Cyber-Sicherheits-Check BSI und ISACA

Dirk Schugardt

ISACA Germany Chapter e.V.
FG-CyberSecurity@isaca.de

Konica Minolta IT-Solutions GmbH
dirk.schugardt@it.konicaminolta.de

Zusammenfassung

IT-Sicherheit wird in mittelständischen Unternehmen oftmals stiefmütterlich behandelt. Hohe Kosten können augenscheinlich keiner Wertschöpfung gegenüber gestellt werden. Die IT-Sicherheit wird oftmals dann angegangen, wenn bereits etwas passiert ist. Dann aber aktionistisch und nur punktuell. Doch gerade im Mittelstand liegen die Innovationen, ohne die das Vorankommen in vielen anderen Unternehmen und gerade auch in Weltkonzernen nicht mehr möglich ist. Der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist als Hilfsmittel für die Einführung und Umsetzung von IT-Sicherheit etabliert, wird im Mittelstand aber als zu aufwändig wahrgenommen. Der Cyber-Sicherheits-Check (CSC) entgegen zeigt eine einfache standardisierte Vorgehensweise auf, wie in mittelständischen Unternehmen der Stand der IT-Sicherheit vor Cyberangriffen analysiert und Schwachstellen kurz-, mittel- und langfristig strukturiert begegnet werden kann. Da die IT-Technik in den Unternehmen in viele neue Bereiche vordringt, reicht es nicht mehr aus, nur die bekannte Office-IT abzusichern. Produktionsmaschinen und -Abläufe der Industrie 4.0, in denen Aktoren, Sensoren und Maschinen unter- und miteinander in einer noch nie dagewesenen Fülle auch und gerade über das Internet kommunizieren, gilt es vor Angriffen aus dem Cyberraum abzusichern. Hierfür wird die Vorgehensweise für den Cyber-Sicherheits-Check ICS adaptiert, um ebenfalls das angestrebte Sicherheitsniveau zu analysieren und Maßnahmen strukturiert auf den Weg bringen zu können.

1 Der Stand der Cybersicherheit

In vielen mittelständischen Unternehmen ist die IT-Sicherheit ein Stiefkind. Wirtschaftlich gesehen bedeuten Ausgaben in die IT-Sicherheit offensichtlich nur Kosten, ohne einen sichtbaren Nutzen, denn „es ist noch nie etwas passiert, warum soll jetzt etwas passieren“. Aber die Gruppe der Betroffenen hat sich massiv erweitert. Ob Privatleute, Klein- und Kleinst-Unternehmen, mittelständische Unternehmen oder Großkonzerne, Mitarbeiter oder Leitungsebenen, alle sind im Fokus der unterschiedlichen Angriffe. Und zwar parallel. Über kommerziell genutzte Schadsoftware erfolgen Datenklau durch Zero-Day-Attacken als Bestandteil permanenter Angriffe wie den Advanced persistent Threads oder Erpressungen durch Verschlüsselung der Kronjuwelen des Unternehmens [ACBS14a]. Jeder ist heute im Fokus von Cyberangriffen und die nicht gemachten Hausaufgaben in der IT-Sicherheit „fallen immer mehr Menschen auf die Füße“. Immerhin, für die notwendige Sensibilisierung wird hierdurch automatisch gesorgt.

