Allianz für Cyber-Sicherheit

VDMA

ZVEI: Die Elektroindustrie

INTERNATIONAL DATA SPACES ASSOCIATION

Leitfaden Cyber-Sicherheits-Check

Ein Leitfaden zur Durchführung von Cyber-Sicherheits-Checks in der Office IT von Unternehmen und Behörden

Version 2

ISACA Germany Chapter

dpunkt.verlag

Herausgeber:
ISACA Germany Chapter e. V.
Storkower Straße 158
D-10407 Berlin

www.isaca.de
info@isaca.de

Autorenteam:
- Dr. Peter Ebinger
- Martin Ennenbach
- Sebastian Fritsch
- Tobias Glemser
- Arne Günther
- Markus Lörsch
- Markus J Neuhaus
- Armin Nilles
- Jan Oetting
- Holger Pfeiffer
- Peter Reiner
- Jan Rozek
- Dr. Tim Sattler
- Dirk Schugardt
- Christian Schwartz
- Andreas Teuscher
- Dr. Karl-Friedrich Thier
- Dr. Jens Vykoukal
- Gregor Wittkowski

Die Inhalte dieses Leitfadens wurden von Mitgliedern des ISACA Germany Chapter e. V. in Kooperation mit dem BSI erarbeitet und sind sorgfältig recherchiert. Trotz größtmöglicher Sorgfalt erhebt die vorliegende Publikation keinen Anspruch auf Vollständigkeit. Sie spiegelt die Auffassung des ISACA Germany Chapter wider. ISACA Germany Chapter e. V. übernimmt keine Haftung für den Inhalt.

Der jeweils aktuelle Leitfaden kann unter *https://www.isaca.de/de/veroeffentlichungen/cyber_security* kostenlos bezogen werden.

Stand: Februar 2020

Leitfaden Cyber-Sicherheits-Check

Ein Leitfaden zur Durchführung von Cyber-Sicherheits-Checks in der Office IT von Unternehmen und Behörden

Version 2

ISACA
Germany Chapter

Allianz für Cyber-Sicherheit

Die Allianz für Cyber-Sicherheit ist eine Initiative des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die in Zusammenarbeit mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) gegründet wurde.

Als Zusammenschluss wichtiger Akteure im Bereich der Cyber-Sicherheit in Deutschland hat die Allianz zum Ziel, die Cyber-Sicherheit in Deutschland zu erhöhen und die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken. Die Allianz für Cyber-Sicherheit unterstützt den Informations- und Erfahrungsaustausch zwischen den verschiedenen Akteuren aus Wirtschaft, Verwaltung, Verbänden, wie z. B. dem ISACA Germany Chapter e. V., und Wissenschaft und erweitert darauf aufbauend kontinuierlich eine umfangreiche Wissensbasis.

Wirtschaftsunternehmen sind aufgerufen, sich aktiv in die Allianz für Cyber-Sicherheit einzubringen und den Erfahrungsaustausch zu stärken. Beispielsweise können sie aktiv dem BSI mitteilen, mit welchen neuartigen Bedrohungen oder IT-Sicherheitsvorfällen sie sich als Unternehmen konfrontiert sehen. Damit tragen sie zur Erstellung eines stark verbesserten Lagebildes bei und helfen, noch zielgerichteter gegen Cyber-Angriffe agieren zu können. Gleichzeitig profitieren auch die Unternehmen von gemeinsam gewonnenen Erkenntnissen und Erfahrungen.

Vorwort

Zentralverband Elektrotechnik- und Elektronikindustrie e. V. (ZVEI)

Täglich werden hunderttausende neue Schadprogramm-Varianten registriert; Botnetze führen Denial-of-Service-Angriffe mit bis zu 300 Gbit/s aus und durch Ransomware-Angriffe kommt es immer häufiger zu Ausfällen von Rechnern und Netzwerken bei Unternehmen, Behörden und Privatanwendern. In einer zunehmend vernetzten Welt spielt Cybersicherheit eine größere Rolle denn je.

Deswegen unterstützt der ZVEI den überarbeiteten Leitfaden »Cyber-Sicherheits-Check« als Mitherausgeber. Die Publikation vermittelt notwendiges Wissen in zugänglicher Form: Der Cyber-Sicherheits-Check erlaubt eine schnelle Bewertung der Risiken und bietet eine Grundlage, um konkrete Sicherheitsmaßnahmen detailliert zu formulieren. Gerade kleinere Unternehmen können so Risiken im Cyberspace leichter identifizieren.

Cybersicherheit durchdringt als Querschnittsthema alle Leitmärkte des ZVEI – von Industrie 4.0 über Mobilität und Gesundheit bis hin zu Energie und Gebäude. Der Verband will das nötige Bewusstsein bei Unternehmen, deren Mitarbeitern, in der Politik sowie bei den Bürgern schaffen. Es gilt, die Security-Kultur innerhalb der Elektrobranche zu stärken und so Vertrauen zu bilden.

In der politischen Arbeit begleitet der ZVEI die entsprechenden Gesetzgebungsinitiativen in Deutschland und Europa und tritt für praktikable Regelungen ein, die möglichst europäisch harmonisiert sein sollen.

Informations- und Erfahrungsaustausch – innerhalb des ZVEI und seiner Mitgliedschaft, mit Behörden wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) oder in Netzwerken wie der Allianz für Cyber-Sicherheit (ACS) – sind essenziell. Insbesondere kleine und mittlere Unternehmen profitieren dabei deutlich von Expertenwissen.

Der Cyber-Sicherheits-Check trifft auf eine hohe Nachfrage: Über 450 Personen haben sich in den letzten Jahren ausbilden und zertifizieren lassen, um diese Checks durchführen zu können. Daneben haben viele

Firmen, auch ohne explizite Zertifizierung, eigenständig interne Cyber-Sicherheits-Checks auf Basis des Leitfadens durchgeführt. Jeder erfolgreich und effizient durchgeführte Check erhöht das Schutzniveau:

»Cybersicherheit ist essenziell zum Schutz von Staat, Wirtschaft und Gesellschaft. Den Herausforderungen vernetzter Daten und Systeme kann man nur gemeinsam begegnen.«

Dr. Klaus Mittelbach
Vorsitzender der Geschäftsführung
ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e. V.

Verband Deutscher Maschinen- und Anlagenbau e. V. (VDMA)

Der Maschinen- und Anlagenbau befindet sich mitten in der digitalen Transformation. Digitale Geschäftsmodelle und die weltweite Vernetzung von Maschinen müssen dabei cyber-sicher entwickelt und betrieben werden. Bereits heute ist ein Drittel der VDMA-Mitglieder von Produktionsausfällen durch Security-Vorfälle betroffen. Der unternehmerische Wert der Security ist in der Geschäftsführung unserer 3.200 Mitglieder angekommen.

Die größtenteils mittelständisch aufgestellten Unternehmen benötigen zur Betrachtung von Security-Risiken und deren Absicherung praktikable Unterstützung. Der Cyber-Sicherheits-Check bietet der Industrie eine dafür passende Möglichkeit und wurde mit dem Ziel entwickelt, die Cyber-Risiken schnell bewerten zu können. Der vorliegende Leitfaden hilft dem deutschen Maschinen- und Anlagenbau, auch in Zukunft sicher auf dem Weltmarkt agieren zu können. Und mit bereits über 450 ausgebildeten Personen ist der Cyber-Sicherheits-Check zudem ein gutes Beispiel für erfolgreiche Zusammenarbeit zwischen Behörden, Unternehmen und der Sicherheitswirtschaft.

Nicht zuletzt bietet zudem die vom VDMA unterstützte Allianz für Cyber-Sicherheit den Mitgliedern des VDMA ein hervorragendes Informationsnetzwerk. Gemeinsam mit Partnerverbänden aus der Industrie und dem Handwerk arbeiten wir in der Allianz und im VDMA Competence Center Industrial Security daran, unseren Beitrag für cyber-sichere Maschinen und Dienstleistungen zu leisten.

»Wir brauchen deutlich mehr Cyber-Resilienz. 100 Prozent Security gibt es nicht. Sich aber auf den Ernstfall vorzubereiten, schafft Vertrauen bei Mitarbeitern und Geschäftspartnern.«

Thilo Brodtmann
Hauptgeschäftsführer
Verband Deutscher Maschinen- und
Anlagenbau e. V.

