Cyberreadiness in kleinen und mittleren Unternehmen

Dr. Sandro Gaycken

Dr. Rex Hughes
Wolfson College, University of Cambridge

Studie Digital Society Institute Berlin, ESMT Berlin, im Auftrag des DIHK

DIGITAL SOCIETY INSTITUTE BERLIN

DIHK Deutscher Industrie- und Handelskammertag

Cyberreadiness in kleinen und mittleren Unternehmen
November 2015

Inhaltsverzeichnis

Executive Summary

Kleine und mittlere Unternehmen sind meist nicht „cyber-ready“. Sie können kaum adäquate Cybersicherheit herstellen. Die Anforderungen sind zu komplex, viele Technologien und Assessments sind zu teuer, Risiken sind schwer einzuschätzen, und sowohl IT- wie IT-Securitymarkt sind im Bezug auf Sicherheit noch als unreif zu bewerten.

Die vorliegende Studie will kleinen und mittleren Unternehmen eine Handreiche zur Verbesserung der Cyberreadiness liefern. Die Autoren gehen dabei davon aus, dass es für kleine und mittlere Unternehmen noch auf absehbare Zeit zu schwierig sein wird, eigene objektive Einschätzungen der Risiken und der Bedürfnisse sowie der Probleme und Möglichkeiten verschiedener Varianten von IT und IT-Sicherheit vorzunehmen.

Als Strategie soll daher empfohlen werden, auf Basis einer ersten Selbsteinschätzung einen guten Partner zu finden, der das Thema Sicherheit ernsthaft und kompetent betreibt. Für diese Schritte wurde in der Studie eine kleine und einfache Methodik für eine erste und grobe Risikoabschätzung entwickelt. Anschließend folgt als Hauptteil der Studie eine Entwicklung von zwei Gruppen von insgesamt 107 Faktoren, anhand derer (1) die potentielle Verwundbarkeit eines IT-Produkts abgeschätzt werden kann und (2) die Qualität eines IT-Sicherheitsprodukts bewertet werden kann. Die Faktoren sind dabei „externe“ Faktoren, da sie sich nicht mit möglichen inneren Funktionen und Effizienz befassen, sondern mit äußeren Merkmalen der Technik und der Unternehmen. Dies hat zur Ursache, dass aussagefähige innere Qualitätsmerkmale gegenwärtig noch nicht definiert und klar und vergleichend messbar sind, so dass also nur durch äußere Faktoren, die klar bestimmbar sind, eine Einschätzung erfolgen kann.

Die Studie wird abgeschlossen mit einer Reihe politischer Empfehlungen der Autoren, mit deren Hilfe sich die Cyberreadiness kleiner und mittlerer Unternehmen verbessern lässt.

1. Die Bewertung von Cyberrisiken für KMUs

Was bedeutet Cybersecurity für mein Unternehmen?

1.1 Einführung: Wie komme ich von verschiedenen Lagebildern zur Praxis?

Inzwischen existieren zahlreiche Lagebilder und Empfehlungen zur IT-Sicherheit oder Cybersicherheit. Für kleine und mittlere Unternehmen sind diese Papiere oft wenig hilfreich. Viele sind zu umfangreich, beschreiben viele verschiedene Angriffsvarianten und Probleme, und arbeiten in Fachsprachen, so dass ein direkter und geordneter Bezug der Relevanz einzelner Themen für das eigene Unternehmen nicht ohne weiteres möglich ist. Die Papiere unterscheiden sich zudem teilweise stark in ihren Einschätzungen von Risiken und Maßnahmen und sind nur bei kleinen, wenig kontroversen und einfachen Punkten wie der Mitarbeitersensibilisierung gegen Betrugsversuche, dem richtigen Einsatz von Passwörtern und dem Patching konkreter, während viele spezifischere technische, organisatorische, operative und rechtliche Fragestellungen nur indiziert werden und erneut recht unterschiedlich ausfallen können.

Die mangelnde Ordnung der Problemlandschaft sowie Unterschiedlichkeit und mangelnde Konkretheit in Risikobewertungen und Empfehlungen sind vier Grundproblemen der Cybersicherheit geschuldet: dauerhafter Wissenslücken, der Problemkomplexität, der Lösungskomplexität und interessensgebundenen Befangenheiten.

Dauerhafte Wissenslücken sind in der Cybersicherheitsforschung bereits lange ein bekanntes Problem.[1] Man weiß stets nur sehr wenig über die Angreifer, weil diese nur schwer zu beobachten sind. Lediglich die besonders schlechten und offensichtlichen Angriffe wie massenhaft maschinell erzeugte Virenvarianten und besonders drastische Betrugsschemata sind leicht erkennbar, aber selbst dort sind die dahinter liegenden Taktiken und Geschäftsmodelle wenig bekannt und nur schwer interpretierbar. Auch bei konkreten Vorfällen ist man nicht unbedingt schlauer. Man sieht oft nur einen Einbruch, mit etwas Glück und gutem Logging erhält man noch eine Ahnung, was passiert sein kann und die Andeutung einer Spur, in welche Richtung die Daten zuerst abgeflossen sind. Warum man aber angegriffen wurde, wer einen angegriffen hat, was insgesamt alles verschwunden ist und was damit gemacht wird – das weiß nur der Angreifer.

[1] Siehe etwa: Royal Society (2013). „Seeking evidence to inform cybersecurity research“, online unter https://royalsociety.org/~/media/Royal_Society_Content/policy/projects/cybersecurity-research/2013-11-20-cybersecurity-research-challenges.pdf?la=en-GB; Frinking, E. & Maarten, G.. „A Bird’s Eye View of the Current Research Portfolio“ (2014), online unter: http://www.hcss.nl/reports/download/190/3147/; Tsohou, Aggeliki, et al. "Investigating information security awareness: research and practice gaps." *Information Security Journal: A Global Perspective* 17.5-6 (2008): 207-227; Biener, Christian, Martin Eling, and Jan Hendrik Wirfs. "Insurability of Cyber Risk: An Empirical Analysis†." *The Geneva Papers on Risk and Insurance-Issues and Practice* 40.1 (2015): 131-158; Anderson, Ross, et al. "Measuring the cost of cybercrime." *The economics of information security and privacy*. Springer Berlin Heidelberg, 2013. 265-300.

Das Opfer ist so mit einem großen Interpretationsraum konfrontiert. Im „best case“ war der Angreifer ein niederrangiger Krimineller, der mit einigen wenigen erbeuteten Daten nichts anfangen kann und diese wieder löscht oder nur als Adressdaten verkauft. Im „worst case“ war es ein organisierter, gezielter Angriff eines Konkurrenten oder ein fremder Staat im Aufbau einer eigenen Industrie, der nun alle technischen, innovativen, operativen und wirtschaftlichen Geheimnisse kennt und die betroffene Firma innerhalb von zwei Jahren gezielt in den Ruin treibt. Dazwischen gibt es viele andere Szenarien. Aber niemand kann exakt sagen, welcher dieser Fälle genau zutrifft und wie er sich letztlich ausprägt.

Neben diesen Wissenslücken, die durch mangelnde Sichtbarkeit der Vorfälle und Angreifer bestehen, gibt es viele fachliche Fragen, die nicht oder nur mangelhaft adressiert werden. So ist – erstaunlicherweise – das Basisproblem der Cybersicherheit, nämlich die Unsicherheit der Informationstechnik gegenüber Angreifern, kaum breit wissenschaftlich und politisch adressiert. Zwar existieren inzwischen Ansätze dazu[2], aber bei der hohen Abhängigkeit von Informationstechnik hätte man erwarten müssen, dass schon früher breit, öffentlich und systematisch Überlegungen und Messungen zu Ursachen und Ausmaß der Unsicherheit gemacht werden. Auch die Effektivität und Effizienz von IT-Sicherheitstechnologien sind nach wie vor weitestgehend unbekannt und wenig systematisch beforscht[3]. Diese letzten beiden Mängel werden inzwischen glücklicherweise stärker in den Vordergrund gebracht und thematisiert, aber in der Vergangenheit ebenso wie in der näheren Zukunft musste und muss man mit beachtlichen Unsicherheiten im Basiswissen und mit großen Interpretationsspielräumen leben.

Problemkomplexität entsteht nun zum einen Teil aus diesen skizzierten Wissensproblemen, vor allem aus den Interpretationsspielräumen. Ein Cybersicherheitsproblem für ein Unternehmen kann eben alles Mögliche sein. Das Spektrum der Szenarien hat eine große Breite, die sich ex ante und für den Laien nur schwer mit Wahrscheinlichkeiten und Schadenssummen bewerten lässt. Cybersicherheit kann eine kleine und kaum nennenswerte, seltene Störung sein, die kaum mehr als 100 Euro Investitionen im Jahr erfordert. Es kann aber auch den Ruin der Firma durch Industriespionage oder Reputationsschäden bedeuten und damit erhebliche Investitionen und organisatorische und operative Umstrukturierungen erfordern. Was aber ist das richtige Szenario? Wovon muss ein Unternehmer mit welcher Wahrscheinlichkeit ausgehen? Und wie sollte er sich trotz aller Unsicherheit sowohl verantwortlich wie auch wirtschaftlich entscheiden?

---

[2] Siehe etwa: Wakchaure, Mr Manoj Ashok, and Shashank D. Joshi. "A Framework to Detect and Analyze Software Vulnerabilities: Analysis Phase in SDLC." *Journal of Modern Electronics* 4.1-2 (2015); Lim, Dae-Eun, and Tae-Sung Kim. "Modeling discovery and removal of security vulnerabilities in software system using priority queueing models." *Journal of Computer Virology and Hacking Techniques* 10.2 (2014): 109-114; Denning, Dorothy E. "Toward more secure software." *Communications of the ACM* 58.4 (2015): 24-26.

[3] Siehe etwa: Yasasin, Emrah, and Guido Schryen. "Requirements for IT Security Metrics-an Argumentation Theory Based Approach." (2015); Pereira, Teresa, and Henrique Santos. "Security metrics to evaluate organizational IT security." *Proceedings of the 8th International Conference on Theory and Practice of Electronic Governance*. ACM, 2014.

Zu dieser Komplexität der möglichen Szenarien und ihrer Gewichtung tritt noch eine weitere, nämlich jene der zu schützenden Landschaft. IT ist komplex. Die Technik selbst ist ungeheuer vielschichtig, mit vielen verschiedenen Teiltechnologien, Expositionen, Modalitäten, Einstellungen, Anbindungen und Einbettungen. Viele Konstellationen werden irrelevant für die Sicherheit sein. Andere Konstellationen dagegen werden ein Unternehmen direkt angreifbar machen, indem sie in besonders hohem Maße besonders gängige und einfache Verwundbarkeit herstellen und so den weit verbreiteten opportunistischen Angreifer anziehen. Auch hier trifft man folglich auf Komplexität in der Ausgangsfrage, die ihrerseits wieder viele weitere Interpretationsspielräume über technisch und operativ relevante oder eben irrelevante Aspekte eröffnet. Und auch hier kann insbesondere der Laie kaum selbst Entscheidungen treffen.

Lösungskomplexität ist der nächste Aspekt, der direkt aufbauend auf der Problemkomplexität entsteht. Die Hersteller von IT-Sicherheitslösungen müssen das komplexe Basisproblem auf einen handhabbaren Zuschnitt reduzieren, um Produkte anbieten zu können. Die klassische IT-Sicherheitsindustrie etwa hat sich vor allem an den Viren an der Internetschnittstelle aufgehalten. Da Online-Angreifer dort ja hindurch müssen und wenn man Viren als Kern des Problems ansieht, so kann man an dieser Stelle Lösungen bauen und von diesen Lösungen behaupten, dass man damit „das gesamte Problem für immer“ in den Griff bekommt. Dies gilt leider auch für viele andere Zuschnitte, die sich machen lassen. Verschlüsselungsingenieure sehen das zentrale Probleme nicht an der Internetschnittstelle, sondern in der Offenheit der Daten, so dass also eine allumfassende Datenverschlüsselung des Rätsels Lösung ist – und nicht die Firewall oder die Detektionsmechanismen, die aufgestellt wurden. Viele weitere ähnliche Behauptungen oder Kombinationen von Behauptungen lassen sich aufstellen, je nachdem, was sich gerade als besonders günstige oder in den Medien besonders präsente Probleminterpretation anbietet. De facto aber braucht ein effektiver Schutz je nach Analyse der eigenen Lage ganz unterschiedliche Kombinationen verschiedener Maßnahmen, meist in recht individuellen Zuschnitten, angepasst und unter Zuhilfenahme nicht-technischer Schutzkonzepte, wobei aber auch hier keine Methodik der Kombination angegeben werden kann, solange Effektivität und Effizienz von IT-Sicherheitstechnologien nicht zuverlässig geprüft werden können. So entsteht eine mitunter hohe weitere Komplexität im Feld der Lösungen.

Befangenheiten sind schließlich meist der Grund, warum der Laie weder sein Problem, noch seine Lösung richtig kennenlernt. Denn wenn der Laie notwendig nicht zu Problem- und Lösungserkennung befähigt ist, dürfen Experten diese Interpretationen vornehmen. Experten allerdings bringen oft eigene Motive mit ein, mit deren Hilfe oder unter deren Gewalt sie ihre je eigenen Zuschnitte aus Problemen und Lösungen und ihre eigenen Antworten auf Unsicherheiten und Lücken finden. Eine Reihe von Wahrnehmungstendenzen lassen sich dabei beobachten. Viele Experten ignorieren etwa Probleme, zu denen sie keine Lösungen anbieten können oder die sie selbst nicht gut verstehen. Dies gilt für Firmen aus dem Sicherheitsbereich genauso wie für Behörden, die etwa besonders schwer zu lösende Angriffe oder Angreifer gern als später zu lösendes Problem nach unten priorisieren.

In der Wissenschaft gibt es die Tendenz, nicht exakt messbare und nur durch Einzelfälle indizierte Probleme als unwissenschaftlich auszugrenzen. So hat etwa eine Studie zu den Kosten der Cyberkriminalität der Universität Cambridge das Problem der Industriespionage aufgrund der mangelnden Meldepraxis in diesem Feld schlicht als nicht messbar ausgegrenzt[4], ist in der Folge bei nur geringen direkten Kosten durch Cybercrime angekommen und hat unglücklicherweise nur daraus die wiederum globalen Empfehlungen für Varianten und Größen von Sicherheitsausgaben abgeleitet – eine recht schiefe Argumentation. Im Gegenzug zur Ausgrenzung des Unbekannten und Unprofitablen werden von vielen Experten diejenigen Probleme, die sie lösen können, zu denen Produkte am Markt sind oder die besser verstanden sind, hoch priorisiert und in ihrer Bedeutung überbetont. Dies wird oft noch implizit durch den Anschein einer Faktenlage unterstützt, da diese Probleme meist diejenigen sind, die bereits lange bekannt und gut sichtbar sind, und bei Lösungen durch einen Anschein von hoher Marktakzeptanz, da alle anderen Marktteilnehmern ja ebenfalls diese Lösungen verwenden.

Hier allerdings besteht das Problem, dass sich mit diesem Fokus viele Experten und Produkte an Problemspezifikationen der Vergangenheit und an meist eher weniger riskanten Szenarien abarbeiten. Die erst seit etwa fünf bis sieben Jahren existenten, sehr hochwertigen und kaum zu detektierenden, zu messenden oder abzuwehrenden Angriffe dagegen sind nicht explizit adressiert, oder zumindest nicht real technisch adressiert. Im Marketing verschiedener Produkte tauchen aber wieder alle möglichen vollmundigen Versprechen auf, die jedoch meist nicht länger als einige Stunden ab Inbetriebnahme eingehalten werden können.

Ein gutes Beispiel für alle vier Probleme ist ein vielgeschwungenes Bonmot der Cybersicherheit. Es lautet: „der Mensch ist das Problem“. Die Aussage ist nicht falsch und in der aktuellen Landschaft sicher oft genug berechtigt. Menschen können mit einer Mail eines vorgetäuschten Kollegen leicht dazu gebracht werden, auf infizierte Links zu klicken oder infizierte Attachments zu öffnen. Menschen, selbst Administratoren, können in einem größeren System durchaus auch unter einigen hundert bis tausend Konfigurationsoptionen mal eine realisieren, die nicht alle Sicherheitsimplikationen berücksichtigt. Und Menschen sind auch nicht gut darin, sich viele verschiedene und dauernd zu ändernde vielstellige Passwörter mit Sonderzeichen auszudenken und zu merken. So entstehen viele für Angreifer besonders einfach und daher besonders gerne genutzte Einfallstore, die bei späteren Analysen gut erkennbar werden und so scheinbar eine wichtige Angriffsoberfläche bilden, der proportional viel Aufmerksamkeit gewidmet werden muss, zu der sich bereits ein großer Konsens gebildet hat, dem man nicht widersprechen möchte, und zu der sich – für viele Experten profitabel – auch viele Handreichen, Trainings und Securityprodukte entwickeln lassen.

Aber es gibt auch andere mögliche Perspektiven. Schon der Common Sense könnte fragen: Ist in den oben genannten Fällen wirklich der Mensch das Problem? Eine (nur

[4] Anderson, Ross, et al. "Measuring the cost of cybercrime." *The economics of information security and privacy*. Springer Berlin Heidelberg, 2013. 265-300.

geringfügig hinkende) Parallele: Würde man Flugzeuge so bauen, dass eine 30%-ige Absturzquote als akzeptabel erachtet und eingepreist wird und dass jede Verantwortung für die Flugsicherheit den Passagieren überantwortet und im Flugzeugbau in keiner Weise berücksichtigt wird, mit einem Nebengeschäft für Fallschirmspringerkurse, wäre das Fliegen vermutlich nicht mehr besonders beliebt.

In der IT aber gibt es diese Situation. Der Endkunde, der am wenigsten an der Sicherheit eines Systems ändern kann, der am wenigsten darüber weiß und der mit der höchsten Komplexität konfrontiert ist, ist für die Sicherheit verantwortlich gemacht worden. Die IT-Industrie gibt an dieser Stelle gern vor, dieser Umstand sei vollkommen natürlich. Aber mit einem breiteren Kenntnisstand kann man dem gegenüber andere Forderungen ableiten. Es gibt viele Methoden und Konzepte, um Informationstechnik deutlich weniger angreifbar zu machen und um dem Endkunden und Nutzer einen großen Teil der Sicherheitsverantwortung abzunehmen. Mit dieser Sichtweise könnte also dafür gehalten werden, dass Sicherheit Aufgabe der Hersteller sein müsste, die diese Verantwortung nicht auf halbtechnische Rahmenmechanismen abwälzen dürfen, die unter normalen Bedingungen des Einsatzes ihres Produkts durch normale betriebliche Prozesse oder menschliche Fähigkeiten gar nicht in der erforderlichen Härte und Konsequenz herstellbar sind. Anders gesagt: Die Tatsache, dass der Mensch überhaupt in dieser Intensität und in so ungünstigen Bedingungen das Problem sein *kann*, muss als Indikator eines schlechten Designs der Informationstechnik gedeutet werden, so dass also das Bonmot hinter dem Bonmot gerade lauten müsste: „weil schlecht entwickelte IT ihn zum Problem macht".

Derart neu gewichtet wären allerdings die meisten Experten, Hersteller von Sicherheitslösungen, Behörden, die großen IT-Firmen sowie viele Sicherheitszuständige mit einer ganz anderen Lage konfrontiert. Die etablierten Maßnahmen des konkreten Security-Managements wären sekundär, und eine andere Menge Prioritäten wäre im Vordergrund, die eher auf einen Abbau verwundbarer Informationstechnik abzielen müsste, auf technische Hochsicherheitslösungen und auf eine Reform und stärkere Regulierung des IT-Marktes.

Das Beispiel zeigt damit, dass die vielen Optionen, dauerhafte Wissenslücken und tendenziöse Wahrnehmungen stets spezifische Ausschnitte aus dem Problem der Cybersicherheit ausbilden. Dies alles prägt leider häufig Lageberichte und Beratungen durch Firmen und Behörden.

Lageberichte und eher generische oder konservative Empfehlungen und Beratungen müssen folglich von einem Unternehmer auf Passgenauigkeit reflektiert werden. Für große Unternehmen ist das bereits eine Herausforderung, aber immerhin durch Erfahrungen und große Sicherheitsabteilungen mit Spezialexpertisen oder das Anmieten teurer Dienstleister machbar. Man weiß dann, wie die eigene Realität genau aussieht, an welchen Stellen man nachbessern muss, wo man eher auf unkonventionelle Lösungen zurückgreift und wo man vielleicht besser gar keine IT oder zumindest keine Vernetzung einbringt.

Kleine und mittlere Unternehmen können dieses „Security Tailoring" nicht eigenständig leisten. Sie müssten auf externe Dienstleister zurückgreifen oder so gut

es geht die generischen und konservativen Empfehlungen umsetzen und auf das Beste hoffen. Für die Herstellung einer „Cyber Readiness“ in einem kleinen und mittleren Unternehmen besteht folglich ein der Einrichtung von Sicherheit vorgelagertes Vertrauensproblem gegenüber Lagebildern, Empfehlungen und Herstellern. Der Unternehmer kann nicht von sich aus entscheiden, welcher Dienstleister zu ihm passt, welches Problem er genau hat, welche Produkte ihm helfen und was für Sicherheitsqualifizierungen er in seinem Personal herstellen muss, um dauerhaft einen möglichst passgenauen und sicheren Betrieb zu gewährleisten.

Die vorliegende Studie will hier Abhilfe schaffen. Sie will kleine und mittlere Unternehmen in die Lage versetzen, eine „Befähigung zur Befähigung“ herzustellen. In den folgenden Abschnitten sollen Grundkenntnisse vermittelt werden, um (1) eine eigene Risikoabschätzung zu machen, um (2) eine systematische und strategische Gestaltung von Cybersicherheit zu ermöglichen, um (3) einen sicherheitssensiblen Einkauf von Informationstechnik allgemein zu gestatten ebenso wie (4) eine Identifikation passgenauer Sicherheitslösungen und um (5) die Anforderungen an die eigene Qualifizierung zu erkennen und zu erfüllen. Schließlich wird diese Studie sich ausgangs mit dem Thema der „Industrie 4.0“ auseinandersetzen und deren besondere Sicherheitsprobleme erläutern.

1.2 Das eigene Risiko abschätzen

Aufgrund der vielen Komplexitäten sollte zuerst ein Prozess der Risikoevaluierung stattfinden, um die eigene Position genauer zu verstehen. Danach erst kann eine Strategie zur Herstellung eigener Sicherheit entwickelt werden. Das Informationssicherheitsrisiko wird nach ISO/IEC 27005:2008 definiert als: „the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization“.

Nach dieser Definition sind die folgenden Elemente zu bestimmen, wobei sich die angedeuteten Fragen entwickeln lassen:

- Bedrohung (Threat): Wer könnte mein Unternehmen angreifen wollen? Mit welchem Motiv könnte ich angegriffen werden? Wie würde so ein Angreifer vorgehen? Wie wahrscheinlich ist ein Angriff?
- Verwundbarkeiten (Vulnerability): Wo kann ich angegriffen werden? Was macht mich besonders verwundbar, was weniger?
- Werte (Assets): Was genau möchte ein Angreifer bei mir? Wie würde sich ein Angriff auf meine Unternehmenswerte ausprägen? Wie kann ich feststellen, was meine digitalen Assets sind?
- Schaden (Harm): Welcher Schaden kann durch einen Angriff entstehen? Wie kann ich Schaden feststellen und abschätzen?

Auch die folgenden strategischen Fragen zur Einrichtung von Cybersicherheit lassen sich an diesen Punkten orientieren:

- Bedrohung (Threat): Was muss man über Bedrohungen wissen? Wie kann man sein Wissen zu Bedrohungen aktuell halten?

- Verwundbarkeit (Vulnerabilities). Wie kann ich ermessen, wie verwundbar ich an verschiedenen Stellen bin? Wie kann ich meine Verwundbarkeit verringern?
- Werte (Assets): Wie lassen sich Assets laufend beobachten? Wie können Veränderungen festgestellt werden? Gibt es Versicherungen und lassen sich Redundanzen aufbauen?
- Schaden (Harm): Wie lässt sich Schaden reduzieren?

Im Folgenden soll in groben Zügen eine eigene Risikoabschätzung ermöglicht werden.[5] Die Bedrohungen für kleine und mittelständische Unternehmen sollen erklärt, die Evaluation der eigenen Werte und möglicher Schäden ermöglicht werden, um eine erste Einschätzung einer eigenen Risikoklasse zu ermöglichen. So können Unternehmen mit einem ersten Blick entscheiden, ob sie überhaupt ein tiefes und detaillierteres Risk Assessment verfolgen wollen. Verwundbarkeiten und Strategien werden dann als eigene Themen im nächsten Abschnitt besprochen.