P. Schartner (Hrsg.) · D•A•CH Security 2016 · syssec (2016) 405-416.

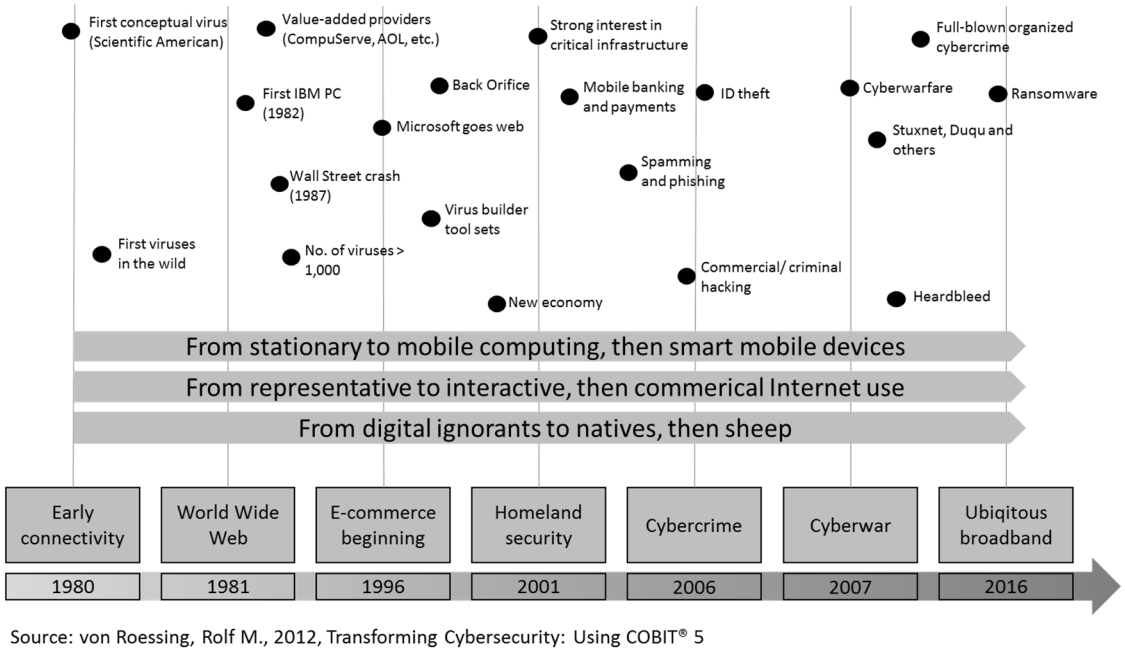

Abb. 1: ISACA Cyberspace Time Line

2 Die Entwicklung des Cyber-Sicherheits-Check

Im Rahmen der Zusammenarbeit der Allianz für Cybersicherheit [ACS16] hat sich das Bundesamt für Sicherheit in der Informationstechnik (nachfolgend auch BSI) [BMI11] und das ISACA Germany Chapter e.V. (nachfolgend auch ISACA) [ISAC16] dazu entschlossen, in Kooperation eine praxisorientierte Vorgehensweise zur Beurteilung der Cybersicherheit in Unternehmen und Behörden zu entwickeln. Aus den Erfahrungen mit dem IT-Grundschutz des BSI [ISAC12], der in mittelständischen Unternehmen nur sehr geringen Anklang gefunden hat, wurde der Fokus auf die Entwicklung eines mittelstandstauglichen Prüfungsleitfadens gelegt.

In der Fachgruppe Informationssicherheit wurde der Prüfungsleitfaden erarbeitet und 2014 herausgegeben. Er dient dazu, dass Unternehmen, insbesondere mit Fokus auf den Mittelstand, sowie Behörden und Institute ihren aktuellen Stand der Cybersicherheit analysieren sowie einen Maßnahmenplan für die Erreichung des gewünschten Sicherheitsniveaus erhalten können.

3 Weiterentwicklung des Cyber-Sicherheits-Check

Die Fortführung und Weiterentwicklung des Cyber-Sicherheits-Checks sowie weiterer Prüfungsleitfäden wurde 2015 von der Fachgruppe Informationssicherheit abgegeben durch die neu gegründete Fachgruppe Cyber Security des ISACA Germany Chapter e.V. übernommen. Auch diese Fachgruppe besteht aus Mitgliedern der Industrie, Hochschulen, Wirtschaftsprüfung, IT-Dienstleister, Sicherheits-Beratern sowie dem BSI, die ehrenamtlich ihren Beitrag zur Weiterentwicklung der Themenfelder erbringen. Zu Spezialfragen sind regelmäßig Spezialisten geladen, die ebenfalls ihr Wissen zur Verbesserung der Cybersicherheit einbringen.

Die großer Herausforderung ist momentan das Themenfeld der Industrie 4.0. Die Sicherheit bei der Vernetzung von Industrieanlagen ist noch recht jung und wie sich zeigt, bisher bei der Entwicklung und der Implementierung dieser Anlagen nicht hinreichend berücksichtigt worden. Proprietäre Protokolle zur Kommunikation zwischen den Komponenten und Anlagen werden

an das IP-Basierte Netzwerk angeschlossen und sind auf einmal genau so Angreifbar wie die so genannte „Office-IT“ der Bürokommunikation. Die Sicherheitslücken können binnen zwei Tagen von versierten Angreifern ausgenutzt, Datenübertragungen gestört, Systemausfälle etc. verursacht werden. Das betrifft unter anderem Energieversorgungs-, Produktions- wie Medizingeräte und -komponenten [BMI07]. Also allesamt wichtige Bereiche unseres alltäglichen Lebens [BSI16].

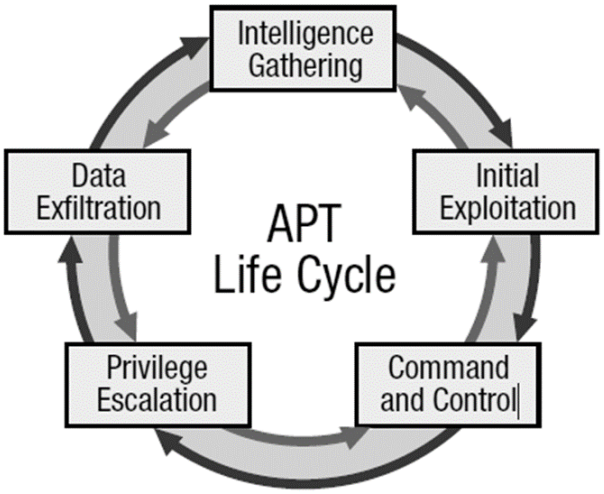

Abb. 2: ISACA APT Life Cycle

Die Fachgruppe Cyber Security hat es sich daher zur Aufgabe gemacht, einen Prüfungsleitfaden für ICS Anlagen (Produktionsmaschinen, Steuerungsnetzwerke etc.) zu entwickeln [ISAC13a]. Hier werden unter anderem die Neuerungen der Branchenverbände des Verband Deutscher Maschinen- und Anlagenbau e.V. (VDMA), NAMUR - Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V. sowie Zentralverband Elektrotechnik- und Elektronikindustrie e.V. (ZVEI) mit berücksichtigt. Ziel ist wieder einen mittelstandstauglichen Prüfungsleitfaden zur Verfügung zu stellen, der es Auditoren mit Grundkenntnissen ermöglicht, sich ein Lagebild der Sicherheit vor Cyberangriffen im ICS-Umfeld zu bilden, diese beurteilen sowie einen Maßnahmenplan zum Erreichen des benötigten Sicherheitsniveaus erstellen zu können.

