit einem hohen oder mittleren Schutzbedarf auskommen.

Dies hat zur Folge, dass die realen Kosten für das betreffende System nur in Relation zu diesem System stehen und umgelegt auf alle anderen Systeme effektiv betrachtet nur noch einen

Bruchteil ausmachen. Anders gesagt leiten sich die Kosten als ein prozentualer Anteil aus dem Anschaffungspreis des zu schützenden IT-Systems ab.

Hinzukommt die Tatsache, dass es durch den immer notwendigen Grundschutz auch einen Grundbetrag gibt, der immer eingeplant werden muss. Wird eine höhere Wirkungsklasse veranschlagt, so erhöhen sich die Kosten also nicht um den vollständigen prozentualen Anteil des Grundbetrags.

7.6 Rechtliche Aspekte

Am Anfang der Überlegungen zu einer Lösungsfindung für die eigene IT-Sicherheit steht, wie bereits diskutiert, die Ermittlung des eigenen Schutzbedarfes. Wie in vielen Bereichen üblich, stellt sich auch innerhalb dieses hier vorgestellten Modells die Frage nach den rechtlichen Aspekten und in wie fern diese hier eine Rolle spielen bzw. berücksichtigt werden müssen.

Die Frage dabei ist: Welche Arten der Verantwortung und der daraus möglichen Haftungsfragen können entstehen, wenn der Schutzbedarf wesentlich unterschätzt oder überschätzt wird?

Es wird Fälle geben, in denen die Treffsicherheit im Sinne der Beurteilung nicht gegeben ist und eine Einschätzung nicht korrekt durchgeführt wird.

Im allgemeinen Fall wird die Ermittlung des eigenen Schutzbedarfs und die Umsetzung in einer Organisation durch einen Verantwortlichen durchgeführt und verantwortet. Der Vorteil hier ist die detaillierte Kenntnis über die eigene Firma und die daraus resultierende Fähigkeit, den Wert eines Systems hinsichtlich der Wichtigkeit besser beurteilen zu können als Außenstehende.

Es kann aber durchaus vorkommen, dass die Umsetzung der IT-Sicherheit und die Einschätzung des Schutzbedarfes sehr schwierig sind und aus verschiedenen Gründen nicht durch die eigenen Mitarbeiter erfolgen können. In diesem Fall gibt es die Option einen externen kompetenten Dienstleister zu beauftragen dies durchzuführen. Hierbei wird im Vorfeld eine vertragliche Vereinbarung getroffen, die Rechte und Pflichten der beiden Parteien dokumentiert und dafür sorgt, dass es im Nachhinein keine bösen Überraschungen auf beiden Seiten gibt.

Wird eine juristisch handfeste Vereinbarung über den erteilten Auftrag unterzeichnet, so stellt sich die Frage nach der Verantwortung bzw. der Haftung für die Einschätzungen und die daraus resultierenden getroffenen Entscheidungen. Es kann natürlich vorkommen, dass der Dienstleister im Falle einer Fehleinschätzung eine zu niedrige Klasse wählt und so die Angriffsfläche vergrößert. Diese hätte dann ggf. vermieden werden können. Die Klasse könnte jedoch auch deutlich zu hoch gewählt worden sein, um Vorwürfen im Schadensfall aus dem Weg zu gehen, trotz möglicherweise deutlich höherer Kosten für den Anwender.

Es muss verhindert werden, dass im Eigeninteresse des beauftragten Dienstleisters die Einstufung aus juristischen Selbstschutzgründen und dessen Interesse hinsichtlich der Vermeidung der Haftung eine zu hohe Klasse empfohlen wird. Wäre eigentlich eine deutlich niedrigere Einstufung notwendig, muss dann der Nutzer diese Risikominimierung für den Auftragnehmer zusätzlich teuer bezahlen.

Hinzu kommt die Tatsache, dass nur der Nutzer und der Verantwortliche innerhalb einer Organisation die eigene IT-Landschaft so gut kennen, dass sie diese hinsichtlich Wichtigkeit, Relevanz und Risiken möglichst treffend beurteilen können. Der Wert eines IT-Systems, egal ob strategisch oder individuell, kann durch Außenstehende manchmal ganz anders (z. B. viel zu niedrig) bewertet werden, als es die Anwender selbst tun würden. Dies gilt es dabei unbedingt zu berücksichtigen.

Ist ein Dienstleister beauftragt worden, muss klar sein, dass er unter Umständen eine Mitverantwortung übernehmen muss, da seine Beurteilungskompetenzen und Verantwortung vertraglicher Bestandteil der Leistungen sind.

Am Ende trägt jedoch die entscheidende Partei die Verantwortung für die getroffenen Entscheidungen und im Normalfall ist es, aus den hier genannten Gründen, der Unternehmer selbst.

Selbst wenn sich in einer Situation die Haftungsfrage stellen sollte, ist oft der reale Wertverlust nach einem erfolgreichen Angriff von größerem Ausmaß entweder nicht zu beziffern oder existenziell bedrohlich und nicht wiedergutzumachen.

Aus all diesen Gründen sollte zum einen die rechtliche Lage vorher geklärt bzw. vereinbart werden und auch die Hauptverantwortung klar definiert sein.

7.7 Kommendes IT Sicherheitsgesetz

In naher Zukunft ist ein neues "IT-Sicherheitsgesetz" geplant, welches im Referentenentwurf vom 04.11.2014 hier Berücksichtigung finden und zu dem in dieser Ausarbeitung ein pragmatischer Verbesserungsvorschlag gemacht werden soll. Dies stützt sich auf das TeleTrusT-Strategiedokument vom 01.09.2014, das dem BMI und BMWi vorliegt.

Ein gutes IT-Sicherheitsgesetz sollte in jedem Fall gewisse Mindeststandards definieren und dadurch eine gesetzliche Basis als Hilfestellung für Anwender und die IT-Sicherheitsindustrie liefern. Dies wäre von großem Vorteil für beide Seiten, da so eine Ebene geschaffen würde, auf der sich auf Augenhöhe begegnet werden kann.

In diesem Fall könnten die hier vorgestellten Wirkungsklassen genau das leisten und sind geradezu dafür prädestiniert hier Berücksichtigung zu finden. Der vom BSI zur Verfügung gestellte "IT-Grundschutz-Katalog - 13. Ergänzungslieferung – 2013" [29] hat einen Umfang von 4.482 Seiten und ist dadurch sehr komplex was darin resultiert, dass eine genaue Evaluation und Umsetzung am Ende sehr schwierig und teuer sein kann.

Trotzdem ist es wesentlich ein System zu haben, welches mit wenig Aufwand und durch seine Übersichtlichkeit in der Lage ist dabei zu helfen, den Schutzbedarf leicht definieren, umsetzen und überprüfen zu können.