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Die Digitalisierung prägt uns Tag für Tag: Während heute bereits zahlreiche Prozesse in unseren Institutionen automatisiert und vernetzt sind, eröffnen sich zeitgleich neue Potenziale für die IT-Projekte und Geschäftsmodelle von morgen – etwa durch das Zukunftsthema »Künstliche Intelligenz«. Die technologische Entwicklung gönnt sich keine Pause und verlangt Entscheidern, Administratoren oder auch Entwicklern vieles ab. Getrieben von dieser rasanten Geschwindigkeit dürfen Sicherheitsüberlegungen aber nicht vernachlässigt werden, schließlich regelt IT inzwischen nicht nur den Alltag in Unternehmen und Behörden, sondern auch unser aller (Über-)Leben – wie ein Blick auf die kritischen Infrastrukturen zeigt. Zukünftig wird diese Abhängigkeit durch das autonome Fahren und andere Entwicklungen weiter zunehmen. Welche Tragweite Cyber-Angriffe haben können, zeigten unter anderem die IT-Ausfälle in Krankenhäusern im September 2019. Auch der Lagebericht des BSI stellt ein hohes Gefährdungspotenzial für Privatanwender, Unternehmen und Behörden fest. Diese Bedrohungen entstehen durch immer professionellere Täter, die zum Beispiel raffinierte Schadprogramme, wie Emotet, entwickeln. Die Liste der Betroffenen ist lang, in vielen Fällen kam es zu massiven Schäden – in manchen Fällen sogar zur Geschäftsaufgabe.

Vor diesem Hintergrund muss ein fundiertes Risikomanagement heute nicht nur zum Standardrepertoire der Unternehmensführung gehören, sondern auch Cyber-Bedrohungen und Sicherheitsmaßnamen beinhalten. ISACA und BSI arbeiten bereits seit 2014 in enger Kooperation, um das Bewusstsein für Cyber-Sicherheit bei den Verantwortlichen zu schärfen und praxistaugliche Handreichungen zur Bestimmung des Status quo zu entwickeln. Dass mit diesem Dokument die zweite Auflage des Leitfadens veröffentlicht wird, ist nur einer von zahlreichen Indikatoren für den Erfolg der Zusammenarbeit. Mehr als 450 inzwischen zertifizierte Cyber Security Practitioner unterstreichen, dass der Bedarf um Cyber-Sicherheitsexperten auch in Unternehmen und Behörden immer größer wird.

Mit der neuen Auflage tragen ISACA und BSI nun dem schnellen Wandel in der Cyber-Welt Rechnung: Bereiche, wie das Thema »Cloud Computing«, haben in den vergangenen Jahren enorm an Bedeutung gewonnen und erfahren daher auch in diesem Leitfaden zusätzliche Beachtung. Gleichzeitig wurde der IT-Grundschutz wesentlich überarbeitet.

Die neuen Möglichkeiten dieser bewährten Methodik sind ebenfalls in die neue Fassung eingeflossen.

»Ich freue mich, dass Sie sich dieses Themas annehmen, und wünsche mir, dass wir Sie mit diesem Leitfaden bestmöglich bei der Optimierung Ihrer Cyber-Sicherheits-maßnahmen unterstützen können.«

Arne Schönbohm
Präsident
Bundesamt für Sicherheit in der Informationstechnik (BSI)

International Data Spaces Association e. V. (IDSA)

Daten sind der Rohstoff für Innovation – vor allem für Künstliche Intelligenz, das Internet of Things und Big Data. Damit Daten ihr Potenzial entfalten, müssen sie in unternehmens- und branchenübergreifenden Geschäftsökosystemen verfügbar gemacht und zu Datenwertschöpfungsketten verknüpft werden.

Die International Data Spaces Association (IDSA) als gemeinnützige Organisation mit über 100 Unternehmen aus 20 Ländern definiert dafür in branchenübergreifenden Arbeitsgruppen und branchenbezogenen Communitys eine Referenzarchitektur und einen formalen Standard für Datensouveränität in virtuellen Datenräumen.

Datensouveränität setzt voraus, dass Daten auf jeder Stufe der Datenwertschöpfungskette mit klar definierten Nutzungsrechten versehen sind. Dies bedarf einer technischen Infrastruktur und schließt vertragliche Regelungen ein: Datenverknüpfung oder -analyse kann unterbunden oder ermöglicht werden, Dritten kann der Zugriff auf Daten verboten oder erlaubt sein.

Um Datenräume gegen Angriffe aus dem Cyber-Raum angemessen zu schützen, sind technische und organisatorische Maßnahmen notwendig. Technisch und semantisch ermöglicht dies der Endpunkt, an dem die Daten von einem Unternehmen nach seinen Bedingungen dem Ökosystem zur Verfügung gestellt werden – der sogenannte IDS-Connector. Mit der DIN SPEC 27070 wurden die technischen Anforderungen definiert. Für die organisatorischen Anforderungen kann der entwickelte Leitfaden Cyber-Sicherheits-Check einen Einstieg speziell für mittelständische Nutzer von Datenräumen darstellen. Das pragmatische Vorgehen in Verbindung mit der Risikoanalyse und der Maßnahmenempfehlung unterstützt den Sicherheitsgedanken der IDSA.

»Wir brauchen Standards und Inspiration für sichere und vertrauenswürdige Cleanrooms für Daten, um den nächsten Schritt in der Datenwirtschaft hin zu mehr Innovation und ökonomischem Erfolg zu gehen.«

Lars Nagel
CEO
International Data Spaces Association

ISACA Germany Chapter e. V.

Das ISACA Germany Chapter e. V. ist der deutsche Zweig des weltweit führenden Berufsverbandes der IT-Revisoren, IT-Sicherheitsmanager und IT-Governance-Beauftragten. Der Verein wurde 1986 gegründet und ist mit ca. 3.000 Mitgliedern Teil des internationalen Verbandes Information Systems Audit and Control Association (ISACA), dem weltweit mehr als 140.000 Know-how-Träger in über 180 Ländern der Welt angehören.

Zweck des Vereins ist es, die Förderung der Ausbildung von Vereinsmitgliedern und Interessenten zur Verbesserung und Weiterentwicklung ihrer Fähigkeiten in Bezug auf die Prüfung, Managementberatung oder Beratung in den Bereichen IT-Governance, IT-Prüfung, Cyber-Sicherheit und interne Kontrollsysteme, dieses Wissen durch Publikationen und Seminare allen Mitgliedern und Interessenten zu vermitteln sowie die Vernetzung zwischen Mitgliedern, Unternehmen und Organisationen in diesen Bereichen zu unterstützen.

Darüber hinaus trägt der Verein zur Förderung der Attraktivität des Berufsbildes und des Nachwuchses von IT-Revisoren, IT-Sicherheitsmanagern und IT-Governance-Beauftragten bei. Die Fachgruppen bündeln die Kompetenz und das Wissen der Mitglieder des ISACA Germany Chapter und machen dieses für die Fachwelt nutzbar. Im Speziellen möchte ich mich bei den Mitgliedern der Fachgruppe Cyber Security und unseren Partnern bedanken, ohne die dieser Leitfaden nicht zustande gekommen wäre.

»Die Bedrohungen aus dem Cyber-Raum sind realer denn je. Um Cyber-Angriffen wirksam zu begegnen, ist eine intensive Kooperation von Staat, Wirtschaft und Verbänden erforderlich. Es gilt, vorhandenes Wissen zu bündeln, um angesichts neuer Angriffsszenarien vorbereitet zu sein.«

Andreas Teuscher
ISACA Germany Chapter e. V.
Leiter der Fachgruppe Cyber Security

Kooperation BSI / ISACA

Dieser Leitfaden wurde durch das ISACA Germany Chapter e. V., Ressort Vorstand für Fachgruppen und Arbeitskreise (Fachgruppe Cyber Security) gemeinsam mit Experten des BSI entwickelt.

Um die korrekte Anwendung des Leitfadens zu vermitteln, wurde vom ISACA Germany Chapter e. V. im Rahmen der Allianz für Cyber-Sicherheit *(www.allianz-für-cybersicherheit.de)* der Zertifikatskurs »Cyber Security Practitioner« *(www.cyber-security-practitioner.de)* geschaffen. Der Kurs umfasst eine Einführung in die wesentlichen Aspekte der Cyber-Sicherheit und die aktuelle Bedrohungslage sowie eine Anleitung zur praktischen Durchführung der in diesem Leitfaden beschriebenen sechs Schritte eines Cyber-Sicherheits-Checks anhand konkreter Anwendungsfälle.

Cyber-Security Practitioner

Mit diesem aktiven Partnerbeitrag dokumentiert das ISACA Germany Chapter e. V., dass es die Ziele der Allianz für Cyber-Sicherheit mit seinem guten Namen, den ihm zur Verfügung stehenden Mitteln und dem Fachwissen seiner Mitglieder unterstützt. Basierend auf diesen und weiteren Aktivitäten aus den Fachgruppen wurde das ISACA Germany Chapter 2019 zum Multiplikator in der Allianz für Cyber-Sicherheit ernannt.