Als weitere Aufgabe der Fachgruppe wird der bestehende Cyber-Sicherheits-Check der Office-IT überarbeitet. Hierzu wird die bestehende Exposition zur Bewertung des Angriffsrisikos überarbeitet, die Zuordnung der Maßnahmen zu aktuellen Standards wie z.B. die ISO 27001:2013 bzw. ISO 27001:2015 oder PCI-DSS 3.0 etc. durchgeführt und ggf. tiefergreifende Fragestellungen aus den jeweiligen Standards mit aufgenommen.

4 Der Cyber-Sicherheits-Check

Waren bis vor wenigen Jahren noch viele Unternehmen und Privatleute uninteressant für Angriffe aus dem Cyberraum, so hat sich dies heute stark gewandelt. Auch Privatleute Arbeiten in Firmen oder haben Bekannte die interessant sind. Informationsgewinnung für gezielte Angriffe, umfasst Mitarbeiter, deren Familie, Freunde und Bekannte oder Kollegen. Informationen von Dienstleistern, Kunden, Lieferanten und Subunternehmen sind genauso interessant, wie das Ziel selbst. Fernzugriffe durch den IT-Dienstleister oder dem Mitarbeiter im Homeoffice sind eine gern genommene Tür [ISAC13e].

Unter diesen Gesichtspunkten ist es heute notwendig, zuerst einmal seine Ist-Situation zu analysieren und die Basismaßnahmen, die bei jedem Unternehmen in irgendeiner Form umgesetzt sein sollten, strukturiert anzugehen und dann durch regelmäßige Status-Analysen seine Sicherheit an die sich ändernden Anforderungen anzupassen [ISAC13c].

Ein Beispiel für die Notwendigkeit die versäumten Sicherheitsmaßnahmen zeitnah nachzuholen ist die aktuelle Welle der Erpressungsviren (Ransomware). Bei einem Vorfall hilft letztendlich nur eine gute Datensicherung. Aber das Risiko eines Auftretens und die Auswirkungen eines Vorfalls lassen sich im Vorfeld durch ein Zusammenspiel von angemessenen Maßnahmen minimieren. Durch gute IT-Richtlinien sowie eine regelmäßige Sensibilisierung der Mitarbeiter wird das Risiko von Fehlhandlungen minimiert. Durch korrekt zugewiesene Benutzer, auf das nötigste reduzierte Berechtigungen sowie die Reduzierung von Zugrängen auf Netzwerkfreigaben und Laufwerke wird der Zugriffsbereich der Ransomware begrenzt. Durch Inventarisierung, Schwachstellen- und Patchmanagement wird sichergestellt, dass Sicherheitslücken durch Schadcode nicht ausgenutzt werden können. Durch aktuelle Applikation-Level-Firewalls wird bereits der Netzwerkverkehr auf Schadcode mit Methoden wie das Sandboxing untersucht. Netzwerksegmentierung mit Steuerung über Firewalls verhindert einen Befall verschiedener Netzwerke. Ein mehrstufiges Antivirus-Konzept und Spam-Schutz verhindern, dass bekannter Schadcode ins Netzwerk eindringen oder aktiv werden kann. Und durch ein umfangreiches Logmanagement werden systemseitige Vorkommnisse protokolliert, gesammelt und ausgewertet, so dass zeitnah eine automatische Alarmierung der IT erfolgt und umgehend Gegenmaßnahmen eingeleitet werden können.