Ein weiterer Punkt ist die bereits im Vorfeld erläuterte und diskutierte Austauschbarkeit von Komponenten innerhalb von IT-Produkten, um die Sicherheit und vor allem die Vertrauenswürdigkeit zu erhöhen.

Das Wirkungsklassenmodell und die in dieser Arbeit geforderte Austauschbarkeit von kritischen Komponenten kann genau das leisten und sollte in jedem Fall Berücksichtigung finden, sofern eine nachhaltige Lösung für die heutige Problematik angestrebt wird.

7.8 Indikationen und mögliche Probleme

Wird eine durchschnittliche IT-Infrastruktur und die darin integrierten Komponenten für den Betrieb und die Nutzung dieser berücksichtigt, ist sie in der Regel sehr bunt gemischt. Geräte aller Klassen und Arten finden sich dort wieder, was natürlich zu Problemen führen kann.

So ist beispielsweise der Einsatz einer Datendiode, die selbst nur über einen sehr begrenzten funktionalen Umfang verfügt, nur dann sinnvoll, wenn die Umgebung als Ganzes passend geplant und umgesetzt worden ist. Eine Datendiode allein ist deshalb noch lange kein Garant für eine sichere unidirektionale Kommunikation. Die Verhinderung der Preisgabe von Informationen in eine ungewollte Richtung, erfordert unbedingt auch eine sorgfältige Planung, Umsetzung und Kontrolle der restlichen Infrastruktur.

Wird hierbei ein einfacherer Fall betrachtet, in dem ein kleineres Unternehmen preiswerte kleinere Geräte (z. B. Router) als Teile seines Netzwerks einsetzt, welche in der Vergangenheit oft durch Lücken aufgefallen sind, muss dies natürlich spätestens bei der Konzeption und Planung, frühestens aber bei der Ermittlung des eigenen Schutzbedarfes berücksichtigt werden.

Es ist ebenfalls bedeutend sich darüber im Klaren zu sein, dass eine Gesamteinstufung in eine bestimmte Wirkungsklasse (z. B. Klasse 2) nicht zwangsläufig den vollständigen Schutzbedarf abdeckt. Richtig ist, dass der ermittelte Gesamtschutzbedarf natürlich richtig und möglichst vollständig abgedeckt sein muss. Wichtig ist es jedoch auch darauf hinzuweisen, dass es in Ausnahmefällen vorkommen kann, dass das eingesetzte Gesamtsystem partiell zu beurteilen ist: In einigen Teilen der IT-Infrastruktur gibt es einen hohen und in anderen einen sehr hohen Schutzbedarf – alles in einer gemeinsamen Umgebung.

Es ist also notwendig, der Frage nachzugehen, ob eine Generaleinstufung möglich ist oder eine partielle Einstufung gewählt werden muss. In einem solchen Fall würden dann unterschiedliche Wirkungsklassen zum Tragen kommen.

7.9 Kontinuierliches und angemessenes IT-Sicherheitsniveau

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.

Angemessenheit: Schutzbedarf gedeckt

Jede mögliche Bedrohung und Problemstellung bringt immer die Frage nach der richtigen Lösungsstrategie mit sich. In manchen Fällen lassen sich bereits existierende Verfahren und IT-Sicherheitskonzepte anwenden, um den neuen Bedrohungen zu begegnen. Dies wird durch aktuell verfügbare Technologien gewährleistet und ermöglicht solide Problemlösungen.

Kontinuierlich: Bedrohungen von morgen und unzureichender Schutzbedarf

Es kommt jedoch durchaus vor, dass durch völlig neue Angriffsszenarien altbewährte Technologien nur unzureichend oder gar nicht schützen können. Dann stellt sich die Frage nach Innovationen, um den Problemen Herr zu werden. Hierbei muss berücksichtigt werden, dass notwendige Innovationen zwar durch Wissenschaft und Forschung gefunden und erarbeitet werden können, dies jedoch seine Zeit in Anspruch nimmt. Dabei gibt es ein gewisses Trägheitsmoment, das eine Verzögerung von fertigen Produkten zur Konsequenz hat. Vorsicht ist bekanntermaßen besser als Nachsicht und so ist es in jedem Fall weise, innovative Lösungen im Vorfeld zu erforschen und zu fördern, statt auf eine Bedrohung zu warten und dann erst mit der Arbeit für geeignete Gegenmaßnahmen zu beginnen.

In beiden Fällen sollte es ein elementares Ziel sein, durch die Zusammenarbeit zwischen Forschung und Industrie, unter dem notwendigen finanziellen Einsatz, schnellstmöglich qualitative Problemlösungen zu erarbeiten.

Ist der Fall gegeben, dass der Ermittlung des eigenen Schutzbedarfs der Schutzbedarf mit den zur Verfügung stehenden Mitteln nicht abgedeckt werden kann, müssen die fehlenden Komponenten definiert und ein Forschungsauftrag erteilt werden, der zu einer möglichen Problemlösung führt.

Der Ablauf ist in der nachfolgenden Abbildung 20 innerhalb eines möglichen Workflows schematisch dargestellt.

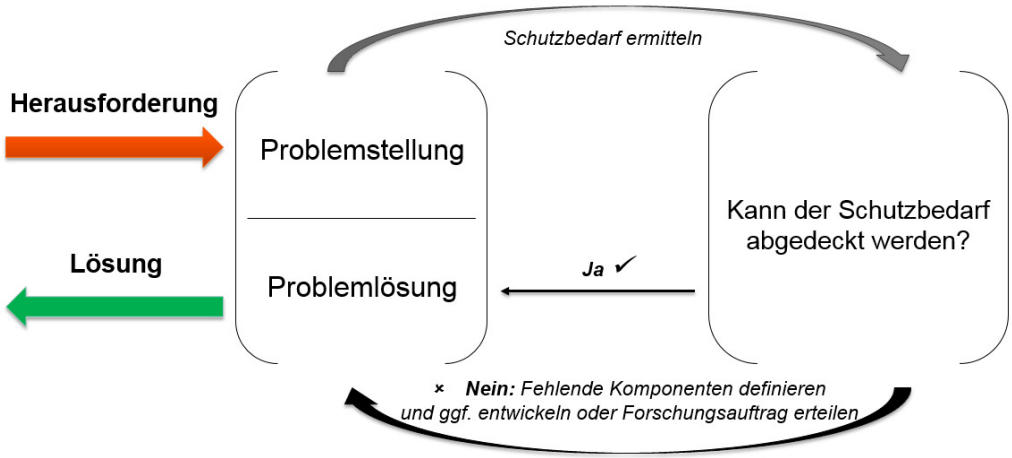


Abbildung 20 - Workflow: Von der Herausforderung zur Lösung

Der hier dargestellte Ablauf kann als eine Art Kreislauf interpretiert werden. Dieser kann dabei helfen, ein komplexes Problem und den sich daraus ergebenden Schutzbedarf zu ermitteln. Es gilt die Frage zu beantworten, ob dieser zum Zeitpunkt der Fragestellung mit den Verfügbaren IT-Sicherheitslösungen und IT-Sicherheitstechnologien abgedeckt werden kann.