1.2.1 Welche Bedrohungen sind für mich relevant?

1. **Diebstahl von Kunden- und Angestelltendaten**
   Die erste Kategorie möglicher Bedrohungen bezieht sich auf die Daten von Kunden und Angestellten. Entsprechende Datensätze stellen nach wie vor ein attraktives Handelsgut auf digitalen Schwarzmärkten dar. Je nach Art und Qualität der Datensätze – also danach, was für Daten es sind, wie viele Daten vorhanden sind, wie aktuell und wie spezifisch die Daten sind und ob Passwörter, PINs oder finanziell verwertbare Daten dabei sind – erzielen einzelne Datensätze recht unterschiedliche Preise. Reine Email-Zugangsdaten etwa sind im Wert massiv abgestürzt (auf 0,5 bis 10 USD pro 100 Stück) und nur noch schlecht handelbar, da hier die offene Verfügbarkeit größer und die Verwertung schwerer geworden ist, wogegen Scans von Ausweisdokument, Kreditkarten, Gaming Accounts und Social Network Zugänge mit vielen Followern durchaus noch gute Einzelpreise erzielen (zwischen 1 und 20 USD pro Datum). In den Preisklassen bilden sich wandelnde Geschäftsmodelle und Methoden der Datendiebe ab, die als Indikatoren der Risikoexposition eines Unternehmens gedeutet werden können. Werden etwa Finanzinformationen und Kreditkartendaten mit Ausweisscans von einem Unternehmen vorgehalten oder werden Gaming und Social Network Accounts betrieben, ist das kriminelle Interesse derzeit höher als bei einer reinen Vorhaltung von Mailinglisten. Allerdings gibt es nach wie vor Interesse an allen Varianten von Daten. Die meisten Datendiebe sind Kleinkriminelle und keine besonders professionellen Angreifer und operieren opportunistisch. Sie probieren sich mit ihrem je eigenen Zuschnitt an Fähigkeiten an verschiedenen Systemen aus, und wenn sie ein System infiltrieren können, nehmen sie alles mit, was

[5] Da sich verschiedene Faktoren wie Bedrohungen, Taktiken, Technologien stetig ändern, erhebt die folgende Schilderung keinen Anspruch auf Vollständigkeit. Für stärker technische Risk Assessments können Methodologien wie OWASP genutzt werden. Siehe auch: Peltier, Thomas R. *Information security risk analysis*. CRC press, 2005; Alberts, Christopher J., and Audrey Dorofee. *Managing information security risks: the OCTAVE approach*. Addison-Wesley Longman Publishing Co., Inc., 2002.

verfügbar ist. Daher können die Schäden trotz „schwacher“ Angreifer teils noch hoch ausfallen. Auch der Verlust von Mailinglisten kann bei Bekanntwerden hohe Schäden nach sich ziehen: Es herrscht eine Anzeigepflicht; es müssen Ermittlungen aufgenommen und bezahlt werden; eventuell muss nachgeforscht werden, wo Daten hingeflossen sind; Schadenersatzforderungen Dritter stehen ins Haus; rechtliche Prozesse werden fällig; Kommunikationskosten und Einnahmeverluste durch Reputationsschäden sind einzuberechnen. Damit liegen Datenschutzvorfälle auch bei KMUs zwischen einigen Hundertausend Euro und vier Millionen Euro pro Vorfall.[6]

2. **Diebstahl von organisatorischen Geschäftsdaten**
   Nicht nur Personendaten unterschiedlicher Provenienz sind interessant für Datendiebe, auch andere Daten aus Unternehmen lassen sich verwerten. Organisatorische Geschäftsdaten haben seit einiger Zeit ebenfalls
   Abnehmer. Sie dienen vor allem dem Targeting.[7] Ein Angreifer kann anhand dieser Informationen sicherheitskritische, strategisch besonders relevante, leicht angreifbare oder voraussichtlich wohlhabende Personen in einem Unternehmen identifizieren, dazu die technischen und geschäftlichen Abhängigkeitsbeziehungen analysieren. So wird dieser Angreifer in die Lage versetzt, Personen und Taktiken für den Aufbau einer betrügerischen Vertrauensbeziehung zu identifizieren und sicherheitstechnische Schwächen zu finden. Ein Unternehmen muss daher mit diesen Informationen sensibel umgehen und bei einem Diebstahl eine Analyse möglicher Schäden vornehmen. Bei diesen Analysen sind auch implizite organisatorische Daten einzubeziehen, die ein Angreifer etwa durch die reine Bewegung interner Kommunikationen ablesen kann. Eine zentrale und hochfrequentierte Person kann zum Beispiel trotz formal niedrigem Status ein interessantes Ziel als Knotenpunkt vertraulicher Informationen sein, während eine nicht breit im Unternehmen kommunizierende Sicherheitsabteilung ein Indikator für eine schlechte Sicherheitskultur sein kann.

3. **Diebstahl von operativen Geschäftsdaten**
   Auch operative Geschäftsdaten treffen auf Interesse – ein Trend, der anwachsen wird. Operative Geschäftsdaten sind oft verkäuflich, da sie für in Konkurrenzbeziehungen stehende Unternehmen kritische Detailinformationen enthalten können. So kann ein Konkurrent über einen Ankauf gestohlener operativer Daten wichtige Schwächen eines gegnerischen Unternehmens herausfinden wie mangelnde Kompetenz oder schlechte Zugänge und Ressourcen für Teilinteressen, er kann Ansprechpartner und den

[6] Siehe auch: Acquisti, Alessandro, Allan Friedman, and Rahul Telang. "Is there a cost to privacy breaches? An event study." *ICIS 2006 Proceedings* (2006): 94; Keaveney, Susan M. "Customer switching behavior in service industries: An exploratory study." *The Journal of Marketing* (1995): 71-82. Oder für den deutschen Kontext: https://www.it-sicherheit.de/news/datenschutzverstoesse-kosten-unternehmen-millionen/

[7] Siehe auch: Abraham, Sherly, and InduShobha Chengalur-Smith. "An overview of social engineering malware: Trends, tactics, and implications." *Technology in Society* 32.3 (2010): 183-196; Workman, Michael. "Gaining access with social engineering: An empirical study of the threat." *Information Systems Security* 16.6 (2007): 315-331.

Status verschiedenster Gespräch mit potentiellen Kunden einsehen, und er kann im schlimmsten Fall Einsicht in Details laufender Merger oder Bieterverfahren erhalten und diese unterwandern. Vor allem zu je ausländischen Firmen werden solche Daten teilweise gerne angekauft. Der Schwarzmarkt ist hier allerdings noch in der Entwicklung. In selteneren Fällen werden operative Geschäftsdaten auch zur Vorbereitung von Spionage genutzt oder um Geschäftsmodelle zu kopieren. Auch für diese Daten müssen folglich Kritikalitätsanalysen unternommen und Schutzmaßnahmen eingeleitet werden.

4. Diebstahl von technischen Steuerungsdaten

Eine weitere Variante von Daten, die gestohlen werden können, sind technische maschinelle Steuerungsdaten.[8] Diese Variante ist noch exotisch, findet aber wachsenden Anklang unter organisierten Kriminellen, Industriespionen und militärischen Nachrichtendiensten. Organisierte Kriminelle können Störungen inszenieren, mit denen Börsenmanipulationen erreicht werden können oder mittels derer einem Unternehmen Imageschäden beigebracht werden können, etwa im Auftrag eines Konkurrenten oder in Vorbereitung einer Erpressung. Industriespione können diese Daten analysieren, um an technische Entwicklungsinformationen zu kommen, oder um sie bei einer bereits vorhandenen analog gebauten Anlage direkt in eine Konkurrenzproduktion einspeisen. Dieses Szenario ist gegenwärtig etwa in China bereits ein mögliches Problem, da dort aufgrund des ausufernden Kontrollinteresses der Regierung verschlüsselte Verbindungen abgeschaltet werden, so dass auch Produktionsdaten und technische Informationen für dort betriebene Anlage in Klardaten übermittelt werden müssen. So besteht die Option, dass diese Daten identifiziert, ausgeleitet und an chinesische Unternehmen weitergeleitet werden, die diese bei ähnlichen Anlagen sofort verwerten können. Militärische Nachrichtendienste schließlich benötigen Steuerungsdaten zur Vorbereitung von Sabotageangriffen, die sich mit nachrichtendienstlichen oder militärischen Methoden zu außen- und sicherheitspolitischen Zwecken anbringen lassen. Ein jüngeres Beispiel hierfür ist die aufgedeckte „Operation Cleaver“, bei der Steuerungsdaten kritischer Energieanlagen, Produktionen und Flugsicherungen in Amerika und Europa beschafft wurden. Urheber des Angriffs ist angeblich der Iran, der tatsächlich als Interessent für Sabotagefähigkeiten in diesen Zielländern eingestuft werden muss.

Sollten Probleme durch Steuerungsdaten mit hohen Schäden auftreten, werden diese für die Hersteller der Steuerungsdaten verschiedentlich problematisch. Verantwortlichkeiten müssen geklärt werden, Störungen lassen sich in Dauer und Ausprägung kaum antizipieren, Haftungsfragen werden auftreten, größere Imageschäden werden wahrscheinlich, vor allem existieren aber keine tragfähigen Methoden zur sauberen Entfernung entsprechend hochwertiger Angreifer, so dass Continuity und Recovery

[8] Siehe etwa die Angriffe Havex (http://www.security-insider.de/themenbereiche/bedrohungen/viren-wuermer-trojaner/articles/450597/) oder Operation Cleaver (http://www.cylance.com/operation-cleaver/)

manuell von in der Regel seltenen und teuren Spezialfirmen unternommen werden müssten, was leicht Kosten im ein- bis zweistelligen Millionenbereich verursachen kann.

Technische maschinelle Steuerungsdaten stellen also ebenfalls ein schützenswertes Gut dar. Da diese Datenvariante und die ihr zuzuordnenden Prozesse jedoch ein vergleichsweise neuartiger Schutzgegenstand sind, lassen sich Standardmaßnahmen der IT-Sicherheit nicht ohne weiteres übertragen, so dass trotz höherer Sicherheitsanforderungen mit höheren Sicherheitsdefiziten zu rechnen. Dieser Punkt soll gegen Ende der Studie in einer Betrachtung der Sicherheitsanforderungen für eine sichere Industrie 4.0 noch erörtert werden.

5. Industriespionage

Eine weitere und wichtige Variante des Datendiebstahls ist die Industriespionage. Hierbei wird ein weiterer Datentyp entwendet: Innovations- und Entwicklungsdaten – gern auch in Kombination mit anderen, oben erwähnten Datentypen. Diese Variante ist für Deutschland und für große wie kleine und mittlere Unternehmen als derzeit größte real präsente Bedrohung anzusehen. Vor allem die sehr breit und kompetitiv angelegte Industriespionage aus China ist ein drängendes und nur unzureichend verstandenes Problem, wobei in niedrigerer Frequenz auch Vorfälle aus westlichen Ländern zu verzeichnen und zu adressieren sind.

Die besondere Höhe dieser Bedrohung entsteht nicht durch direkte Kosten, sondern durch strategische Langzeitfolgen.[9] Direkte Kosten können hoch sein, da ebenfalls oft von hochwertigen Angreifern und daher von teuren Prozessen für Continuity und Recovery ausgegangen werden muss. Allerdings wiegen die strategischen Langzeitfolgen schwerer, wenn mithilfe der gestohlenen Entwicklungsdaten eine Konkurrenzproduktion aufgebaut wird. Ob dies geschieht und wie dies geschieht ist leider fast nie erkennbar oder nachvollziehbar. Man weiß nicht, ob die Daten wirklich verstanden wurden, ob sie in ein Unternehmen weitergeleitet werden, dass diese verarbeiten kann, ob dieses Unternehmen ein funktionierendes Produkt hervorbringt und ob dieses Produkt konkurrenzfähig in den gleichen Märkten angeboten werden wird. Zudem haben professionelle Industriespione ihre Verfahren deutlich verbessert, um jede Erkennung der Angriffe, des Diebstahlsprozesses, des Transfers der Daten oder der Verwendung der Daten zu behindern. Neuere Angreifer aus diesem Feld verfahren etwa so, dass sie Entwicklungsinformationen aus vielen ähnlichen, sonst in Konkurrenz zueinander stehenden Unternehmen stehlen, diese auf die besten Merkmale und Funktionen hin analysieren, um dann genau diesen besten Zuschnitt in einem „Superprodukt“ zu fusionieren, das aufgrund des Wegfalls der Entwicklungskosten zu einem deutlich niedrigeren Preis angeboten werden

[9] Siehe auch: Lewis, James, and Stewart Baker. "The economic impact of cybercrime and cyber espionage." *Center for Strategic and International Studies, Washington, DC* (2013); Moore, Tyler. "The economics of cybersecurity: Principles and policy options." *International Journal of Critical Infrastructure Protection* 3.3 (2010): 103-117.

kann. Oft werden die so entstehenden Unternehmen in Staaten wie China noch umfangreich aufgebaut, so dass im Vergleich mit den Ursprungsunternehmen eine größere Zahl technischer Entwickler das zusammengestohlene Superprodukt über die nächsten Jahre weiterentwickelt und einen nachhaltigen Marktvorsprung konsolidieren kann. Der Diebstahl wird so noch schlechter erkennbar.

Durch diese Unsicherheiten ist dieses Phänomen kaum gut zu bewerten, auch in der individuellen Risikoerwägung. Selbst Extrapolationen müssen mit einer Reihe hypothetischer Annahmen arbeiten, deren Basis in mangelnder Kenntnis des konkreten Interesses, der Zahl und der Prozesse der Angreifer recht brüchig ist.

Die Kosten der Cyber-Industriespionage
Die Kosten der Cyber-Industriespionage lassen sich aufgrund der genannten Probleme kaum klar beziffern und sorgen für eine große Unsicherheit in der Bewertung der Folgen von Cybersecurity allgemein. So haben in der Vergangenheit die Schätzungen der globalen Kosten von Cyberunsicherheit zwischen 4 MRD US-Dollar[1] und 1000 MRD US-Dollar[1] jährlich geschwankt (aktuell hat man sich in einer weiteren Studie der IT-Sicherheitsfirma MacAfee in der Mitte getroffen und ist bei 445 MRD US-Dollar gelandet[1]), wobei diese großen Spielräume vor allem in den systemischen Problemen der Bewertung der Folgen von Cyber-Industriespionage liegen. Einige Studien klammern dieses Phänomen aufgrund der extrem schlechten Messbarkeit einfach aus, andere dagegen setzen erfundene Werte wie 1% des GDP ein. Beide Verfahren führen allerdings nur zu Verunsicherung und Verunsachlichung der hier dringend notwendigen Debatten.

Doch selbst wenn die Wahrscheinlichkeit eines vollständigen erfolgreichen Aktes der Industriespionage als niedrig eingestuft wird, ist das Risiko immer noch hoch, da die Schäden in erfolgreichen Fällen als hoch und vor allem als langfristig begleitende und wirkende Schäden anzusetzen sind. Ein einmal auf dem Markt befindliches, nachhaltig weiterentwickeltes, gleichzeitig billigeres Konkurrenzprodukt ist nicht leicht wieder einzuholen.

Auch aus wirtschaftsstrategischer Perspektive sind Langzeitschäden anzusetzen. Eine wie im Falle von China tolerierte Kultur von Diebstahl, Auswertung, Nachbau und Verbesserung vermittelt über die Zeit auch ein breites und tiefes technisches und prozedurales Wissen. Akteure werden nicht nur zu konkreten Kopien befähigt, sondern zu einem allgemeineren Verständnis deutscher Technologien, Entwicklungsmethoden und Produktionsverfahren, sowie zu effizienten Methoden des kompetitiven Diebstahls, was sich als eigene Entwicklungs- und Industriekultur etablieren kann und so auch neue technische Bereiche eigenständig zugänglich macht. Zudem vermittelt die implizite Toleranz bei potentiellen Nachahmer einen

Eindruck der Tolerabilität solcher Vergehen, was inzentivierend auf neue Angreifer wirken wird.

6. **Systemische Industriespionage**
   Für kleine und mittlere Unternehmen ist neben der direkten Industriespionage noch die Variante der systemischen Industriespionage relevant, sofern diese größeren Unternehmen mit innovativen Großtechnologien zuliefern. In diesem Fall werden die Zulieferer von vielen Angreifern als Hintertür in die nachgelagerten Großkonzerne betrachtet. Während es oft anforderungsreich und umständlich ist, in die Großkonzerne selbst einzubrechen, sind Einbrüche auf Subunternehmer deutlich einfacher und ermöglichen oft bereits einen Diebstahl einiger Teilinformationen der interessanten Großtechnologien oder eröffnen sogar einen weiteren Angriffsweg in den Großkonzern hinein, über die zum Zulieferer etablierten Kommunikations- und Vertrauensbeziehungen. Diese besonders gefährdete Variante der KMUs muss also ihre Sicherheit sehr sorgfältig konzipieren, sollte die Risikoperzeption des Großkonzerns adaptieren und sollte vor allem die besser zur Sicherheit befähigten Konzerne um Hilfe bei der Absicherung bitten. Hier wäre anzuregen, dass die DIHK ein Programm aufsetzt, das einen Technologie- und Knowhowflow von den deutschen Großkonzernen in die kleinen und mittleren Unternehmen ermöglicht.

7. **Strategische Aufklärung**
   Den kleinen und mittleren Unternehmen aus sicherheitspolitisch relevanten Industriezweigen wie Rüstung und Aerospace kommt ebenfalls eine Sonderposition zu. In diesem Fall ist nicht nur mit kommerziell orientierter Industriespionage, sondern auch mit strategischer Aufklärung der Unternehmen durch fremde Nachrichtendienste zu rechnen. Hier muss das Schutzniveau daher besonders hoch sein. [10]

8. **Löschung, Sperrung und Störung von Daten, Programmen und Protokollen**
   Das böswillige Löschen, Sperren oder Stören fremder Daten, Programmen und Protokollen ist länger bekannt.[11] Diese Aktivitäten haben verschiedene Hintergründe. Es gibt etwa politische Motive, ein politisches Ziel zu schädigen oder mediale Aufmerksamkeit zu generieren. Es gibt persönliche Gründe wie Rache an einem als ungerecht empfundenen Arbeitgeber oder Kollegen. Es existieren kriminell-wirtschaftliche Motive wie im Falle der Erpressung oder der Börsenmanipulation. Und es entstehen – neuerdings – auch im Kontext nachrichtendienstlich-militärischer Taktiken Kalküle, auf diese Weise Fähigkeiten und Potentiale zu demonstrieren, Ablenkungen zu schaffen oder

[10] Gaycken, Sandro. "Does not compute—old security vs new threats." *Datenschutz und Datensicherheit-DuD* 36.9 (2012): 666-669.
[11] Siehe etwa: Lewis, James Andrew. *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Washington, DC: Center for Strategic & International Studies, 2002; Nazario, Jose. "Politically motivated denial of service attacks." *The Virtual Battlefield: Perspectives on Cyber Warfare* (2009): 163-181.

größere monetäre Schäden zu bewirken. Die taktischen und technischen Verfahren für das Löschen, Sperren und Stören sind recht unterschiedlich. Eine effektive Sperrung wird oft mit einer Fremd-Verschlüsselung der Daten realisiert. Dieses Szenario findet sich etwa in Erpressungsversuchen, bei denen der Erpresser die Entschlüsselung der durch ihn verschlüsselten Daten gegen einen Geldbetrag anbietet. Technische Störungen können durch Fehleingaben oder massenhafte Anfragen wie in verschiedenen Varianten der bekannteren „Denial Of Service"/"Resource Depletion"-Angriffe ausgelöst werden. Oft ist daran besonders attraktiv, dass die Störangriffe auf legitime Funktionen zugreifen und daher schwerer abzuwehren sind, dass sie in komplexer IT oft einfach herzustellen sind und dass sie oft auch problemlos „remote", also aus großer Entfernung und risikoarm durchgeführt werden können. Löschungen sind eine gegenwärtig besonders interessante und zunehmend genutzte oder eingebaute Angriffsform.[12] Sie werden gern durch ein zweistufiges Verfahren vorgenommen, bei dem man zuerst alle Daten löscht, um sie direkt danach mit verschlüsselten Nonsens-Daten zu überschreiben. So sind die Daten nicht wiederherstellbar. In neueren und weiter entwickelten Versionen dieser Löschungsangriffe werden dabei auch Backups identifiziert und gelöscht, sofern diese über direkte oder indirekte Verbindungen erreichbar sind. Löschungen sind auch eine eher einfache Form des Angriffs, die viele Standardmechanismen der IT nutzen kann und daher auch nur schwer strukturell präventiv vermieden werden kann. Daher bietet sich diese Form des Angriffs gut für einfache und direkte Industriesabotagen an, sofern ein Interesse besteht. Dem Risiko der Löschung ist dringend mit der Schaffung mehrerer möglichst heterogener, isolierter und gut gesicherter Backups zu begegnen.

Die Schäden durch Löschungen, Sperrungen und Störungen können immens sein, je nachdem, welche geschäftlichen und technischen Prozesse in welcher Intensität und Dauer betroffen sind. Unternehmen müssen hier im Kontext der Risikoerfassung ihre gesamten IT-Abhängigkeiten abprüfen. Die Blockierung des Web-Interfaces eines Online-Händlers vor den Weihnachtstagen ist ein Beispiel für eine schwere Störung, die Behinderung der Kommunikation in einem Bieterverfahren kann ebenfalls hohe Schäden verursachen, und der Verlust aller Steuerungsdaten inklusive aller Backups einer großen Industrieanlage etwa wird eine nahezu vollständige Neueinrichtung der Anlage bedingen, mit entsprechenden Zeiten und Kosten.[13]

9. **Manipulation von Daten, Programmen und Protokollen**
   Auch die Manipulation ist ein wachsendes Feld mit interessanten Optionen für Angreifer. Viele der hier entstehenden Möglichkeiten zur Veränderung von Daten, Programmen oder Kommunikationsprotokollen sind vor allem für die Finanzbranche kritisch. Durch die hohe Komplexität der Finanz-IT, die großen

[12] Siehe etwa: Zhioua, Sami. "The Middle East under Malware Attack Dissecting Cyber Weapons." *Distributed Computing Systems Workshops (ICDCSW), 2013 IEEE 33rd International Conference on*. IEEE, 2013.
[13] Siehe etwa: Scott, Jonathan, and Eur Ing. "Shutdown! What would that do to your production and profit margins?." *Loss Prevention Bulletin* 242 (2015).

Datenvolumina und die zahlreichen kleinen Mechanismen bestehen viele Optionen, unentdeckt und stark asymmetrisch zu manipulieren, um direkte monetäre Vorteile zu erhalten, die auch durch Buchprüfungsverfahren nicht erfassbar sind. Aber auch die Manipulation operativer Geschäftsdaten und technischer Steuerungsdaten bieten viele Möglichkeiten der Sabotage und Schädigung von Unternehmen, von laufenden Geschäftsprozessen wie etwa Bieterverfahren oder sogar von Produktionsanlagen, Infrastrukturen und mit IT ausgestatteter Geräte (Smart X). Derartige Cybersabotagen waren in der Vergangenheit selten, da sie für Kriminelle zu riskant und zu wenig profitabel waren. Aktuell allerdings treten viele neue Akteure mit anderen Interessen auf, während gleichzeitig die deutlich stärkere Informatisierung der Wirtschaft und Industrie auch neue kriminelle Perspektiven auf Datensabotage eröffnet.

10. **Missbrauch als Proxy**
    Eine Variante einer Manipulation besteht in dem Missbrauch eines Unternehmens als „Zwischenpunkt“ (Fachsprache: Proxy) eines Angriffs. Dabei wird das Unternehmen von einem Angreifer gehackt, der dann weitere Angriffe auf Dritte von den Rechnern des Unternehmens aus durchführt, um so besser seine Identität zu verschleiern. Dieses Verfahren ist gängig und findet besonders bei schlecht gesicherten Systemen oft Anwendung. Für das Unternehmen entsteht damit die Gefahr, haftbar für die Ermöglichung entsprechender Schäden Dritter gemacht zu werden oder zu aufwendigen Säuberungsmaßnahmen gezwungen zu werden. In einigen Fällen sind die Missbräuche auch so voluminös, dass sich normale Funktionen nur noch sehr langsam ausführen lassen und den Betrieb behindern.

Dies sind einige grundlegende Bedrohungen, die durch Informatisierung und Vernetzung entstehen. Viele der erwähnten Risiken existieren sogar für Systeme und Unternehmen, die sich nicht unbedingt in einem Zielraster verorten würden. Oft migrieren Angriffe aus einem Kontext in einen anderen und oft finden Angreifer neue Anwendungsfelder und Geschäftsmodelle für unkonventionelle und damit eben schlechter gesicherte und besser erreichbare Ziele.

1.2.2 Ein KMU Risiko Barometer: Wie hoch ist mein individuelles Risiko?

Jedes Unternehmen sollte eine Cyber-Risikoanalyse machen. Eine vollständige und systematische Cyber-Risikoanalyse kann nur durch Fachexperten in gesonderten Beratungsverhältnissen unternommen werden. Für eine erste Einschätzung allerdings, ob eine teure Beratung in Anspruch und in welchem Umfang sie vorgenommen werden sollte, soll an dieser Stelle ein einfaches Risiko-Barometer eine erste Verortung im Feld der Cyber-Risiken ermöglichen. Es wird allerdings explizit darauf hingewiesen, dass aufgrund der hohen Innovationsdynamik im Angreiferfeld kein Anspruch auf Vollständigkeit oder längere Gültigkeit besteht.

Zunächst sind einige Vorüberlegungen anzusetzen. Es muss eine Auflistung aller Geschäftsprozesse und aller technischen Prozesse pro Geschäftsprozess erfolgen. Ausgehend von dieser ersten Auflistung muss erfasst werden, in welcher Form Daten und IT-Anwendungen in diesen Prozessen vorkommen. Dazu werden in diesem

einfachen Verfahren einer Erstbewertung Punkte vergeben, die pro Geschäftsprozess addiert werden.