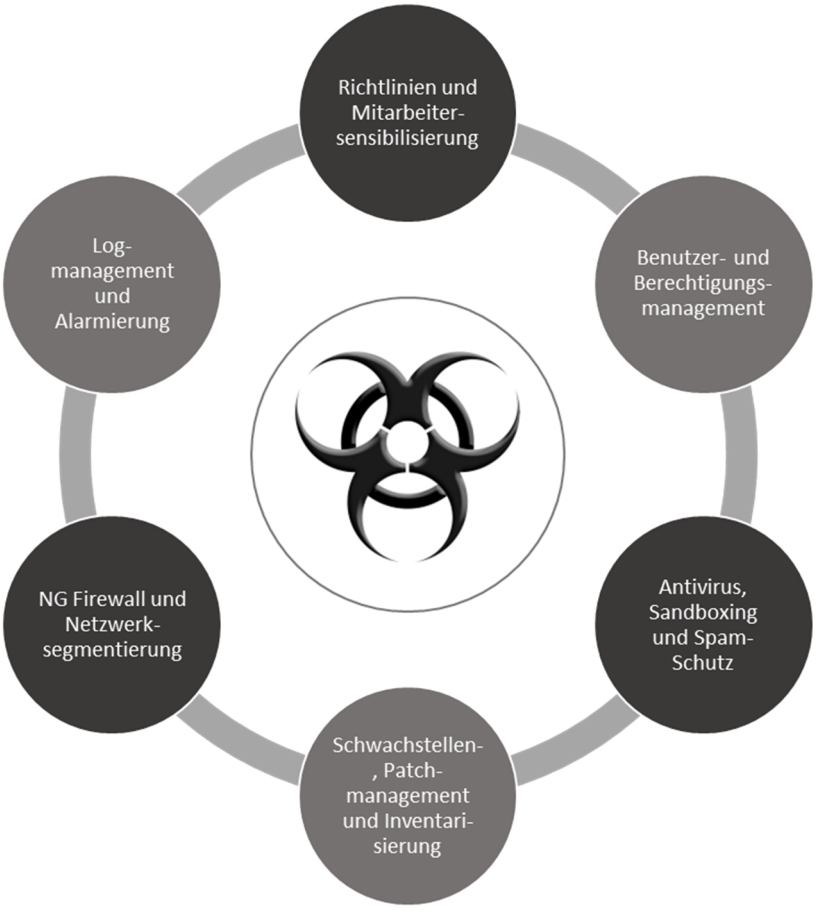

Abb. 3: Übersicht der Ransomware Maßnahmen

Der Cyber-Sicherheits-Check bietet ein vorgefertigtes Prüfungswerkzeug [ISAC13d] mit dem die technischen und organisatorischen Maßnahmen der IT-Sicherheit gegen Cyber-Angriffe durch fachkundige und zuverlässige Prüfer [ISAC13b] auditiert werden können. Sinnvoll ist es hierzu auch oftmals eine tiefergehende technische Analyse durch einen qualifizierten Penetrationstest durchzuführen [ACBS14c]. Hierdurch wird sichergestellt, dass die organisatorischen und technischen Maßnahmen auch in ihrer technischen Umsetzung die Sicherheitsanforderungen erfüllen sowie technische Lücken noch aufgedeckt und bereinigt werden können.

Im ersten Schritt des Cyber-Sicherheits-Checks wird zuerst die Cyber-Sicherheits-Exposition erstellt.

4.1 Cyber-Sicherheits-Exposition

Die Cyber-Sicherheits-Exposition [ACBS12a] bildet ein Maß für die Wahrscheinlichkeit, in das Zielspektrum von Angreifern zu geraten. Dabei sind solche Täterkreise von besonderer Relevanz, denen es nicht um Breitenangriffe gegen mehr oder minder wahllose Ziele geht, sondern die es vielmehr gezielt auf eine bewusst ausgewählte Organisation abgesehen haben. Die Abwehr solch gezielter Angriffe, deren Techniken von Angreifern auf die spezielle Situation der angegriffenen Organisation angepasst werden, stellt eine der größten Herausforderungen der Cyber-Sicherheit dar.

Die zu schützende IT-Infrastruktur sowie deren einzelne Elemente sind somit einem breiten Spektrum von Angriffsmethoden ausgesetzt. In der Praxis ist es aber zunächst notwendig, das konkrete Risiko für das zu auditierende Unternehmen festzulegen sowie die Prüfung dafür auszurichten. In der dafür durch die Cyber-Sicherheits-Exposition zu erstellenden Risikobewertung der gespeicherten und übertragenen Daten und Prozesse lässt aus der Betrachtung des Zusammenwirkens unterschiedlicher Faktoren systematisch darstellen, wie groß die Angriffsfläche des Unternehmens ist.

Die Cyber-Sicherheits-Exposition orientiert sich zwar an der Schutzbedarfsfeststellung nach dem BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise, stellt aber eine praktische und leicht umzusetzende Bewertungsmethode dar. Sie wird durch mehrere Faktoren bestimmt:

- die Attraktivität der zu schützenden Infrastruktur,
- die Charakterisierung der Angreifer,
- der Wert der angegriffenen Daten und Prozesse,
- die Zielgerichtetheit der Angriffe und ob bereits Erfahrungswerte zu Angriffen in der Vergangenheit vorhanden sind.

Dabei wird in der Cyber-Sicherheits-Exposition die Vertraulichkeit als auch die Verfügbarkeit sowie die Integrität betrachtet und kann die Werte normal, hoch oder sehr hoch annehmen. Die Cyber-Sicherheits-Exposition wird zudem im Hinblick auf die Transparenz der Infrastruktur für Angreifer gewichtet.

Damit ergeben sich folgende Leitfragen zur Bestimmung der Cyber-Sicherheits-Exposition:

- Wert der Informationen und Prozesse
  - Welche Daten stellen den größten Wert dar, sowohl im Hinblick auf ihre Vertraulichkeit als auch ihre Verfügbarkeit und Integrität?
  - Welche Prozesse stellen den größten Wert dar, sowohl im Hinblick auf ihre Vertraulichkeit als auch ihre Verfügbarkeit und Integrität?

  - Wie abhängig sind geschäftskritische Prozesse der Institution von den Daten?
- Attraktivität für Angreifer
  - Wie attraktiv ist es für Angreifer, Zugriff auf die vertraulichen Daten zu erlangen?
  - Wie attraktiv ist es für Angreifer, die Verfügbarkeit der Daten oder Prozesse einzuschränken?
  - Wie attraktiv ist es für Angreifer, die Integrität der Daten oder Prozesse durch Manipulationen zu verletzen?
- Charakterisierung der Angreifer
  - Wer kommt für Angriffe gegen die Vertraulichkeit, die Verfügbarkeit und/oder die Integrität in Betracht?
    - Täter, die in ihrer Freizeit und aus reiner Neugier agieren (Hobbyisten)?
    - IT-Sicherheitsforscher, die zunächst ein akademisches Interesse in Bezug auf Angriffsmöglichkeiten verfolgen, ihre Ergebnisse dann jedoch auch breit veröffentlichen?
    - Cyber-Kleinkriminelle, für die insbesondere die monetäre Verwertbarkeit erbeuteter Daten im Vordergrund steht?
    - Professionelle, organisierte Cyber-Kriminelle, auch professionelle Konkurrenz-Spionage?
    - Hacktivisten, die mit ihren Angriffen politische und gesellschaftliche Ziele verfolgen?
    - Staatliche Stellen wie z. B. Nachrichtendienste, die auf umfangreiche Ressourcen zur Planung und Durchführung ihrer Angriffe zurückgreifen können?
- Zielgerichtetheit der Cyber-Angriffe
  - Ist davon auszugehen, dass die Institution von Flächenangriffen betroffen sein wird, deren Ziele diese Angreifergruppen eher zufällig in großer Zahl auswählen?
  - Oder ist zu vermuten, dass die Institution gezielt angegriffen wird, was eine bessere Vorbereitung und Durchführung des Angriffs erlaubt?
- Erfahrungswerte über Angriffe in der Vergangenheit
  - Sind in der Vergangenheit Cyber-Angriffe auf die Institution detektiert worden?
  - Gab es in der Vergangenheit erfolgreiche Cyber-Angriffe, die zu Schäden geführt haben?