Das eigene IT-Sicherheitsniveau bleibt zwar absolut gesehen grundsätzlich konstant, kann sich aber, relativ zur Entwicklung der IT-Bedrohungen gesehen, von einem auf den anderen Tag ändern. Daher ist dieser Schritt der wiederkehrenden Fragestellung nach dem eigenen Schutzbedarf notwendig und dem darauf folgenden Definitionsprozess eine hohe Dringlichkeit zuzuordnen. Es muss also die kontinuierliche Überprüfung und Erhöhung eines angemessenen IT-Sicherheitsniveaus und der Vertrauenswürdigkeit mit Hilfe deutscher Sicherheitstechnologien erreicht werden.

7.10 IT-Sicherheitsbedrohungen und -maßnahmen

Es gibt verschiedene Ansätze wie mit einer Situation umgegangen werden kann, bei der eine mögliche Lösung oder eine Expertise fehlt. Ziel ist es, eine bessere Erreichbarkeit zwischen Schutzbedürftigen und der IT-Sicherheitsindustrie herzustellen.

Lücken, die geschlossen werden müssen

Um eine gute Erreichbarkeit und Verfügbarkeit von Problemlösungen (Bezugsquellen, Expertise, Rat) zu ermöglichen, gibt es verschiedene Möglichkeiten und Hilfsmittel, die nachfolgend vorgestellt werden.

1. Problemlösungen, die existieren, sollten leicht erreichbar sein

Um Suchende und Anbieter zusammenzuführen, ist ein Werkzeug notwendig, welches als Plattform dient und den Anbietern die Möglichkeit gibt ihre Kompetenzen gut auffindbar und aktuell darzustellen. Andererseits sollte der Suchende die Möglichkeit haben, schnell und unkompliziert Hilfe zu erhalten.

Beim Finden von IT-Sicherheitstechnologien und -Lösungen helfen Plattformen wie z. B. der Marktplatz IT-Sicherheit[32] oder die Webpräsenz des TeleTrusT Bundesverbandes IT-Sicherheit e.V.[33] im Internet.

2. Forschungsinitiativen helfen bei fehlenden IT-Sicherheitstechnologien

Wie bereits diskutiert kann es vorkommen, dass IT-Prozesse, IT-Sicherheitslösungen und Innovationen fehlen. Zielführend ist es dann die fehlenden Komponenten und Prozesse auszuschreiben, um der Forschung die notwendigen Mittel zu geben, sie möglichst zeitnah zu erarbeiten.

Im Optimalfall werden diese Schritte zur Lösungsfindung zusammen mit Partnern aus der Wirtschaft durchgeführt. So ist die größtmögliche Nähe zum Markt gewährleistet.

7.11 Umgang mit Restrisiken

Werden alle Möglichkeiten ausgeschöpft und jegliche Risiken abgewogen, diskutiert und durch Vorkehrungen abgedeckt, so ist trotz allem immer noch keinesfalls garantiert, dass der Schutzbedarf vollständig gedeckt ist.

Unabhängig von der verwendeten IT-Sicherheitslösung wird es immer Restrisiken geben, die letztendlich in jedem Fall verantwortet werden müssen. Diese können verschiedene Gründe haben und hängen sowohl vom Umfeld ab, in dem sie eingesetzt werden als auch von vielen anderen gewichtigen Faktoren. Fakt ist in jedem Fall, dass manche IT-Sicherheitsgebiete nicht durch "made in Germany" abgedeckt werden können.

Jede Wahl einer Wirkungsklasse, nimmt auch bewusst ein definiertes Risiko in Kauf. Hierbei ist es entscheidend, nicht zu versuchen das Restrisiko auf 0% herabzusenken, was mit höchster Wahrscheinlichkeit niemals gelingen wird, sondern sich darüber im Klaren zu sein, dass in jedem Fall ein Restrisiko existiert. Dieses muss sich allerdings in vertretbaren Grenzen halten.

Dieses verbleibende Restrisiko kann entweder einfach akzeptiert oder im klassischen Sinne versichert werden. Hierbei kann die Versicherungsbranche passende Lösungen anbieten, um einem solchen Bedarf gerecht zu werden. Es ist jedoch auch möglich, die durchgeführte Einstufung zu überdenken und für eine finanzielle Risikominimierung eine höhere Wirkungsklasse zu nutzen.

[32] it-sicherheit.de – Der Marktplatz IT-Sicherheit: https://www.it-sicherheit.de/
[33] TeleTrusT – Bundesverband IT-Sicherheit e.V. - Pioneers in IT security. - https://www.teletrust.de/

Restrisiken sind nur dann akzeptabel, wenn zum einen alle Optionen ausgeschöpft, alle verfügbaren Wirkungsklassen in Erwägung gezogen und zum anderen die personalen Sicherheitsmaßnahmen auf angemessene Art und Weise im notwendigen Umfang durchgeführt worden sind.

8 Die nächsten Aufgaben und Schritte

Die vielen diskutierten Aspekte, Modelle und Analysen sowie auch Ideen und Vorschläge, wie die "IT Security Replaceability" sind für den Standort Deutschland von enormer Bedeutung. Möglicherweise gibt es Bereiche und Ideen, die in der Form nicht umgehend umgesetzt werden können, aber genau hier ist es bedeutsam, dass ein Versuch unternommen wird neue Wege zu gehen, Problemlösungen zu finden und geschlossen auf der einen Seite Forderungen zu stellen und auf der anderen Seite für dessen Umsetzung zu sorgen.

Nachfolgend werden die nächsten möglichen Aufgaben und Schritte diskutiert.

Die Einbindung der Stakeholder ist der Weg zum Ziel.

Wie die Abbildung 21 schematisch darstellt, müssen alle Stakeholder gemeinsam berücksichtigt werden. In der Addition aller Rollen lässt sich das gemeinsame Ziel dann schnell und effektiv umsetzen.

Zusätzlich wird für jede Gruppe der Stakeholder eine bestimmte prägnante **Rolle** als wegweisende Motivation definiert, innerhalb dieser sich die Verantwortlichen wiederfinden sollten.