Allianz für Cyber-Sicherheit

Multiplikator

Inhaltsverzeichnis

1 Einleitung

Geschäftsprozesse hängen heute wesentlich vom verlässlichen und fehlerfreien Funktionieren der Informations- und Kommunikationstechnik ab. Viele Ratingagenturen bewerten daher die Sicherheit der Informationstechnik schon als Teil der operationellen Risiken eines Unternehmens. Jedoch sind die von Cyber-Angriffen ausgehenden Bedrohungen und die durch erfolgreiche Angriffe verursachten Schäden nicht immer sofort offensichtlich. So führt z. B. der Diebstahl von Know-how durch das unberechtigte Einsehen und Kopieren von Daten nicht zu einem unmittelbaren Geschäftsausfall und wird möglicherweise erst sehr viel später erkannt.

Umfragen zufolge waren bereits über 70 % der größeren Unternehmen in Deutschland von Cyber-Angriffen betroffen. Dabei nehmen Anzahl, Komplexität und Professionalität der Angriffe kontinuierlich zu. In modernen Unternehmen mit großer Abhängigkeit von der IT kann die Unternehmenstätigkeit durch Sicherheitsvorfälle komplett und längerfristig zum Stillstand gebracht werden (siehe z. B. die Cyber-Angriffe mit WannaCry im Mai 2017 und mit NotPetya im Juni 2017) – mit allen Konsequenzen, die damit verbunden sind. Neueste Untersuchungen zeigen ebenso, dass lang anhaltende unentdeckte Angriffe (Advanced Persistent Threats – APTs) auf immer kleinere Unternehmen stark zunehmen. Eine in vielen Unternehmen immer noch verbreitete »Bisher ist ja auch nichts passiert«-Einstellung kann daher schnell zu ernsthaften Problemen führen, wenn die bestehenden Sicherheitskonzepte nicht regelmäßig und angemessen an die geänderte Bedrohungslage angepasst werden.

»Cyber-Sicherheit muss daher Chefsache sein.«

Aus diesem Grunde haben sich das Bundesamt für Sicherheit in der Informationstechnik und das ISACA Germany Chapter e. V. dazu entschlossen, Unternehmen und Behörden einen praxisorientierten Leitfaden mit entsprechender Vorgehensweise zur Beurteilung der Cyber-Sicherheit an die Hand zu geben. Der so entstandene »Cyber-Sicherheits-Check« ermöglicht es, den Status der Cyber-Sicherheit auf Basis einer Cyber-Sicherheits-Risikoeinschätzung (siehe Abschnitt 4.2, Schritt 2) zu bestimmen, um aktuellen Bedrohungen aus dem Cyber-Raum wirksam zu begegnen.

Aufgrund der Relevanz und Wichtigkeit dieses Themas sollten sich alle Ebenen, also Leitung/Management einer Institution, Information Security Manager/IT-Sicherheitsbeauftragte, Corporate Security Manager, IT-Administratoren und IT-Revisoren bis hin zum Endanwender, mit Cyber-Sicherheit befassen. Dieser Leitfaden beschreibt die strukturierte Durchführung des Cyber-Sicherheits-Checks in Unternehmen und Behörden und kann von unterschiedlichen Rollen genutzt werden:

- Verantwortlichen Managern ohne ausgewiesene Security-Kenntnisse liefert er eine Orientierungshilfe und ist die Grundlage für die Veranlassung und Beauftragung von Cyber-Security-Checks.
- IT-Sicherheitsbeauftragten und sonstigen Verantwortlichen für die Informationssicherheit wird dieser Leitfaden insbesondere dazu dienen, sich einen fachlichen Überblick über die zu adressierenden Sicherheitsaspekte zu verschaffen und sich mit dem Ablauf eines Cyber-Sicherheits-Checks vertraut zu machen.
- Revisoren und Beratern wird ein praxisnaher Handlungsleitfaden zur Verfügung gestellt, der konkrete Vorgaben und Hinweise für die Durchführung eines Cyber-Sicherheits-Checks und die Berichterstellung enthält. Die Vereinheitlichung der Vorgehensweise gewährleistet eine gleichbleibend hohe Qualität. Darüber hinaus soll hierdurch die Transparenz für Unternehmen und Behörden beim Vergleich unterschiedlicher Angebote im Rahmen der Ausschreibung und Beauftragung der Dienstleistung »Cyber-Sicherheits-Check« erhöht werden.

Die fachliche Grundlage des Cyber-Sicherheits-Checks bilden die im Rahmen der Allianz für Cyber-Sicherheit definierten »Basismaßnahmen der Cyber-Sicherheit« (siehe Kap. 7). Als besonders interessanten Mehrwert stellen BSI und ISACA darüber hinaus eine Zuordnung der zu beurteilenden Maßnahmenziele zu bekannten Standards der Informationssicherheit (IT-Grundschutz, ISO 27001, COBIT, PCI DSS) zur Verfügung. Eine Mustervorlage für einen Abschlussbericht, der in kompakter Form sowohl die festgestellten Mängel als auch Empfehlungen zum Abstellen dieser Mängel darstellt, vervollständigt die bereitgestellten Hilfsmittel zur Durchführung eines Cyber-Sicherheits-Checks.

Ein Cyber-Sicherheits-Check kann sowohl durch qualifiziertes, eigenes Personal als auch durch externe Dienstleister, die ihre Kompetenz zur Durchführung von Cyber-Sicherheits-Checks durch eine Personenzertifizierung zum »Cyber Security Practitioner« nachgewiesen haben, durchgeführt werden. Die Dauer eines Cyber-Sicherheits-Checks kann durch Anpassung der Beurteilungstiefe an die zu beurteilende Institution und die gegebenen Rahmenbedingungen von einem bis zu mehreren Tagen variiert werden.

Das Bundesamt für Sicherheit in der Informationstechnik und das ISACA Germany Chapter e. V. bedanken sich bei den Autoren der ISACA-Fachgruppe Informationssicherheit für die Erstellung der Version 1 dieses Leitfadens: Matthias Becker, Olaf Bormann, Ingrid Dubois, Gerhard Funk, Nikolai Jeliazkov, Oliver Knörle, Andrea Rupprich, Dr. Tim Sattler und Andreas Teuscher.

Für die Überarbeitung des Leitfadens in der Version 2 war die ISACA-Fachgruppe Cyber Security verantwortlich: Dr. Peter Ebinger, Martin Ennenbach, Sebastian Fritsch, Tobias Glemser, Arne Günther, Markus Lörsch, Markus J Neuhaus, Armin Nilles, Jan Oetting, Holger Pfeiffer, Peter Reiner, Jan Rozek, Dr. Tim Sattler, Dirk Schugardt, Christian Schwartz, Andreas Teuscher, Dr. Karl-Friedrich Thier, Dr. Jens Vykoukal und Gregor Wittkowski.

1.1 Der Cyber-Sicherheits-Check Version 2

Dass Cyber-Sicherheit in der digitalisierten Welt von heute die Grundlage für sichere Dienste darstellt, ist von jedem akzeptiert worden. Institutionen und Konzerne unternehmen große Anstrengungen, um ihre vernetzten Systeme und Anwendungen widerstandsfähiger gegen Cyber-Angriffe zu machen. Die Summe der Maßnahmen scheinen dabei nur mit großem Aufwand umsetzbar zu sein. Doch wie sollen mittelständische und kleine Institutionen und Firmen das anpacken. Diese Fragestellung war Ziel des Cyber-Sicherheits-Checks der Version 1. In Zusammenarbeit von BSI und ISACA wurde ein Leitfaden geschaffen, mit dem diese Zielgruppe sich mit der Cyber-Sicherheit vertraut machen und schrittweise das Sicherheitsniveau erhöhen kann. Der Zuspruch, das anhaltende Interesse und die Erfolge bei der Anwendung am Leitfaden haben die Ersteller

dazu bewogen, den Leitfaden an die neuen Gegebenheiten anzupassen. Ferner flossen die vielen hilfreichen Rückmeldungen und Verbesserungsvorschläge in die Version 2 mit ein.

Bei der Überarbeitung wurde an die Ersteller mehrfach der Wunsch herangetragen, für die Operation Technology (OT) einen vergleichbaren Leitfaden zu erstellen. Diese Idee haben wird gerne aufgenommen und werden mithilfe unserer Partner einen Leitfaden für dieses Thema entwickeln.