Aus der Analyse dieser Leitfragen lässt sich die Bewertung des Grundrisikos, wie in den nachfolgenden Tabellen dargestellt, durchführen. Dabei ist zunächst in jeder Zeile dem Bedrohungsgrad der Vertraulichkeit, Verfügbarkeit und Integrität ein individueller Wert zuzuordnen, aus dem dann der maximale Wert für jeden Grundwert ermittelt wird.

Tab. 1: Bestimmung des Bedrohungsgrades

Bestimmung des Bedrohungsgrad	Vertraulichkeit	Verfügbarkeit	Integrität
Wert der Daten und Prozesse	Gering 0 Normal 1 Hoch 2 sehr hoch 4	Gering 0 Normal 1 Hoch 2 sehr hoch 4	Gering 0 Normal 1 Hoch 2 sehr hoch 4
Attraktivität für Angreifer	Gering 0 Normal 1 hoch 2 sehr hoch 4	Gering 0 Normal 1 Hoch 2 sehr hoch 4	Gering 0 Normal 1 Hoch 2 sehr hoch 4
Art der Angreifer	Hobbyisten 0 Forscher 1 Kleinkriminelle 2 prof. Kriminelle 4 Hacktivisten 4 staatl. Akteure 5	Hobbyisten 0 Forscher 1 Kleinkriminelle 2 prof. Kriminelle 4 Hacktivisten 4 staatl. Akteure 5	Hobbyisten 0 Forscher 1 Kleinkriminelle 2 prof. Kriminelle 4 Hacktivisten 4 staatl. Akteure 5
Zielgerichtetheit des Angriffs	Flächenangriff 1 gezielter Angriff 5	Flächenangriff 1 gezielter Angriff 4	Flächenangriff 1 gezielter Angriff 5
Angriffe der Vergangenheit	Unbekannt 1 Abgewehrt 3 Erfolgreich 5	Unbekannt 1 Abgewehrt 3 Erfolgreich 5	Unbekannt 1 Abgewehrt 3 Erfolgreich 5
	Maximum ↓	Maximum ↓	Maximum ↓
Maximumwert des Bedrohungsgrad	max. Punktwert 1 … 5	max. Punktwert 1 … 5	max. Punktwert 1 … 5

Für die erfolgreiche Durchführung eines Cyber-Angriffes benötigt der Angreifer möglichst viele Informationen über das Ziel. Hierbei ist ausschlaggebend, wie transparent sich dieses für den Angreifer darstellt. Die folgenden Leitfragen sind daher für die Einschätzung der Transparenz zu beantworten:

- Welche Informationen über den Aufbau der zu schützenden Infrastruktur sind öffentlich verfügbar?
  - Können aus dem Internetauftritt der Behörde oder des Unternehmens Rückschlüsse auf die IT-Infrastruktur gezogen werden?
  - Welche Informationen werden über Stellenangebote für technisches Personal preisgegeben?
  - Enthalten Veröffentlichungen der Behörde oder des Unternehmens, wie Geschäftsberichte oder (insbesondere in der öffentlichen Verwaltung) durchgeführte Beschaffungen, direkte oder indirekte Angaben über die IT-Infrastruktur?
  - Wie verhalten sich Angehörige der Behörde oder des Unternehmens beruflich und privat in Sozialen Netzen? Welche Informationen zur technischen Ausstattung geben sie dabei bewusst oder unbewusst preis? Welche Rückschlüsse auf Schlüsselpositionen in der Organisation und mögliche technische und menschliche Einfallstore sind möglich?
- Können Angreifer mit technischen Methoden Einzelheiten der Infrastruktur aufklären?

- Welche technischen Daten werden von den mit dem Internet verbundenen Systemen nach außen weitergegeben, z.B. von Webservern einer Organisation?
- Können durch die Analyse der von Internet-Browsern der Organisation beim Aufruf von externen Webseiten mitgesendeten Informationen Details der installierten Software in Erfahrung gebracht werden?
- Enthalten die Datenfelder von E-Mails der Behörde oder des Unternehmens z.B. Informationen über die eingesetzte Groupware und deren Struktur?
- Sind in Dokumenten der Behörde oder des Unternehmens offene oder versteckte Metadaten enthalten, die unbeabsichtigt weitere Informationen preisgeben?

- Werden über die Behörde oder das Unternehmen von Dritten in halboffenen oder geschlossenen Foren im Internet Informationen gesammelt, die für Angreifer, die diese Foren beobachten, von Nutzen sein könnten?

Für die Transparenz sind nun die Werte wie nachfolgend aufgezeigt zu klassifizieren.