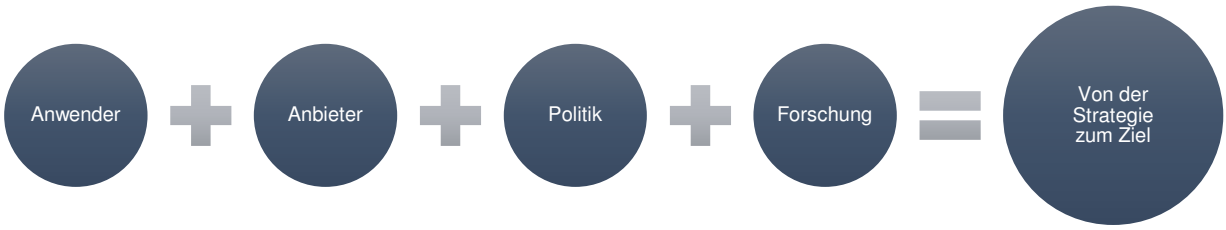


Abbildung 21 - Der Weg ist das Ziel: Wichtigkeit der Einbindung aller Stakeholder

Die Gewichtung bedeutet jedoch nicht, dass die Sichtweise der einzelnen Gruppen abgegrenzt voneinander Gehör finden sollte, ganz im Gegenteil. Dieses Konzept kann nur dann sinnvoll umgesetzt werden und seine Wirkung entfalten, wenn wirklich alle Stakeholder gemeinsam die vorgegebenen Rollen wahrnehmen und zeitlich und räumlich zusammenfinden, um Verantwortung zu übernehmen und den Aufgaben in jeder Rolle gerecht zu werden. Das Ziel dabei:

- Eine **gemeinsame** Strategie festlegen, so dass alle Stakeholder das gemeinsame Ziel kennen und sich über **Forderungen und Wünsche im Klaren sind**.
- **Jeder Stakeholder spielt eine wesentliche Rolle**, damit das gemeinsame Ziel erreicht werden kann.
- Die gemeinsame Strategie und der **gesamte Prozess** müssen strukturiert werden und sollten **systematisch** angegangen werden.

8.1 Die wichtigsten Stakeholder

Die erarbeiteten Ergebnisse und die sich daraus ergebenden Aufgaben müssen durch die wichtigsten Stakeholder getragen werden. Dies sind im Kern:

- **Anwender** (Verbände, Vereine, Gruppen)
- **IT-Sicherheitsanbieter** (Verbände, Vereine, Gruppen)
- **Politik, Gesetzgeber**
- **Wissenschaft und Forschung**

Jede Gruppe muss eine bestimmte Art von Verantwortung übernehmen, die nachfolgend im Detail erläutert wird.

8.1.1 Anwender

Der Anwender ist hier die benutzende Person eines IT-Systems, die einzeln oder in einer gemeinsamen Gruppierung (z. B. eine bestimmte Abteilung oder eine Interessen geprägte Formation) auftreten kann. Die Gruppe der Anwender muss möglichst klar definieren, welche Features hinsichtlich Ausstattungs- und Leistungsmerkmalen sie in welchen Wirkungsklassen benötigt.

Die Anwender müssen möglichst genau definieren, welche Technologien mit welchen IT-Sicherheitsfeatures sie brauchen, damit sie sicher ihre Ziele erreichen können.

Die Anwender müssen sich zusammentun, damit sie gegenüber IT-Marktführern die **IT Security Replaceability** motivieren können: Geschlossen etwas zu verlangen, hat eine größere Marktmacht.

IT-Sicherheitslösungen, die alle IT-Sicherheitsaspekte einfach von einer Stelle verwalten lassen, ermöglichen eine höhere Sicherheit.

Grundsätzlich wären hier Empfehlungen für mögliche Wünsche beispielsweise mehr Verschlüsselung, mehr Isolierung und Separierung und höherer Bedienkomfort.

Zudem sollte sich die Gruppe der Anwender an den Wirkungsklassen orientieren, damit die Strategie schnell und effektiv umgesetzt werden kann.

Rolle: Äußerung eines spezifischen Verlangens.

8.1.2 IT-Sicherheitsanbieter

Die Sicherheitsanbieter haben von Ihrer Seite aus die Aufgabe, IT-Sicherheits-Bundles als maßgeschneiderte und vertrauenswürdige Produkte und Lösungen zu definieren und umzusetzen, die für die einzelnen Wirkungsklassen zum Einsatz kommen sollen.

Die IT-Sicherheitsanbieter müssen passende Produkte möglichst zusammenfassend so anbieten, dass sie sich leicht in die IT-Umgebungen einbinden lassen. Dabei sollten sie möglichst schnell und international sein, damit ihre Produkte einen guten Preis erzielen können.

Die Stärken der IT-Sicherheit in Deutschland müssen noch besser werden. Die existierenden Lücken gilt es dabei auszugleichen, wie die Technologieanalyse zusammenfassend offenbart hat.

Ein wichtiges Ziel dabei ist es, dass Produkte **unkompliziert**, **einheitlich**, **benutzbar**, **stabil** und **sicher** sein müssen. Auch die reibungslose Integration in bereits vorhandene IT-Lösungen muss sichergestellt werden.

Nur so ist es möglich, auf lange Sicht gesehen sowohl hochwertige als auch sichere IT-Sicherheitslösungen zu etablieren.

Auch die Hersteller sollten sich dabei an den Wirkungsklassen orientieren, damit die Strategie effektiv umgesetzt werden kann.

Rolle: Bundleanbieter abgestimmter Produkte.

8.1.3 Politik, Gesetzgeber

Die Politik und im Detail auch der Gesetzgeber müssen zukünftig viel stärker und bewusster, unter Berücksichtigung der Marktsituation und der internationalen Mitbewerber, mit den ihnen zur Verfügung stehenden Mitteln neue Anreize schaffen. Dies können verschiedene Werkzeuge wie Motivation, Regulierung verschiedener insbesondere kritischer Bereiche, dem Aussprechen von Empfehlungen und einer nachhaltigen Gesetzgebung sein, die hier eine wesentliche Rolle spielen.

Ein besonders bedeutsamer Aspekt ist die Wahrung der technologischen Souveränität und der Verhinderung von Abwanderung und Veräußerung deutscher IT-Sicherheitstechnologien ins Ausland.

Gibt es beispielsweise nur einen Anbieter für Technologien, die innerhalb von kritischen Infrastrukturen Anwendung finden - sprich eine besondere Rolle in den höheren Wirkungsklassen spielen - muss ein Verkauf ins Ausland oder andere Wege der Einflussnahme durch ausländische Interessensgruppen unbedingt verhindert werden. Versäumnisse an dieser Stelle und der Verlust von Souveränität haben negative Konsequenzen für diese Technologien.