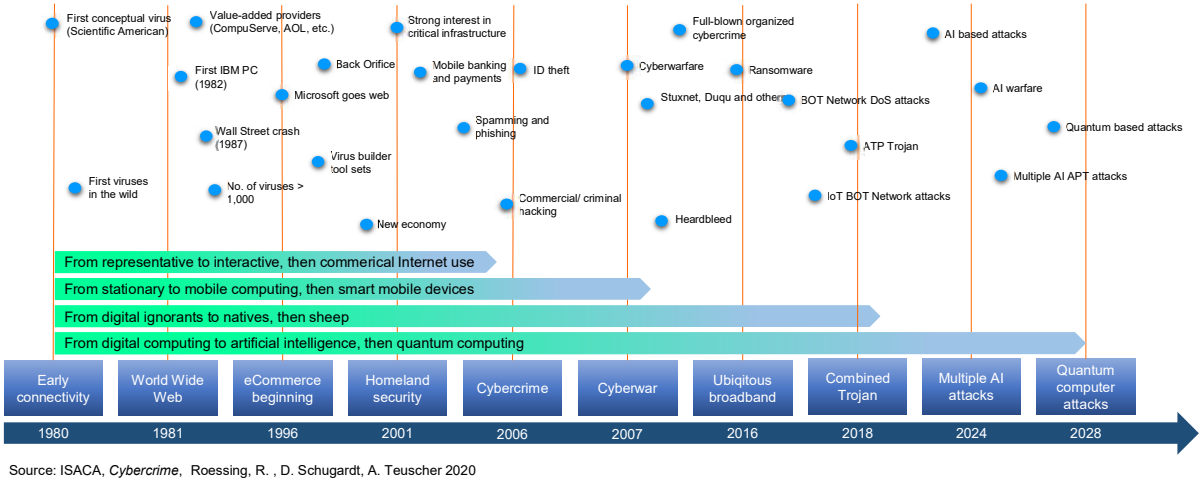
2 Einführung in die Cyber-Sicherheit

2.1 Was ist Cyber-Sicherheit?

Cyber-Sicherheit, Cyber-Angriff, Cyber-Kriminalität und Cyber-Spionage sind längst bekannte Schlagwörter in Presse und öffentlicher Diskussion. Das ist zum Teil der technischen Entwicklung geschuldet, liegt im Wesentlichen aber an der stetig steigenden Zahl von Sicherheitsvorfällen, kriminellen Handlungen und neuartigen informationsbasierten Angriffsmethoden. Der Mythos, dass es sich bei Hackern um Personen mit ausgewiesenen Spezialkenntnissen handelt, ist mittlerweile der Erkenntnis gewichen, dass hier meist organisierte und profitorientierte Organisationen und Gruppen hinter den Angriffen stehen. Folglich wird auch Cyber-Sicherheit eine immer wichtigere Facette der Informationssicherheit sein und muss von der Leitung bzw. vom Management einer Institution gezielt angegangen werden. Sie erfordert den Einsatz angemessener Ressourcen und sollte fester Bestandteil des unternehmerischen Risikomanagements sein. Die Überprüfung der vorhandenen Sicherheitsmaßnahmen auf Angemessenheit im Rahmen eines Cyber-Sicherheits-Checks kann die Institutionen und Einzelpersonen davor bewahren, Opfer eines Cyber-Angriffs, von Cyber-Kriminalität oder Cyber-Spionage zu werden.

Der Begriff »Cyber« im Kontext der Informationssicherheit erfordert jedoch eine zusätzliche Erklärung, da er oft missverstanden oder zu sehr verallgemeinert wird. Er bezieht sich auf den »Cyber-Raum« als offenen Raum, in dem informationsverarbeitende Systeme aufgestellt und miteinander verbunden sind. Im Hinblick auf diesen Leitfaden umfasst Cyber-Sicherheit die Absicherung der Schnittstellen gegen Bedrohungen aus dem Cyber-Raum zu den informationsverarbeitenden Systemen einer Institution, insbesondere der »Nahtstelle« zwischen öffentlichem Cyber-Raum und kontrollierten Unternehmensumgebungen.

In der Praxis fokussiert sich Cyber-Sicherheit meist auf fortgeschrittene und zielgerichtete Angriffe, die entsprechend schwer zu entdecken und abzuwehren sind (siehe Advanced Persistent Threats (APTs)). Cyber-Sicherheit ist somit auch ein wichtiger Teil der generellen Kriminalitätsbekämpfung, wobei die Täter bei ihren Angriffen bewusst und gezielt Informationstechnologie als Waffe einsetzen.



Source: ISACA, *Cybercrime*, Roessing, R. , D. Schugardt, A. Teuscher 2020

Abb. 2–1 Entwicklung im Cyber-Raum (nach [ISACA2])

Wie in Abbildung 2–1 dargestellt ist, hat Cyber-Sicherheit eine Geschichte, die bis in die frühen 1980er-Jahre zurückreicht, als Kriminelle begannen, technische Angriffe in Form von Hacking, Cracking und Schadprogrammen (z. B. Viren, Würmer und trojanische Pferde) auf IT-Systemen durchzuführen.

2.2 Cyber-Angriffe und Advanced Persistent Threats (APTs)

Institutionen müssen sich täglich mit IT-bezogenen Bedrohungen, Risikoszenarien und Schwachstellen auseinandersetzen. Die höchste Gefährdung für Unternehmen und Behörden sowie deren Partner stellen aktuell zielgerichtete Cyber-Angriffe durch fortgeschrittene, gut organisierte und professionell ausgestattete Angreifer dar. Diese Art der Angriffe wird häufig unter dem Begriff APT (Advanced Persistent Threat) zusammengefasst (siehe [ISACA7]). APTs sind sowohl in ihrer Vorbereitung als auch in ihrer Durchführung meist sehr komplex und werden typischerweise in mehreren Phasen vollzogen. Das Ziel eines APT ist es, möglichst lange unentdeckt zu bleiben, um über einen längeren Zeitraum sensible Informationen auszuspähen oder anderweitig Schaden anzurichten. Diese Art von Cyber-Angriffen hat häufig einen professionellen Hintergrund (z. B. Cyber-Kriminalität oder Wirtschaftsspionage), ist schwer zu detektieren und die Angreifer sind nur mit erheblichem Aufwand zu identifizieren. Abbildung 2–2 zeigt, wie sich die Bedrohungen über die Zeit entwickelt haben und welche Motivation dahinterstecken kann.

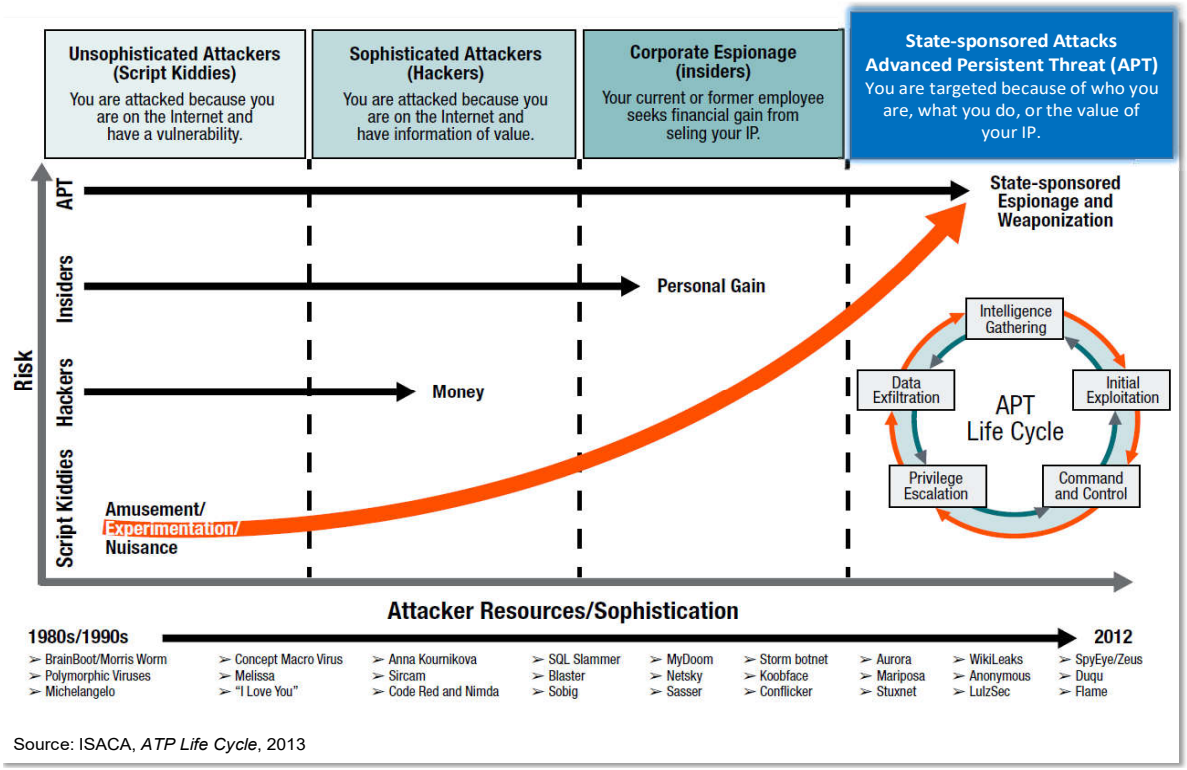


Abb. 2–2 Entwicklung der Bedrohungslandschaft (aus [ISACA7])

Der vorliegende Leitfaden und die zugrunde liegenden Maßnahmenziele für die Beurteilung der Sicherheit wurden so konzipiert, dass APT-basierte Cyber-Angriffe grundsätzlich erschwert und die Fähigkeiten zur Entdeckung eines Angriffs und zur adäquaten Reaktion gestärkt werden. Das Risiko, einem APT-basierten Cyber-Angriff zum Opfer zu fallen, kann durch die regelmäßige Durchführung eines Cyber-Sicherheits-Checks zwar nicht ganz ausgeschlossen, aber sehr stark minimiert werden. Falls eine Institution bereits Opfer eines APT-Angriffs wurde bzw. der Verdacht auf einen APT-Angriff besteht, sollten weitere Maßnahmen über denen des Cyber-Sicherheits-Check ergriffen werden.