Tab. 2: Bestimmung der Transparenz

Bestimmung der Transparenz	Vertraulichkeit		Verfügbarkeit		Integrität	
Transparenz für den Angreifer	Gering mittel Hoch	-1 0 +1	Gering mittel Hoch	-1 0 +1	Gering mittel Hoch	-1 0 +1

Nach der Bewertung des Bedrohungsgrads und der Transparenz kann die Cyber-Sicherheits-Exposition bestimmt werden. Sie ergibt sich jetzt aus der Summe des Bedrohungsgrads und des Transparenzwerts

Cyber-Sicherheits-Exposition = Bedrohungsgrad + Transparenz

und kann Werte zwischen 0 und 6 annehmen, die zu einer normalen, hohen oder sehr hohen Risikobewertung führen.

Tab. 3: Bestimmung der Cyber-Sicherheits-Exposition

Bestimmung der Cyber-Sicherheits-Exposition		Vertraulichkeit	Verfügbarkeit	Integrität
Cyber-Sicherheits-Exposition	normal	max. Punktwert 0 … 1	max. Punktwert 0 … 1	max. Punktwert 0 … 1
	hoch	max. Punktwert 2 … 3	max. Punktwert 2 … 3	max. Punktwert 2 … 3
	Sehr hoch	max. Punktwert 4 … 6	max. Punktwert 4 … 6	max. Punktwert 4 … 6

Die so bestimmte Cyber-Sicherheits-Exposition fasst die Bedrohungslage für die zu untersuchende Infrastruktur in Bezug auf die Transparenz und Attraktivität für Angreifer, die Art und Zielgerichtetheit der Angreifer, mögliche Schadenshöhen sowie Erkenntnisse zu bereits stattgefundenen Angriffen zusammen und bildet damit das entscheidende Kriterium dafür, welche Maßnahmenziele in den Schlüsselbereichen des Audit des Cyber-Sicherheits-Check in welcher Intensität zu bewerten sind.

4.2 Audit des Maßnahmenkatalogs

Der Cyber-Sicherheits-Check bietet bereits einen umfangreichen Katalog von Maßnahmenzielen [ACBS12b]. Der Katalog umfasst dabei zusammengefasst folgende Fragestellungen:

- Sind sämtliche Netzübergänge identifiziert und hinreichend abgesichert?
- Wird die Infektion mit Schadprogrammen mit wirksamen Maßnahmen unterbunden?
- Werden die IT-Systeme inventarisiert und auf ihre sicherheitstechnische Beherrschbarkeit hin geprüft?
- Werden offene Sicherheitslücken auf IT-Systemen vermieden?
- Findet eine Interaktion mit dem Internet nur über abgesicherte Komponenten statt?
- Werden Protokolldaten zentral erfasst und automatisiert ausgewertet?
- Wird die eigene Organisation mit allen notwendigen Informationen versorgt?
- Ist die Organisation auf die Bewältigung von Sicherheitsvorfällen vorbereitet?
- Verhindern die eingesetzten Mechanismen zur Authentisierung eine missbräuchliche Nutzung durch Dritte?
- Stehen ausreichende interne Ressourcen zur Verfügung und werden externe Dienstleister eingebunden?
- Wird das eigene Personal in Fragen der Cyber-Sicherheit kontinuierlich sensibilisiert?
- Werden nutzerorientierte Maßnahmen zur Rollentrennung durchgesetzt?
- Bewegen sich die Organisation und ihre Mitglieder sicher in „Sozialen Netzen“?
- Werden Vertraulichkeit, Verfügbarkeit und Integrität durch wirksame Maßnahmen gewährleistet und Penetrationstests durchgeführt?
- Werden zur Abwehr gezielter Angriffe unterstützende Schutzmaßnahmen ergriffen?

Diese Maßnahmenziele sind bereits durch Basismaßnahmen aus relevanten Standards (ISO27001:2013/PCI DSS 3.0/Cobit 5/BSI-IT-GSK) zusammengetragen und können als Prüffelder durch den Auditor mit dem Unternehmen analysiert werden. Das schöne ist, dass hier bereits umfangreiche Vorarbeit geleistet wurde und sich auf eine standardisierte Vorgehensweise gestützt werden kann [ACSB14d].

Tab. 4: Beispiel aus dem Katalog der Maßnahmenziele

Maßnahmen		Basismaßnahmen	Referenzen
A	**Absicherung von Netzübergängen** Die Absicherung von Netzübergängen ist einer der entscheidenden Faktoren für eine wirksame Abwehr von Angriffen aus dem Internet. Auf Grundlage der Netzwerkarchitektur müssen Abwehrmaßnahmen für alle internen und externen Netzübergänge sowie die entsprechenden Prozesse (wie z. B. ein	• Alle Netzübergänge sind identifiziert und dokumentiert. • Das Netz ist in Segmente aufgeteilt und die Anzahl der Netzübergänge wird minimal gehalten. • Alle Netzübergänge sind durch geeignete Sicherheitsgateways abgesichert und werden regelmäßig überprüft. • Auf Client- und Serversystemen findet eine technische	**BSI IT-GSK 13. Erg.-Lieferung:** B 3.301, B 3.302, B 4.1, B 5.14, M 2.204 **COBIT 5:** DSS05.02, DSS05.03, DSS06.06 **ISO/IEC 27001:2005:** A.10.6, A.10.7.1, A.11.4, A.11.6.2, A11.7, A.12.5.4 **ISO/IEC 27001:2013:**