Auch sollte die Politik die Chance ergreifen und die Förderung von Forschung und Entwicklung deutlich weiter ausbauen. Nichts ist nachhaltiger und sinnvoller als die Investition in zukünftige Innovationen im Bereich von IT-Sicherheitstechnologien und der sich daraus ergebenden Möglichkeiten und Chancen.

Eine weitere Möglichkeit wäre der Abbau von Bürokratie innerhalb der zuständigen Behörden und in den Hochschulen selbst: Beispielsweise unkompliziertere Verfahren und kürzere Dienstwege.

Die Gesetzgeber müssen ihre Rolle bei der Hilfestellung für den deutschen Mittelstand während der Einführung der Wirkungsklassen erkennen und die notwendige Verantwortung übernehmen.

Rolle: Regulierung und Hilfestellung.

8.1.4 Wissenschaft und Forschung

Häufig müssen neue und richtungsweisende Denkansätze erarbeitet werden, weil die alten nicht ausreichend, ungenügend oder veraltet sind. In Kompetenzzentren an den Hochschulen und vergleichbaren Institutionen gibt es viele Expertisen, mit denen diesen Herausforderungen begegnet werden kann.

Also dort wo sich Lücken und wichtige IT-Sicherheitstechnologiefelder befinden, muss besonders geforscht werden. Wie die Technologieanalyse aufzeigt, gibt es dafür sehr viel Raum und eine große Notwendigkeit.

Die Wissenschaft und Forschung kann, mit entsprechenden finanziellen Ressourcen, die Entwicklung von modernen und notwendigen IT-Sicherheitstechnologien umsetzen. Nur so kann den kontinuierlich steigenden Anforderungen genüge getan werden.

Hierbei ist zukünftig eine noch engere Zusammenarbeit mit der IT-Sicherheitsindustrie notwendig.

Rolle: Finden und Erarbeiten von Innovationen.

8.2 Vorgehen: Der nächste Schritt zum Ziel

Um die hier aufgeführten Ziele zu erreichen, ist die Einführung und Umsetzung eines strukturierten Prozesses notwendig, damit die gemeinsamen Aufgaben zielgerichtet umgesetzt werden können.

Eine Möglichkeit dieses Ziel zu erreichen ist es, den Großteil der wichtigsten Stakeholder an einem runden Tisch zu versammeln. Es sei nochmals aufgrund der Relevanz darauf hingewiesen, dass die Umsetzung dieses Konzeptes nur dann gelingen kann, wenn sich die einzelnen Interessensgruppen gemeinsam zusammensetzen und über die Wünsche und möglichen Lösungen sprechen.

Von einer Zusammenkunft einzelner Stakeholder ohne die anderen Gruppen wird in jedem Fall abgeraten, da dies im Widerspruch zu der hier vorgestellten Idee steht und nicht zielführend ist. Hierbei gilt:

"TeleTrusT ist bereit, hier eine besondere Verantwortung zu übernehmen."

Einige Vorschläge für weitere Schritte sind beispielsweise die exaktere Definition und Umsetzung der vorgeschlagenen Wirkungsklassen oder als gesetztes Ziel eine stärkere Verwendung von E-Mail-Verschlüsselung. Weitere zu erreichende Ziele sind ein besserer Schutz der Infrastruktur in Deutschland vor Sabotage und die deutliche Absenkung von Malware-Infektionen.

8.3 Umsetzungsvorschlag

Nachfolgend ist ein mögliches Vorgehen dargelegt, mit dessen Hilfe sich der Vorschlag dieses Konzeptes umsetzen lässt. Der Umsetzungsplan lässt sich in zwei Bereiche unterteilen. Der erste Bereich beinhaltet die einmalig auszuführenden Schritte, welche im zeitlichen Verlauf einem bestimmten Zeitpunkt zugeordnet sind. Der zweite Bereich beinhaltet wiederkehrende Aufgaben, welche periodisch immer wieder ausgeführt werden müssen.

Einmalig:

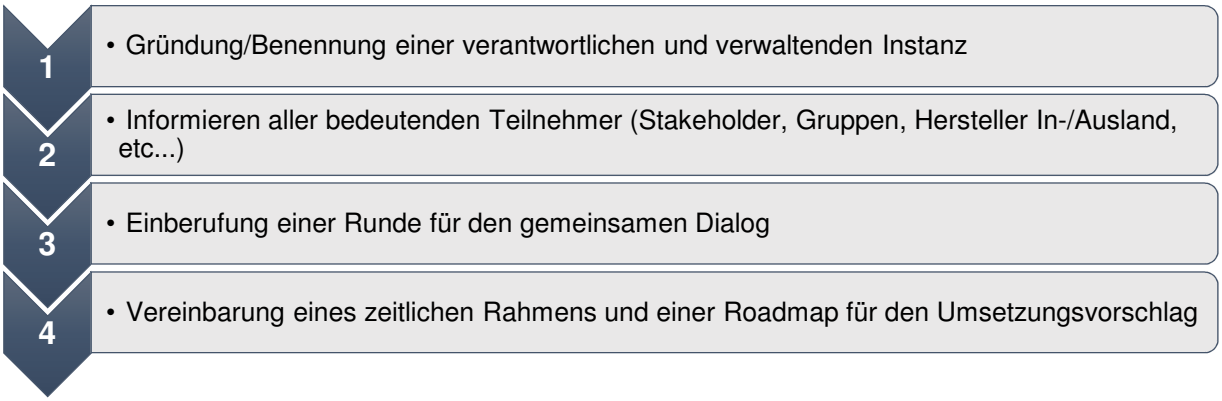


Abbildung 22 - Abfolge der einmalig auszuführenden Schritte

Periodisch:

Abbildung 23 - Periodisch sich wiederholende Schritte

Nur ein koordiniertes und **gemeinsames** Vorgehen setzt genug Energie frei, um das Ziel **gemeinschaftlich** zu erreichen.

9 Fazit und Ausblick

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 endlich 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.

Wirkungsklassen

Soll ein angemessener Schutz geplant und umgesetzt werden, stehen einem Verantwortlichen zwar einige Werkzeuge in Form von Katalogen und Richtlinien zu Verfügung, aber der Umfang und die Kosten sind im Falle einer Umsetzung immens. Selbst die Entscheidung zu treffen, was genau zu berücksichtigen ist und was nicht, scheint bereits eine nur schwer überwindbare Hürde zu sein.