2.3 Auswirkungen der Cyber-Kriminalität auf Institutionen und Gesellschaft

Die Bedrohungen durch Cyber-Kriminalität und Cyber-Spionage haben heute zahlreiche Auswirkungen auf die Gesellschaft, Institutionen und Betroffene. Seit 2006 kann beobachtet werden, dass sich das organisierte Verbrechen und auch staatliche Stellen damit beschäftigen, wie mögliche Ziele von Cyber-Angriffen aussehen könnten. Die Resultate waren:

- Diebstahl von vertraulichen Informationen, Produktdaten und Entwicklungen bis hin zur systematischen Spionage
- Diebstahl von geistigem Eigentum, Manipulation von Handelsgeschäften, Unterschlagung von Werten
- Finanzbetrug, Missbrauch von Kreditkarten, Fälschung und Missbrauch von Identitäten
- Sabotage von Geschäftsprozessen durch destruktive Cyber-Angriffe und Denial-of-Service-Attacken

Die Cyber-Kriminalität (Cybercrime) ist, wie der gesamte Bereich der Informationstechnik, von einer hohen Dynamik geprägt. Während die Verbrechensstatistik in vielen Bereichen eher rückläufig ist, zeigt sich bei Cybercrime im engeren Sinne ein kontinuierliches Wachstum. So wies die Polizeikriminalstatistik (PKS) beispielsweise für das Jahr 2017 insgesamt 85.960 Delikte aus. Dies bedeutete einen Anstieg gegenüber dem Vorjahr um 4,0 % (2016: 82.649). Bei der Bewertung solcher Fallzahlen ist zu berücksichtigen, dass jede rechtswidrige Handlung, unabhängig von der Anzahl der Geschädigten, immer nur als ein Fall erfasst wird. So wurde beispielsweise die Softwaremanipulation von ca. 1,3 Mio. DSL-Routern eines deutschen Internetproviders durch Malware (Mirai) im November 2016 – trotz der siebenstelligen Anzahl von Geschädigten – als nur ein Fall der Computersabotage in der PKS ausgewiesen (siehe [BKA17]).

Weiterhin ist von einer hohen Dunkelziffer auszugehen, die gar nie in Statistiken auftaucht: Gemäß einer Umfrage[1] des BSI waren im Jahr 2017 70 % der befragten deutschen Wirtschaftsunternehmen von Cyber-Angriffen betroffen. Der Großteil dieser Angriffe (57 %) sei mittels Schadsoftware durchgeführt worden. Diese Einschätzung zur Bedrohungslage wird durch den Lagebericht[2] des BSI aus 2019 gestützt.

Die Auswirkungen auf Gesellschaft, Institutionen und Betroffene sind somit immens. Und das Vermeiden des Risikos in Form einer »Nicht-Teilnahme am Cyber-Raum« ist im Zeitalter der Digitalisierung keine realistische Option mehr. Vielmehr muss die Erkenntnis erwachsen, dass jede Institution, die sich im Cyber-Raum bewegt, auch unweigerlich sol-

1. *https://www.bsi.bund.de/DE/Pressemitteilungen/Presse2018/Allianz_digitalundsicher_15022018.html*
2. *https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html*

chen Angriffen ausgesetzt ist. Die Leitung einer Institution sollte dieses Bewusstsein in ihre Risikobetrachtung mit aufnehmen und Ressourcen bereitstellen, um angemessene Schutzvorkehrungen umzusetzen.

2.4 Cyber-Sicherheitsstrategie der Bundesregierung

Der Cyber-Raum umfasst alle durch das Internet weltweit über territoriale Grenzen hinweg erreichbaren Informationsinfrastrukturen. In Deutschland nutzen alle Bereiche des gesellschaftlichen und wirtschaftlichen Lebens die vom Cyber-Raum zur Verfügung gestellten Möglichkeiten. Staat, kritische Infrastrukturen, Wirtschaft und Bevölkerung in Deutschland sind als Teil einer zunehmend vernetzten Welt auf das verlässliche Funktionieren der Informations- und Kommunikationstechnik sowie des Internets angewiesen.

Im Rahmen des Umsetzungsplans Kritische Infrastrukturen (UP KRITIS) kooperiert das BSI bereits seit 2007 intensiv mit Betreibern kritischer Infrastrukturen. Die »Cyber-Sicherheitsstrategie für Deutschland« (siehe [BMI2]), die 2011 von der Bundesregierung beschlossen und 2016 aktualisiert wurde, ermöglicht es Staat, Wirtschaft und Privatanwendern, im Rahmen ihrer jeweiligen Verantwortungsbereiche und Handlungsmöglichkeiten aktuellen und künftigen Bedrohungen aus dem Cyber-Raum begegnen zu können. Cyber-Sicherheit wird dabei durch die im Vordergrund stehenden zivilen Ansätze und Maßnahmen als Teil der gesamtstaatlichen Sicherheitsvorsorge verankert. Bei den kritischen Informationsstrukturen steht die stärkere Verzahnung von Staat und Wirtschaft auf der Grundlage eines intensiven Informationsaustausches im Mittelpunkt.

3 Grundsätze des Cyber-Sicherheits-Checks

Mithilfe eines Cyber-Sicherheits-Checks können Unternehmen und Behörden das in ihrer Institution aktuell umgesetzte Niveau der Cyber-Sicherheit bestimmen. Wie bereits aus der Informationssicherheit bekannt, muss eine solche Beurteilung auf Basis eines umfassenden und sorgfältig erstellten Rahmenwerks erfolgen, um fundierte Aussagen liefern zu können. Der vorliegende Leitfaden und die zugrunde liegenden Maßnahmenziele für die Beurteilung setzen daher auf dem bewährten Konzept der drei Verteidigungslinien auf, fokussieren sich dabei aber ganz auf den Aspekt Cyber-Sicherheit. Abbildung 3–1 zeigt beispielhaft solche Cyber-Sicherheits-relevanten Aspekte für die jeweiligen Verteidigungslinien auf.

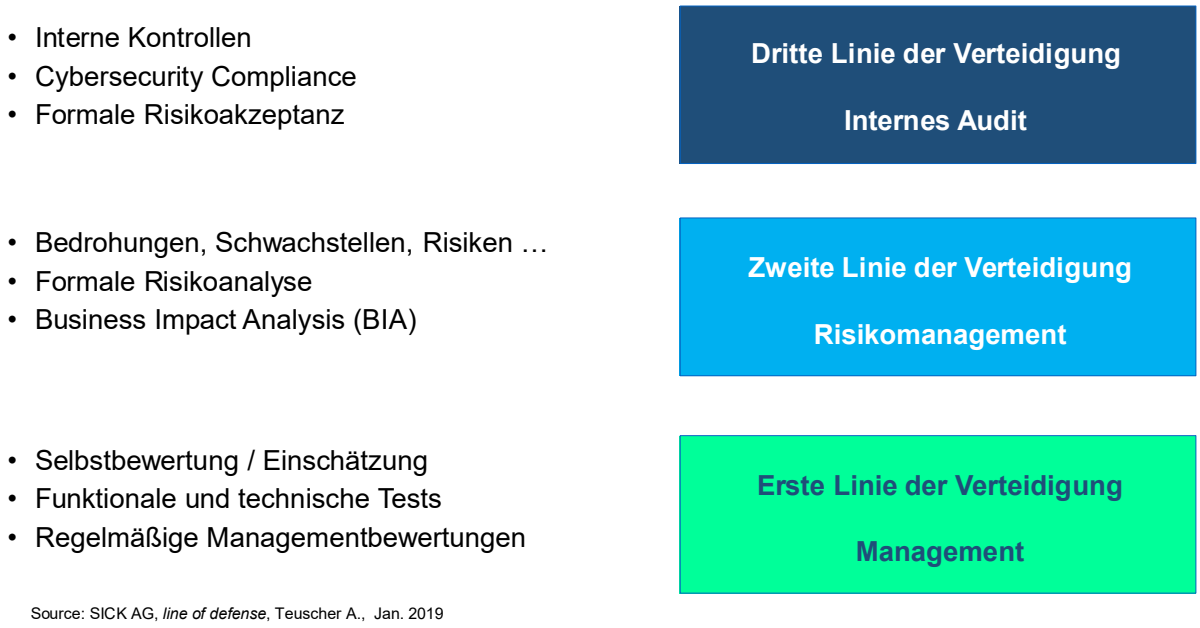


Abb. 3–1 Konzept der drei Verteidigungslinien

Eine wichtige Anforderung an die erste Verteidigungslinie – das operative Management einer Institution – ist, dass ein grundlegendes Verständnis für die Notwendigkeit von Maßnahmen zur Cyber-Sicherheit, den Schutzbedarf der Geschäftsprozesse sowie deren Abhängigkeiten und Bedrohungen vorhanden sein muss.