Die Vergabe der Punkte entspricht grundlegenden Risikoindikatoren, wobei Wahrscheinlichkeit und Schaden nicht genauer ausdifferenziert sind und sich unterschiedlich ausprägen können. Die Punkte können wie folgt gelesen werden:

- 5 Punkte = Risiko
- 10 Punkte = hohes Risiko
- > 15 Punkte = sehr hohes Risiko

Daten und IT-Vorgänge können als Typen unterschieden und bewertet werden in:

1. Personenbezogene Daten (Angestellte oder Kunden)
    a. Viele personenbezogene Daten über Angestellte: 5 Pkt
    b. Viele personenbezogene Daten über Kunden: 5 Pkt
    c. Detaillierte Personendaten oder Ausweiskopien: 5 Pkt
    d. Daten zu Online-Accounts: 5 Pkt
    e. Personenbezogene Daten sind an mehr als drei Orten in großer Zahl zugänglich: 5 Pkt
    f. Personenbezogene Daten sind nicht gesondert explizit gesichert: 5 Pkt

2. Finanzbezogene Daten (Bankdaten, Kreditkartendaten, handelsrelevante Informationen)
    a. Börsenhandelsrelevante geschützte Informationen: 25 Pkt
    b. Bankdaten von Angestellten: 5 Pkt
    c. Bankdaten von Kunden: 5 Pkt
    d. Kreditkartendaten: 5 Pkt
    e. Informationen mit hoher Relevanz für laufende oder anstehende Bieterverfahren 35 Pkt

3. Gesundheitsbezogene Daten (Krankeninformationen)
    a. Nicht mehr als zwei und nur unkritische Gesundheitsdaten: 5 Pkt
    b. Mehr als zwei Gesundheitsdaten: 10 Pkt
    c. Zusätzlich kritische Gesundheitsdaten (schwere Krankheiten etc): 15 Pkt

4. Operative Daten Geschäftsprozesse
    a. Informationen zu sensiblen Kontakten 5 Pkt
    b. Dokumente zu sensiblen Prozessen 5 Pkt

5. Organisatorische Daten
    a. Detaillierte und personenbezogene Hierarchie 5 Pkt
    b. Technische Daten zur Hierarchie 5 Pkt
    c. Dokumente mit Funktionen und Kontakten 5 Pkt

6. Eigene Innovations- und Entwicklungsdaten
    a. Explizite Entwicklungsdaten zu geschütztem geistigem Eigentum, eigenen Erfindungen und Verfahren 15 Pkt
    b. Implizite Entwicklungsdaten durch Steuerungsdaten entsprechender Produktionsanlagen 10 Pkt
    c. Implizites Entwicklungswissen durch hinterlegte Entwicklungsmethoden und –verfahren 10 Pkt
    d. Entwicklungsdaten zu politisch relevanten Technologien 35 Pkt
    e. Technologietyp entspricht einem aktuellen Interessensraster eines Angreifers 35 Pkt

7. Fremde Innovations- und Entwicklungsdaten eines belieferten Konzerns
    a. Explizite Entwicklungsdaten zu geschütztem geistigem Eigentum, eigenen Erfindungen und Verfahren, auch in Auszügen 15 Pkt
    b. Implizite Entwicklungsdaten durch Steuerungsdaten entsprechender Produktionsanlagen 10 Pkt
    c. Implizites Entwicklungswissen durch hinterlegte Entwicklungsmethoden und –verfahren 10 Pkt
    d. Entwicklungsdaten zu politisch relevanten Technologien 35 Pkt
    e. Technologietyp entspricht einem aktuellen Interessensraster eines Angreifers 35 Pkt

8. Technische Daten und Prozesse
    a. Produktionsdaten – und prozesse für Maschinen als Steuerungsdaten für Maschinen, CAD-Informationen 15 Pkt
    b. Steuerungsdaten und –prozesse für kritische Infrastrukturen 35 Pkt
    c. Technische Daten und Prozesse für Online-Angebote 10 Pkt
    d. Technische Daten und Prozesse für digitale Kommunikation 5 Pkt
    e. Technische Daten und Prozesse für Netzwerke 5 Pkt
    f. Sicherheitsrelevante technische Daten (Schlüssel/Passwörter, Konfigurationen, Versionen) 10 Pkt
    g. Technischer Prozess entspricht einem aktuellen Interessensraster eines Angreifers 35 Pkt

Zusätzliche Erwägungen

In diesen Punktbewertungen sind Risiken abgebildet, indem Wahrscheinlichkeiten und Schäden Eingang gefunden haben. Ein Unternehmen sollte allerdings an als kritisch bewerteten Stellen noch eine stärker nach eigenem Empfinden verfahrende Analyse zu erwartender Folgeschäden für spezifische Angriffe auf den jeweils betrachteten Prozess unternehmen. Hierzu kann das Unternehmen einen für sich wahrscheinlichen, in einer relevanten Größe stattfindenden Vorfall bestimmen, als Szenario durchdenken und dabei die folgenden, teils überschneidenden und unterschiedlich langen Vorfallsphasen auf ihre Relevanz und auf eine ungefähr mögliche Schadenshöhe festlegen:

- Erkennen des Angriffs
- Abstellen des Angriffs unter Herstellen einer Continuity und Aufbau einer Kommunikation nach Außen und mit betroffenen Dritten oder Behörden
- Entfernen des Angriffs unter möglicher forensischer Ermittlung und möglichem neuem Aufsetzen bis zu vollständiger Recovery
- Bewältigen rechtlicher, regulativer, kommunikativer wie kooperativer Folgen
- Analyse des Angriffs und Neuformulierung der Security-Policy
- Mögliche Anschaffung neuer Technologie und Ausbau der Sicherheitskompetenzen im Unternehmen

Dabei sollten jeweils die folgenden Schadensvarianten nach den oben erwähten Angriffsformen durchdacht werden:

- Schäden durch Diebstahl
- Schäden durch Verwendung gestohlener Daten
- Schäden durch Bekanntwerden eines Vorfalls
- Schäden durch Löschung
- Schäden durch Sperrung
- Schäden durch Störung
- Schäden durch Manipulation
- Schäden an Dritten
- Direkte und indirekte Schäden
- Kurzfristige und langfristige Schäden

Fallen im Rahmen dieser Betrachtungen betroffene Bewertungen anders aus als oben nach den Risikoindikationen, so kann eine Neubewertung durch Aufaddieren der notwendigen Punktzahl vorgenommen werden.

Folgend gibt es sich als Faktoren auswirkende Beziehungen, die eine Bewertung verbessern oder verschlechtern können. Der Faktor 1 dient als Standardannahme und wurde bei der obigen Verteilung der Punkte als Normalfall berücksichtigt. Davon abgesehen gibt es verschiedene Zusatzbeziehungen, die diesen Normalfall positiv oder negativ beeinflussen können. Als besonders relevant werden hier Abhängigkeiten, Vernetzungen und Verwundbarkeiten angesetzt. Diese Beziehungen sind im Unternehmen möglichst detailscharf zu ermitteln und wie folgt zu bewerten.

9. Abhängigkeitsgrade können beschrieben werden als:
    a. Keine Abhängigkeit: Der Prozess kommt nicht mit IT in Berührung, auch nicht indirekt oder mittelbar.

       Faktor 0
    b. Geringe Abhängigkeit: Der Prozess kommt peripher mit IT in Berührung, kann aber ohne IT durchgeführt werden. Dafür notwendige Daten und Kenntnisse sind analog vorhanden und verfügbar.

       Faktor 0,5
    c. Abhängigkeit: Der Prozess ist in essentiellen Funktionen von IT abhängig und kann ohne IT nicht durchgeführt werden.

       Faktor 1

Dabei können folgende ergänzende Elemente wieder additiv berücksichtigt werden.

10. Wichtige Merkmale in Abhängigkeitsbeziehungen:
    a. Individualität: Abhängigkeit liegt nicht auf Standardsystemen oder leicht neu zu generierenden Daten. Ausfallende IT-Systeme und Daten können nicht schnell neu aufgesetzt oder neu beschafft werden. 15 Pkt
    b. Anhängigkeit Dritter: Vorfälle haben unmittelbar kritische Auswirkungen auf abhängige Dritte. 15 Pkt
    c. Systemische Wirkungen: Vorfälle in einem Prozess bedingen den Ausfall weiterer Prozesse. 15 Pkt
    d. Anhängigkeit rechtlicher Prozesse: Vorfälle in einem Prozesse sind haftungs- oder strafrechtlich relevant. 15 Pkt
    e. Kritikalität des Prozesses: Der Prozess kann in besonders hohem Maße dauerhaft oder temporär kritisch sein 15 Pkt

11. Vernetzung als nächstes Thema prägt sich stark aus. Einmal sind die Risiken externer Angriffe mit oder ohne Vernetzung grundlegend anders. Dann müssen auch bei großen internen Netzwerken Risiken durch versehentliche externe Vernetzungen (über BYOD-Policies etwa) oder durch Innentäter einbezogen werden. Es können vier Stufen angesetzt werden:
    a. keine Vernetzung Faktor 0,1
    b. nach Außen hart isoliertes, kleines internes (< 20 Rechner) Netzwerk Faktor 0,2
    c. nach Außen offenes, aber grundlegend abgesichertes oder großes internes (> 20 Rechner inkl. BYODs) Netzwerk Faktor 1
    d. nach Außen offenes, unklar oder nicht abgesichertes oder sehr großes internes (> 500 Rechner inkl. BYODs) Netzwerk Faktor 2

12. Verwundbarkeit kann nach der im nächsten Abschnitt folgenden Analysetabelle eingeschätzt werden. Hier sollen daher nur vier Abstufungen mit einigen groben Indikatoren berücksichtigt werden:
    a. kaum Verwundbarkeit (zentral nach Sicherheit entwickelte und vollständig korrekt implementierte Basis-IT) Faktor 0,3
    b. geringe Verwundbarkeit (Basis-IT mit langer Sicherheitserfahrung und vielen Sicherheitsmechanismen mit tiefer struktureller Wirkung) Faktor 0,8
    c. normale Verwundbarkeit (Basis-IT mit mäßiger Sicherheitserfahrung und einigen Standardsicherheitsmechanismen ohne strukturelle Verankerung) Faktor 1
    d. hohe Verwundbarkeit (Basis-IT mit wenig Sicherheitserfahrung, veralteter Technologie oder wenigen Sicherheitsmechanismen im möglichen Konflikt mit Standardfunktionen) Faktor 2

Die Ermittlung der Ersteinschätzung des eigenen Risikos kann nun wie folgt vorgenommen werden:

1. Pro Prozess werden die Punktzahlen aus dem Merkmalen (1, 2, 3, 4, 5, 6, 7, 8, 10) aufaddiert.
2. Folgend werden auf die Gesamtpunktzahl die Faktoren der Merkmale (9, 11, 12) angewendet.
3. Das Ergebnis ist der individuelle Risikoindikator für den spezifischen Prozess.

Je nach Ergebnis würde sich eine Risikogruppierung ergeben.

Gesamtpunktzahl:	**Risikogruppe:**
0 – 4	Kein Risiko
5 – 14	Geringes Risiko
15 – 34	Mittleres Risiko
35 – 74	Hohes Risiko
ab 75	Sehr hohes Risiko

Zwei Beispiele sollen das Verfahren illustrieren.

Beispiel 1: Ein Steuerberater

Unternehmen A ist ein kleines Unternehmen der Steuerberatung. Es unterhält weniger als zwanzig Rechner. Relevante Prozesse sind die operative Steuerberechnung und die Kundenkommunikation. Für die Berechnung wird mit Excel-Tabellen und einer Steuerberatersoftware gearbeitet. Die Kundenkommunikation erfolgt weitestgehend per Email.

Das Unternehmen identifiziert für sich die folgenden Punktzahlen:

Prozess Operative Steuerberechnung:

1. b.	Viele personenbezogene Daten über Kunden	5 Punkte
1. c.	Detaillierte Personendaten	5 Punkte
2. c.	Bankdaten von Kunden	5 Punkte
10. d.	Anhängigkeit rechtlicher Prozesse	15 Punkte

Merkmal 10. b. wurde in der Firma diskutiert und nicht als unmittelbar kritisch bewertet.

Die Gesamtpunktzahl liegt bei 30 Punkten.

Die Faktoren wurden wie folgt bestimmt:

9. c.	Abhängigkeit	Faktor 1
11. c.	nach Außen offenes, aber grundlegend abgesichertes Netzwerk	Faktor 1
12. c.	normale Verwundbarkeit	Faktor 1

Die Gesamtpunktzahl bleibt also bei 30 Punkten.

Prozess Kundenkommunikation:

1. b.	Viele personenbezogene Daten über Kunden	5 Punkte
8. d.	Technische Daten für digitale Kommunikation	5 Punkte

Die Gesamtpunktzahl liegt bei 10 Punkten.

Die Faktoren wurden genauso bestimmt:

9. c.	Abhängigkeit	Faktor 1
11. c.	nach Außen offenes, aber grundlegend abgesichertes Netzwerk	Faktor 1
12. c.	normale Verwundbarkeit	Faktor 1

Die Gesamtpunktzahl bleibt also bei 10 Punkten.

Analyse:
Es ist erkennbar, dass die operative Steuerberechnung kritischer ist als die Kundenkommunikation. Die Kundenkommunikation ist ein Prozess mit geringer Risikoexposition, für die ein Schutz über effektive und gut implementierte Standardmaßnahmen im Regelfall ausreichen wird. Die operative Steuerberechnung hingegen ist ein Prozess mit mittlerer Risikoexposition und sollte entsprechend etwas stärker geschützt werden. Hier wird eine Folgeanalyse empfehlenswert sein, die mehr in die Tiefe geht und die eventuell spezifische und härtere Sicherheitsmaßnahmen anvisiert.

Beispiel 2: Ein Zulieferer für Aerospace
Unternehmen B ist ein kleines Unternehmen mit einer Maschinenproduktion, das spezielle und hochwertige Schrauben für den zivilen und militärischen Flugzeugbau nach einem geschützten Verfahren fertigt, für die Logistik wird eine Enterprise Resource Planning (ERP) Software genutzt, auf der auch Produktionsdaten vorgehalten werden. Die Maschinenproduktion ist neueren Datums und erhält Updates über das Internet. Als kritisch wird vor allem der stärker informatisierte Produktionsprozess erachtet.

Für diesen Prozess identifiziert das Unternehmen für sich die folgenden Punktzahlen:

4. b.	Sensible Prozesse	5 Punkte
6. b.	Implizite Entwicklungsdaten	10 Punkte
6. d.	Entwicklungsdaten zu politisch relevanten Technologien	35 Punkte
7. b.	Implizite Entwicklungsdaten Fremder	10 Punkte
7. d.	Entwicklungsdaten zu politisch relevanten Technologien	35 Punkte
8. a.	Produktionsdaten und –prozesse	15 Punkte
10. a.	Individualität	15 Punkte
10. e.	Kritikalität	15 Punkte

Die Gesamtpunktzahl liegt damit bei 140 Punkten. Das Unternehmen gehört in die höchste Risikogruppe. Hochwertige Industriespionage und strategische Spionage sind

hier sehr wahrscheinlich, angriffsbedingte Ausfälle der Anlage oder Datenlöschung hätten gravierende Auswirkungen für die Produktion.

Die Faktoren werden wie folgt festgelegt:

9. c.	Abhängigkeit	Faktor 1
11. c.	Nach Außen offenes, grundlegend abgesichertes Netzwerk	Faktor 1
12. d.	Hohe Verwundbarkeit	Faktor 2

Die Gesamtpunktzahl wird damit auf 280 Punkte katapultiert. Dies ist vor allem dem Einsatz einer ERP-Software geschuldet, die allgemein als höher verwundbar eingestuft wird.

Analyse:
Das Unternehmen ist hochgradig gefährdet und muss dringend eine detaillierte Risikoanalyse aufnehmen, unter Einbindung spezialisierter unabhängiger Berater. Abhängigkeiten und Verwundbarkeiten sowie Vernetzung sollten soweit es geht reduziert werden. Eine Reduzierung der Vernetzung auf ein hart isoliertes System und das Migrieren aller Produktionsdaten aus der ERP-Software in das isolierte System etwa würde die Faktoren ändern auf:

9. c.	Abhängigkeit	Faktor 1
11. c.	Nach Außen hart isoliertes Netzwerk	Faktor 0,2
12. d.	Normale Verwundbarkeit	Faktor 1

Damit würde sich die hohe Punktzahl auf 28 Punkte reduzieren, es hätte also nur noch eine mittlere Risikoexposition.

2. Der Aufbau von Cybersicherheit für KMUs

2.1 Strategischer Aufbau von Cybersicherheit bei KMUs

Warum benötigt Cybersicherheit einen strategischen Ansatz?
Cybersicherheit hat eine hohe inhärente Komplexität. Die zu schützende Landschaft ist hochgradig komplex, die Angriffsoptionen und die Schutzoptionen inklusive aller Trade-Offs und Bedingungen sind es ebenfalls. Infolgedessen benötigt die Einrichtung von Cybersicherheit ab einer gewissen Größe der IT-Landschaft eine Strategie.

In der Theorie ist Cyberstrategie einfach. Unter Berücksichtigung des Risikos und der Schutzziele ist aus den insgesamt verfügbaren Schutzoptionen die nach einem hierarchischen Zielsystem definierte beste Kombination zu finden. Dabei ist Cybersicherheit als kontinuierlicher Prozess zu verstehen, der stete Aufmerksamkeit auf Veränderungen in der Bedrohungs- und Schutzlandschaft und stete Anpassung der eigenen Fähigkeiten und Mittel erfordert.

In der Praxis ist dieser theoretische Ansatz aber nicht konsistent durchführbar. Ein wichtiger Grund ist auch ein politisch brisantes Problem der Cybersicherheit: Eine exakte Formulierung idealer Konstellationen von Risiken und Sicherheiten ist gegenwärtig nicht möglich. Aus Forschungssicht sind in diesen Fragen zu viele Wissenslücken bei zu hoher Basiskomplexität zu verzeichnen, um eine Methodik entwickeln zu können. Vor allem sind zwei fundamentale Größen immer noch weitgehend unbekannt: (1) das exakte Ausmaß der durch Fehler oder Struktur angelegten und operativ nutzbaren Verwundbarkeiten normaler Basis-IT inklusive Typen von Verwundbarkeiten bezogen auf spezifische Systemvarianten und Hersteller sowie (2) Abdeckung, Effektivität und Effizienz von Sicherheitstechnologien referenziert auf Verwundbarkeiten und Angriffstypen. Mit anderen Worten: Im Moment weiß niemand, wo und wie groß das zugrundeliegende Basisproblem ist oder was wirklich dagegen hilft.

Damit ist die Entwicklung einer Strategie grundlegend behindert. Auch bestehende Cybersicherheitsansätze können nicht als im vollen Sinne strategisch bewertet werden. Sie haben lediglich Teilstrategien für (oft zurechtgesetzte) Problemausschnitte entwickelt. Die traditionellen Ansätze sind ein Beispiel. Sie arbeiten sich an den Symptomen des Problems ab, an konkret entdeckten Schwachstellen, konkret bekannten individuellen Angriffen, an maschinell gut erkennbaren Angriffstypen oder an partikularen Schutzmechanismen für einige kleine, scheinbar isolierbare Probleme. Dafür gibt es Verfahren und Methoden, deren Zusammenstellung in eine zeitliche oder operative Folge dann oft als „Strategie“ bezeichnet wird. Ohne Adressierung der Basisprobleme oder der Abdeckung und Effektivität ist diese „Strategie“ aber ein Katz-Und-Maus-Spiel, allerdings mit hohem Abstand zwischen beiden, ohne jede Nachhaltigkeit und ohne Entwicklung solider Prävention. Erschwerend ist auch die technische Entwicklung dieser symptomatischen Lösungen kaum strategisch oder auch nur systematisch. In der Fachgemeinschaft hat sich als Einschätzung dieser Ansätze der Begriff „Tinker by Tinker“ („Von Gebastel zu Gebastel“) etabliert. Es wird gebastelt, was man gerade gut

kann oder gut verkaufen kann und wenn das Gebastelte versagt, wird auf dessen Basis weiter gebastelt, bis es wieder anders aussieht und neu verkauft werden kann.

Ein systematischer oder zumindest systematisch informierter Ansatz ist zwar bekannt – dies wäre ein Austausch verwundbarer Basis-IT durch unverwundbare Hochsicherheits-IT – wird allerdings bislang noch nicht industrialisiert, da die traditionellen Ansätze zumindest einen Anschein von Sicherheit vermitteln, ohne viel zu kosten, und da ihr regelmäßiges Scheitern nicht zu deutlich als struktureller Mangel, sondern als „Fact of Digital Life" thematisiert wird.

Der Cybersicherheitsmarkt muss also übergreifend als nur teilstrategisch und als unreif betrachtet werden. Auf einige Probleme werden wir eingangs des übernächsten Abschnitts noch kurz zu sprechen kommen.

Für die notwendige strategische Entwicklung einer Cybersicherheit sind die hohe Basiskomplexität, die Unbekanntheit des Problems und der Sicherheitseffektivität sowie der unreife Cybersicherheitsmarkt fundamentale Probleme. Eine exakte Strategieentwicklung nach Lehrbuch ist schlicht nicht möglich, vor allem für kleine und mittlere Unternehmen, die keine hohen Investitionen in eine teilweise Behebung dieser fundamentalen Probleme setzen können. Daher muss Cyberstrategie besonders für kleine und mittlere Unternehmen anders strategisch aufgebaut werden, mit gröberen, aber in Abwesenheit präziser Methoden hilfreichen verkürzten Verfahren und mithilfe einiger Optionen zur Komplexitätsreduktion.

Die Befähigung zu einem strategischen Ansatz

Die Strategie muss in diesem Fall vor allem gute Partner finden, gute Hersteller und Dienstleister sowie gutes Personal, die in aufbauenden Schritten in ein kooperatives Gesamtkonzept eingepasst werden. Eine solche einfache und verkürzte Strategieentwicklung kann dann in den folgenden Schritten angegangen werden:

0. Fortschritt mit IT kritisch einschätzen

Ein vor allen Sicherheitsüberlegungen stehender Schritt wäre, die Vorhaben zum Einsatz von IT im Unternehmen und im eigenen Produkt kritisch zu hinterfragen. Wo keine IT ist, können keine IT-basierten Risiken und Kosten entstehen. IT sollte also in unternehmenskritischen Prozessen und Produkten stets hart auf ihre operative und wirtschaftliche Notwendigkeit überprüft werden. Dazu gehört die kritische Prüfung der auf- und abwogenden Trends, die von der IT-Industrie produziert und in den Markt gedrückt werden. Spezifisch zum Trend Industrie 4.0 wird sich diese Studie noch gegen Ende äußern.

Leider ist es bei einer vorgreifenden Abschätzung schwer, objektive und belastbare Einschätzungen zum realen Betrieb und Marktverlauf zu erhalten. Bestehende Einschätzungen sind oft visionär unterinformiert, da die Technologie meist noch nicht breit verbreitet und abgeprüft ist, und sind zudem von Meinungsströmungen und Verkaufsinteressen geprägt. Bei angepriesenen Innovationspotentialen im Produkt ist etwa oft unklar, ob diese auch wirklich auf ein nachhaltig gehobenes Marktinteresse treffen und ob nicht für die IT-basierten Innovationen hohe entwicklungsstrategische Abhängigkeiten von fremden Technologietypen, neuen

Standards und Regulierungen und anderen Marktteilnehmern entstehen. Bei angepriesenen Einsparungen im Betrieb dagegen wird oft verschwiegen, welche Folgekosten durch die IT entstehen wie in der Einstellung von IT-Fachpersonal oder durch hohe Betriebs- und Wartungskosten. Selbst unabhängig von Datensicherheits- und Datenschutzrisiken bestehen also hinreichend Gründe zum Zweifel an IT-basiertem Fortschritt, die eine kritische Prüfung vorab empfehlen.

Neben der Frage nach der Notwendigkeit lässt sich in diesem Kontext auch die Frage stellen, ob man mit dem Verbau der IT noch warten kann. Oft wird hier ein hoher externer Druck zur schnellen Innovation aufgebaut, der aber in vielen Fällen unbegründet ist. Sind keine strategischen Verluste in Marktanteilen zu erwarten, ist ein Abwarten sogar empfehlenswert. In diesem Fall kann man die reale Implementierung in anderen Unternehmen beobachten, Risiken und Folgekosten später deutlich besser einschätzen. Zudem kommt es im Verlauf der Zeit bei wirklich erfolgreichen IT-Innovationen zu einer größeren Ausdifferenzierung der Anbieter, wobei Bedingungen und Effizienzcharakteristiken klarer erkennbar werden, das Spektrum der Optionen deutlich breiter und die Kosteneffizienz durch günstigere Angebote deutlich besser wird.

Dies führt zu einer letzten Frage, die im Kontext IT-basierter Innovation kritisch gestellt werden kann. Die spezifische Variante der Innovation und ihr Durchdringungsgrad sollten ebenfalls geprüft werden. Sind verschiedene Formen der IT-Innovation bereits im Markt, sollten diese auf ihre Kennmerkmale, aber auch auf weniger bekannte Effekte wie die Tiefe der in Prozessen und Produkten entstehenden Abhängigkeiten befragt werden. Dabei sollte auch bedacht werden, dass ein technisches, operatives und vertragliches „Customizing“ vom Hersteller oder im eigenen Verbau unternommen werden kann, um Abhängigkeiten und Funktionalitäten zu verändern.

Die Vorab-Prüfung einer Informatisierung sollte also drei Fragen stellen:

1. Braucht das Unternehmen/das Produkt diese IT wirklich?
2. Wie lange kann man mit Einkauf und Implementierung noch warten?
3. Welche Variante dieser IT würde am besten in das Unternehmen/das Produkt passen?

Zur Ermöglichung genauerer Prüfungen empfehlen die Autoren der DIHK die Entwicklung einer entsprechenden Methodologie.

1. Risiko- und Bedarfsmodellierung

Dieser Punkt wurde bereits früher in der Studie angesprochen. Die Risiko- und Bedarfskonzeption muss den Ausgangspunkt einer strategischen Cybersicherheit bilden. Das Unternehmen muss antizipieren, wer als Angreifer in Frage kommt und in welcher Weise es an welchen Orten zu welchen Zwecken angegriffen werden könnte. Daraus lässt sich eine erste Landkarte des Problems entwerfen, auf der problematische Prozesse, Systeme, Personen, Daten in einer Gewichtung verortet sind und auf deren Basis die Security Strategy (und ein erster Teil der Policy) beschrieben werden kann.

2. Zuständigkeit, Prozesse und Organisation herstellen

Ein Unternehmen muss bei einer Herstellung von IT-Sicherheit im Unternehmen auch personale Zuständigkeit und Verantwortlichkeit herstellen, verschiedene Sicherheitsprozesse wie Einkauf, Implementierung, Betrieb, Evaluation, Tests, Sensibilisierung, Weiterbildung planen und durchführen und Sicherheit organisatorisch in einer möglichst unabhängigen und direkt der Geschäftsführung unterstehenden Einheit verankern.

3. Kompetenzen, Ausbildung und Weiterbildung

Das mit IT-Sicherheit betraute Personal muss der Aufgabe entsprechend kompetent sein und die notwendige Qualifizierung und Qualifizierbarkeit nachweisen. Später in diesem Abschnitt sind Erfordernisse für die Qualifizierung und Qualifizierungsmöglichkeiten aufgeführt. Dabei ist darauf zu achten, dass sowohl gute Kenntnisse der zu schützenden Basissysteme und Geschäftsprozesse vorhanden sind wie gute Kenntnisse der avisierten Sicherheitsmaßnahmen und dass diese Kenntnisse kontinuierlich weiter ausgebildet werden. Dabei sollte nicht vergessen werden, dass für Aufbau und Betrieb der Sicherheit auch externe Anbieter genutzt oder Partnerschaften aufgebaut werden können. Ein Unternehmen kann meist und muss auch nicht alle Expertise selbst vorhalten. Jedoch ist eine Meta-Expertise notwendig, die das Unternehmen zumindest in die Lage versetzt, die eigenen Bedarfe richtig zu erkennen und Angebote und Implementierungen kritisch zu prüfen.