In diese Kerbe schlagen die Wirkungsklassen hervorragend hinein und können genau an dieser Stelle enorme Hilfestellung leisten. Werden in Zukunft die Forderungen aus dieser Arbeit konsequent umgesetzt, wäre dies ein großer Gewinn für den Stand der IT-Sicherheit in Deutschland. Der Anwender sollte nun einfordern was er benötigt, wie zum Beispiel eine einfache und sichere E-Mail-Verschlüsselung, die nach Wirkungsklassennorm von Herstellerseite aus eingestuft ist. Die IT-Sicherheitshersteller sollten dann die geforderten Produkte in hoher Qualität liefern.

Technologieanalyse

Der IT-Sicherheitsmarkt ist sehr dynamisch und unterliegt stetigen Veränderungen. Im Hinblick auf die zukünftige Forschungsarbeit in diesem Bereich ist es sinnvoll, die Technologieanalyse weiter zu optimieren und zu erweitern. Neben inhaltlichen Anpassungen zwecks weiteren Vervollständigungen für ein besseres Abbild der IT-Sicherheitslandschaft, wäre es denkbar eine Art Infografik zu erstellen. Diese könnte, basierend auf der Technologieanalyse, eine grafisch bessere und umfangreichere Darstellung ermöglichen. Auch eine Webversion mit einer aktiven Suchmöglichkeit und der Verlinkung auf die relevanten Produkte und deren Anbieter wäre als sinnvolle Ergänzung zum "Marktplatz IT-Sicherheit"[34] denkbar.

Im Hinblick auf die zukünftige Entwicklung wäre es sinnvoll zu evaluieren, ob neue Kategorien ihren Weg in die Analyse finden sollten. Das Feld ist sehr breit und eine Erweiterung um weitere Themenbereichen sollte in Betracht gezogen werden. Hierbei sind neben der Konsolidierung bestehender Kategorien auch neue denkbar, wie sicheres Löschen oder BDSG[35]-konformes Netzwerk-Monitoring.

Zusätzlich ist für die reale Stärke der Unternehmen eine Recherche notwendig. Diese sollte national und international durchgeführt werden. Ein Hauptziel dabei wäre es zu ermitteln, in welcher Relation sich die einzelnen Kontrahenten gegenüberstehen. So würden kommende Start-ups in den einzelnen Bereichen anders bewertet werden als etablierte Marktgiganten.

Denkbar ist auch eine formale Beschreibung jeder Technologie mit Hilfe einer mathematischen Formel. Dabei könnten verschiedene Faktoren eine Gewichtung bekommen, die dann in der Summe einen Wert ergeben. Je nach Bedeutung der Faktoren wäre die Gewichtung höher oder niedriger anzusetzen. Wünschenswert wäre am Ende eine konkrete Kennzahl, an der sich auf den ersten Blick ablesen lässt, wie gut oder schlecht der Stand der deutschen IT-

[34] „Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.“ - https://www.it-sicherheit.de/

[35] „Bundesdatenschutzgesetz“ - http://www.gesetze-im-internet.de/bdsg_1990/

Sicherheitsindustrie ist. Dieser Punkt ist keinesfalls trivial, da zahlreiche Faktoren wie Unternehmensgröße, Marktwert und die Marktgegebenheiten der einzelnen Kategorien sehr unterschiedlich ausfallen.

Insgesamt gilt es die Ohnmacht **gemeinsam** zu überwinden und die Energie nicht auf "verschiedenen Baustellen" aufzuwenden, sondern sie **zu bündeln** und in eine einzige gemeinsame Richtung zu lenken.

Wenn dies gelingt, wird sich der Erfolg gar nicht vermeiden lassen.

» In zweifelhaften Fällen entscheide man sich für das Richtige. «

Karl Kraus (1874-1936),
östr. Kritiker, Satiriker, Essayist u. Dramatiker

10 Literaturverzeichnis

1. DOMINIQUE PETERSEN, NORBERT POHLMANN. Wiederaufbau - Verschlüsselung als Mittel gegen die Überwachung. Nach dem Heartbleed-Desaster ist es nicht damit getan, alle Web-Passwörter zu ändern, denn Webbrowser können selbst dann auf unsichere Weise kommunizieren, wenn das grüne Zertifikatssymbol erscheint und der Server keine SSL-Lücke mehr aufweist. *iX,* 2014, (5), 82-86.

2. PETER PAGEL. Aktuelle Studie belegt Zunahme von Cyber-Kriminalität [online]. Trotz steigender Investitionen in die IT-Sicherheit nimmt die Bedrohung durch Angriffe aus dem Cyberspace weiter zu. Während sich Kriminelle neuester Technologien bedienen, unterschätzen viele Unternehmen die Risiken. *Redaktion Springer für Professionals - Business IT,* 30. Sep. 2013. Verfügbar unter: http://www.springerprofessional.de/studie-cyberkriminalitaet/4717598.html

3. NORBERT POHLMANN und HELMUT REIMER. *Trusted Computing. Ein Weg zu neuen IT-Sicherheitsarchitekturen.* Wiesbaden: Friedr. Vieweg & Sohn Verlag / GWV Fachverlage, Wiesbaden, 2008. ISBN 978-3-8348-0309-2.

4. NORBERT POHLMANN und HARTMUT F. BLUMBERG. *Der IT-Sicherheitsleitfaden. [das Pflichtenheft zur Implementierung von IT-Sicherheitsstandards im Unternehmen ; IT-Sicherheit als kontinuierlichen Geschäftsprozess gestalten und steuern, IT-Sicherheitslösungen konzipieren und in ihrer Wirksamkeit kontrollieren, Normen der IT-Sicherheit adaptieren und anwenden (ISO/IEC 13335, ISO/IEC 27001 etc.)].* 2., aktualisierte Aufl. Heidelberg: mitp, Redline, 2006. ISBN 3826616359.

5. JUDITH HORCHERT. Spähaffäre: NSA kauft Infos über Sicherheitslücken bei französischer Firma [online]. Je schwächer das System, desto leichter hat es die NSA: Laut einem jetzt veröffentlichten Dokument soll der Geheimdienst bei der Sicherheitsfirma Vupen Informationen über Schwachstellen und Lücken gezielt einkaufen. *Spiegel Online,* 17. Sep. 2013. Verfügbar unter: http://www.spiegel.de/netzwelt/netzpolitik/nsa-kauft-infos-ueber-sicherheitsluecken-von-vupen-a-922765.html

6. WIKIPEDIA. *Fehlerquotient,* 2014. 9 Dezember 2014, 12:00 [Zugriff am: 14. Dezember 2014]. Verfügbar unter: https://de.wikipedia.org/w/index.php?oldid=136301178