Innerhalb des Risiko- und Sicherheitsmanagements, das sich in der zweiten Linie befindet, sollte es dann zu einer Analyse kommen, inwieweit sich Cyber-Sicherheitsrisiken auf die Institution und deren Prozesse auswirken und mit welchen Maßnahmen dies gegebenenfalls verhindert

werden kann. Dabei prüft das Risikomanagement der Institution als erste unabhängige Instanz die Entscheidungen der Leitung/des Managements und bewertet diese, allerdings ohne eigene Entscheidungskompetenz. Die finale Entscheidung über die Umsetzung von Sicherheitsmaßnahmen verbleibt bei der Leitung/dem Management.

Die dritte Verteidigungslinie bildet die interne oder externe Prüfung, z. B. durch die IT-Revision. Hier kommt der Cyber-Sicherheits-Check zum Einsatz, durch den eine unabhängige und objektive Beurteilung des vorhandenen Sicherheitsniveaus erfolgen kann. Der Beurteiler unterstützt die Institution bei der Erreichung ihrer Ziele, indem er mit einem systematischen und zielgerichteten Ansatz die Cyber-Sicherheit in der Institution bewertet und durch seine Arbeit die Optimierung der Sicherheitsmaßnahmen fördert.

Um Vertrauen in eine objektive Beurteilung zu schaffen, müssen folgende Veraussetzungen sowohl durch Einzelpersonen als auch durch Unternehmen, die Dienstleistungen im Bereich der Cyber-Sicherheit erbringen, eingehalten werden:

- Eine formale Beauftragung des Cyber-Sicherheits-Checks durch die Institution (siehe dazu ISACA IT-Prüfungsstandard 1001 – Audit-Charter [ISACA6])
- Unabhängigkeit (siehe dazu ISACA IT-Prüfungsstandard 1002 – Organisatorische Unabhängigkeit und 1004 – Persönliche Unabhängigkeit [ISACA6])
- Rechtschaffenheit und Vertraulichkeit (siehe dazu ISACA IT-Prüfungsstandard 1005 – Berufsübliche Sorgfalt [ISACA6])
- Fachkompetenz (siehe dazu ISACA IT-Prüfungsstandard 1006 – Expertise [ISACA6])
- Nachweise und Nachvollziehbarkeit (siehe dazu ISACA IT-Prüfungsstandard 1205 – Nachweise [ISACA6])
- Objektivität und Sorgfalt (siehe dazu ISACA IT-Prüfungsstandards 1207 – Unregelmäßigkeiten und gesetzeswidrige Handlungen und 1204 – Wesentlichkeit [ISACA6])
- Sachliche Darstellung (siehe dazu ISACA IT-Prüfungsstandard 1401 – Berichterstattung [ISACA6])

Grundvoraussetzung für jede Beurteilung im Rahmen des Cyber-Sicherheits-Checks ist ein uneingeschränktes Informations- und Einsichtnahmerecht. Dies bedeutet, dass dem Beurteiler keine Informationen vorenthalten werden dürfen. Hierzu gehört auch die Einsichtnahme in sensible oder amtlich geheim gehaltene Informationen, die das Informationssicherheitsmanagement und/oder den IT-Betrieb betreffen, sofern der Beurteiler ein entsprechend berechtigtes Interesse glaubhaft machen kann. Dieser muss im letzten Fall entsprechend der »Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen« (VSA – siehe [BMI3]) bzw. dem Handbuch für den Geheimschutz in der Wirtschaft (siehe [BMWi]) sicherheitsüberprüft und ermächtigt sein. Dabei ist die Stufe der Sicherheitsüberprüfung vom Vertraulichkeitsgrad der betreffenden Informationen abhängig.

Grundlagen für den Cyber-Sicherheits-Check sind neben diesem Leitfaden die beiden BSI-Empfehlungen zur Cyber-Sicherheit »Basismaßnahmen der Cyber-Sicherheit« (siehe Kap. 7) und »Cyber-Sicherheits-Risikoeinschätzung« (siehe Abschnitt 4.2, Schritt 2). Insofern diese zu einzelnen Teilen des Beurteilungsgegenstands keine Aussage treffen, sind andere einschlägige Vorschriften, Gesetze, Standards oder Vorgaben durch Hersteller oder Berufsverbände zu verwenden. Die Nutzung dieser Regelwerke ist im Beurteilungsbericht zu dokumentieren und zu begründen.

Die Vor-Ort-Beurteilung kann sowohl von einem Beurteiler allein als auch in einem Team von mehreren Personen durchgeführt werden.

Grundsätzlich sollte bereits bei der Initiierung eines Cyber-Sicherheits-Checks beachtet werden, dass der laufende Betrieb in der Institution durch die Beurteilung nicht wesentlich gestört wird. Der Beurteiler greift niemals selbst aktiv in Systeme ein und erteilt auch keine Handlungsanweisungen zu Änderungen an IT-Systemen, Infrastrukturen, Dokumenten oder organisatorischen Abläufen. Er benötigt jeweils ausschließlich lesenden Zugriff.

4 Durchführung eines Cyber-Sicherheits-Checks

4.1 Beurteilungsgegenstand

Gegenstand eines Cyber-Sicherheits-Checks (auch CSC) ist grundsätzlich die gesamte Institution einschließlich ihrer Anbindungen an das Internet, der Anbindungen über andere Organisationseinheiten an das Internet mit Ausnahme der Operational Technology sowie aller Anbindungen an weitere Netze, wie z. B. Netze von Partnern, Dienstleistern und Kunden. Ergänzend kommt hinzu, dass auch Steuerungssysteme z. B. zur Brandmeldung, Zugangsregelung und Videoüberwachung, auch wenn sie nicht direkt über das Internet erreichbar sind, über indirekte Angriffe betroffen sind. Hier kommen manipulierte USB-Sticks und QR-Codes zum Einsatz, die dann diese Geräte veranlassen, eine Kommunikation nach außen aufzubauen. Die physische Sicherheit (Umweltereignisse, räumliche Sicherheit etc.) ist nicht Bestandteil des Cyber-Raumes und spielt daher im Cyber-Sicherheits-Check nur eine untergeordnete Rolle.

Sofern wesentliche logische IT-Systeme oder IT-Dienste von der Beurteilung ausgenommen werden, ist dies als Abgrenzung des Beurteilungsgegenstands im Beurteilungsbericht zu dokumentieren und zu begründen.

4.2 Vorgehensweise

Die Vorgehensweise zur Durchführung eines Cyber-Sicherheits-Checks wird im Folgenden schrittweise erläutert:

Schritt 1 – »Auftragserteilung«

Um eine umfangreiche und wirksame Beurteilung sicherzustellen, sollte der Auftrag zur Durchführung eines Cyber-Sicherheits-Checks durch die Leitung/das Management der betreffenden Institution erfolgen.

Es ist möglich, einen Cyber-Sicherheits-Check in jedem Umfeld und in jedem Stadium des Sicherheitsprozesses zu initiieren. Insbesondere müssen zur Durchführung eines Cyber-Sicherheits-Checks weder obligatorische Dokumente zum Sicherheitsprozess existieren, noch muss ein definierter Umsetzungsstatus bestimmter Sicherheitsmaßnahmen erreicht sein.

Schritt – 2 »Risikoeinschätzung«

Zur Bestimmung des Risikos für die zu beurteilende Institution muss vor der Vor-Ort-Beurteilung eine Risikoeinschätzung durchgeführt werden. Hierbei wird mittels Schadenshöhe und Eintrittswahrscheinlichkeit eine Risikokennzahl ermittelt. Darauf basierend können der zu erwartende Zeitaufwand, die Beurteilungstiefe sowie die Wahl der Stichproben bei der Durchführung des Cyber-Sicherheits-Checks risikoorientiert bestimmt werden.