4. Lagebild und Revision der IT-Architektur nach Sicherheitsaspekten

Die gesamte IT-Architektur muss auf Komponenten, systemische Zusammenhänge und Abhängigkeiten hin analysiert und transparent gemacht werden. Verwundbare Technologien müssen sofort verortbar werden, Reduzierungen von Vernetzungsgraden und Abhängigkeiten sollten wo immer möglich direkt durchgeführt werden. Ein Beispiel hierfür ist eine vollständige Entnetzung und Isolierung besonders kritischer Daten. Ist eine solche Entnetzung effektiv, müsste ein Angreifer auf Innentäter zurückgreifen, um einen Datenabfluss herzustellen, was mit deutlich erhöhten Risiken und Kosten verbunden ist. Für besonders kritische Bereiche der IT-Architektur müssen Sonderkonzepte gefunden werden.

5. Formulierung der Policy für sicheren Einkauf und sichere Innovation

Vor der Security Policy sollte eine Policy für den Einkauf von und für die Innovation mit weniger verwundbaren Basistechnologien aufgestellt werden. Zu diesem Zweck ist weiter unten in diesem Abschnitt eine Liste von Indikatoren aufgestellt, anhand derer die sicherheitsbezogene Qualität eines normalen IT-Produkts im Rahmen der Angebotserstellung abgeprüft werden kann.

6. Bandbreite der Angebote berücksichtigen

Für einige Sicherheitsprobleme oder für Restrisiken hilft es oft, anstelle komplexer technischer Sicherheitslösungen andere Maßnahmen zu ergreifen. So können in Einzelfällen Dienstleistungen wie eine Cloud eine bessere Sicherheit bieten als eine eigene Vorhaltung von Daten, sofern das Unternehmen etwa keine Ressourcen und kein Verständnis von Sicherheit hat. Interessant kann auch der Einkauf einer Cyber-

Versicherung sein, um mittlere bis geringe Risiken abzudecken.[14] In diesen Fällen muss allerdings auf Qualität geachtet werden. Bei einer Cloud etwa ist darauf zu achten, dass die Dienstleistungen auf ihre Sicherheitsqualitäten und auf Procedere und Auflagen bei Vorfällen geprüft werden müssen, da die Hoheit über die eigenen Daten und Prozesse zu weiten Teilen abgegeben wird. Bei einer Versicherung müssen Art und Umfang der Deckung verstanden werden.

Cyber-Versicherungen und Restrisiken
Für viele kleine und mittlere Unternehmen mit kleiner bis mittlerer Risiko-Exposition wird eine Kombination aus einer soliden technischen Basis-Sicherheit und einer Cyber-Versicherung mit einer guten Deckung und mit Möglichkeiten, auf bestimmte Schutzinteressen einzugehen, einen hinreichenden und gleichzeitig kosteneffizienten Schutz entfalten. Cyber-Versicherungen sind zwar gegenwärtig noch in der Entwicklung, gerade für das Segment KMUs für gängige und bekannte Risiken aber schon in einer guten Produktreife. So kann die Basis-Sicherheit kleinere Vorfälle und Störungen abfangen, während die Versicherung einen signifikanten Teil der konkret auftretenden Kosten schwerwiegenderer Vorfälle abdecken kann. Damit ist die Wahrscheinlichkeit einer Schockwirkung durch einen Vorfall bereits deutlich reduziert. Der Unternehmer muss allerdings seine Risiken gut kennen und die Kosten und Konsequenzen dieser Risiken gut abschätzen können, um noch verbleibende Restrisiken zu erkennen und weitere Schutzmaßnahmen ergreifen zu können. Hier ist in der Praxis bei einigen Versicherungsanbietern noch eine Unreife im Produkt zu erkennen, indem dort gelegentlich nicht auf spezifische Sicherheitsbedürfnisse eingegangen wird, was eine Unsicherheit für ein mögliches späteres Verfahren bedeutet. Der Versicherungsnehmer sollte in diesen Fällen das Gespräch mit der Versicherung suchen und unabhängige Vergleiche von Cyber-Versicherungen zu Rate ziehen.

7. Beschaffung von Sicherheitstechnologie und Erstellung einer Security Policy
Schließlich sollten ausgehend von der Kenntnis der eigenen Risiken, der eigenen Ausgangslage und der eigenen Fähigkeiten sowie möglicher Maßnahmen und Optionen Sicherheitstechnologien angeschafft und implementiert werden, die exakt auf die modellierte Situation passen. Auch hierfür ist weiter unten eine Liste von Indikatoren angegeben. Ist die gesamte Sicherheitslage präsent und modellierbar, lässt sich die Security Policy formulieren, um einen funktionalen Umgang und den effektiven Ausbau von Sicherheit zu ermöglichen.

Einige Leser mögen es erstaunlich finden, dass der Einkauf von IT-Sicherheitslösungen am Ende des Prozesses steht. In der Praxis findet der Einkauf oft direkt am Anfang statt, in der Meinung, man müsse schnell etwas tun. Allerdings stellt

[14] Siehe hierzu auch: Shackelford, Scott J. "Should your firm invest in cyber risk insurance?." *Business Horizons* 55.4 (2012): 349-356.

sich dabei oft heraus, dass man das Falsche getan hat und die Ungenauigkeiten und Anpassungsleistungen – innerhalb derer die anderen Schritte dann doch gegangen werden müssen – stellen oft zusätzliche Probleme, Verzögerungen und Kosten auf, ohne signifikant die Risikoexposition zu verringern. Nur wer noch gar keinen Schutz verbaut hat, sollte möglichst schnell etwas einkaufen. Dann ist es empfehlenswert, ein gutes Standardprodukt ohne hohe Abhängigkeiten anzuschaffen, um zumindest vor weiteren Anschaffungen noch die Entwicklungsschritte durchlaufen zu können.

Eine verkürzte Strategie wird keine harte Sicherheit für hohe und sehr hohe Anforderungen herstellen können und muss eine gewisse Toleranz für Vorfälle mitbringen, kann aber zu einer deutlichen Verbesserung der Ausgangslage führen und Risiken stark reduzieren. Eine genauere Methodik der Strategieentwicklung muss passgenau nach Risikoklassen und Varianten der IT-Nutzung entwickelt werden und wird viele weitere Faktoren enthalten, die hier nicht aufgeführt werden sollen. Die im weiteren Teil dieser Studie erwähnten Faktoren sollten dabei einbezogen werden.

Entwicklung eigener Fähigkeiten
Vorbereitend und parallel zu jedem strategischen Bemühen sollten aufgrund der hohen Komplexität komplexitätsreduzierende Fähigkeiten entwickelt werden, als Entwicklung von Metakompetenz und in der Anpassung von Profilen.

Metakompetenz ist eine reine Bewertungskompetenz. Anstatt selbst die volle Komplexität einer Cybersicherheitskompetenz zu erarbeiten, muss Metakompetenz lediglich erkennen können, wie sich gute und hochwertige Cybersicherheitskompetenz bei Beratern und Anbietern ausprägt. So kann ein zuverlässiger Berater oder Anbieter sicherheitssensibler Basis-IT oder guter Sicherheitstechnologie gewählt werden, dessen eigene Kompetenz folgend zur Herstellung der Sicherheit genutzt wird. Metakompetenz erstreckt sich auf die Bewertung der Qualität der Fähigkeit zur Risikomodellierung, die Bewertung der Sicherheitsqualität der Basis-IT eines Herstellers und die Bewertung der Qualität einer Sicherheitstechnologie (eingeschlossen Dienstleistungen) eines Anbieters. Metakompetenz muss nur zum Teil selbst generiert werden und kann auch von externen unabhängigen Stellen erstellt werden. Ein dezidierter unabhängiger Vertreter einer Bewertungskompetenz hätte den Vorteil, tiefer in eine Bewertung einsteigen zu können und entsprechend Methodiken und Prüfverfahren entwickeln zu können, die bessere und breitere Bewertungen ermöglichen.

Anpassung von Profilen kann selbst oder durch einen vertrauenswürdigen Anbieter unternommen werden und beschreibt den Prozess, die eigenen Fähigkeiten an einen Sicherheitsansatz anzupassen und umgekehrt. Diese Anpassung kann einerseits durch Auswahl und Qualifizierung von Personal erfolgen, auf der anderen Seite durch Auswahl und Customizing eines Sicherheitsansatzes, der den Einkauf der Basis-IT, den Einkauf der Sicherheitstechnologie aber auch Elemente wie die Architektur der Abhängigkeiten einschließt. Beide Profile sollten dringend als Einheit konzipiert werden, wobei jedoch aufgrund der gegenwärtig schlechten Verfügbarkeit von Cybersicherheitsexpertise die Verfügbarkeit von Personal und Qualifizierung deutlich begrenzter und daher als grundlegender anzusetzen ist. Mit anderen Worten: Man

fährt oft besser mit einer Technologie, die von dem verfügbaren Personal verstanden wird und präziser fehlerfrei genutzt werden kann. Dennoch müssen eventuell auftretende Schutzlücken in dieser Auswahl erkannt und durch Organisation oder Produkte gedeckt werden, wobei folgend das Personal wieder für ein passendes Produkt qualifiziert werden muss.

2.2 Indikatoren zur Bewertung von Verwundbarkeit und Sicherheitsqualität

Diese Studie will ihre Leser zu einer grundlegenden Metakompetenz befähigen. In den kommenden Abschnitten dieses Teils der Studie werden charakteristische Indikatoren für eine einfache Bewertungen der grundlegenden Verwundbarkeit einer Basis-IT (2.2.1), der Qualität einer Sicherheitstechnologie (2.2.2) sowie der notwendigen Ausdehnung einer Sicherheitsqualifizierung des eigenen Personals (2.2.3) angegeben.

Diese Charakteristiken sind Kernelemente im Aufbau von Sicherheit. Ihre präzise Abfrage, vergleichende Prüfung oder sogar vollumfängliche und unabhängige Messung benötigt viele produkt- oder unternehmensinterne Details, und ist gegenwärtig nicht möglich, da kaum entsprechende Methodologien und Verfahren entwickelt sind, da viele für solche Methodologien erforderlichen Fragen noch nicht beforscht sind und da die IT- und IT-Sicherheitshersteller der Offenlegung oder der unabhängigen und harten Prüfungen dieser sicherheitsrelevanten Qualitätsmerkmale oft ablehnend und wenig kooperativ gegenüberstehen.

In Abwesenheit methodischer, präziser und unabhängiger Prüfungen und Tests kann eine Abschätzung dieser Eigenschaften daher vorrangig über extern ermittelbare Indikatoren vorgenommen werden, also Eigenschaften der Unternehmen und Produkte, die keine Beforschung oder Messung innerer Eigenschaften erfordern, sondern die prinzipiell bekannt, erkennbar und anzugeben sind.

Für Sicherheit lässt sich eine Reihe aus praktischen Erfahrungen bekannte äußerliche Merkmale entwickeln, die nicht immer, aber häufig in enger, kausaler Korrelation und unterschiedlicher kausaler Härte mit guter oder schlechter Sicherheit auftreten. Die Indikatoren sind nur ein Ausschnitt und generisch, so dass also keine vollständigen, exakten und in jedem Fall zutreffenden Urteile damit gefällt, sondern nur Indizien gesammelt werden können. In Abwesenheit präziserer Prüfmöglichkeiten und expliziter Testverfahren ist dies jedoch die beste realiter verfügbare Option einer Vorab-Prüfung von Sicherheitsqualität im Vergleich verschiedener Optionen. Kommen viele Negativindikatoren unter Abwesenheit von Positivindikatoren zusammen, ist ein System eher als gefährdet zu betrachten, als eines mit wenigen Negativindikatoren und vielen Positivindikatoren.

Die im Folgenden angeführten extern ermittelbaren Indikatoren können somit als grobe erste Prüfrichtlinien verwendet werden, um einen Eindruck von der Qualität eines IT-Produkts oder eines Partners zu erlangen. **Sie sollten in alle Anschaffungsprozesse von IT und IT-Sicherheit einfließen, in dem die Indikatoren im Rahmen einer Angebotsstellung von Herstellern und Dienstleistern abgefragt werden.** So werden verschiedene Anbieter von IT und IT-

Sicherheit in ihrer Sicherheitsqualität vergleichbar. Gleichzeitig wird im Sinne der oben angedeuteten strategischen Schritte Sicherheit von Grund auf konzipiert, und es können die besten und nachhaltigsten Wirkungen erzielt werden. Direkt im Einkauf der Basis-IT und der Sicherheitstechnologien lassen sich die größten Sicherheitsgewinne mit der höchsten Kosteneffizienz erzielen, da an dieser Stelle ideal wenig verwundbare Basis-IT in geringer Abhängigkeit mit gut implementierbarer, bedienbarer und effizienter Sicherheitstechnologie kombiniert werden kann, so dass die Wahrscheinlichkeit erfolgreicher Angriffe durch diese Ausgangsbedingung deutlich sinkt, während gleichzeitig keine hohen Folgekosten durch permanente Anpassungen der Systeme, teure Dienstleistungen, direkte und indirekte Schäden und Personalnotwendigkeiten zu erwarten sind.

Die Autoren empfehlen der DIHK eine genauere und umfangreichere Ausarbeitung der Indikatorenliste sowie die Entwicklung einer standardisierbaren Prüfmethodik, um Vergleichbarkeit herzustellen.

2.2.1 Anforderungen an wenig verwundbare Basis-Informationstechnik im Unternehmen

Aufgrund der vielen Hürden und Probleme bei der Herstellung einer effektiven IT-Sicherheit ist es aus strategischer Perspektive für eine grundlegende und nachhaltige Sicherung eines Unternehmens überaus wichtig und hilfreich, von Beginn an eine möglichst wenig angreifbare, also wenig verwundbare Informationstechnik im Unternehmen einzusetzen. Hiermit ist nicht eine Sicherheitstechnik gemeint, sondern die „normalen“ Systeme, die das Unternehmen für seine IT-Belange einkauft: normale PCs, Betriebssysteme, Datenbanken, Anwendungen. Dies führen wir als Basis-IT. Für die Einrichtung von Sicherheit sind diese Elemente äußerst relevant, da nicht jede Variante der Basis- IT gleichartig verwundbar ist. Betriebssysteme, Anwendungen, sogar Hardware können in einigen Varianten einfacher, in anderen deutlich schwieriger anzugreifen sein. Einzig bei einer Erwartung hochwertiger gezielter Angriffe ist diese Auswahl weniger relevant, da diese Angreifer breite und tiefe Expertisen vorhalten, die auch in exotischen und kaum verwundbaren Systemen noch hinreichend viele Angriffsvektoren finden. Für alle anderen Angreifer dagegen wird die Auswahl einer von Beginn an weniger verwundbaren Basis-IT bereits eine Hürde herstellen, auf deren Basis sich deutlich besser weitere Sicherheitsmaßnahmen aufbauen lassen, um letztlich Angreifer auf andere, leichtere Opfer umschwenken zu lassen.

Bei der Bewertung der Basisverwundbarkeit einer IT besteht nun allerdings eine Schwierigkeit. Die verschiedenen Hersteller geben dieses Negativmerkmal nicht bereitwillig preis. Und wenn sie es doch tun, dann meist in dem dualen Hinweis, dass Verwundbarkeit universal verbreitet und quasi ein Naturgesetz sei, dass man selbst aber in dieser Hinsicht aufgrund der Maßnahmen X, Y und Z besonders sicher und bedenkenlos einzusetzen sei.

Solche Behauptungen sind meist irreführend. Erstens ist Verwundbarkeit kein universales Naturgesetz, sondern eine von vielen wirtschaftlichen,

entwicklungsmethodischen und technischen Faktoren abhängige Schwäche, die zwar fast universal verbreitet ist, aber stark unterschiedlich ausfallen kann. So gibt es gravierende Unterschiede bei unterschiedlichen Varianten von IT sowie unter Herstellern, und es gibt sogar unverwundbare Systeme, bei deren Einsatz so gut wie keine Sicherheitsprobleme mehr zu erwarten (die allerdings gegenwärtig nicht im Massenmarkt erhältlich sind). Zweitens gelten Behauptungen über eine hinreichende Beherrschung eigener Schwachstellen nur in thematisch eng zurechtgeschnittenen Szenarien. Hier nutzen Hersteller oft die vielen Lücken in Risikobekanntheit und Effizienzermittlung, um sich einen vorteilhaften Zuschnitt des Problems zurechtzulegen. Um bei dem oben erwähnten Beispiel zu bleiben: Ein Produkt kann durch Maßnahmen X, Y und Z die Verwundbarkeiten 23 bis 42 absichern. Wie viele Verwundbarkeiten das System allerdings noch eröffnet, ob diese kritisch sind, und wie effizient und nachhaltig die Verwundbarkeiten 23 bis 42 abgesichert werden, ist meist weitgehend unbekannt und wird als irrelevant betrachtet. Gerade in größeren Basissystemen werden jedoch aus der Theorie heraus viele tausend bis hunderttausend kritische Verwundbarkeiten angenommen, in kleineren Anwendungen immerhin noch einige hundert, so dass also bei Beherrschung einiger weniger Varianten noch lange nicht von einer hinreichenden Sicherheit gesprochen werden kann.

Wie viele kritische bis sehr kritische Verwundbarkeiten in einem System vorhanden sind, sollte also durchaus in Erwägung gezogen und unabhängig von den Versprechen der Hersteller geprüft werden. Leider gibt es keinen Index für diese Merkmale. Ein solcher Index ist zwar an verschiedenen Stellen in Entwicklung, gegenwärtig aber noch nicht verfügbar. Für eine Abschätzung der Verwundbarkeiten helfen daher zeitweilig wie oben angedeutet extern ermittelbare Indikatoren, die im folgenden aufgeführt und wie empfohlen bei Einkäufen abgefragt und verglichen werden können.

Sicherheitstechnologien und -maßnahmen sind an dieser Stelle nur dann aufgegriffen, wenn sie inhärenter Bestandteil eines Systems sind und keine zuzukaufenden externen Produkte. Sie werden ansonsten separat im nächsten Abschnitt behandelt.

Indikator für Verwundbarkeit	**Relevanz**	**Ausprägungen mit schlechter Auswirkung für die Sicherheit**	**Ausprägungen mit positiver Auswirkung für die Sicherheit**
Codemenge Die absolute Menge Code in Programmzeilen (Single Lines of Code (SLOC)). Viel Code beinhaltet in der Regel viele Fehler und erhöht Komplexität mit Option auf unvorhersehbares Verhalten	Sehr hoch	Große Mengen Codes enthalten mehr Programmierfehler, produzieren so mehr ausbeutbare Verwundbarkeiten, und erhöhen die Codekomplexität drastisch; alter oder toter Code wird nicht gesucht und entfernt; Codemengen wachsen	Kleine Mengen Code enthalten weniger Fehler, also weniger Verwundbarkeiten und reduzieren die Codekomplexität deutlich; Codemengen werden bei jeder Gelegenheit reduziert und bei Systemreformen als relevanter Faktor beachtet

		kontinuierlich	
Codekomplexität Möglichkeiten von Interaktionen zwischen Codesegmenten, die auch unabsichtlich entstehen können	Sehr hoch	Viele Optionen für Interaktionen und schlechte Separationen im Code erlauben unüberschaubar viele Funktionalitäten für Angreifer, die Herstellung neuer und unbeabsichtigter Funktionalität, die Herstellung neuer Verwundbarkeit durch Kombinationen von Programmfehlern, die Erweiterung von Verwundbarkeiten in andere Programmbereiche, eine leichtere laterale Bewegung des Angreifers im Systems und eine deutlich bessere Tarnung des Angreifers und aller Aktivitäten	Geringe Optionen für Interaktionen und gute Separationen des Codes limitieren die Möglichkeiten der Angreifer und isolieren Angreifer stärker (aber nicht vollständig) innerhalb funktionaler Segmente
Funktionalität Normale Funktionen haben oft Sicherheitsimplikationen und können von Angreifer zum Zugriff oder für Störungen, Manipulationen und Exfiltrationen missbraucht werden	Hoch	Übermäßige unnötige Funktionalität erhöht die Codekomplexität, bietet dem Angreifer mehr Angriffsflächen und mehr Angriffsvarianten, die zudem als „legale Funktionen“ ausgeführt kaum als Probleme definierbar und detektierbar sind	Begrenzte Funktionalität begrenzt auch den Angreifer in seinen Aktionsräumen und zwingt ihn zu teuren, umständlichen und leichter als Aberrationen bemerkbaren Zusatzentwicklungen
Konfigurations-optionen Möglichkeiten zur Konfiguration einer Software. Fehlkonfigurationen sind ein gängiger Angriffsvektor, viele Konfigurationsoptionen bieten zudem Möglichkeiten für erweiterte	Sehr hoch	Eine hohe Zahl von Konfigurationsoptionen bietet eine hohe Menge teils sicherheitsrelevanter Optionen für Basiseinstellungen mit teilweise unüberschaubar komplexen Interaktionen zwischen Konfigurationspara-	Eine geringe Zahl von Konfigurationsoptionen kann von Sicherheitssoftware und Sicherheitszuständigen deutlich besser auf mögliche Lücken geprüft und besser kontinuierlich beobachtet werden

Angriffstaktiken		metern und damit neu auftretenden und nicht zu antizipierenden Sicherheitslücken; viele Konfigurationsoptionen bieten zudem viele Optionen, dezidierte Sicherheitsmechanismen zu umgehen oder partiell abzuschalten und zu manipulieren; zu viele Konfigurationsoptionen überfordern zudem Admins und Nutzer, so dass meist einfache und funktionale Optionen gewählt werden, die oft nicht sicherheitssensitiv sind	
Change Rate Die Geschwindigkeit, mit der sich eine Software verändert, womit neue ausbeutbare Fehler oder Interaktionen möglich werden	Hoch	Wird der Code besonders häufig in Teilen verändert oder angepasst oder erweitert und handelt es sich nicht um sicherheitsfokussierte Änderungen oder um gezielte Reduzierungen unnötigen Codes, wächst die Menge der Verwundbarkeiten insgesamt wie aber auch die Codekomplexität in besonders unüberschaubarer Weise	Werden keine oder nur sicherheitsrelevante Veränderungen am Code vorgenommen, ist das Verständnis der Software besser, die Sicherheitsreife des Produkts wächst kontinuierlich und ein Angriff wird stetig schwerer
Change Management Das Management des Wachstums und der Veränderung einer Software	Hoch	Gibt es bei Code-Veränderungen keinen geordneten Prozess mit ausschließlich vertrauenswürdigen Akteuren, einem zentralisiertem Management-Prozess mit sicherheitsorientierten Peer Reviews, so können leicht sicherheitsfeindliche Veränderungen	Ein geordneter, nach Sicherheit priorisierter, forcierter und zentral geplanter und durchgeführter Prozess der Code-Modifikation mit ausschließlich vertrauenswürdigen Akteuren erhöht macht negative Veränderungen unwahrscheinlicher und ermöglicht gezielt positive Veränderungen

		eingebracht oder indirekt verursacht werden	
Coding Praxis Die operative Gestaltung und Methodik der Software-Entwicklung	Sehr hoch	Wird Software von möglichst billigen Programmierern, die häufig wechseln und oft mit anderen oder nur generischen Expertisen arbeiten, so schnell wie möglich und meist unreif erstellt, sind Fehlerrate, Verwundbarkeiten und Dokumentationen besonders schlecht und das Produkt ist entsprechend angreifbar	Haben die Programmierer eine gute spezifische Fachexpertise und viel spezifische Projekterfahrung, hat man hohe Qualität im Code und gute und lückenlose Dokumentationen forciert, sind die Endprodukte besser verstanden, haben damit auch eine höhere Sicherheitskompatibilität und sind weniger fehlerbehaftet
Trustworthy Computing Prinzipien „Trustworthy Computing“ ist ein Paradigma der sicheren Entwicklung von Software; Verpflichtung auf einige TWC Prinzipien zeigt Engagement und erhöht Sicherheit	Sehr hoch	Werden keine Prinzipien zur Kontrolle der Sicherheitsqualität eines Codes im Entwicklungsprozess eingeführt und durchgesetzt, ist das Endprodukt in der Regel auf vielfach unbekannte Weise unsicher	Mit Einführung und kontinuierlicher Durchsetzung verschiedener Prinzipien vollständiger Kontrolle der Sicherheitsqualität vor, während und nach des Entwicklungsprozesses kann die Sicherheitsqualität des Endprodukts deutlich erhöht werden
Trustworthy Computing Methoden Zur Realisierung der TWC Prinzipien gibt es verschiedene Methoden unterschiedlicher Qualität	Sehr hoch	Werden keinerlei oder nur einige wenige Methoden der Security Quality Assurance mit wenig Einfluss auf den Prozess der Entwicklung angesetzt, ist die Sicherheit des Endprodukts dem Hersteller unbekannt und wird viele vermeidbare und leicht zu findende Schwachstellen enthalten	Sind viele gute Methoden für die Entwicklung sicheren Codes beim Hersteller integrativer Bestandteil der Entwicklung, ist die Sicherheit deutlich höher als im Normalfall. Gute Methoden für die Entwicklung sicheren Codes in jeder Form von Software sind ein Security Training der Entwickler, Security Monitoring der gesamten Entwicklung, gute Kenntnis und Umsetzung von Security Design Best Practices, das Aufsetzen eines Threat Models für

			jedes Projekt, Entwicklung und Anwendung von Security Development Tools und Security Tests, das Enforcement einer nachweisbaren Security Dokumentation, ein Security Quality Review am Ende der Entwicklung, das Erstellen eines Security Reponse Plans, eines Patching Programms und eines Security Service Modells
Integration von Sicherheit im Innovationsprozess Werden neue Systeme und Funktionen entwickelt, kann Sicherheit als „Security By Design“ früh und strukturell in den Innovationsprozess integriert werden	Hoch	Innovation wird hauptsächlich in den Kernfunktionen des System betrieben und nur dort als wertvoll betrachtet, muss dort schnell und marktorientiert stattfinden; Sicherheit ist gar nicht oder weit unten in der Liste der Spezifikationen; es gibt nur eine kleine oder gar keine Abteilung für sichere Entwicklung; Sicherheit wird als etwas externes, zuzukaufendes konzipiert, das ex post facto nach dem Innovationsprozess stattfindet	Sicherheit ist ein integrierter Bestandteil jeder Innovation und wird ex ante als wichtig und wertvoll erachtet, ist entsprechend hoch in der Liste der zu erfüllenden Spezifikationen angesiedelt und darf den Innovationsprozess insgesamt verzögern und komplizieren; Sicherheit hat ein Veto-Recht bei Innovation; die Personalressourcen exklusiv abgestellt für Realisierung von Sicherheit sind fünf bis zehn Prozent der gesamten Entwicklerbasis
Veraltete Software Veraltete Software wird in der Regel nicht mehr gepatcht und hält meist viele hundert bekannte und sofort ausbeutbare Schwachstellen vor. WICHTIGER HINWEIS: Veraltete Software ist ein gerichtlich einklagbarer Sachmangel!	Sehr hoch	Teile der verwendeten Software sind veraltet und werden nicht länger unterstützt; Workarounds oder externe Patches sind nicht verfügbar	Jede Softwarekomponente ist hinreichend neu und wird noch mit Sicherheitspatches versorgt