7. KASPERSKY LAB. *Jahresstatistik 2013: Kaspersky Lab entdeckt täglich 315.000 neue Schadprogramme. Kaspersky Lab gibt seine Jahresstatistiken für 2013 bekannt [1]. Der IT-Sicherheitsexperte entdeckt täglich 315.000 neue Schadprogramme – das entspricht einer Steigerung von über 57 Prozent gegenüber dem Vorjahr. Deutschland taucht mit Platz 13 im Jahr 2013 erstmals unter den Top-20 der am meisten über das Internet gefährdeten Länder weltweit auf. Zudem stieg im Vergleich zum Vorjahr das Aufkommen mobiler Schädlinge um 125 Prozent an.,* 2013. Verfügbar unter: http://www.kaspersky.com/de/about_kaspersky/news/virus/2013/Jahresstatistik_2013_Kaspersky_Lab_entdeckt_taglich_315000_neue_Schadprogramme_

8. FRIEDHELM GREIS, EDWARD SNOWDEN. Überwachung: Snowden empfiehlt Spideroak statt Dropbox [online]. US-Whistleblower Edward Snowden vertraut seine Daten einem Dienst an, der mit "Zero Knowledge" wirbt. Für bestimmte Berufsgruppen sei Verschlüsselung inzwischen unentbehrlich. *Golem.de,* 18. Jul. 2014. Verfügbar unter: http://www.golem.de/news/ueberwachung-snowden-empfiehlt-spideroak-statt-dropbox-1407-107970.html

9. AMMAR ALKASSAR, STEFFEN SCHULZ und CHRISTIAN STÜBLE. Sicherheitskern(e) für Smartphones: Ansätze und Lösungen. Vom Mikrokern bis zu Capabilities – Verschiedene Lösungsansätze für die App-Trennung und -Kontrolle. *DuD • Datenschutz und Datensicherheit,* 2012, (3), 175-179.

10. JÖRG THOMA. *Windows XP: Britische Regierung zahlt bis 2015 für Support - Golem.de,* 2014 [Zugriff am: 14. Dezember 2014]. Verfügbar unter: http://www.golem.de/news/windows-xp-britische-regierung-zahlt-bis-2015-fuer-support-1404-105637.html

11. ULI RIES. *Def Con 22: Millionen DSL-Router durch TR-069-Fernwartung kompromittierbar,* 2014. 15 August 2014, 12:00 [Zugriff am: 14. Dezember 2014]. Verfügbar unter: http://www.heise.de/netze/meldung/Def-Con-22-Millionen-DSL-Router-durch-TR-069-Fernwartung-kompromittierbar-2292576.html

12. NORBERT POHLMANN. *Firewall-Systeme. [Firewall-Elemente und Sicherheitskonzepte ; Verschlüsselungs- und Authentikationsverfahren ; Security Audit, Bedrohungsprofile, IT-Kostenschätzung].* 5., aktualisierte Aufl. Bonn: Mitp, 2003. Sicherheit. ISBN 3826609883.

13. NORBERT POHLMANN. Die Krise als Chance begreifen [online]. Der IT-Sicherheitsexperte Prof. Pohlmann sieht die Enthüllungen über die Aktivitäten der NSA als große Chance, zu lernen wie Spione und Hacker unseren Schutz umgehen und darauf aufbauend bessere IT-Sicherheitstechnologien anzubieten. *heise Security,* 1. Nov. 2013, 2014. Verfügbar unter: http://heise.de/-2037053

14. BRIGITTE ZYPRIES, MDB, PARLAMENTARISCHE STAATSSEKRETÄRIN BEIM BUNDESMINISTER FÜR WIRTSCHAFT UND ENERGIE. *Geleitwort zu "IT Security made in Germany",* 2014.

15. TELETRUST – BUNDESVERBAND IT-SICHERHEIT E.V. *Voraussetzungen für die Mitwirkung/Teilnahme.* Verfügbar unter: https://www.teletrust.de/itsmig/teilnahme/

16. BERND UNGERER. *Datendiode gegen Datendiebe,* 10. Mrz. 2014. 10 März 2014, 12:00 [Zugriff am: 8. Dezember 2014]. Verfügbar unter: http://www.heise.de/newsticker/meldung/Datendiode-gegen-Datendiebe-2139499.html

17. BSI. *Remote-Controlled Browsers System (ReCoBS). Grundlagen und Anforderungen,* 2006. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/recobslanginfo_pdf.pdf?__blob=publicationFile

18. ITWATCH GMBH. *ReCAppS: Remote Controlled Sessions - Sicherheit durch Virtualisierung* [Zugriff am: 8. Dezember 2014]. Verfügbar unter: http://www.itwatch.de/Produkte/ReCAppS

19. DOMINIQUE PETERSEN, SEBASTIAN BARCHNICKI, NORBERT POHLMANN. Schutz- und Frühwarnsysteme für mobile Anwendungen. Angriffspotentiale, Schutzmechanismen und Forschungsaspekte für Smart Mobile Devices. *DuD • Datenschutz und Datensicherheit,* 2014, (01).

20. JÜRGEN SEEGER. *To cloud or not to cloud,* 12. Okt. 2011. 12 Oktober 2011, 12:00 [Zugriff am: 14. Dezember 2014]. Verfügbar unter: http://www.heise.de/ix/artikel/To-cloud-or-not-to-cloud-1355056.html

21. VOGEL BUSINESS MEDIA GMBH & CO. KG. *60 Prozent der KMU beklagen Malware-Infektionen* [Zugriff am: 15. Dezember 2014]. Verfügbar unter: http://www.security-insider.de/themenbereiche/sicherheits-management/sicherheitsvorfaelle/articles/385379/

22. 2013, *Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management*.

23. BUNDESNETZAGENTUR. *Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung. Übersicht über geeignete Algorithmen.* Mainz, 18. Feb. 2013.

24. TELETRUST – BUNDESVERBAND IT-SICHERHEIT E.V. *Kriterienkatalog. Bewertungskatalog zur Vergleichbarkeit biometrischer Verfahren*.

25. AFP/RAS. Kreml-Jugend bekennt sich zu Attacke auf Estland [online]. Russische Hacker rüsten auf. Die Jugendorganisation des Kreml hat sich zu den Sabotageakten gegen Webseiten estnischer Behörden vor zwei Jahren bekannt. Die Internet-Angriffe hatten zu einer vorübergehenden Schließung von estnischen Regierungsseiten geführt und die Geschäfte führender Unternehmen behindert., 11. Mrz. 2009. Verfügbar unter: http://www.welt.de/wirtschaft/webwelt/article3355416/Kreml-Jugend-bekennt-sich-zu-Attacke-auf-Estland.html

26. Estland im Visier "Ist ein Internetangriff der Ernstfall?" [online]. Eine beispiellose Computerattacke legte vor kurzem in Estland Banken, Behörden, Polizei und Regierung für mehrere Tage lahm. Bis heute ist unklar, wer dafür verantwortlich war. Im F.A.Z.-Interview spricht der estnische Präsident Ilves über die Attacke, Russland und die Nato. *FAZ,* 18. Jun. 2007. Verfügbar unter: http://www.faz.net/aktuell/politik/ausland/estland-im-visier-ist-ein-internetangriff-der-ernstfall-1436040.html

27. BUNDESMINISTERIUM DES INNERN. *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Definition "Kritische Infrastrukturen"*.