	Change Management) geplant und umgesetzt werden.	Schnittstellenkontrolle statt, die eine zulässige Nutzung kontrolliert und eine unzulässige Nutzung verhindert. • Zugänge mobiler ITGeräte sind angemessen abgesichert und auf das erforderliche Mindestmaß beschränkt. • Zugänge für Remote-Administration und -Überwachung sind angemessen abgesichert. • Es werden nur zeitgemäße Verschlüsselungs- und Authentisierungsverfahren eingesetzt.	A.6.2, A.8.3.1, A.9.1.2, A.13.1 **PCI DSS 3.0:** 1.1, 1.1.2, 1.1.4, 1.1.6, 1.2, 1.2.3, 1.3, 1.3.1-1.3.8, 1.4, 2.2.3, 2.2.4, 4.1, 4.1.1, 8.3, 11.4, 12.3.8, 12.3.9

Werden im Rahmen eines Cyber-Sicherheits-Checks Sicherheitsmängel in den Basismaßnahmen festgestellt, so hat der Auditor diese spätestens bei der Berichtserstellung in ihrer Kritikalität zu bewerten. Dies erfolgt nach folgendem Schema:

„Kein Sicherheitsmangel“

Zum Zeitpunkt der Beurteilung konnte kein Sicherheitsmangel festgestellt werden. Es gibt keine ergänzenden Hinweise.

„Sicherheitsempfehlung“

Auch eine voll umgesetzte IT-Sicherheitsmaßnahme kann um eine Sicherheitsempfehlung ergänzt werden. Durch die Umsetzung der im Sachverhalt beschriebenen Maßnahmenempfehlungen kann die Sicherheit erhöht werden. Verbesserungsvorschläge für die Umsetzung von Maßnahmen, ergänzende Maßnahmen, die sich in der Praxis bewährt haben oder Kommentare hinsichtlich der Angemessenheit von Maßnahmen können ebenfalls als Sicherheitsempfehlung aufgeführt werden.

„Sicherheitsmangel“

Bei einem „Sicherheitsmangel“ liegt eine Sicherheitslücke vor, die mittelfristig behoben werden sollte. Die Vertraulichkeit, Integrität oder Verfügbarkeit der Informationen kann beeinträchtigt sein.

„Schwerwiegender Sicherheitsmangel“

Ein „schwerwiegender Sicherheitsmangel“ ist eine Sicherheitslücke, die umgehend geschlossen werden sollte, da die Vertraulichkeit, die Integrität und/oder die Verfügbarkeit der Informationen stark gefährdet und erheblicher Schaden zu erwarten ist.

Hier kommt auch das Zusammenspiel der Cyber-Sicherheits-Exposition mit der Schwachstellenbewertung zum Tragen. Wird beispielsweise in einem Unternehmen als Perimeterschutz nur eine Stateful-Firewall eingesetzt bei der das Regelwerk Lücken aufweist, wäre das bei einer normalen Risikobewertung in der Cyber-Sicherheits-Exposition ein Sicherheitsmangel. Bei einer hohen bis sehr hohen Risikobewertung ist diese Feststellung als schwerwiegender Mangel einzustufen. Auch sind die Empfehlungen daran auszurichten. Wenn in dem aufgeführten Beispiel bei einem Sicherheitsmangel der Einsatz einer Applikation-Level-Firewall genügen würde, so sollte bei einem schwerwiegenden Mangel über ein mehrstufiges Firewall-Konzept mit unterschiedlichen Schutzstufen nachgedacht werden.

Der Cyber-Sicherheits-Check wird mit einem Beurteilungsbericht abgeschlossen [ACBS14b]. Hier wird über ein Zusammengefasstes Ergebnis ein managementkonformer Überblick über die Cyber-Sicherheits-Lage im Unternehmen aufgezeigt. Die Aufstellung der festgestellten Mängel und der Empfehlungen ermöglicht es einen Maßnahmenplan aufzubauen und nach entsprechend durch das Unternehmen festgelegter Priorisierung umzusetzen.