Abwärtskompatibilität Einige Hersteller müssen alte Versionen ihrer Systeme unterstützen und daher problematische Bestandteile weiter unterhalten	Sehr hoch	Der Hersteller muss viele alte Versionen seines Systems unterstützen, selbst wenn diese alten Versionen unlösbare Sicherheitsprobleme beinhalten; das System muss mit vielen Varianten kompatibel gehalten werden; alte Versionen werden nicht aus dem Kernsystem entfernt	Der Hersteller bietet um Altlasten bereinigte neue Versionen mit hohem und aktuellem Sicherheitsstand an, wobei alte Versionen seines Systems problemlos und kostenfrei auf neue Versionen überführt werden können
Bekannte Defekt Raten Bekannte Fehlerraten können Indikatoren für die Codequalität einzelner Hersteller oder Softwarevarianten sein, hängen allerdings von vielen verschiedenen Faktoren ab, sind methodisch schlecht modelliert, kaum prüfbar und liefern oft sehr unvollständige und fleckenhafte Bilder, so dass die Relevanz derzeit noch gering ist	Gering	Fehlerraten sind bekannt, hoch und steigen kontinuierlich	Fehlerraten sind bekannt, niedrig, und sinken kontinuierlich
Quellcode-Verfügbarkeit Die Verfügbarkeit von Quellcode macht es für Angreifer teilweise einfacher, Angriffe zu entwickelt, ist aber ohnehin über Reverse Engineering herstellbar und führt andererseits auch zum Teil zur Erhöhung von Sicherheit, indem externe Akteure Sicherheitsprobleme	Gering	Quellcode ist frei verfügbar, wird allerdings nicht oder kaum von einer Community auf Fehler untersucht und steht vor allem Angreifern zur Verfügung	Quellcode ist nicht verfügbar oder aber frei verfügbar und wird von einer Community regelmäßig aktiv auf Fehler untersucht, ohne kontinuierlich erweitert zu werden

entdecken und melden können			
Customizability Die Möglichkeit, als Nutzer oder als Dritter Software zu verändern, um Funktionalitäten zu erweitern	Sehr hoch	Stark durch den Endkunden oder berechtigte und unberechtigte Dritte veränderbare Systeme erhöhen Codemenge und Codekomplexität an fremden Orten ohne genauere Kenntnis der Sicherheitsimplikationen oder Möglichkeiten der Aufnahmen in einen Sicherheitsprozess. Sind diese Veränderungen zudem anderen Nutzern zugänglich, wird die Intransparenz zusätzlich erhöht. Sicherheitsdefektive Funktionen können leichter eingebaut werden	Werden Codebereiche nur und langfristig von ausgewiesenen und autorisierten Kernentwickler betreut ohne externe Zugriffe, sind Kenntnis und Sicherheitsqualität des Codes deutlich besser, angelagerte Sicherheitsprozesse wie Patching, Service, Response und Recovery sind deutlich besser zu organisieren
Beherrschbarkeit der Systemgröße Die Systemgröße bezieht sich auf den Umfang der fertigen Implementierung des gesamten Systems, etwa in einem Konzern über einige tausend Nutzer. Verschiedene Systeme machen hier eine zentrale oder dezentrale Beherrschung der Systemgröße unterschiedlich schwer oder leicht	Sehr hoch	Ist das letztendlich mit dem Hersteller vollständig implementierte System sehr groß, mit vielen verschiedenen Nutzern, vielen Funktionen und vielen Verwendungen, so muss das System besonderen Zusatzanforderungen genügen. Existiert kein oder nur ein schlechtes oder schlecht real systemweit implementierbares Konzept für eine sichere, transparente und souveräne Handhabung der entstehenden hohen Zahl sicherheitsrelevanter Prozesse und Daten, entstehen schnell	Es besteht ein dezidiertes und bereits in der Systementwickung mit eingebautes Konzept der Skalierung des sicheren Gebrauchs über große und sehr große Systemausdehnungen, das insbesondere die Entstehung von Single Points of Failure vermeidet oder leicht erkennbar macht

		zahlreiche Lücken in der Sicherheitskonzeption, von denen viele als Single Points of Failure ein systemweites Sicherheitsversagen nach sich ziehen	
Strukturelle Schwachstellen Strukturelle Schwachstellen sind sicherheitsrelevante Entwicklungsfehler, die strukturelle Bestandteile des Systems und infolgedessen persistent und nicht zu entfernen sind	Sehr hoch bis hoch, je nach Schwach-stelle	Es sind strukturelle Fehler in der Entwicklung begangen worden wie leichte Erreichbarkeit unbeschränkter Zugriffe, hardcodierte Passwörter, leicht erreichbare und bekannte Hintertüren, Varianten automatischer Programmausführung, leicht möglicher Zugriff auf Passwörter und Zertifikate in Datenbanken etc.	Trustworthy Computing Methoden und Testverfahren wurden eingesetzt, um bekannte strukturelle Schwachstellen weitestgehend zu erkennen und zu entfernen
Single Points of Failure Single Points of Failure sind Funktionen oder Prozesse, die vollständige Eskalationen von Rechten, systemweite kritische Zugriffe und Modifikationen zulassen	Sehr hoch	Das System bietet besonders viele bekannte und unbekannte „Single Points of Failure“, die zudem schlecht isoliert oder isolierbar sind	Das System bietet nur die durch Kernfunktionen absolut notwendigen Single Points of Failure, die aber sämtlich bekannt sind und um die herum besondere Sicherheitsmaßnahmen, insbesondere funktionale Isolierungen, errichtet wurden
Systeminhärente Sicherheitskon-zeption Sicherheitsfunktionalitäten wie Rechte, Rollen, Mechanismen zu Identifikationen und Autorisierungen, Übertragungssicherung und Protokollierung die das System von sich aus und möglichst als Strukturmerkmal anbietet	Hoch	Das System hat keine oder nur eine sehr oberflächliche und in der Realität des Kunden schwer verständliche oder implementierbare Sicherheitskonzeption, die keinen oder nur einen lückenhaften Beweis zu Qualität, Abdeckung, Effektivität und Effizienz von Sicherheit liefert	Das System hat ein systeminhärentes Sicherheitskonzept, das qualitativ hochwertig und funktional ist, für den Kunden problemlos benutzbar ist und das beweisbar, kontinuierlich, vollständig, effektiv und effizient eine hohe Zahl kritischer bekannter und vorhersehbarer Sicherheitsprobleme adressiert

Zertifizierungen und Anerkennungen Einige Zertifizierungen wie Common Criteria, ISO 27001 und ITSEC liefern grundlegenden Indikatoren, ob bei der Entwicklung einer Software auf Sicherheit geachtet wurde. Leider beschränken sich die Indikatoren allerdings auf klassische ad hoc Sicherheitsmerkmale wie etwa Rechte und Rollen, die in der gegenwärtigen Sicherheitslandschaft nicht mehr als hinreichend erachtet werden können, so dass die Relevanz für die Vermessung der Basisverwundbarkeit nicht hoch ist	Medi-um	Sind keinerlei Zertifizierungen oder Anerkennungen vorhanden, können hierüber keine Indikatoren für die Verwundbarkeit des Produkts abgelesen werden	Sind Zertifizierungen und Anerkennungen vorhanden, so geben diese zumindest einen Indikator für die Korrektheit einiger grundlegender Sicherheitsmechanismen und für ein Sicherheitsinteresse und –bemühen des Herstellers
Systeminhärente Sicherheitskompa-tibilität Die Eignung eines Systems für den effektiven und effizienten Anbau externer Sicherheitstechnolo-gien	Medi-um	Das System bewegt sich außerhalb des normalen Anwendungsfeldes der IT-Sicherheit oder ist in hohem Maße inkompatibel mit den Anforderungen von Sicherheitslösungen, Zugänge sind unklar, schwer zu definieren und zu kontrollieren und leicht modifizierbar, Prozesse sind nicht transparent und kontrollierbar	Das System ist offen für Funktionalitäten von Sicherheitslösungen, die zudem besonders leicht und effizient in allen relevanten Bereichen arbeiten können; Zugangs- und Detektionssicherheit sind durch starke und effektive Restriktion der Zugänge sowie durch transparente, minimal komplexe Prozesse ermöglicht
Bedingungen für Forensik und Recovery Forensik und Recovery sind oft nach Vorfällen notwendig,	Hoch	Systeme müssen für Forensik oder Recovery vollständig und lange getrennt und runtergefahren werden; Forensik ist kompliziert,	Systeme erlauben durch geschickte Separation und Backups einen parallelen Betrieb und Business Continuity ohne Sicherheitsgefahren; sie

um Angreifer zu erkennen, sie zu verstehen, um sie sicher und endgültig zu entfernen und um möglichst schnell wieder einen sicheren Betrieb zu gewährleisten		dauert lange und liefert nur wenige Einsichten; Recovery erfordert ein vollumfängliches, manuelles Neuaufsetzen des gesamten Systems, da die Entfernung des Angreifers anders nicht gewährleistet werden kann	können im Betrieb analysiert und in Teilen sicher wieder hergestellt werden; Systeme sind transparent, Prozesse sicherheitssensible geloggt, so dass Forensik gut arbeiten kann; eine Entfernung des Angreifers kann geprüft und gewährleistet werden
Service und Support bei Sicherheitspro-blemen Einige Hersteller bieten Service und Support bei Sicherheitsproblemen an	Medi-um	Es gibt keine Handreichen und keinen herstellerseitigen Service und Support bei Sicherheitsproblemen; der Hersteller fühlt sich nicht zuständig und ist nicht ansprechbar für Sicherheitsprobleme; entsprechende Dienstleister sind selten, sehr ausgebucht und sehr teuer	Der Hersteller liefert Handreichen und Informationen für den Umgang mit Sicherheitsproblemen im Kontext mit seinem Produkt; Response und Recovery Verfahren existieren, werden Nutzern vermittelt und sind nutzerseitig umsetzbar; es gibt eine jederzeit verfügbare und erreichbare Abteilung und Hotline als konstanten Ansprechpartner; bei schwerwiegenden Vorfällen können Experten geschickt werden; entsprechende externe Dienstleister sind zahlreich, verfügbar und kosteneffizient
Datenbankkon-zeption Datenbanken können sicherheitssensibel konzipiert und implementiert werden	Medi-um	Daten sind nicht klassifizierbar und nach Relevanz für den Kunden bewertbar; sie lassen sich nicht nach verschiedenen Sicherheitsanforderunge n separat speichern und lassen entweder bereits technisch oder durch reale Implementierungsproble me keine harte und eindeutige Zuschreibung von Rollen und Rechten	Das System bietet eine klare Klassifizierung von Daten, wobei sicherheitssensible Daten in besonders geschützten Bereichen mit hoher und gut bedienbarer Sicherheitsfunktionalität gelagert werden und nicht ohne hohen Aufwand von unberechtigten Personen oder Prozessen aufgerufen werden können

		zu	
Anforderung Systemkenntnis beim Administrator/ Nutzer Software muss nicht nur sicher entwickelt werden, sie muss auch sicher implementierbar und nutzbar sein. Dies stellt oft hohe Zusatzanforderungen an Administratoren und Nutzer	Hoch	Sichere Implementierung und sicherer Betrieb sind nur unter hoher und detaillierter Fachkenntnis des Systems und seiner Sicherheitsschwächen möglich; hinreichende Fachkenntnis des Systems und seiner Sicherheitsschwächen ist aufgrund der Größe, der Komplexität oder der Geheimhaltung von Sicherheitsproblemen nicht oder nur stark eingeschränkt möglich	Sichere Implementierung und sicherer Betrieb sind auch mit eingeschränkter Fachkenntnis des Systems möglich; hinreichende Fachkenntnis zur Sicherheit des Systems ist prinzipiell möglich und wird durch den Hersteller unterstützt
Systemkenntnis in Sicherheitsindustrie Systeme sind in der IT-Sicherheitsindustrie markthistorisch bedingt unterschiedlich beliebt und bekannt	Medi-um	Das System ist für die IT-Sicherheitsindustrie ein Exot und wenig relevant oder nur schwer zugänglich, so dass kein längerer industrieller Sicherheitsprozess mit guter und heterogener Sicherheitskenntnis für das System existiert und so dass keine oder keine gut passenden Sicherheitslösungen für das System entwickelt wurden	Das System ist für die IT-Sicherheitsindustrie bereits lange ein Thema, System und Hersteller sind gut zugänglich und kooperativ, so dass bereits lange ein Sicherheitsprozess mit guter Kenntnis der Schwächen des Systems existiert, auf dem verschiedene in Konkurrenz stehende, gut passende und in Teilen nachweisbar bewährte Sicherheitslösungen aufbauen
Patching Praxis Das Verfahren eines Herstellers bei der Schließung von Sicherheitslücken	Sehr hoch	Bei Bekanntwerden von Sicherheitslücken werden nur zögerlich und langsam oder gar nicht Patches erstellt; die Patches dauern lange, die zuständige Abteilung ist zu klein und kaum erreichbar oder ansprechbar; es werden nur die billigen und prominenten Lücken überhaupt gepatcht; Nutzer werden nicht	Bei Bekanntwerden von Sicherheitslücken wird sofort reagiert und mit der Entwicklung von Patches begonnen; die Abteilungen sind erreichbar und hinreichend groß, um jederzeit an Patches zu arbeiten; Patching wird sehr ernst genommen und findet strukturiert und effizient statt; alle Lücken werden so schnell wie möglich gepatcht; Patching

		über Schwachstellen oder Patches informiert	wird beim Kunden forciert und sofort initiiert, sobald ein Patch fertig ist
Patch Implementierbarkeit und Qualität Die Einfachheit des Schließens von Sicherheitslücken durch Herstellerpatches beim Nutzer	Sehr hoch	Das Einspielen von Patches ist kompliziert und erfordert hohe Fachkenntnis; es dauert lange und erfordert nicht tolerable Downtimes der System und hohe Offline-Zeiten; Patches sind oft schlecht gebaut und produzieren später Systemabstürze oder erfordern weitere Anpassungen	Patches können von normalen Nutzern problemlos und passgenau eingespielt werden; Anforderungen an Downtimes und Offline-Zeiten sind tolerabel; Patches sind qualitativ hochwertig und werden vor jedem Deployment gut getestet
Akzeptanz von Verwundbarkeiten Akzeptanz und Umgang eines Herstellers mit Verwundbarkeiten im eigenen Produkt	Sehr hoch	Der Hersteller empfindet Verwundbarkeiten in seinem System als naturgegeben und irrelevant; Sicherheitsverantwortung lokalisiert er bei ad hoc Sicherheitslösungen, in schlechter Strafverfolgung sowie in der mangelnden Sicherheitskompetenz der Nutzer (und zitiert vermutlich gern das Security-Bonmot „der Mensch ist das Problem“); strukturelle Sicherheitsprobleme interessieren ihn nicht, es werden keine Prozesse und Strukturen aufgesetzt; er unterhält keine kooperativen Dialoge mit externen Akteuren und hält sich von Debatten und Prüfungen fern	Der Hersteller akzeptiert Verwundbarkeiten in seinem System als Problem und unterhält offene Dialoge mit Behörden, Sicherheitsexperten, Kunden und Wissenschaft; er bekennt sich zu Schwachstellen und hat proportional zum Problem Strukturen und Prozesse zur Verbesserung der Lage geschaffen; der Hersteller akzeptiert Verantwortung für Sicherheitslücken und versucht nicht, diese auf Nutzer oder Behörden abzustreifen
Reaktionen auf externe Akteure Der Kooperationswille eines Herstellers in der Arbeit mit	Hoch	Der Hersteller möchte keine externen Meldungen von strukturellen Problemen und Schwachstellen	Der Hersteller begrüßt externe Meldungen von strukturellen Problemen und Schwachstellen; er unterhält ein „Bug Bounty“

externen Experten an Sicherheitsthemen		erhalten; Schwächen des Herstellers dürfen nicht an Kunden oder an die Öffentlichkeit gelangen und werden aktiv verschwiegen oder verleugnet; externe Experten werden bedroht, bestochen, isoliert, vertraglich gebunden oder in das Unternehmen inkorporiert; vertrauensvollen Meldungen wird nicht nachgegangen und Meldungen werden nicht belohnt; offene Meldungen und Kritik werden rechtlich verfolgt oder mit impliziten Bestrafungen und Drohungen beantwortet	Programm mit geregeltem Disclosure-Prozess und mit angemessenen Zahlungen für extern gefundene Schwachstellen; er betreibt offene Dialoge über strukturelle Probleme und scheut nicht die öffentliche Debatte über seine eigenen Produkte; kritische Experten werden zur Kritik befähigt und dürfen unabhängig arbeiten und sprechen
Struktur der Abteilung für Produktsicherheit Wie eine Abteilung für Produktsicherheit aufgebaut und im Unternehmen des Herstellers verankert ist	Sehr hoch	Es gibt keine oder nur eine kleine Abteilung (unter 1% der Entwicklerbasis); die Produktsicherheit ist ein Feigenblatt ohne Funktion im Unternehmen, hat keinen klaren Auftrag oder ist dem Marketing unterstellt, um nur einen Anschein von Sicherheit zu liefern; die Sicherheitsabteilung wurde erst vor Kurzem überhaupt gegründet; das Personal in der Sicherheitsabteilung erhält nur niedrige Gehälter und verfügt nur über unpassende und generische Expertise ohne explizite Sicherheitsausbildung oder	Die Abteilung ist groß (5-10% der Entwicklerbasis) und alt (mindestens sieben Jahre), hat klare Aufträge, eigene Visionen und Konzepte und hohe Zugriffsrechte im Unternehmen und in der Innovation; es gibt einen IT-Sicherheitszuständigen auf Board-Level als CIO oder CISO; die Ressourcen für Produktsicherheit betragen mindestens 10% des Entwicklungsbudgets; die Sicherheitsabteilung ist unabhängig im Unternehmen aufgebaut und direkt dem Vorstand unterstellt; das Personal ist hochqualifiziert, spezialisiert, wird kontinuierlich weiter ausgebildet, ist gut vernetzt und beinhaltet heterogene

		Sicherheitserfahrung	Expertisen und Erfahrungen für spezifische Sicherheitsthemen der Herstellers

Zusatz: Dienstleister
Bei intensiver Nutzung von IT-Dienstleistern wie etwa durch Cloud-Dienste sind zudem die Qualität und Zuverlässigkeit dieses Dienstleisters zu prüfen. In diesem Fall sind andere Indikatoren zu adressieren. Auch Mischformen zwischen „Verwundbarer IT“ und „Verwundbarem Dienstleister“ existieren, etwa in Form der On-Premise-Cloud. In diesem Fall müssen beide Indikatorenlisten angewendet werden.

Indikator	**Relevanz**	**Ausprägungen mit schlechter Auswirkung für die Sicherheit**	**Ausprägungen mit positiver Auswirkung für die Sicherheit**
Sicherheit der Datenwege zum Dienstleister Die Art der Vernetzung mit dem Dienstleister zum Zwecke des Datenaustauschs kann unterschiedlich sicherheitsrelevant sein	Hoch	Datenverbindungen sind unverschlüsselt und gehen durch verschiedene Länder; der Anbieter erklärt keine Zuständigkeit für Datenwege und bietet keine Hilfestellungen an	Datenverbindungen sind per default gut verschlüsselt; Datenwege sind zuverlässig determiniert und gehen nicht durch andere Länder; der Anbieter schließt die Sicherheit der Datenwege in seine Zuständigkeit ein
Datenhaltung externer Daten Die Qualität der Datenhaltung externer Daten ist sofort relevant für deren Sicherheit	Hoch	Daten werden unverschlüsselt gehalten, es gibt keine Segregationen zwischen Kundendaten an Speicherorten; das Datenbankmanagement ist nicht auf Sicherheit optimiert; die Datenbanksoftware ist verwundbar	Daten werden immer verschlüsselt und fragmentiert an mehreren Orten gehalten; Daten unterschiedlicher Kunden werden an anderen Orten gehalten; es wird Wert gelegt auf sicheres Datenbankmanagement und sichere Datenbanksoftware
Redundanzen und Backups Werden Daten extern gehalten und Prozesse extern ermöglicht, müssen die Dienstleister Continuity,	Sehr hoch	Es werden keine Redundanzen für Serviceausfälle bereitgehalten; Daten werden nicht mehrfach an verschiedenen Orten vorgehalten; er hat kein	Bei Ausfällen der IT des Dienstleistern stehen heterogene Redundanzen sofort zur Verfügung; es existieren Verfahren zur sofortigen Business

Backups und Recovery gewährleisten		Konzept zu Business Continuity und zur Desaster und Data Recovery	Continuity für alle Angriffsszenarien; Daten werden mehrfach an verschiedenen Orten auf heterogenen Systemen vorgehalten; Desaster und Data Recovery sind explizierte, personell gut besetzte Prozesse
Insgesamt vorgehaltene Datenmenge Die Menge der insgesamt von einem Dienstleister vorgehaltenen Daten verschiedener Kunden bestimmt zum Teil dessen Attraktivität für Angreifer	Hoch	Der Dienstleister hält viele Daten verschiedener Kunden vor	Der Dienstleister ist klein und hält nur wenige Daten insgesamt vor
Sensitivität der insgesamt vorgehaltenen Daten Die Sensitivität der insgesamt von einem Dienstleister vorgehaltenen Daten verschiedener Kunden bestimmt dessen Attraktivität für Angreifer	Sehr hoch	Der Dienstleister hält insgesamt ein breites Spektrum unterschiedlichster Daten für Kunden vor, von denen viele als sensibel und attraktiv erachtet werden müssen; der Dienstleister weiß nichts über die Sensitivität der Daten, die er vorhält	Der Dienstleister hält nur spezifisch zugeschnittene und uninteressante Daten vor
Sicherheitspolicy Das Vorhandensein einer guten Sicherheitspolicy ist Indikator eines Sicherheitsverständnisses und bestehender Sicherheitsprozesse	Hoch	Der Dienstleister unterhält keine Sicherheitspolicy und keine explizite Leitlinien	Der Dienstleister unterhält eine umfangreiche und systematische Sicherheitspolicy, die alle bekannten Bedrohungen und Risiken abdeckt; er hat konkrete Leitlinien aus der Policy entwickelt und unterzieht die Policy regelmäßigen Reviews

Implementierte Sicherheitsmaß-nahmen Art und Qualität der implementierten Sicherheitsmaßnahmen sind ebenfalls ein Indikator der Kompetenz und des Interesses an Sicherheit seitens des Dienstleisters	Hoch	Der Dienstleister hat keine spezifischen oder nur einige wenige Standardmaßnahmen implementiert; er hält sich nur an gesetzlich vorgeschriebene Mindeststandards	Der Dienstleister hat auf Basis eines individuellen Risikomodells als effektiv und effizient erwogene Sicherheitstechnologien im Stand der Technik implementiert; der Dienstleister demonstriert ein Interesse an Sicherheit durch Übertreffen vorgeschriebener Mindeststandards
Verifikation der Sicherheit Datenschutz- und Datensicherheitsmaßnahmen müssen unabhängig geprüft werden	Sehr hoch	Der Dienstleister lässt sich nicht unabhängig zu Datenschutz und Datensicherheit prüfen	Die Implementierung von Sicherheit ist dokumentiert und von unabhängigem Fachpersonal auf Korrektheit geprüft worden; auch die Vollständigkeit der Abdeckung ist geprüft und die Korrektheit der Konfigurationen aller Systeme im Bezug auf die Sicherheitstechnologien; Verifikationen werden regelmäßig wiederholt; Ergebnisse werden den Kunden ohne Details zugänglich gemacht; zusätzliche Sicherheitstests wie Penetation Testing werden extra angefordert
Transparenz bei Vorfällen Hat ein Dienstleister einen Sicherheitsvorfall besteht ein hoher Anreiz, diesen Vorfall zu verheimlichen, da Reputationsschäden zu	Sehr hoch	Der Dienstleister meldet keine Sicherheitsvorfälle und hat vorsorglich keine Maßnahmen zur Detektion von Vorfällen implementiert; bekannte Vorfälle	Der Dienstleister ist im Stand der Technik bemüht, über Detektionstechnologien Vorfälle zu erkennen; er meldet Vorfälle sofort an seine Kunden und an Behörden,

Kundenverlusten führen werden. Bei einer Verheimlichung von Vorfällen weiß der geschädigte Kunde allerdings nichts von seiner Schädigung und kann keine Gegenmaßnahmen einleiten		werden verheimlicht	sofern dies rechtlich notwendig ist; er klärt vollständig über die Vorfälle auf und bemüht sich auch über forensische Maßnahmen um ein Verständnis des Umfangs der Vorfälle
Garantien und Haftungen Dienstleister können Garantien aussprechen und so über Haftungen eine höhere Selbstverpflichtungen zu Sicherheit anbieten	Hoch	Der Dienstleister lehnt Haftungen so weit es geht ab und übernimmt keine Garantien für Datensicherheit und Datenschutz	Der Dienstleister bietet zahlreiche Garantien und deklariert sich als haftbar im hohen Maße für Vorfälle zu Datensicherheit und Datenschutz
Versicherungen Inzwischen gibt es verschiedene Cyber-Versicherungen, die digitalen Dienstleistern und damit auch deren Kunden eine höhere Absicherung ermöglichen	Hoch	Der Dienstleister lehnt Versicherungen ab	Der Dienstleister hat in hohem Umfang Versicherungen abgeschlossen, um Ansprüchen Dritter im Falle von Vorfällen genügen zu können
Datenschutz Dienstleister können unterschiedliche Verpflichtungen zum Datenschutz anerkennen	Hoch	Der Dienstleister übernimmt nur die gesetzlich vorgegebenen Datenschutzver-pflichtungen	Der Dienstleister bietet zusätzlich zu den gesetzlich vorgegeben Datenschutzverpflichtungen zusätzliche Maßnahmen und Optionen zu Privacy und Datenschutz an
Nationalität und Transnationalität Die Nationalität eines Unternehmens bestimmt dessen rechtliche Pflichten in Bezug auf Datenschutz und Datensicherheit	Sehr hoch	Der Dienstleister ist rechtlich in einem Land ohne besondere Anforderungen an Datenschutz und Datensicherheit verankert oder sogar in einem Land, das für Verletzungen von Datenschutz und Datensicherheit von staatlicher Seite bekannt ist	Der Dienstleister ist rechtlich in einem Land mit hohen rechtlichen Anforderungen an Datenschutz und Datensicherheit verankert; transnationale Verflechtungen sind klar expliziert und rechtlich von betroffenen Prozessen

			isoliert
Service und Support bei Sicherheitsvorfällen Wie schon bei Software können auch IT-Dienstleister Service und Support bei Vorfällen anbieten und damit Kunden helfen	Hoch	Es gibt keine entsprechenden Verfahren; der Dienstleister fühlt sich nicht zuständig und ist nicht ansprechbar für Sicherheitsprobleme	Der Dienstleister hat Verfahren und mit Menschen besetzte 24/7-Hotlines eingerichtet; Response und Recovery Verfahren existieren; es wird bei Vorfällen eng mit Kunden zusammengearbeitet; es gibt eine jederzeit verfügbare und erreichbare Abteilung als konstanten Ansprechpartner; bei schwerwiegenden Vorfällen können Experten geschickt werden
Struktur der Sicherheitsabteilung Erneut ist auch die Struktur der Sicherheitsabteilung des IT-Dienstleisters ein wichtiger Indikator für dessen Sicherheit	Sehr hoch	Es gibt keine oder nur eine kleine Abteilung (unter 1% der Angestellten); Sicherheit ist ein Feigenblatt und wird als PR-Maßnahmen verstanden; die Sicherheitsabteilung wurde erst vor Kurzem überhaupt gegründet; das Personal in der Sicherheitsabteilung erhält nur niedrige Gehälter und verfügt nur über unpassende und generische Expertise ohne explizite Sicherheitsausbildung oder Sicherheitserfahrung	Die Abteilung ist groß (10-20% der Angestellten) und alt (mindestens vier Jahre oder seit Bestehen), ist organisatorisch und operativ gut aufgestellt und unabhängig und hat hohe Zugriffsrechte im Unternehmen und in der Innovation; es gibt einen IT-Sicherheitszuständigen auf Board-Level als CIO oder CISO; die Ressourcen für Sicherheit betragen mindestens 15% des Entwicklungsbudgets; das Personal ist hochqualifiziert, spezialisiert, wird kontinuierlich weiter ausgebildet, ist gut vernetzt und beinhaltet heterogene Expertisen und Erfahrungen für

			spezifische Sicherheitsthemen der Herstellers

2.2.2 Anforderungen an IT-Sicherheitstechnologien

Wie eingangs erwähnt arbeiten sich die meisten Cybersicherheitslösungen in unsystematischen Ansätzen und vorrangig an Symptomen des Problems ab. In der Vergangenheit war dies ein wirtschaftlich gangbares Verfahren. Aufgrund der niedrigen Toleranz für Security-Ausgaben mussten die meisten Lösungen zu Cybersicherheit minimal invasiv und generisch sein, um mit möglichst geringen Kosten, aber universalen Ansätzen alle Probleme auf allen Plattformen lösen zu können. Dies war noch bis in die letzten Jahre hinein für viele der ausschließlich kleinen, mittelständischen IT-Sicherheitsfirmen eine wichtige Überlebensstrategie, um mit möglichst wenig und möglichst gezieltem Innovationsinvest möglichst breit zu verkaufen und so einen maximalen Return on Invest generieren zu können. Die Persistenz dieser Ansätze führte dann zu hoher Bekanntheit im Markt und zur Ausbildung als Paradigmen, die folgend auch die ebenfalls kleine Forschungsgemeinde ausgerichtet haben. Disruptive Lösungen, grundlegende Kritiken zu Verwundbarkeiten im IT-Markt und sichere Computer existierten und existieren daher nur in Randbereichen und sind nie in großem Maße industrialisiert worden.