28. DOMINIQUE PETERSEN, NORBERT POHLMANN. *Advances in IT early warning. An Ideal Internet Early Warning System.* Stuttgart: Fraunhofer Verlag, 2013. ISBN 9783839604748.

29. BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK. *IT-Grundschutzkataloge 13. Ersatzlieferung-2013.* Bonn, September 2013.

11 Abbildungsverzeichnis

Abbildung 1 - Mögliche farbliche Indikationen 6
Abbildung 2 - Grafische Darstellung der zeitlichen Entwicklung von IT-Sicherheitsstandards 7
Abbildung 3 - Wirksamkeit von IT-Sicherheit [12, S.405] 21
Abbildung 4 - Penetration von IT-Systemen und Mindeststärke [12, S.406] 22
Abbildung 5 - TeleTrusT-Initiative "IT Security made in Germany" Siegel 24
Abbildung 6 - Bewertungselement zur visuellen Darstellung von A bis D 27
Abbildung 7 - Durchschnitt für den Bereich: Sichere Vernetzung 44
Abbildung 8 - Durchschnitt für den Bereich: Sicherer Internetzugang 44
Abbildung 9 - Durchschnitt für den Bereich: Digital Enterprise Security 45
Abbildung 10 - Durchschnitt für den Bereich: Client- und Serversicherheit 45
Abbildung 11 - Durchschnitt für den Bereich: Mobile Security 45
Abbildung 12 - Prinzipielle Einstufung der Vertrauenswürdigkeit und Wirkung 51
Abbildung 13 - IT Security Replaceability innerhalb eines Betriebssystems (Schema) 52
Abbildung 14 - Beispiele möglicher Ziele 55
Abbildung 15 - Notwendigkeit der Erbringung von Nachweisen 59
Abbildung 16 - Wirkung per Definition gegeben 59
Abbildung 17 - Wirkungsklassen aus der Perspektive von IT-Sicherheitsbedrohungen 61
Abbildung 18 - Das Wirkungsklassenmodell 65
Abbildung 19 - Definition einer Wirkungsklasse und ihrer Elemente 68
Abbildung 20 - Workflow: Von der Herausforderung zur Lösung 75
Abbildung 21 - Der Weg ist das Ziel: Wichtigkeit der Einbindung aller Stakeholder 79
Abbildung 22 - Abfolge der einmalig auszuführenden Schritte 83
Abbildung 23 - Periodisch sich wiederholende Schritte 83

12 Tabellenverzeichnis

Tabelle 1 – Fehlerdichte pro 1000 Zeilen Code und Klassifizierung von Programmen [6].....18
Tabelle 2 - Erläuterung des Aufbaus der Tabellen innerhalb der Analyse.....26
Tabelle 3 - Legende für die Bewertungskriterien und deren Interpretation.....27
Tabelle 4 - Legende der farblichen Bewertungsskala für die Eigenschaften A, B, C und D...27
Tabelle 5 - Technologiebetrachtung sichere Anbindung mobiler User / Telearbeiter 28
Tabelle 6 - Technologiebetrachtung Layer3 Virtual Private Network (L3VPN) 28
Tabelle 7 - Technologiebetrachtung Layer2-Encryption.....29
Tabelle 8 - Technologiebetrachtung Datendiode 29
Tabelle 9 - Technologiebetrachtung Firewall-Systeme 30
Tabelle 10 - Technologiebetrachtung IPS/IDS.....30
Tabelle 11 - Technologiebetrachtung Remote-Controlled Browsers System (ReCoBS) 31
Tabelle 12 - Technologiebetrachtung Virtuelle Schleuse 31
Tabelle 13 - Technologiebetrachtung Authentifikation 32
Tabelle 14 - Technologiebetrachtung sichere Anbindung zwischen Anbieter und Anwender32
Tabelle 15 - Technologiebetrachtung Hardware-Sicherheitsmodul (HSM).....32
Tabelle 16 - Technologiebetrachtung Public-Key-Infrastruktur (PKI).....33
Tabelle 17 - Technologiebetrachtung Antivirus und Personal Firewall 34
Tabelle 18 - Technologiebetrachtung Exploit Protection / Sicherer Browser 34
Tabelle 19 - Technologiebetrachtung Device- und Portkontrolle.....35
Tabelle 20 - Technologiebetrachtung Festplattenvollverschlüsselung 36
Tabelle 21 - Technologiebetrachtung File & Folder Encryption (Objektverschlüsselung) 36
Tabelle 22 - Technologiebetrachtung Voll-Virtualisierung/Trusted Computing, Separation ...37
Tabelle 23 - Technologiebetrachtung Data Leakage Prevention.....37
Tabelle 24 - Technologiebetrachtung E-Mail-Verschlüsselung 38
Tabelle 25 - Technologiebetrachtung Sicheres Logon (Smartcard etc.).....38
Tabelle 26 - Technologiebetrachtung Remote Access / Secured VPN 39
Tabelle 27 - Technologiebetrachtung App Security / Secure Marketplace 39
Tabelle 28 - Technologiebetrachtung Sichere Plattform 40
Tabelle 29 - Technologiebetrachtung Cloud Encryption (Cloud Verschlüsselung) 40
Tabelle 30 - Technologiebetrachtung Voice Encryption (Sprachverschlüsselung) 41
Tabelle 31 - Technologiebetrachtung Secure Instant Messaging.....42
Tabelle 32 - Technologiebetrachtung Mobile Device Management.....42
Tabelle 33 - Technologiebetrachtung Basistechnologie (Secure Execution Environment) 43
Tabelle 34 - Übersicht aller Ergebnisse im Durchschnitt als Gesamtmatrix 46
Tabelle 35 - Übersicht aller Einzelergebnisse im Detail als Gesamtmatrix.....47
Tabelle 36 - Darstellung: Prinzipielle Wirkung 57
Tabelle 37 - Darstellung: Konkrete Wirkung 58
Tabelle 38 - Darstellung: Gewollte Wirkung.....59
Tabelle 39 - Definition von Begriffen aus Sicht der Anwender 67
Tabelle 40 - Definition von Begriffen aus Bedrohungssicht.....67