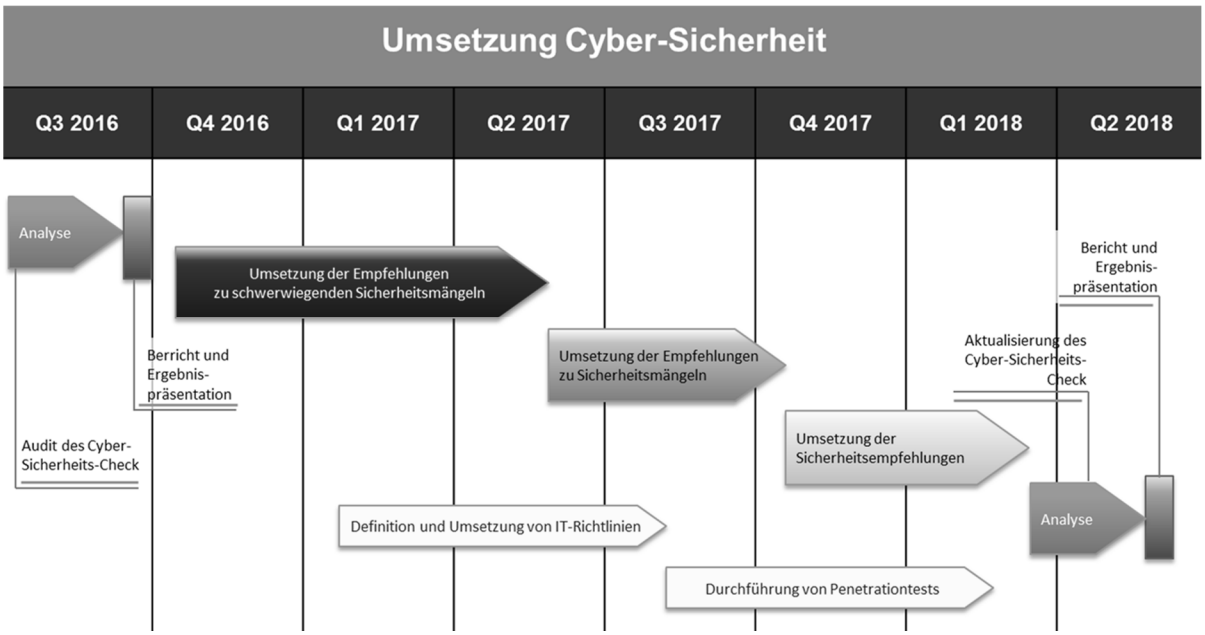

Abb. 4: Beispiel der Maßnahmenplanung

4.3 Ausbildung zum Cyber-Security-Practitioner

Der Zertifikatskurs „Cyber Security Practitioner“ wurde ebenfalls im Rahmen der Allianz für Cyber-Sicherheit vom Bundesamt für Sicherheit in der Informationstechnik und dem ISACA Germany Chapter e.V. in Kooperation entwickelt.

Der eintägige Kurs gibt eine Einführung in wesentliche Aspekte der Cyber-Sicherheit und vermittelt den Teilnehmern insbesondere Vorgehensweise und Prinzipien zur Durchführung eines Cyber-Sicherheits-Checks.

Voraussetzung zum Bestehen des „Cyber Security Practitioner“ ist neben der Kursteilnahme ein Selbststudium des Leitfadens „Cyber-Sicherheits-Check“ sowie der BSI-Publikationen BSI-CS_006 „Basismaßnahmen der Cyber-Sicherheit“ und BSI-CS_013 „Cyber-Sicherheits-Exposition“.

Am Ende des Kurses findet eine Prüfung in Form von 30 bis 40 Multiple Choice Fragen aus den oben aufgeführten Dokumenten statt.

5 Ausblick

Durch die immer stärkere Vernetzung von Industrie, Produktion, Versorgungsunternehmen und Intuitionen sowie Behörden und Privatleuten wird auch der Schutz vor Cyberangriffen immer wichtiger. Das hat die Gesetzgebung in Deutschland durch das IT-Sicherheitsgesetz bereits erkannt und für kritische Infrastrukturen eine bisher nicht gekannte Welle der Verbesserung der

Informationssicherheit in Gang gesetzt. Das wurde auch in der Fachgruppe Cyber-Security erkannt und auch die Cyber-Sicherheit des Internet of Things ist einer der Punkte der in der Fachgruppe erarbeitet wird, um zukünftig z.B. durch „Security by design“ die notwendige Sicherheit zu erreichen. Gerne freuen wir uns über Unterstützung und rege Mitarbeit.

Literatur

[ACS16] Allianz für Cyber-Sicherheit, Webauftritt, www.allianz-fuer-cybersicherheit.de

[ACBS12a] Allianz für Cyber-Sicherheit, BSI-CS_013 „Cyber-Sicherheits-Exposition“.

[ACBS12b] Allianz für Cyber-Sicherheit, BSI-CS_006 „Basismaßnahmen der Cyber-Sicherheit“.

[ACBS14a] Allianz für Cyber-Sicherheit, BSI-CS_072 „Erste-Hilfe bei einem APT-Angriff“.

[ACBS14b] Allianz für Cyber-Sicherheit, Muster-Bericht für den Cyber-Sicherheits-Check.

[ACBS14c] Allianz für Cyber-Sicherheit, Praxis-Leitfaden für IS-Penetrationstests.

[ACSB14d] Allianz für Cyber-Sicherheit, Leitfaden Cyber-Sicherheits-Check, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/CyberSicherheitsCheck/csc.html

[BMI07] Bundesministerium des Innern, Nationaler Plan zum Schutz der Informationsinfrastrukturen in Deutschland, Umsetzungsplan KRITIS (UP-KRITIS), September 2007, www.bmi.bund.de

[BMI11] Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland, Februar 2011, www.bmi.bund.de

[BSI16] Bundesamt für Sicherheit in der Informationstechnik, Broschüre Das IT-Sicherheitsgesetz, www.bsi.bund.de

[ISAC16] ISACA Germany Chapter e.V., Webauftritt, www.isaca.de

[ISAC13a] ISACA, Transforming Cybersecurity Using COBIT 5, 2013. www.isaca.org/cybersecurity-cobit

[ISAC13b] ISACA, Berufs-Ehrenkodex, 2013, www.isaca.org

[ISAC12] ISACA, COBIT 5 for Information Security, 2012. http://www.isaca.org/cobit5security

[ISAC13c] ISACA, Responding to Targeted Cyberattacks, 2013, www.isaca.org/cyberattacks

[ISAC13d] ISACA, IT-Prüfungsstandards, 2013, www.isaca.org/Knowledge-Center/Standards/Pages/Standards-forIS-Audit-and-Assurance-German.aspx

[ISAC13e] ISACA, Advanced Persistent Threats: How to Manage the Risk to Your Business, 2013, www.isaca.org/apt-book