Mit dieser vorherrschenden reaktiven Wendung an die äußere Topologie der Probleme sind die Cybersicherheitsprodukte auch aktuell noch wirtschaftlich passabel aufgestellt. Sie haben einen permanent ungesättigten Markt vor sich, der fortlaufend neue Lösungen benötigt. Parallel dazu besteht bei den Kunden dieser Ansätze die Hoffnung, dass viele inkrementelle Verbesserungen an diesen Technologien irgendwann auch einen hinreichenden Schutz herstellen werden.

Das könnte aber nur der Fall sein, wenn die Angriffsvarianten (eingeschlossen schmutzige Tricks und Seitenkanäle) alle bekannt und es nicht zu viele wären und wenn Angriffsvarianten immer schwerer und teurer werden, je mehr Angriffe „von unten nach oben“ unmöglich gemacht werden. So ließe sich das Katz-und-Maus-Spiel als Gewinnerstrategie modellieren.

Zumindest in der Theorie aber scheint das unwahrscheinlich. Die Anzahl der möglichen strukturellen Verwundbarkeiten ist durch hohe Code-Komplexität und schlecht gewählte Programmiersprachen noch auf lange Sicht sehr hoch, was eine große Vielfalt taktischer und technischer Angriffsverfahren ermöglicht. Auch operative Verwundbarkeiten wie Konfigurationsfehler sind in der Realität der Systeme kaum auszuräumen. Zudem wird zu jedem Zeitpunkt deutlich mehr Code produziert als geprüft, so dass die Anzahl von Verwundbarkeiten trotz verstärkter Bemühungen immer noch anwächst und nicht absinkt. Viele neue Technologien ermöglichen auch vollkommen neue Angriffsformen.

Auch die Hypothese, dass Angriffe schwerer und teurer werden lässt sich kaum erhärten. Modalitäten und Evolution der Wissensentwicklung und der Arbeits- und Kompetenzteilung in der Offensive sowie die immer noch fantastischen Return On Invests für Angreifer deuten eher auf das Gegenteil. Zudem sind Abstand und Asymmetrie im Rennen zwischen Katze und Maus sehr hoch. Ein Angreifer muss nur eine von hunderttausenden Schwachstellen finden, mit einer unbegrenzten Zahl von Gratisversuchen, um monatelang erfolgreich in einem System operieren zu können. Der Verteidiger dagegen muss ein sehr großes und sehr verwundbares System mit unsicheren Werkzeugen zu jeder Zeit ohne Ausnahme erfolgreich verteidigen. Die Bezeichnung als Katz-Und-Maus-Spiel ist in diesem Verhältnis eine eher irreführende Metapher.

Aufgrund der vielen Schwierigkeiten sind Effektivität und Effizienz von IT-Sicherheitstechnologien kritisch zu hinterfragen. In Abwesenheit entsprechender Testverfahren sollen in dieser Studie erneut externe Indikatoren zu einer oberflächlichen Abfrage der Qualität entwickelt werden. Dazu werden nun einige Sicherheitsmaßnahmen und Technologien besprochen, um danach auch für diese Variante von Technologie eine Indikatorenliste für deren Qualität anzugeben, die für einen Einkauf entsprechender Produkte vergleichend ermitteln und herangezogen werden kann.

2.2.2.1 Typen von IT-Sicherheitsmaßnahmen

Die folgenden Typen sind eine unvollständige Aufzählung einiger besonders gängiger Ansätze.

Sicherheitssensibilisierung
Ein wesentlicher Bestandteil in der Herstellung grundlegender Sicherheit ist die Sensibilisierung zu sicherem Verhalten mit Informationstechnik, da der menschliche Nutzer nach wie vor einer der einfachsten und effizientesten Angriffsvektoren ist. Fingierte Emails mit infizierten Attachments oder Links zu infizierten Webseiten sind nach wie vor sehr erfolgreiche Angriffsvektoren. Sensibilisierung betrifft so vor allem Aufmerksamkeit gegenüber Social Engineering, kann aber auch Aufmerksamkeit gegenüber abnormalem Systemverhalten oder Innentätern einschließen und stärker betriebsinterne Probleme wie eine hinreichende Sicherheitssensibilisierung der Geschäftsführung. Sensibilisierungen haben allerdings klare Grenzen. Insbesondere bessere Angreifer können sehr hochwertige Vertrauensverhältnisse herstellen (sog. Spear-Phishing) oder sogar vollständig darauf verzichten und auf stärker technischen Wegen angreifen.

Authentifizierung und Zugriffskontrollen durch Rechte und Rollen
Eine grundlegende Maßnahme der Sicherung eines Rechners besteht in der Authentifizierung seines legitimen Nutzers sowie verschiedener Prozesse zueinander. Dies wird zumeist durch Sicherheitsprotokolle festgelegt, wie das Needham-Schroeder Protokoll oder das Kerberos-Protokoll, die folgend Nutzer über eine Verbindung von Nutzernamen und Passwort authentifizieren. Weitere Faktoren der Identifikationen können hinzugefügt werden (sog. Multi-Factor-Authentication). In

einer dominanten Variante werden Authentifizierungen für Zugriffskontrollen genutzt. Diese Kontrollen sind grundlegend und systeminhärent vorbereitet und organisieren den Zugriff einzelner Nutzer als Personen, als Gruppenzugehörige oder in bestimmten Rollen auf Daten, Prozesse, Programme, Ports oder Ressourcen. Sie werden von den Administratoren eines Systems eingerichtet und meist über Passwörter realisiert, die vom Administrator in Tabellen im System hinterlegt und dort abgefragt werden können. Nachteile an diesem Ansatz sind, dass die Passwörter in der Regel nicht besonders hochwertig, meist generisch und einfach sind und dass sie oft leicht über Social Engineering, also über betrügerischen Aufbau einer Vertrauensbeziehung, von Nutzern direkt erhalten werden können. Außerdem bedingt der Umstand, dass diese Konzepte systeminhärent sind, dass sie auch in dem Maße verwundbar sind, in dem das Basissystem unter hoher Komplexität, kritischen Verwundbarkeiten oder schlechten und unvollständigen Konzeptionen der Rechte und Rollen leidet. Auch die Anforderungen sind zum Teil sehr hoch und insbesondere bei komplexen Systemen nur schwer vollständig und korrekt implementierbar und konfigurierbar. Operative Anforderungen an Nutzer und Prozesse sind teilweise zu hoch und zu zeitintensiv. Es gibt verschiedene konzeptionelle Single Points of Failure wie zB ein zentrales Key Management. Vor allem aber haben Angreifer für diese Standardmaßnahmen inzwischen viele Angriffe und Workarounds entwickelt, so dass die Relevanz selbst sauber implementierter Lösungen inzwischen deutlich reduziert ist. Sichere Identitäten bieten einen notwendigen Grundschutz an notwendigen Mechanismen, liefern aber keine umfängliche Sicherheit und dürfen folglich nur als Baustein einer Sicherheitsstrategie betrachtet werden.

Begrenzte Ausführungsumgebungen

Einige Systeme erlauben in sich oder durch Zusätze die Erstellung oder Emulation abgeschlossener kleiner „Systeme im System“. Beispiele sind Sandboxes und Virtualisierungen. Sind diese Teilsysteme gut abgegrenzt, können einige Angriffe, die darin ausgeführt werden, gar nicht erst funktionieren oder nur durch zusätzlichen Aufwand durch den Angreifer ausgeführt werden. Da diese Mechanismen allerdings bereits länger in Betrieb sind, haben Angreifer inzwischen einige Gegenlösungen entwickelt, mit deren Hilfe sie dann doch Verbindungen zu den interessanteren Zielsystemen herstellen können.

Verschlüsselung und Signaturen

Die Verschlüsselung von Daten wie durch ein Public Key Algorithmus wie GPG oder PGP oder durch stärker spezialisierte und proprietäre Lösungen macht ein Auslesen dieser Daten im verschlüsselten Zustand sehr schwierig. Eine Signatur erlaubt als Teilmechanismus einer Verschlüsselung eine eindeutige Zuschreibung eines Absenders, so dass den Nachrichten dieses Absenders stärker vertraut werden kann.
Allerdings ist die Verschlüsselung ebenfalls ein älterer Mechanismus und hat entsprechend viele Gegner, die kreative Lösungen entwickelt haben. Insbesondere bei Militärs, inzwischen aber auch bei Kriminellen ist die Disziplin des Codebreaking gut ausgebildet. Hat man folglich eine hohe oder sehr hohe Risikoexposition, muss man einen guten Codebreaker auf der Seite seiner potentiellen Gegner annehmen, was das Vertrauen in Verschlüsselung erschwert. Gute Codebreaker kennen viele Seitenkanäle, andere Angriffsvektoren, Methoden des Codeknackens und nicht selten finden oder fabrizieren sie Fehler in den Verschlüsselungsalgorithmen. Ein weiterer

Nachteil ist, dass es gegenwärtig nicht zufriedenstellend möglich ist, auf verschlüsselten Daten zu arbeiten. Verschlüsselte Daten müssen nach wie vor für den Gebrauch entschlüsselt werden. Zu diesem Zeitpunkt kann folglich auch ein Angreifer auf sie zugreifen, sofern er sich auf dem System befindet, auf dem die Daten entschlüsselt wurden. Schließlich ist Verschlüsselung leider nach wie vor schwierig zu implementieren und zu nutzen, besonders bei verschiedenen oder komplexen Systemen. Selbst Experten scheitern regelmäßig, wenn etwa unterschiedliche Plattformen genutzt werden. Folglich werden Verschlüsselungen oft schlicht vom Nutzer abgeschaltet oder umgangen. Dies senkt meist die Attraktivität dieser Maßnahme in der Verwendung in einem Unternehmen.

Detektion und Filter

Detektions- und Filtertechnologien wie durch Firewalls, Virenscanner und IDS-, IPS- oder – operativ erweitert – SIEM-Systeme realisiert haben verschiedene Nachteile. Einmal interagieren sie oft stark mit geschäftsrelevanten Prozessen und können diese verzögern oder verkomplizieren. Außerdem funktioniert Detektion in all diesen Technologien nur begrenzt. Bei Standardtechnologien wird eine unbekannte Zahl Angriffe nicht oder zu spät erkannt, da viele Möglichkeiten der Variation bestehen. Das Bundesamt für Sicherheit in der Informationstechnik etwa berichtet von 15-20 Angriffen auf Regierungsnetzwerke pro Tag, die durch Standardmaßnahmen aus diesem Feld nicht detektiert werden konnten.[15] Bei besseren Angriffen geht man inzwischen von einer Mean-Time-To-Detection von etwa 243 Tagen aus.[16] Auch der bessere konzeptionelle Ansatz, bestimmte Muster der Angriffsentwicklung im Ziel zu detektieren (oft als „0-Day-Detektion“ angepriesen) sind letztlich darauf angewiesen, dass die Angreifer sich an spezifische Rahmenbedingungen und Muster halten. Da (ausgehend von Turings Halteproblem[17]) aber eine unendliche Anzahl von Mustern möglich ist, basiert der Erfolg dieser Technologien letztlich auf der Präzision der Trendanalyse der Angriffsmethoden und der Linientreue der Angreifer innerhalb dieser Trends. Übergreifend gilt zudem, dass alle Detektionstechnologien besonders von besseren Angreifern im Rahmen der Offensiv-Defensiv-Evolution bislang immer schnell und zuverlässig ausgeschaltet oder umgangen wurden.

Diese Situation soll gegenwärtig durch viele verschiedene Maßnahmen des Information Sharing verbessert werden. Hier ist die Idee, dass Opfer von Cyberangriffe die technischen Informationen darüber teilen und zu Signaturen verarbeiten, die wiederum den Detektionstechnologien zur Verfügung gestellt werden, so dass Angriffe von Angreifern nicht länger mehrfach verwendet werden können. So sollen Netzwerke von potentiellen Opfern vor Wiederholungsangriffen geschützt werden, während gleichzeitig die Kosten für Angreifer nach oben getrieben

---

15 Siehe: BSI, Lagebericht 2014, online unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile&v=1

16 Siehe: BSI, BSI Magazin 2013/2014, online unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2013-14.pdf?__blob=publicationFile&v=1

17 Siehe: Sassaman. L., "The Halting Problems of Network Stack Insecurity.", usenix.org, online at: https://www.usenix.org/legacy/publications/login/2011-12/openpdfs/Sassaman.pdf

werden, um eine dauerhafte Abschreckung zu erzielen. Allerdings funktioniert dieser Mechanismus nicht effektiv. Es gibt nach wie vor viele erfolgreiche Angriffe, und es lässt sich keine Reduzierung der Zahl der Angreifer erkennen, nur ein stetiges Wachstum. Angreifern bleiben auch noch viele andere Optionen der Angriffsskalierung durch andere Taktiken. Der Ansatz funktioniert zudem nur bis in mittlere Risikogruppen. Hohe und sehr hohe Risikogruppen ziehen gezielte und hochwertige Angriffe an, die von Detektionssystemen wie skizziert nur schlecht und meist gar nicht erkannt werden, so dass also auch Information Sharing nicht funktionieren kann. Nur einige hochspezialisierte Entwicklungen liefern hier gegenwärtig geringe Leistungen, die meist auch nur so lange gut funktionieren, bis Angreifer sich dezidiert um die Entwicklung von Gegenlösungen bemühen. Für Detektionsansätze gilt folglich wie für die Authentifizierung, dass es sich um eine gegenwärtig noch notwendige Basismaßnahme handelt, die aber allein (oder auch in Kombination mit Zugriffskontrollen) nicht als ausreichend behandelt werden darf – vor allem, sobald die Risikoexposition als „hoch“ oder „sehr hoch“ einzustufen ist.

Redundanzen, Backups und Continuity

Eine weitere wichtige Maßnahme besteht in der Einrichtung von Redundanzen, Backups und der Erstellung eines Continuity-Konzepts für einen Parallelbetrieb bei einem Vorfall. Dabei ist es wichtig, darauf zu achten, dass die Redundanzen möglichst heterogen, also andersartig sind als die Originalkapazitäten, damit ein gefährlicher Angriff nicht einfach auch auf den Parallelbetrieb umgelenkt werden kann. Bei Backups ist es wichtig, dass diese gut gesichert und isoliert sowie immer aktuell gehalten werden. Das Continuity-Konzept sollte auf dem Risikomodell aufgebaut werden und insbesondere die verschiedenen Abhängigkeitsrelationen von Technik und Prozessen berücksichtigen.

Isolierungen und Entnetzung

Eine der derzeit wichtigsten Maßnahmen vor allem für hohe und sehr hohe Risikoexpositionen ist die Entnetzung, die Isolierung wichtiger Daten und Prozesse von größeren Netzwerken und insbesondere vom Internet. Mit einer effektiven Isolierung ist für einen Angreifer eine hohe Hürde realisiert. Er kann nicht mehr von jedem Ort der Welt aus nahezu risikofrei und repetitiv solange angreifen, bis er Erfolg hat. Er muss sich an den Ort begeben, eventuell einbrechen oder einen Innentäter anwerben, sich die Informationen über die Zielsysteme vorher besorgen, und er kann seine Angriffe nicht gut steuern, weil er keinen Feedbackkanal aufbauen kann. Solche Angriffe sind zwar immer noch möglich, aber nur in sehr wertvollen oder sehr großen Zielsystemen noch interessant und implementierbar. Der Nachteil dieser besten aller Sicherheitsmaßnahmen besteht im zumindest partiellen Verzicht auf die Vernetzung. Ein Unternehmen muss daher abwägen, wie mögliche Effizienzgewinne durch Vernetzung mit den möglichen Verlusten durch Sicherheitsprobleme zu verrechnen sind.

Penetrationstests

Sicherheit kann man testen. Ein solcher Test wird entweder durch Prüfung der Erfüllung verschiedener Implementierungsmerkmale erreicht oder durch einen Penetrationstest. Bei einem Penetrationstest greifen Auftragshacker das eigene System an und testen, wie lange sie brauchen und wie hoch der Aufwand ist, um in

ein System hinein zu kommen. Penetrationstests sind meist erfolgreich in dem Sinne, dass die Hacker Schwachstellen finden, durch die sie in die Systeme eindringen können und die später geschlossen werden können. Allerdings sind die Schwachstellen in der Regel noch so zahlreich, dass selbst mir großer Regelmäßigkeit durchgeführte Penetrationstests keinen sehr großen Sicherheitsgewinn liefern. Diese Tests dienen eher der Absicherung gegen spezifisch ausgeschnittene Angriffsmethoden sowie zur Sensibilisierung.

Forensik
Ein weiterer weit verbreiteter Ansatz ist die Forensik, also die digitale Spurensicherung. Forensik ist allerdings keine präventive Maßnahme mehr, sondern eine „ex post facto" Maßnahme, bei der ein Angriff bereits erfolgreich war und man nur daran interessiert ist, die Angriffsdetails und die Folgen besser zu verstehen oder daran, diese aus Compliance- oder Versicherungsgründen nachzuweisen.

Es gibt eine große Zahl weiterer Sicherheitsmechanismen, die nicht oder nicht einwandfrei in dieses Raster passen. Für einen ersten Überblick jedoch soll diese Klassifizierung genügen.

2.2.2.2 Indikatoren für die Qualität von IT-Sicherheitstechnologien

Schlechte IT-Sicherheit kann den Betrieb von IT nicht nur nicht absichern, sondern sie sogar zusätzlich gefährden. Dabei muss auch der Umstand berücksichtigt werden, dass Cybersicherheitslösungen ebenfalls Software, also auch selbst angreifbar sind. Dieser Punkt wird gern von der Cyberindustrie vergessen oder verharmlost, da diese Situation natürlich immer für alle Softwarevarianten gilt. Bei Cybersicherheitssoftware ist Angreifbarkeit aber im direkten Widerspruch mit der versprochenen Funktionalität, so dass sie in diesem Kontext als Sachmangel ausgelegt werden kann und zumindest eine deutliche Relativierung aller Sicherheitsversprechen erforderlich macht. ***Daher sollten auch alle oben im Abschnitt 2.2.1 genannten Indikatoren für Softwarequalität auf die Befragung von IT-Sicherheitstechnologie angewandt werden!*** Eine besonders „schlampige" Konfiguration und hohe Verwundbarkeit eines Sicherheitsprodukts ist ein hohes Risiko für den Kunden und für dessen Kunden und Partner und darf daher nicht als Bagatelle betrachtet werden. Ein in dieser Hinsicht eindrücklicher Fall hat sich erst vor kurzem mit der Firma FireEye ereignet.[18] Die Firma, ein globaler Marktführer und stark vertreten in vielen Konzernen, hatte über Jahre banale und seit 1997 eigentlich bekannte Konfigurationsfehler in ihren Apache-Servern und weitere einfache und vermeidbare Programmierfehler wie Buffer Overflows in ihrem Produktcode, so dass mit dem Produkt versorgte Firmen sogar in besonders hohem Maße angreifbar waren. Angreifer konnten (theoretisch – die Fehler wurden über einen deutschen Forscher, Felix Wilhelm, gefunden) über Zugriffe auf die Server ihre eigenen Angriffsmuster dort löschen, und sie konnten Kunden von FireEye mit spezifisch zugeschnittenen Emails angreifen, deren Angriffe von der FireEye-Software automatisch ausgeführt worden wären, ohne jede Notwendigkeit der Interaktion mit

[18] Siehe: Gaycken, S., „Leichte Beute für Hacker", Süddeutsche Zeitung vom 14.10.2015, online unter: http://www.sueddeutsche.de/politik/aussenansicht-leichte-beute-fuer-hacker-1.2691944

dem potentiellen Opfer. In diesem Fall wäre man also ohne die teure Lösung sogar besser dran gewesen.

Schlechte IT-Sicherheitsprodukte können aber auch andere Ärgernisse mit sich bringen. Sie können Störungen und Unterbrechungen verursachen, können schwer bis unmöglich zu implementieren, zu konfigurieren und zu bedienen sein und so selbst ihre Abschaltung oder harte Einschränkung nahelegen. Eine hohe Qualität ist daher aus verschiedenen Perspektiven wünschenswert.

Leider muss schließlich noch betont werden, dass bunte, futuristische Benutzeroberflächen, eine Herkunft aus dem Silicon Valley, eine lebendige Demonstration oder eine hohe Verbreitung am Markt explizit **keine** Merkmale für hohe Sicherheitsqualität sind. All diese Eckpunkte wurden etwa von FireEye erfüllt, während das Produkt selbst praktisch nur eingeschränkt überhaupt als Sicherheitsprodukt hätte bewertet werden dürfen.