Wurde die Risikoeinschätzung bereits durch die Institution durchgeführt, kann der Beurteiler diese ohne weitere eigene Aktivitäten übernehmen (soweit Schadenshöhe und Eintrittswahrscheinlichkeit bestimmt worden sind), wenn ihm diese nachvollziehbar und angemessen erscheint.

Sofern die Risikoeinschätzung für die betreffende Institution noch nicht durchgeführt wurde, sollte diese erstmalig durch die Institution oder in Kooperation mit dem Beurteiler nach dem nachfolgenden Schema erfolgen.

Startpunkt der Risikoeinschätzung ist die Bestimmung der Schadenshöhe für jedes Schutzziel (Vertraulichkeit, Verfügbarkeit und Integrität) anhand der nachfolgenden Tabelle 4–1.

	Vertraulichkeit	**Verfügbarkeit**	**Integrität**
Wert der Daten und Prozesse	gering 0 normal 1 hoch 2 sehr hoch 3	gering 0 normal 1 hoch 2 sehr hoch 3	gering 0 normal 1 hoch 2 sehr hoch 3
Schadenshöhe = Wert je Schutzziel			

Tab. 4–1 Bestimmung der Schadenshöhe

Als Nächstes erfolgt die Bestimmung der Eintrittswahrscheinlichkeit anhand der Tabelle 4–2.

	Vertraulichkeit		Verfügbarkeit		Integrität	
Abhängigkeit von der IT und Grad der Vernetzung (Attraktivität für Angreifer)	lokal[3] teilweise vernetzt[4] voll vernetzt[5]	1 2 3	lokal teilweise vernetzt voll vernetzt	1 2 3	lokal teilweise vernetzt voll vernetzt	1 2 3
Kompetenz (Wissen) der Angreifer	allgemein[6] moderat[7] fachspezifisch[8]	1 2 3	allgemein moderat fachspezifisch	1 2 3	allgemein moderat fachspezifisch	1 2 3
Angriffe in der Vergangenheit	abgewehrt unbekannt/ erfolgreich	1 3	abgewehrt unbekannt/ erfolgreich	1 3	abgewehrt unbekannt/ erfolgreich	1 3
Eintrittswahrscheinlichkeit = Addition der Werte je Schutzziel						

Tab. 4–2 Bestimmung der Eintrittswahrscheinlichkeit

Der Risikowert wird nun pro Schutzziel durch Multiplikation der Schadenshöhe mit der Eintrittswahrscheinlichkeit (Summe der Einzelwerte je Schutzziel) ermittelt.

3 Prozesse IT-gestützt, aber auch manuell durchführbar, nachweislich in einem geschlossenen Netz ohne Internet-Anbindung.

4 Prozesse IT-gestützt, zeitlich begrenzt manuell durchführbar, separierte Netze mit kontrolliertem Datenaustausch (Fernwartung) und begrenzter Internetnutzung (z. B. Webshop).

5 Prozesse vollständig IT-gestützt, separierte Netze mit kontrolliertem Datenaustausch (Fernwartung) und Internetnutzung (z. B. E-Mail, Internetrecherche, Einsatz von Cloud-Services, mobile Anwendungen).

6 Der Angreifer verfügt über einfaches Wissen, Ressourcen und Werkzeuge, um unautorisiert auf Daten und Prozesse zuzugreifen und diese ggf. zu verändern oder zu löschen.

7 Der Angreifer verfügt über Wissen in Bezug auf die Organisation, besitzt geeignete Ressourcen und Werkzeuge, um unautorisiert auf Daten und Prozesse zuzugreifen und diese ggf. zu verändern oder zu löschen.

8 Der Angreifer verfügt über spezifisches Wissen in Bezug auf die Organisation, besitzt umfangreiche Ressourcen und zielgerichtete Werkzeuge, um unautorisiert auf Daten und Prozesse zuzugreifen und diese ggf. zu verändern oder zu löschen.

Formel je Schutzziel (VVI):
(Abhängigkeit + Kompetenz + Angriffe) × Schadenshöhe = Risikokennzahl

Im Cyber-Sicherheits-Check wird für die Risikoeinschätzung und die weitere Bearbeitung der Maximalwert aus den drei Risikokennzahlen genutzt.

Hieraus ergeben sich die nachfolgenden Risikoeinschätzungen:

normal = 0 – 9

hoch = 10 – 18

sehr hoch = 19 – 27

Die Risikoeinschätzung (normal, hoch, sehr hoch) wird bei der Durchführung des Cyber-Sicherheits-Checks für die Beurteilung der Angemessenheit von zu bewertenden Maßnahmen innerhalb der Vor-Ort-Beurteilung (Schritt 5) und der Berichterstellung (Schritt 6) genutzt.

Schritt 3 – »Dokumentensichtung«

Die Dokumentensichtung dient dazu, einen Überblick über die Aufgaben, die Organisation und die IT-Infrastrukturen der Institution zu gewinnen. Die Dokumentensichtung beinhaltet lediglich eine grobe Sichtung der zur Verfügung gestellten Dokumente. Hierbei werden (soweit vorliegend) insbesondere das IT-Rahmenkonzept, die Liste der kritischen Geschäftsprozesse, die Sicherheitsleitlinie und das Sicherheitskonzept inklusive Netzplan beurteilt.

Sind keine ausreichend informativen Dokumente vorhanden, wird die Dokumentensichtung durch Gespräche ergänzt, in denen sich der Beurteiler den erforderlichen Überblick verschaffen kann. Auf Basis der gewonnenen Erkenntnisse bestimmt der Beurteiler risikoorientiert die Stichproben und Schwerpunkte der Beurteilung.

Schritt 4 – »Vorbereitung der Vor-Ort-Beurteilung«

Zur Vorbereitung der Vor-Ort-Beurteilung sollte ein Ablaufplan unter Einbeziehung der Cyber-Sicherheits-Risikoeinschätzung erstellt werden. Dieser gibt an, welche Inhalte wann beurteilt werden sollen und welche Ansprechpartner (Rollen/Funktionen) hierzu erforderlich sind. Der Ablaufplan ist der betreffenden Institution vorab zu übersenden.

Schritt 5 – »Vor-Ort-Beurteilung«

Die Vor-Ort-Beurteilung selbst beginnt immer mit einem kurzen Eröffnungsgespräch und endet mit einem Abschlussgespräch. Im Eröffnungsgespräch wird der Institution die Vorgehensweise und Zielrichtung des Cyber-Sicherheits-Checks erläutert. Außerdem werden organisatorische Punkte geklärt, wie z. B. Zutrittskontrolle, Besprechungsraum oder etwaige Änderungen zum Ablauf.

Im Rahmen der Vor-Ort-Beurteilung werden Interviews geführt, IT-Systeme in Augenschein genommen und evtl. weitere Dokumente gesichtet. Bei der Durchführung der Vor-Ort-Beurteilung sollten die für die jeweiligen Themen zu befragenden Ansprechpartner zur Verfügung stehen. Die zu beurteilenden Stichproben (z. B. Dokumente, IT-Systeme) und die festgestellten Sachverhalte sollten vom Beurteiler ausreichend detailliert dokumentiert werden, um diese Informationen später für die Erstellung des Berichtes angemessen verwenden zu können.

Im Abschlussgespräch, an dem auch die Leitungsebene der Institution teilnehmen sollte, wird eine erste allgemeine Einschätzung zum Niveau der Cyber-Sicherheit in der Institution gegeben. Darüber hinaus eröffnet der Beurteiler schwerwiegende Sicherheitsmängel, die die Cyber-Sicherheit der Institution unmittelbar stark gefährden und deshalb zeitnah behandelt werden sollten.

Schritt 6 – »Nachbereitung / Berichterstellung«

Der Cyber-Sicherheits-Check wird mit einem Beurteilungsbericht abgeschlossen. Der Bericht eröffnet einen Überblick zur Cyber-Sicherheit in der Institution und beinhaltet neben der Darlegung der Cyber-Sicherheits-Risikoeinschätzung eine Liste der festgestellten Mängel. Zu jedem Maßnahmenziel (siehe Kap. 7) sollte das jeweilige Beurteilungsergebnis dokumentiert werden. Im Bericht werden allgemeine Empfehlungen zur Behandlung der festgestellten Mängel aufgezeigt. Hieraus kann die beurteilte Institution entnehmen, in welchen Bereichen vermehrt Aktivitäten erforderlich sind, um das Cyber-Sicherheits-Niveau zu erhöhen.

Nähere Informationen zur Erstellung des Berichtes finden sich in Abschnitt 4.6 »Erstellung des Beurteilungsberichtes«.