Indikator	**Relevanz**	**Negative Ausprägung auf Sicherheit**	**Positive Ausprägung auf Sicherheit**
Sicherheitsqualität der Software Hier können und sollten die unter 2.2.1 erwähnten Merkmale vollständig abgeprüft werden	Sehr hoch	Angreifbare Securitysoftware kann nur geringe, aber keine solide Sicherheit schaffen, dafür aber Unsicherheiten vertiefen	Qualitativ hochwertig entwickelte, schwer angreifbare Securitysoftware kann ihre Sicherheitsversprech-en deutlich eher erfüllen
Betriebskomplexität des Sicherheitsmodells Der Betrieb einer Sicherheitslösung kann sich über viele verschiedene Systeme und Akteure erstrecken. So entsteht erneut Verwundbarkeit durch mögliche Fehler	Sehr hoch	Es gibt kein explizites Modell, aber viele Akteure in verteilten Sicherheitslösungen mit undeutlich vielen Möglichkeiten der Einrichtung	Es bestehen einfache Betriebsmodelle, transparent und verständlich, mit wenigen Akteuren in überschaubaren Implementierungen und kontrollierten Möglichkeiten der Einrichtung erhöhen Sicherheit
Zentralisierung des Sicherheitsmodells Sicherheit kann unter Umständen stark von zentralen Orten oder Techniken abhängen, die von Angreifern als Single Point of Failure angegriffen werden	Hoch	Sicherheitsfunktionen hängen stark von zentralisierten Punkten und Techniken ab, deren Ausfall einen Ausfall der Sicherheitsfunktio-nen zur Folge hat	Sicherheitsfunktionen agieren stark dezentral und sind von einem Ausfall einzelner Referenzpunkte nicht betroffen

können			
Bekanntheit der Implikationen der Sicherheitsfunktionen Sicherheitsfunktionen können in einem IT-System unterschiedliche Konsequenzen haben, die nicht unbedingt alle vorher abschätzbar sind	Mittel	Die Interaktionen zwischen System und Sicherheitsfunktionen wurden nicht typenartig entworfen und sind unbekannt und ungetestet	Das Zielsystem ist als Typ gut bekannt, viele mögliche Interaktionen sind entworfen und bekannt, Varianten sind getestet, Erfahrungen im realen Betrieb mit anderen Kunden wurden in Projektionen und Design umgesetzt und kommen anderen Kunden zugute
Konflikte mit normalen technischen Funktionen Sicherheitsfunktionen können in Konflikten mit normalen technischen Funktionen stehen, was oft zu ihrer Abschaltung oder Einschränkung führt	Sehr hoch	Sicherheitsfunktionen behindern normale technische Funktionen und erfordern teils harte Einschränkungen im Widerspruch mit dem technischen Normalbetrieb und Erwartungen an Kennzahlen	Sicherheitsfunktionen behindern normale technische Funktionen in keiner erkennbaren oder sich anderweitig auf Erwartungen ausprägenden Weise
Falschpositiv-Taktik des Herstellers Zu viele Fehlalarme einer Sicherheitstechnologie führen zum Verlust von Aufmerksamkeit und zu Unzufriedenheit mit dem Produkt, weshalb Hersteller dies gern vorher ausjustieren, was aber wieder Sicherheitslücken ermöglicht	Mittel	Der Hersteller möchte seine Kunden gar nicht mit möglichen Fehlalarmen konfrontieren und unternimmt eine grobe und nicht methodische Justierung der Falschpositive	Der Hersteller akzeptiert Falschpositive und hat Verfahren entwickelt, um selbst oder gemeinsam mit dem Kunden mit vielen Alarmen umzugehen. Jede Justierung der Falschpositive ist granular und methodisch reflektiert
Konflikte mit normalen Arbeitsprozessen Sicherheitsfunktionen können mit normalen Arbeitsprozessen der Angestellten konfligieren. Bei hoher	Sehr hoch	Die Sicherheitsfunktionalität schränkt normale Arbeitsprozesse stark ein und fordert dem Nutzer viele und komplizierte	Die Sicherheitsfunktionalität schränkt normale Arbeitsprozesse nicht ein und erfordert höchstens minimale und seltene Interaktionen mit dem Nutzer

Lästigkeit tendieren Nutzer und oft auch Betreiber selbst zur Umgehung von Sicherheit		Interaktionen ab	
Downtimes und Verzögerungen Sicherheitsfunktionen können Downtimes und Verzögerungen erfordern	Hoch	Prozesse wie Patching, Scannen, Filtern oder Verschlüsselung fordern zum Teil hohe Rechenlasten für den Betrieb, so dass der Real-Time-Betrieb eingeschränkt ist und verursachen größere Downtimes zur Implementierung und für Veränderungen/ Updates, so dass Sicherheitsfunktionen im Interesse des Betriebs abgestellt oder eingeschränkt werden	Das Sicherheitssystem ist vollständig Real-Time-kompatibel ohne Verlust von Funktionalität; Updates, Implementierung und Veränderungen können ohne Risiken eines Absturzes im laufenden Betrieb vorgenommen werden
Konflikte mit Datenschutz Sicherheitsfunktionen können im Konflikt mit Datenschutzanforderungen stehen und dann in ihrer Funktionalität nachhaltig stark begrenzt werden	Hoch	Sicherheitsfunktionen können nicht ausgeführt werden, ohne massive Datenschutzverletzungen nach sich zu ziehen, was zu starken operativen Selbstbeschränkungen führt	Sicherheitsfunktionen sind so gebaut, dass keine Zugriffe auf datenschutzsensible Daten notwendig sind, oder es existieren integrierte technische Datenschutzverfahren, die Datenschutz und Sicherheitsbetrieb optimal aufeinander abstimmen
Akteur mit der größten Sicherheitsverantwortung Sicherheit ist schwierig, weshalb eher Experten entsprechende Entscheidungen treffen sollten	Sehr hoch	Die Sicherheitsverantwortung ist umfangreich an der äußeren Systemperipherie am Einzelnutzer festgemacht, der leicht sicherheitskritische Fehlentscheidungen machen kann, die ein	Sicherheitsentscheidungen können nur von Entwicklern und Sicherheitsadministratoren im Rahmen ihrer Kenntnisse und Rechte getroffen werden; Laien und Endnutzer sind von Sicherheitsentscheidungen technisch isoliert

		Versagen des Sicherheitssystems nach sich ziehen	
Anforderungen an Sicherheitsverant-wortliche Sicherheitsverantwortl iche können pro Technologie unterschiedlich tief und breit qualifiziert sein müssen	Hoch	Die Anforderungen an den Sicherheitsverant-wortlichen sind sehr spezifisch, hoch und weitgehend unbekannt, wobei das System sensibel auf Fehlbedienungen reagiert	Die Anforderungen an den Sicherheitsverantwort-lichen sind sämtlich bekannt und expliziert orientieren sich an etablierten Ausbildungen und breit vorhandenen Fähigkeiten; Spezialwissen ist nicht notwendig
Nutzerkontrolle Eine Sicherheitstechnologie kann die Nutzer eines Systems beobachten und auf sicherheitssensibles Verhalten achten	Hoch	Nutzer können Sicherheit umgehen und abschalten und werden von der Sicherheitssoftware nicht automatisiert auf sicherheitsrelevan-tes Verhalten überprüft	Nutzer können Sicherheitsfunktionen nicht beeinflussen; das Sicherheitssystem erkennt sicherheitsrelevant Anomalien durch Nutzer und kann Innentäter erkennbar machen
Security Bedienungsdesign Bedienungen müssen effizient die richtigen Entscheidungen ermöglichen	Mittel	Bedienungsfunk-tionen und Interfaces sind wenig funktional aufgebaut und ermöglichen keine klaren und schnellen Prozesse des Erkennens, der Steuerung und der Konfiguration	Bedienungsfunktionen und Interfaces sind funktional nach klaren Funktionshierarchie-bäumen aufgebaut und ermächtigen den Nutzer zu vollständigen und zu maximal effizienten Prozessen des Erkennens, der Steuerung und der Konfiguration
Visualisierung Visualisierungen sollten nicht ablenkend sein, sondern funktional und selektiv	Mittel	Visualisierungen zeigen viele irrelevante Informationen in ablenkenden und anstrengenden Visualisierungen	Visualisierungen zeigen ansprechend und engagierend in aufmerksamkeitspsychol ogisch gestalteten Formen selektiv besonders relevante Informationen und langweilen oder überfordern die Operateure nicht
Bekannte Umgehungsoptionen	Hoch	Zu der Sicherheitstechno-	Zu der Sicherheitstechnologie

Einige Sicherheitstechnologien lassen sich leicht mit taktischen Methoden wie etwa dem Missbrauch einer Passwort-Wiederherstellungsfunktion umgehen		logie existieren bekannte Taktiken und Techniken der Umgehung, die nur schlecht abstellt oder effektiv isoliert werden können	existieren keine oder nur wenige und streng über weitere effektive Sicherheitsfaktoren kontrollierte Taktiken und Techniken der Umgehung
Zugangs- und Multilevel-Sicherheit der Sicherheitssoftware In Technologien oder Prozessen angelegte Optionen für eine Administration von Sicherheit müssen selbst sicher vor Betrug sein	Sehr hoch	Der Hersteller hat keine oder keine harten Konzepte der Multilevel-Sicherheit im Produkt; jeder mit Zugang zu dem Produkt kann Konfigurationen und Funktionen beeinflussen; es gibt bekannte Schwachstellen in der Multilevel-Sicherheit	Das Produkt hat harte Multilevel-Konzepte mit harten Mehrfaktor-Authentifizierungen und Identitätskonzepten sowie einem guten und sicheren Key Management, die solide und unumgehbar im Produkt verankert sind; es sind keine Schwachstellen der Multilevel-Sicherheit bekannt
Normales Kundenfeld und Erfahrungsgrad Kundenfelder nach Sektoren haben verschiedene Sicherheitsanforderungen und Einsatzbedingungen, in denen Hersteller unterschiedlich Erfahrungen sammeln können	Sehr hoch	Das Produkt wurde bislang nicht in dem Sektor genutzt, in dem es jetzt angeboten wird und kommt aus einem deutlich fremden, anderen Sektor; der Hersteller hat keine Berührung mit diesem Sektor gehabt und kennt die technischen und operativen Bedingungen des Sektors nicht	Das Produkt ist in dem Sektor des Kunden aufgewachsen; der Hersteller kennt diesen Sektor seit viele Jahren, hat alle technischen und operativen Einsatzbedingungen im Detail verstanden und hat Konzepte für dieses Anforderungen bereit
Verständnis und agile Beschreibung der Sicherheitsgegenstände (Assets) und Perimeter Die Sicherheitssoftware muss agil verstehen,	Sehr hoch	Der Hersteller kennt die Sicherheitsgegenstände und Perimeter seines Kunden nicht und kann diese auch prima facie nicht gut einschätzen; ein Verständnis muss	Der Hersteller kennt die Sicherheitsgegen-stände und Perimeter seines Kunden sehr gut technisch und wirtschaftlich sowie in Datentypen im Detail und kann gut weitere Ausdehnungen und

was genau die durch sie zu schützenden Gegenstände und Bereiche sind		mühsam erarbeitet werden und bleibt statisch	Probleme abschätzen; er kann agil neue Bedrohungen erfassen und deren Implikationen sofort auf die Sicherheits-gegenstände und Perimeter seines Kunden beziehen
Technischer Spezialisierungsgrad Stärker spezialisierte Sicherheitssoftware kann durch den Zuschnitt ausgewählte Sicherheitsfunktionen oft besser bedienen und hat vermutlich mehr Geld in Sicherheitsinnovation investiert	Sehr hoch	Die Sicherheitssoftware ist sehr generisch und nicht spezialisiert und will viele unterschiedliche Plattformen und Systemtypen gleichzeitig bedienen	Die Sicherheitssoftware ist für ihren technischen und operativen Einsatzbereich hochgradig spezialisiert und auf viele besondere Anforderungen dieses Bereichs optimiert
Systemisches Sicherheitsverständnis Hersteller und Sicherheitstechnik müssen kompetent beurteilen können, wie das insgesamt zu schützende System aussieht und welche Lücken vom eigenen Produkt nicht abgedeckt werden	Hoch	Der Hersteller und seine Technik konzipieren Sicherheit nur selektiv für die durch ihr Produkt abgedeckte Vektoren; andere Vektoren sind nicht bekannt oder werden verschwiegen; es lässt sich kein prozedurales oder systemisches Sicherheitsver-ständnis erkennen	Der Hersteller und seine Technik haben erkennbar ein prozedurales und systemisches Sicherheitsverständnis und kennen viele verschiedene Vektoren auf ganz unterschiedlichen Systemebenen; Vektoren, die nicht von seinem Produkt abgedeckt werden, werden nicht verschwiegen, sondern explizit thematisiert
Möglichkeit der Abdeckung der Security Policy Die vom Kunden formulierte Security Policy sollte mit dem Produkt abgedeckt werden können	Hoch	Die Anforderungen der Security Policy können nicht eindeutig in Spezifikationen abgebildet werden; Lücken sind wahrscheinlich, aber nicht erkennbar	Die Security Policy kann in Teilen oder vollständig eindeutig durch das Produkt realisiert werden; Lücken sind erkennbar und adressierbar; auch stärker spezifische Anforderungen können umgesetzt werden
Stand der Technik der	Sehr hoch	Die Sicherheitsfunktionen	Die Sicherheitsfunktionen

Sicherheitsfunktionalität Ein Produkt muss Aussagen zur Vollständigkeit der technischen Sicherheitsfunktionen gemäß normaler Funktionserwartungen pro Technologie am Stand der Technik machen können		lassen gemessen am Stand der Technik viele bekannte und etablierte Punkte offen oder adressieren diese nur oberflächlich	der Technologie entsprechen und erweitern technisch sinnvoll den Stand der Technik für die entsprechende Technologie
Systemtiefe der Sicherheitsfunktionalität Sicherheitsfunktionen, die tief in den Stack des System hineinreichen oder von unten nach oben gebaut sind, reduzieren Angriffsvektoren deutlicher	Sehr hoch	Die Sicherheitsfunktionen befinden sich nur oberflächlich im Stack auf Anwendungen	Die Sicherheitsfunktionen reichen tief in den Stack hinein, beinhalten ein sicheres Betriebssystem und sichere Hardware und sind nicht über Angriffe auf unteren Systemebenen auszuhebeln
Integration der Sicherheitsfunktionen ineinander Die verschiedenen Sicherheitsfunktionen eines Produkts oder einer Produktgruppe können unterschiedlich gut ineinander integriert werden	Sehr hoch	Die Sicherheitsfunktionen des Produkts sind separat voneinander entwickelt worden und laufen ohne Integration aber mit wechselseitig behindernden Interaktionen nebeneinander	Die Sicherheitsfunktionen des Produkts sind als holistisches Konzept in einem übergreifenden Entwicklungsansatz entwickelt worden und sind eng miteinander integriert, ergänzen sich funktional und behindern einander weder direkt über konfligierende Funktionen noch indirekt über hohe Belastungen o.ä.
Customizing von Sicherheitsfunktionen Sicherheitsfunktionen sollten sich an besondere Bedingungen anpassen lassen	Hoch	Die Sicherheitsfunktionen können in keiner Weise auf besondere Umgebungsbedingungen angepasst werden; Konzepte dafür sind nicht vorhanden; der	Die Sicherheitsfunktionen können und dürfen in hohem Maße auf besondere Umgebungsbedingungen angepasst werden; der Kunde darf Anpassungen selbst vornehmen; der

		Hersteller verbietet Anpassungen	Hersteller stellt Tools, offenen Code oder Serviceleistungen dafür zur Verfügung und bietet Verifikationen des Erhalts der Sicher-heitsfunktionalität bei Anpassungen an
Integration von Sicherheitsfunktionen anderer Hersteller Da die meisten Produkte nicht alle Sicherheitsfunktionen gleichzeitig anbieten, müssen oft verschiedene Produkte miteinander betrieben werden, die ineinander integriert werden müssen	Sehr hoch	Das Produkt lässt den Betrieb anderer Sicherheitspro-dukte nicht zu oder behindert diese in Implementierung und Betrieb	Das Produkt ist offen für einen parallelen oder direkt integrierten Betrieb anderer Sicherheitsprodukte; es bietet Schnittstellen und gemeinsame Integrationsverfahren und Services; „Known Issues“ der Integration sind bekannt, werden kommuniziert und man ist um Behebung bemüht
Konfigurationskomplexi-tät Die Komplexität der Konfiguration der Sicherheitsfunktion muss in Proportion zu Notwendigkeit und Kompetenz zur Komplexität gesehen werden	Sehr hoch	Das Produkt bietet unnötig viele Konfigurationsoptionen mit vielen unklaren und kaum beherrschbaren Wirkungen und Interaktionen im Produkt selbst und im System	Das Produkt bietet hinreichend viele Konfigurationsoptio-nen, um das Produkt gut an den Nutzungskontext anzupassen; die Optionen sind dem Kunden klar verständlich und für den Kunden gemäß dessen Fähigkeiten in Wirkungen und Interaktionen in Produkt und System jederzeit erkennbar und beherrschbar; es gibt Handreichen und Voreinstellungen zur sicheren Konfiguration
Grad der Basiskompatibilität Ein Sicherheitsprodukt kann unterschiedlich gut auf eine seine Zielplattform abgestimmt sein	Hoch	Das System wurde auf anderen Plattformen entwickelt und bringt nur eine rudimentäre Basiskompatibilität für die zu nutzende Plattform mit, bei der mit Lücken und Systemabstürzen zu	Das System wurde für die Zielplattform entwickelt und befindet sich dort bereits lange Zeit im Einsatz; der Hersteller war und ist stets bemüht, die Basiskompatibilität zu erhöhen und Fehler direkt zu bearbeiten

		rechnen ist	
Klassische Kennzahlen Einige referentielle Kennzahlen werden üblicherweise für das Ermessen der Qualität und Effizienz des Produkts verwendet, die möglichst unabhängig verglichen werden sollten	Hoch	Die Kennzahlen sind im unabhängig Vergleich in vielen Punkten deutlich schlechter als die vergleichbarer Produkte	Die Kennzahlen sind im unabhängigen Vergleich in der Breite deutlich besser als die vergleichbarer Produkte
Checks der Funktionalität Hersteller sollten die Funktionalität ihrer Technologie prüfen	Hoch	Der Hersteller unternimmt keine Prüfungen der Funktionalität des Produkts und reagiert aggressiv auf externe Prüfungen; nur positive Prüfergebnisse werden mitgeteilt	Die Funktionalität des Produkts wird regelmäßig und hart selbst und unabhängig extern geprüft; Prüfungen werden öffentlich sichtbar und zugänglich gemacht; schlechte Prüfergebnisse werden mitgeteilt und Ursachen dafür umgehend behoben
Abhängigkeit von Dienstleistungen Mit einem Produkt können explizit oder implizit Dienstleistungen verbunden sein	Hoch	Das Produkt bedingt dauerhaft und agil explizit wie implizit weitere, schlecht dauerhaft zu erhaltende, schlecht abgesicherte oder teure Dienstleistungen, deren Wegfall eine sofortige Degradierung des Sicherheitsstatus nach sich zieht	Das Produkt erfordert keine oder nur einige wenige explizite Dienstleistungen, die zudem gut erhältlich, qualitativ hochwertig, gut gesichert und preislich akzeptabel sind; ein zeitweiliger Ausfall der Dienstleistung bewirkt keine Degradierung des Sicherheitsstatus
Abhängigkeit von Dritten Ein Produkt kann von Dritten wie von Behörden oder anderen Firmen abhängig sein	Hoch	Das Produkt bezieht viele Informationen und Funktionsvoraussetzungen von unzuverlässigen Dritten und ist in seiner Effektivität stark von diesen Dritten abhängig	Das Produkt kann Impulse und Informationen von Dritten einbringen, ist aber in keiner Weise funktional oder operativ von diesen abhängig

Relevante rechtliche Zwänge in Herkunftsländern und Betriebsländern Rechtliche und geheimrechtliche Bedingungen können Sicherheitsunternehmen zu Kooperationen und zum Einbau von absichtlichen Fehlern oder anderen indirekten Hintertüren zwingen	Sehr hoch	Herkunfts- und Betriebsländer sind sicherheitspolitisch sehr aktiv oder „Supermächte“ mit starken Nachrichtendiensten und hoher Regulierungsge-walt; es existieren bereits für anderen Technologien Zugriffsregelungen; Hersteller sind wirtschaftlich stark von staatlichen Aufträgen abhängig; das Produkt oder die Dienstleistung öffnet Wege zu sensiblen Daten und Prozessen	Herkunfts- und Betriebsländer sind stark industriepolitisch und nur wenig sicherheitspolitisch aktiv, mit streng regulierten und eingehegten Nachrichtendiensten; Hersteller sind wirtschaftlich unabhängig von staatlichen Aufträgen
Logging und Auswertung von Incidents Wenn der Hersteller viel über Angriffe weiß, kann die Sicherheitsqualität verbessert werden	Sehr hoch	Für das Produkt relevante Angriffe aus Theorie oder Praxis werden nicht aufgezeichnet oder ausgewertet; es gibt keinen Austausch zu Angriffsvarianten; andere aktuelle Angriffsinformationen werden weitestgehend ignoriert	Relevante Angriffe aus Theorie oder Praxis werden angekauft, aufgezeichnet und ausgewertet, auch wenn sie in anderen Systemen stattgefunden haben; der Hersteller pflegt einen regen Austausch über Angriffe und deren Analyse und ist in entsprechenden Netzwerken vertreten; schwerwiegende aktuelle Vorfälle können sofort gesondert
Breite der Datenbasis relevanter Incidents Eine breite Kenntnis der Angriffsbasis ist eine breite Kenntnis der notwendigen Spezifikationen	Sehr hoch	Der Hersteller sammelt keine Daten zu relevanten Angriffen aus Praxis oder Theorie und kennt viele Vorfälle und Produktschwächen gar nicht	Der Hersteller hat eigenes Personal und eigene Prozesse zur Sammlung und methodischen Behandlung solcher Daten
Strategische Umsetzung von	Sehr hoch	Der Hersteller bezieht relevante Angriffe in	Relevante Angriffe werden laufend

Incidents Aus Angriffen müssen „Lessons Learned“ werden, vor allem für betroffene Produkte		der Regel nicht oder nur unter hohem externen Druck in seinen Innovationspro-zess ein	methodisch auf deren Innovationen und Innovationsmethodik analysiert; Ergebnisse werden direkt und zeitnah in konkrete neue Spezifikationen für das eigene Produkt übersetzt; unlösbare Probleme aus Vorfällen werden als Restrisiko offengelegt
Sicherheit der Datenwege zum Dienstleister Datenwege zu und von Sicherheitsdienstleiste rn sind sicherheitsfunktional und müssen sicher sein, um keine indirekte Manipulation der Sicherheitsfunktionalit ät zu ermöglichen	Sehr hoch	Die Datenwege unterliegen keinen besonderen oder nur schlechten, veralteten oder schlecht konfigurierten Sicherheitsmaßnahm en; die Sicherung der Datenwege ist kein explizierter und dauerhafter Arbeitspunkt	Die Datenwege sind am Stand der Technik hochwertig gesichert und Sicherheit ist korrekt implementiert; für die Sicherung steht laufend entsprechend ausgebildetes und hochwertiges Personal zur Verfügung, das nur dafür abgestellt ist
Sicherheit der Datenhaltung und der Protokolle beim Dienstleister Wenn ein Sicherheitsdienstleiste r selbst angreifbar ist, können seine Produkte keine Sicherheitsfunktionen nicht zuverlässig arbeiten	Sehr hoch	Daten und Protokolle des Dienstleisters sind nicht sicher; Vorfälle mit besonders einfachen und schlechten Problemen sind bekannt geworden; bei dem Dienstleister wurde eingebrochen	Daten und Protokolle des Dienstleisters sind am Stand der Technik abgesichert, besonders sensible Entwicklungsinfor-mationen befinden sich auf isolierten Rechnern; es gibt keine bekannten Vorfälle
Größe der Entwicklungsabteilu ng Eine große Entwicklungsabteilung kann mehr Innovation in das Produkt bringen	Hoch	Die Entwicklungsabtei-lung des Herstellers ist nur klein und hat verschiedene Aufgaben	Die Entwicklungsabteilung des Herstellers ist groß und hat spezialisierte Aufgaben
Hintergrund der Entwicklerbasis Eine Entwicklungsabteilung	Hoch	Die Entwicklerbasis ist kaum erfahren oder spezialisiert in den von ihr	Die Entwicklerbasis hat viele verschiedene Erfahrungen vorzuweisen, hat

muss einen spezialisierten Hintergrund mit engem Bezug und Erfahrung auf die betroffenen Technologien haben		bearbeiteten Bereichen und ist allgemein als recht einfach und generisch zu bewerten	teilweise hohe Spezialisierungen und besondere Ausbildungen und ist allgemein als sehr hochwertig anzusehen
Breite der Expertise der Entwicklerbasis Eine Entwicklerbasis muss eine breite Sicherheitskompetenz mitbringen, um systemische Schwächen und Lücken verstehen zu können	Hoch	Die Entwickler der Herstellers haben nur allgemeine, fragmentarische oder produktferne Kompetenzen und wissen im Allgemeinen nicht viel über konkrete oder konzeptionelle Schwächen und Lücken des eigenen Produkts	Die Entwickler des Herstellers verstehen alle anzuwendenden Sicherheitsprobleme im Bezug auf das Produkt und kennen alle damit zusammenhängenden Lösungsansätze; auch neue Lösungsansätze sind über Netzwerke direkt zugänglich; die Entwickler sind in der Lage, neue Probleme oder Lösungen zu verstehen und umzusetzen
Innere Sicherheit der Entwicklung Große und wichtige Sicherheitsunternehmen können von Kriminellen und Nachrichtendiensten unterwandert werden	Hoch	Das Unternehmen hat keine umfangreichen und trennscharfen Konzepte für innere Sicherheit	Das Unternehmen hat umfängliche innere Sicherheitsmaßnah-men eingeschlossen hohe physische Sicherheiten, Air Gaps für kritische Entwicklungsabteilungen und Sicherheitsüberprü-fungen für Entwickler
Bedrohungsmodell taktisch Ein gutes und stetig agil verbessertes taktisches Bedrohungsmodell gibt die Rahmenbedingungen für Spezifikationen vor	Hoch	Der Hersteller verfügt über kein Verständnis taktischer Bedrohungen und entwickelt keine Bedrohungsmodelle als Prämissen der Entwicklung	Der Hersteller setzt sich bereits länger und mit eigenem Personal mit der Analyse taktischer Bedrohungen auseinander und kann diese für sein Kundenfeld gut theoretisch durchmodellieren; Bedrohungsmodelle bilden die Ausgangsbasis jeder Entwicklung
Bedrohungsmodell technisch Ein gutes und stetig agil verbessertes	Hoch	Der Hersteller informiert sich nur über Schadensmel-dungen ohne Analyse	Der Hersteller setzt sich bereits länger und mit eigenem Personal mit der Analyse technischer

technisches Bedrohungsmodell gibt die exakten Detailspezifikationen vor		und ohne ein systemisches und systematisches Verständnis technischer Bedrohungen; er entwickelt keine Bedrohungsmo-delle als Prämissen der Entwicklung	Bedrohungen auseinander und kann diese für sein Kundenfeld auch in besonderen technischen Umgebungen detailreich und gut theoretisch durchmodellieren; Bedrohungsmodelle bilden die Ausgangsbasis jeder Entwicklung
Expliziter Einbezug von Evolution Die Evolution von Angreifern wird nur selten von Sicherheitsprodukten berücksichtigt und technisch agil ermöglicht	Mittel	Der Hersteller entwickelt Produkte nur anhand konkreter technischer Problemspezifi-kationen aus der Vergangenheit	Der Hersteller analysiert Probleme aus der Vergangenheit auf Fähigkeiten und Geschwindigkeiten der Angreifer zur Offensivinnovation, projiziert daraus deren zukünftige Angriffe in technischen Spezifikationen und entwickelt gegen diese Spezifikationen zukunftsgewandte Produkte
Modellbasierte Entwicklung Entwicklung kann auf theoretisch entwickelten Modellen und Methodologien stattfinden und damit eine deutlich bessere Abdeckung und Effizienz herstellen	Hoch	Der Hersteller unternimmt keine modellbasierte Entwicklung	Der Hersteller kennt modellbasierte Entwicklung und hat eine in ihrer Methodologie etablierte und für seine Zwecke angepasste Variante im Rückgrat seines Entwicklungspro-zesses
Servicemodelle Hersteller können unterschiedliche serviceorientiert sein, um Fehlfunktionen oder Angriffe mit dem Kunden zu bearbeiten	Hoch	Der Hersteller bietet keine oder nur automatisierte und schlecht verfügbare Serviceleistungen	Der Hersteller bietet viele Serviceleistungen, hat jederzeit kompetente menschliche Ansprechpartner dafür bereit und kann auch ungewöhnliche Anfragen bearbeiten
Technische und operative Continuity- und Recovery-Konzepte	Hoch	Der Hersteller hat einen Ausfall seines Produkts nicht antizipiert oder	Der Hersteller hat vollständig durchdachte und erprobte Prozesse der Continuity und

Hersteller können für den Ausfall ihrer Sicherheitsprodukte Continuity- und Recovery-Prozesse entwickeln und anbieten		konzeptionell externalisiert und bietet entsprechend keine Prozesse an	Recovery in Tools und Services für den Ausfall seiner Sicherheitsprodukte, vielleicht sogar in Zusammenarbeit mit einem Konkurrenten
Patching und Updates Schlechte Verfahren für Patching und Updates produzieren hohe Risiken in Sicherheitsprodukten	Sehr hoch	Der Hersteller patcht eigene Lücken nicht, kaum oder unregelmäßig; Patching und Updates sind nicht an Sicherheitsgefah-ren, sondern an Geschäftsprozessen orientiert; Verfahren zu Patching und Updates sind komplex, schlecht verfügbar und können zu technischen Problemen führen	Der Hersteller patcht eigene Lücken sofort; Patching und Updates sind in Geschwindigkeit, Verfügbarkeit und Qualität streng an Sicherheitsgefahren orientiert; Kommunikation und Geschäftsprozesse sind untergeordnet; Patches und Updates sind jederzeit gut geschrieben und schnell und problemlos implementierbar
Optionen für Security-by-Design und Security-by-Default Sicherheit kann eng in Basis-IT-Systeme integriert werden und damit deutlich bessere Sicherheitsfunktionen ermöglichen	Hoch	Der Hersteller verfolgt ein reines ad hoc Konzept mit seinen Produkten	Der Hersteller arbeitet mit IT-Herstellern zusammen, um seine Sicherheitsfunktionen tief und struktural in Basis-IT-Systeme einzubringen, in denen sie zudem mit hochsicheren Grundeinstellungen eingebaut werden
Störungsanfälligkeit Einige Varianten von Sicherheitstechnologie n können leicht gestört werden	Sehr hoch	Das Produkt ist bekanntermaßen einfach zu stören; Störungen lassen sich kaum erkennen oder abschalten	Das Produkt ist unabhängig von einfachen Störoptionen oder Störungen erfordern einen hohen Angriffsaufwand und sind leicht erkennbar und abschaltbar
Implizite Incident Toleranz Hersteller können von ihren Kunden ganz unterschiedliche	Sehr hoch	Der Hersteller empfindet es als normal, „keine 100%ige Sicherheit“ sondern nur	Der Hersteller bemüht sich um eine exakte Abgrenzung seiner Sicherheitsfunktionalität und um ein so vollständig

Toleranzen für Art und Schwere von Vorfällen anfordern		ungefähre und unbestimmte Sicherheit liefern zu können und erwartet von seinen Kunden eine hohe Toleranz für Produktschwächen und -lücken und Vorfälle	wie mögliches Abweisen von Vorfällen; er entwickelt und arbeitet gemäß der Perspektive, von seinen Kunden kaum eine oder nur eine geringe Toleranz für Schwächen und Lücken erwarten zu dürfen
Garantien und Gewährleistung Hersteller können für bestimmte Basisbedingungen und Funktionen Garantien und Gewährleistung bieten	Sehr hoch	Der Hersteller übernimmt explizit keinerlei Garantien und Gewährleistungen und betreibt Aufwand, um sich rechtlich möglichst weit entziehen zu können	Der Hersteller übernimmt Garantien und Gewährleistungen für definierte Sicherheitsfunktionen, deren Qualität, Effektivität und Effizienz und stellt sich rechtlich den Konsequenzen
Umgebungskontrolle Sicherheitssoftware sollte es merken, wenn die Umgebung sich in signifikanter Weise ändert und sollte sich anpassen können	Sehr hoch	Die Sicherheitssoftware bemüht sich jenseits der Basiskonfiguratio-nen kaum um ein Erkennen der Umgebung und ist leicht davon gestört	Die Sicherheitssoftware erkennt viele Veränderungen der Umgebung, macht darauf aufmerksam und kann sich zum Teil selbst in sicherer Weise darauf anpassen
Co-Evolution mit Plattformen Plattformen, auf denen Sicherheitssoftware läuft, verändern sich häufig und schnell, womit Funktionslücken und Sicherheitslücken in den Sicherheitsprodukten entstehen können	Sehr hoch	Das Produkt wird nicht, kaum oder nur langsam und oberflächlich auf Veränderungen in den Plattformen angepasst; es gibt keine etablierten Prozesse mit den Plattformher-stellern	Das Produkt reagiert vorgreifend und vollständig auf Plattformverände-rungen und kann jede Plattformveränderung fehlerfrei begleiten; dafür existieren etablierte Austauschdialoge mit den Plattformherstellern
Innovationsinvesti-tionsverhältnisse zwischen Plattformenbreite (Anzahl der bedien-ten Plattformen), Basiskompatibilität,	Hoch	Innovationsinvest in Plattformenbreite ist hoch, während andere Investionen niedrig und ereignisgetrieben sind	Innovationsinvest in Basiskompatibilität, Tiefe, Qualität, sichere Entwicklung ist sehr hoch und konstant im Verhältnis zu Investi-tionen in die Breite

Breite der Sicherheitsfunktionalität, Tiefe der Sicherheitsfunktionalität, Qualität der Sicherheitsfunktionalität, sichere Entwicklung Die Verhältnisse verschiedener Investitionen zueinander sind bedingt aussagekräftig über die Schwerpunkte des Herstellers und des Produkts			
Zertifizierungen und Anerkennungen Einige Zertifizierungen wie Common Criteria, ISO 27001 und ITSEC liefern grundlegenden Indikatoren, ob bei der Entwicklung einer Software auf den Einbau inhärenter Sicherheit geachtet wurde. Leider beschränken sich die Indikatoren auf klassische ad hoc Sicherheitsmerkmale wie etwa Rechte und Rollen, die in der gegenwärtigen Sicherheitslandschaft nicht mehr als hinreichend erachtet werden können, so dass die Relevanz für die Vermessung der Basisverwundbarkeit nicht hoch ist	Mittel	Sind keinerlei Zertifizierungen oder Anerkennungen vorhanden, können hierüber keine Indikatoren für die Verwundbarkeit des Produkts abgelesen werden	Sind Zertifizierungen und Anerkennungen vorhanden, so geben diese zumindest einen Indikator für die Korrektheit einiger grundlegender Sicherheitsmechanismen und für ein Sicherheitsinteresse und –bemühen des Herstellers

2.2.3 Anforderungen an Fähigkeiten eines IT-Sicherheitszuständigen

Ebenfalls wichtig ist es, die eigenen Fähigkeiten zu Einkauf, Implementierung und Bedienung einer Sicherheitstechnologie gut abzuschätzen und einzuplanen. Ist das eigene IT-Personal nicht in der Lage, eine zwar in der Leistung bessere, aber in Implementierung und Betrieb anspruchsvolle Technologie zu bedienen, kann die Sicherheitswirkung dieser Technologie nicht garantiert werden und eine bedienbare Variante ist möglicherweise eine bessere Wahl. Unternehmen mit mittlerer oder hoher bis sehr hoher Risikoexposition müssen sich allerdings darüber im Klaren sein, dass eine zu einfache und zu stark automatisierte Lösung nicht auf Feinheiten im Schutzbedarf eingehen kann. In diesen Fällen muss eine bessere Sicherheitsqualifizierung stattfinden.

Ab einer gewissen Unternehmensgröße und einer mittleren Risikoexposition sollten auch kleine und mittlere Unternehmen einen IT-Sicherheitszuständigen einrichten, der zumindest einen Teil seiner Arbeitszeit mit IT-Sicherheit verbringt. Infolge der hohen Komplexität der IT-Sicherheit selbst sind allerdings viele unterschiedliche Expertisen dafür auszubilden. Je nach verwendetem Sicherheitsmechanismus müssen unterschiedliche Fähigkeiten nachgewiesen werden. Die folgende Tabelle gibt einen Überblick.

Sicherheitsmechanismus	**Fähigkeiten**
Übergreifend notwendige Kenntnisse	Asset Analyse und Asset Management; Netzwerktopologie; Change Management; IT-Inventuren; Change Operations; Sichere Konfiguration; Updating und Patching; Abnormales Systemverhalten; Indicators of Compromise; Incident Handling; Alerting und Reporting; Crisis Management; IT-Security Management
Sicherheitssensibilisierung	Aufstellen von Guidelines; Durchführung von Awareness-Veranstaltungen im Unternehmen; Verständnis und Kommunikation von Risiken
Authentifizierung und Zugriffskontrollen	Sehr gute Systemkenntnis; Kenntnis der Bedeutung aller Rollen und Rechte; Kenntnis der Konsequenzen aller dazugehörigen Geschäftsprozesse; Kenntnis typischer Sicherheitsschwächen des Systems; Formulierung einer Policy; Erzwingen einer guten Passwortkultur; gutes Passwortmanagement; Key Management; Implementierung eines Schutzes vor Memory Overwriting und User Interface Failures
Begrenzte Ausführungsumgebungen	Sichere Herstellung von Sandboxes und sicherer Nutzung von VMs; sichere Isolierung verschiedener VMs
Verschlüsselung und Signaturen	Kenntnis der Kommunikationswege;

	Kenntnis der Daten-Assets; Verschlüsselungsmechanismen; Public Key Encryption; Signaturen; Verschlüsselungszertifikate; Key Management
Detektions- und Filtersysteme	Malware Patterns; sog. APT-Detektion/ 0-Day-Detektion; Datenschutz; Information Sharing; Knowledge Base Management; Threat Intelligence; Alerts und Reporting; Logs und Log Analyse;
Redundanzen, Backups und Continuity	Backup; Restoring; Recovery; Business Continuity; Konfigurationsmanagement
Isolierungen und Entnetzung	CBR-Analysen Isolierung; weiche und harte Isolierung und Entnetzung; Wechselmedien-Handhabung
Penetrationstests	Test Konzeption; Schwachstellenanalyse; White Box Testing; Black Box Testing nach NIST SP 00-115; OWASP; Reporting
Forensik	Netzwerkforensik; Datenschutz; mobile Forensik; Logs und Log Analyse; Malware-Analyse in Sandboxes; Daten-Wiederherstellung; Beweissicherung; Intrusion Analysis

Viele Technologien erfordern noch gesonderte und herstellerspezifische Schulungen. Bei Betrieb eigener Sicherheitsabteilungen oder eines SIEM kommen zudem Anforderungen des technischen, organisatorischen und operativen Sicherheitsmanagements hinzu. Auch Führungspersonen müssen fachgerecht ausgebildet sein, um kompetent entscheiden zu können.

3. Sicherheitsverbessernde Empfehlungen der Autoren

Einige der in den vorangegangenen Teilen erwähnten Desiderate sind gegenwärtig schwer zu erfüllen. Viele KMUs etwa sind nicht in der Lage, ausreichend qualifiziertes Personal anzustellen oder qualitativ hochwertige Weiterbildungsangebote zu identifizieren. Die genaue und vergleichende Prüfung von Verwundbarkeiten in der Basis-IT oder von Effektivität und Effizienz der IT-Sicherheitstechnik benötigt Verfahren und Institutionen, die gegenwärtig nicht in unmittelbar brauchbarer Form vorliegen. Zudem sind kaum Verfahren implementiert, mit denen „Sicherheitsverweigerer" in der IT im Sinne einer grundlegenden Gewährleistung belangt werden können. So ergeben sich aus der Studie eine Reihe möglicher Empfehlungen zur Verbesserung der IT-Sicherheit in kleinen und mittleren Unternehmen.

Forschung zu Prüfungsverfahren fördern
Verwundbarkeit und Sicherheit müssen in Gänze messbar gemacht werden, um kompetente Sicherheitsentscheidungen treffen zu können und um Marktmechanismen einsetzen zu lassen. Gegenwärtige Verfahren sind dafür unzureichend. Neue Ansätze und Methodologien müssen entwickelt werden.

Unabhängige Prüfungen von Verwundbarkeiten, Effektivität und Effizienz ermöglichen
Verwundbarkeiten in Basis-IT und Sicherheits-IT sowie Effektivität und Effizienz von Sicherheits-IT müssen öfter, stärker und öffentlicher vergleichend geprüft werden. Prüfungen müssen unabhängig stattfinden. Es dürfen keine direkten oder indirekten „Selbst-Abnahmen" der IT-Hersteller stattfinden. Unabhängige und kritische Instanzen müssen aufgebaut und gefördert werden. Desinteresse an Sicherheit seitens der Hersteller und Dienstleister muss sichtbar werden, um Marktmechanismen einsetzen zu lassen. Harte und dauerhafte Sicherheitsversager müssen gesetzlich belangbar gemacht werden. Eine harte und zu echten Sicherheitsinvestitionen anreizende Regulierung darf auch nicht mit Ausrichtung auf den „Comfort Space" und die Möglichkeiten der IT-Industrie, sondern muss mit dem Blick auf die realen Risiken formuliert werden.

Offenlegungspflichten definieren
Hersteller und Dienstleister der IT und der IT-Sicherheit müssen verpflichtet werden, Sicherheitslücken und konzeptionelle Schwächen gegenüber Kunden offenzulegen. Insbesondere im Kontext von Einkauf und Angebotsstellungen sollten verpflichtend Hinweise auf bekannte Probleme und Vorfälle gegeben werden, um Einkäufern einen Eindruck der Risikoexposition zu vermitteln. Offenlegungen akuter Lücken und Schwächen müssen schnell und verantwortlich unternommen werden, um den Kunden selbst Möglichkeiten

der Absicherung zu geben und eigene Risikoentscheidungen zu ermöglichen. Verschweigen darf nicht als verantwortliches Verhalten gewertet werden.

Unabhängigkeit in Richtungsgremien herstellen
Richtungsweisende Gremien sind oft direkt oder indirekt durch die IT-Industrie besetzt. Sofern eine Regulierung aber nicht hersteller- sondern anwenderorientiert stattfinden soll, muss härtere Unabhängigkeit hergestellt werden. Experten in direkten oder indirekten Interessenskonflikten oder unter laufenden NDAs mit IT-Firmen dürfen nicht in entsprechende Gremien gesetzt werden.

Aus konkreten Vorfällen systemische Lektionen ziehen
Wiederholt auftretende Sicherheitsprobleme, Lücken, Schwächen oder Kritikpunkte sind in der Regel Indikatoren für tiefergehende und kontinuierlich Sicherheitsprobleme verursachende Missstände. Vorfälle müssen auf systemische Ursachen geprüft werden. Unlösbare systemische Ursachen müssen als persistente Sicherheitsrisiken kenntlich gemacht werden.

Kompetenzqualität BSI ausbauen
Das BSI muss härter in der kritischen Bewertung von verwundbarer IT und schlechter IT-Sicherheitsprodukte werden. Allein eine Ausschreibung von Mindeststandards ist eine zu niedrige und wenig nachhaltige und effiziente Maßnahme.

Selbstverpflichtungen der IT-Industrie anregen
Verfahren könnten entwickelt werden, mit deren Hilfe die IT-Industrie eine kompetitive Selbstverpflichtung zu besserer Sicherheitsqualität eingehen könnte.

Passive Informationsangebote gesetzlich aktiv umgestalten
Threat Infos oder relevante Verwundbarkeiten müssen von Herstellern nicht nur gelesen, sondern gesetzlich verpflichtend bearbeitet werden. Beim BSI muss erfasst, vorgehalten und nachgeprüft werden, welche Informationen für welches Produkt und Sicherheitsprodukt in welcher Weise relevant sind und wie schnell und effektiv die Probleme behoben werden. Informationen darüber sind öffentlich zu machen, um den Markt besser zu steuern.

Sicherheitszyklen gesetzlich verbessern
Typische Sicherheitsmechanismen und Zyklen wie das eigene Testen und Auffinden von Schwachstellen, das Belohnen der fremden Meldung von Schwachstellen (sog. Bug Bountys), das Patching und sicherheitsfunktionale Updates können an vielen Stellen noch deutlich beschleunigt und verbessert werden. Viele IT-Unternehmen weigern sich immer noch, selbst intensiv zu testen, fremde Meldungen angemessen zu entlohnen oder auch nur anzunehmen oder ihr Patch- und Update-Prozesse auf das beste Maß zu beschleunigen und zu professionalisieren. Mit diesen einfachen und bekannten Maßnahmen können jedoch viele einfache Sicherheitsprobleme effektiv

behoben und Risiken verringert werden. Best Practice bei in dieser Hinsicht führenden Unternehmen sollte gesetzlich zum Normalfall gemacht werden.

Schlechte Eigen-Sicherheit in Sicherheitsprodukten als Sachmangel deklarieren
In letzter Zeit sind wiederholt Fälle bekannt geworden, in den IT-Sicherheitsprodukte selbst gravierende und vermeidbare Sicherheitsmängel hatten. Eine selbst angreifbare Sicherheitssoftware hat keine Schutzwirkung mehr, sondern vertieft Unsicherheit. Unsichere Sicherheitssoftware stellt einen Sachmangel dar. Der Markt sollte zu besserer Qualität angeleitet werden.

Ausbildungsangebote verbreitern und vertiefen
Ausbildungsangebote für Cybersecurity müssen verbreitert und vertieft werden. Die oben erwähnten Kompetenzen müssen zumindest grundlegend für jeden IT-Administrator zugänglich und erlernbar gemacht werden. Bei besonderem Bedarf muss Ausbildung auch in die erforderliche Tiefe gehen können. Für neue Anwendungsfelder wie den Bereich Embedded- und Industrial-IT müssen neue Sicherheitskompetenzen entwickelt und verfügbar gemacht werden. Ausbildungsangebote sollten umsonst oder kostengünstig gestaltet werden.

Mehr IT-Sicherheit im Studium
IT-Sicherheit ist an Universitäten immer noch unterrepräsentiert. Es existieren kaum Lehrstühle, was sowohl Forschung wie auch Lehre nachdrücklich behindert und einschränkt, obwohl erkennbar deutlich mehr Experten in diesem Feld generiert werden müssen. Auch für IT-Sicherheits-Mittelbau müssen dringend mehr Gelder freigemacht werden.

Mehr „Sichere IT“ im Studium
Viele Informatikstudenten lernen im Studium nichts über Sicherheitsstandards oder über sicheres Programmieren. Software Security Quality, High Assurance Programming und Methoden des Trustworthy Computing sollten dringend als Pflichtkurse in das Informatikstudium aufgenommen werden.

Expertise messbar machen
Expertise muss messbar werden. Die beste Expertise entsteht immer noch durch hohe Problemexposition und Systemerfahrung. Standardisierte Fragebögen und Prüfverfahren sollten generiert und laufend aktualisiert betrieben werden, um Expertisen bei Einstellungen besser einschätzen zu können.

Kritische Informationen einfacher zugänglich machen
Sicherheitskritische Informationen werden immer noch zu stark als „Staatsgeheimnisse“ behandelt. Ohne klare Risikoinformationen kann jedoch keine effektive Sicherheitssensibilisierung und kann kein informiertes Risikomanagement stattfinden. Staat und Wirtschaft sollte Verfahren

entwickeln und Institutionen aufbauen, die sicherheitskritische Geheiminformationen aufarbeiten und bereinigen und zugänglich machen kann („Trusted Third Party"-Ansatz).

Sicherheit stärker verständlich machen
IT-Sicherheit muss in Risiko und Lösungsansätzen deutlich besser verständlich gemacht werden. Aufklärungsarbeit darf sich nicht nur auf Schlaglichter in der Presse begrenzen, sondern muss an verschiedenen Stellen heuristisch sortiert und pädagogisch aufgearbeitet an die betroffenen Parteien gebracht werden. Informationsmaterial und regelmäßige unabhängige Informationsmechanismen sollten entwickelt vertrieben werden

Cybersicherheit als Managementaufgabe definieren
Das Management trifft zu Cybersicherheit gegenwärtig noch ungern Entscheidungen, da zu viele Unsicherheiten bestehen und da unter Umständen hohe Kosten zu erwarten sind. Hier müssen einerseits Möglichkeiten des Bewertens von Cybersicherheit auf Managementebene hergestellt werden, durch gezielte Managementausbildung sowie durch entsprechende Entscheidungshilfen. Andererseits muss eine klare Verantwortlichkeit für Sicherheit im oberen Management angesiedelt werden. Nur von dort aus kann effektiv durch eine größere IT-Landschaft in Beschaffung, Betrieb und Innovation durchreguliert werden.

Sicherheit einfacher nutzbar machen
IT-Sicherheitstechniken müssen dringend verständlicher und nutzbarer werden für Laien. Dabei ist der Konflikt zu bewältigen, dass durch die höhere Nutzbarkeit durch Automatisierung Sicherheitsverluste durch Fehleinstellungen entstehen können. Für die Bewältigung dieser Verluste im Rahmen eines Paradigmas „Functional Usability" können Modelle aus erfolgreichen Fällen wie TOR entwickelt werden. Diese Entwicklung muss als Forschungsaufgabe definiert und in der Forschung gefördert werden.

Hochsicherheits-IT fördern
Die beste Sicherheit liefern Computer, die gar nicht erst angegriffen werden können. Forschung und Entwicklung in diesem Bereich könnte Deutschland nicht nur absichern, sondern auch wieder zu einem Marktführer in der IT werden lassen – vor allem für den neuen Bereich der Embedded und Industrial IT. Hier müssten mehr Anreize für Investoren und Großkonzerne geschaffen werden, um in disruptive Innovationen zu investieren. Eine staatliche Absicherung eines Teils der Risikoinvestitionen würde Anreize deutlich verstärken und mehr hochwertige Technologie generieren.

Passgenaue Werkzeuge ermöglichen
KMUs benötigen für viele ihrer Sicherheitsbedarfe eigene Technik und verfügbare Ansprechpartner. Ein Prozess sollte aufgesetzt werden, in dem KMUs ihre Bedarfe genau prüfen, diese formulieren und an die IT-Sicherheitsindustrie kommunizieren können.

Werkzeuge zur Selbstprüfung von Sicherheitslücken fördern und begrenzt legalisieren

Sicherheitsüberprüfungen lassen sich oft nur über Dienstleister vornehmen und sind oft nur teure Momentaufnahmen. Werkzeuge wie „Hackertools“ dagegen können von KMUs zur kostenneutralen und kontinuierlichen Selbstüberprüfung genutzt werden. Ausgewählte Werkzeuge könnten weiterentwickelt und verständlicher gestaltet werden, um folgend für den Gebrauch im KMU legalisiert und empfohlen zu werden.

Ansprechpartner herstellen

Für Einkauf und Betrieb von sicherer IT und von IT-Sicherheit sowie bei Sicherheitsvorfällen brauchen KMUs kompetente Expertise, die auch besondere Anwendungsfälle abdeckt und die möglichst jederzeit kostengünstig oder umsonst verfügbar ist. Hier könnten die IHKs regional Hilfeleistungen und Netzwerke aufbauen, um den Unternehmen bei Rückfragen oder Problemen zur Seite zu stehen.

Die Autoren

Dr. Sandro Gaycken (Author)

Dr. Sandro Gaycken is the director of the Digital Society Institute Berlin, a strategic research institute for digital topics of German DAX-companies. Sandro has published more than 60 articles and books on his topics, regularly writes op-eds in leading newspapers and has authored official government publications. He is a fellow of Oxford university's Martin College, in the working group on cyberdefence and cyberintelligence, a director for strategic cyberdefense projects in the NATO SPS Program where he presently designs and implements the national cybersecurity and cyberdefense strategy for Jordan, a member of the benchmarking group for „Industrie 4.0" standards for the German Ministry of Research BMBF, the director of the cybersecurity working group and associate fellow of the German Council on Foreign Relations (DGAP), a senior fellow at EastWest Institute, and he serves as CTO in a German industrial effort to bring high security IT to the „Industrie 4.0" universe.

He served in government as a strategist in the first design of a German Foreign and Security Policy on IT-matters, having been the lead-author of the Internet freedom and the cybersecurity/cyberdefence part of the policy, defining some first proposals for German Cyber Foreign Policy, and lead-authoring the first speech given by a German Minister of Foreign Affairs on Internet matters. He also served as a commentator for Germany's position in the UN GGE work on international cybersecurity, and addressed the UNO general assembly ambassadors in New York in their first session on international cyberpeace. He testified as a subject-matter expert in many hearings in the Bundestag and a range of ministries, provided strategic advice to NATO, UNO, OSCE, G8, EU, IAEA, and a few other governments. He has served as a principal expert witness in international court cases concerned with military cyber espionage and cyber sabotage, and is involved in other military cybercounterintelligence activities. Recently, he was involved in the construction of the No-Syp agreement between China and Germany.

Dr. Rex Hughes (Commentator)

Rex B. Hughes is a visiting fellow for cyber security at Wolfson College, University of Cambridge and at the Munk School of Global Affairs, University of Toronto. Internationally recognised for his expertise on the global political economy of the Internet, Dr Hughes is a regular speaker at Euro-Atlantic leadership fora including the NATO Parliamentary Assembly, Global Economic Symposium, and St Gallen Forum. He provides expert advice to North Atlantic business and government entities.

From 2005-07, Hughes served as a Cambridge-MIT Institute research associate contributing to disruptive technology roadmaps for British Telecom, Nortel, Nokia, and T-Mobile. During this period he successfully defended his Cambridge doctoral dissertation, *The British Response to Global Telecom Convergence*. From 2009-2010, Hughes served as first Chatham House associate fellow in cyber security.

From 1999-2003, whilst a student at the Henry M. Jackson School of International Studies at the University of Washington (UW), Hughes founded and directed the first university based Internet studies programme, the Center for Internet Studies. There in partnership with IBM and Lotus, Hughes led the development of *iEnvoy*™, the first secure Internet communications platform for diplomats, successfully deployed in 21 APEC and ASEAN foreign ministries through US Department of State sponsorship.