Qualität der Durchführung / Personenzertifikat

Einen Cyber-Sicherheits-Check kann eine Institution sowohl durch qualifiziertes eigenes Personal als auch durch einen kompetenten Dienstleister (Mindestanforderung Cyber Security Practitioner oder äquivalente Qualifikation, z. B. CISA oder ISO 27001 Lead Auditor nativ oder auf Basis von IT-Grundschutz) durchführen lassen. In beiden Fällen ist jedoch sicherzustellen, dass die in diesem Leitfaden vorgegebene Herangehensweise genutzt wird.

4.3 Beurteilungsmethoden

Unter »Beurteilungsmethoden« werden alle für die Ermittlung eines Sachverhaltes verwendeten Handlungen verstanden. Während eines Cyber-Sicherheits-Checks können vom Beurteiler folgende Beurteilungsmethoden genutzt werden:

- Mündliche Befragung (Interview)
- Inaugenscheinnahme von IT-Systemen, Orten, Räumlichkeiten und Gegenständen
- Beobachtung (Wahrnehmungen im Rahmen der Vor-Ort-Beurteilung)
- Aktenanalyse (hierzu gehören auch elektronische Daten oder statistische Auswertungen)
- Datenanalyse (z. B. Konfigurationsdateien, Logfiles, Auswertung von Datenbanken)
- Schriftliche Befragung (z. B. Fragebogen)

Welche dieser Methoden angewendet werden, hängt vom konkreten Sachverhalt ab und ist durch den Beurteiler festzulegen. Dieser hat weiterhin zu beachten, dass in jedem Fall der Grundsatz der Verhältnismäßigkeit eingehalten wird. Für die Ermittlung eines Sachverhaltes können auch mehrere Beurteilungsmethoden kombiniert zur Anwendung kommen.

4.4 Verbindliche Maßnahmenziele

Durch die Etablierung verbindlicher Maßnahmenziele (siehe Kap. 7) soll sowohl eine gleichbleibend hohe Qualität des Cyber-Sicherheits-Checks als auch eine Vergleichbarkeit der Tätigkeit unterschiedlicher Beurteiler gewährleistet werden.

Die verbindlichen Maßnahmenziele für einen Cyber-Sicherheits-Check basieren auf den »Basismaßnahmen der Cyber-Sicherheit«.

Die Beurteilungstiefe (Intensität) wird vom Beurteiler je nach Ergebnis der Risikoeinschätzung risikoorientiert angepasst.

4.5 Bewertungsschema

Werden im Rahmen eines Cyber-Sicherheits-Checks Sicherheitsmängel festgestellt, so hat der Beurteiler spätestens bei der Berichterstellung festzulegen, wie die betreffenden Mängel in ihrer Kritikalität zu bewerten sind.

Sicherheitsmängel sind wie folgt einzuordnen:

- **»kein Sicherheitsmangel«**

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

- **»Sicherheitsempfehlung«**

  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. Auch eine voll umgesetzte IT-Sicherheitsmaßnahme kann um eine Sicherheitsempfehlung ergänzt werden.

- **»Sicherheitsmangel«**

  Bei einem »Sicherheitsmangel« liegt eine Sicherheitslücke vor, die mittelfristig behoben werden sollte. Die Vertraulichkeit, Integrität oder Verfügbarkeit der Informationen kann dadurch 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.

Sicherheitsmängel und -empfehlungen sind im Abschlussbericht so zu dokumentieren, dass die Bewertung für einen sachkundigen Dritten nachvollziehbar ist.

4.6 Erstellung des Beurteilungsberichtes

Der Beurteilungsbericht eines Cyber-Sicherheits-Checks ist der Leitung/dem Management der Institution bzw. dem Auftraggeber schriftlich bekannt zu geben. Eine Entwurfsversion des Berichtes sollte der geprüften Institution vorab übermittelt werden, um zu verifizieren, ob die festgestellten Sachverhalte (nur festgestellte Sachverhalte – ohne Bewertungen und Empfehlungen) sachlich richtig aufgenommen wurden.

Der Beurteilungsbericht besteht mindestens aus den folgenden drei Teilen:

- den Rahmendaten, inklusive detaillierter Beschreibung des Beurteilungsgegenstands,
- einer Zusammenfassung (Management Summary, einschließlich Cyber-Sicherheits-Risikoeinschätzung) sowie
- der Detailbeurteilung (ausführliche Darstellung der festgestellten Mängel, deren Bewertung und Empfehlungen zum Abstellen der Mängel).

Der Beurteilungsbericht ist als Mängelbericht ohne Würdigung positiver Aspekte zu erstellen.

Teil I – Rahmendaten

Dieser Teil enthält die organisatorischen Informationen:

- Beurteilungsgegenstand
- Abgrenzung des Beurteilungsgegenstands
- Beurteiler
- Ansprechpartner der beurteilten Institution
- Beurteilungsgrundlagen
- zeitlicher Ablauf
- Verteiler für den Beurteilungsbericht
- Rahmendaten des Beurteilungsdokuments bzw. der Dokumentenlenkung
  - Dateiname
  - Druckdatum
  - Dokumentenstatus

Teil II – Management Summary

Dieser Teil enthält eine Zusammenfassung für das Management. In knapper, verständlicher Form sollten die wesentlichen Mängel und daraus hervorgehende Empfehlungen zusammengefasst werden.

- Summary
- Cyber-Sicherheits-Risikoeinschätzung
- Übersicht der Beurteilungsergebnisse (für alle Maßnahmenziele)

Teil III – Detailbeurteilung je Maßnahmenziel

Dieser Teil des Berichtes beinhaltet die ausführliche Darstellung der beurteilten Themenfelder, die festgestellten Mängel, deren Bewertung sowie Empfehlungen zum Abstellen der bemängelten Sachverhalte. Bei der Bewertung der festgestellten Mängel ist das in Abschnitt 4.5 dargestellte Schema zu verwenden.

- Maßnahmenziel (siehe Kap. 7)
- Ergebnis einschließlich Bewertung
- Stichprobe(n)
- Beschreibung festgestellter Mängel inkl. Maßnahmenempfehlung(en)

Formale Aspekte zum Abschlussbericht

Bei der Erstellung des Beurteilungsberichtes sind folgende formale Aspekte zu berücksichtigen:

- Die Seitenkennzeichnung muss so gestaltet sein, dass jede Seite eindeutig identifiziert werden kann (z. B. mit Seitennummer sowie Versionsnummer, Bezeichnung und Datum des Berichtes).
- Verwendete Fachbegriffe oder Abkürzungen, die nicht allgemein gebräuchlich sind, müssen in einem Glossar bzw. Abkürzungsverzeichnis zusammengefasst werden.
- Der Bericht muss die geprüften Organisationseinheiten und die Empfänger des Berichtes eindeutig bezeichnen sowie etwaige Verwendungsbeschränkungen vermerken.
- Der Bericht ist durch den Beurteiler zu unterschreiben.
- Form und Inhalt eines Berichtes können je nach Art der in Auftrag gegebenen Beurteilungsarbeiten unterschiedlich sein, jedoch sind für den Cyber-Sicherheits-Check die Mindestanforderungen an den Beurteilungsbericht (siehe dieses Kapitel) sowie der ISACA IT-Prüfungsstandard 1401 (siehe [ISACA6]) einzuhalten.

Ein Musterbericht für einen Cyber-Sicherheits-Check findet sich auf den Webseiten der Allianz für Cyber-Sicherheit (siehe [ACS2]).

5 Glossar und Begriffsdefinition

Die folgenden Begrifflichkeiten werden in diesem Dokument verwendet:

APT (Advanced Persistent Threat) bezeichnet einen sehr komplexen, zielgerichteten, aufwendig vorbereiteten und durchgeführten Cyber-Angriff (siehe auch Kapitel 2.2).

Beurteiler ist eine Person, die einen Cyber-Sicherheits-Check auf Basis dieses Leitfadens durchführt.

BSI (Bundesamt für Sicherheit in der Informationstechnik) ist der zentrale IT-Sicherheitsdienstleister der Bundesverwaltung.

CPE (Continuing Professional Education) ist ein Maß für die Erbringung von kontinuierlicher beruflicher Weiterbildung.

CSP (Cyber Security Practitioner) ist ein Zertifikat der ISACA. Um die Kenntnis der wesentlichen Prinzipien der Cyber-Sicherheit und der Durchführung von Cyber-Sicherheits-Checks nach außen hin zu dokumentieren, bietet die ISACA interessierten Teilnehmern eine eintägige Fortbildung zum Thema Cyber-Sicherheit. Nach erfolgreichem Ablegen einer Prüfung kann ein Zertifikat als »Cyber Security Practitioner« erlangt werden. Das Zertifikat ist 3 Jahre lang gültig und kann durch Durchführungsnachweise (Bestätigung durch den Arbeitgeber oder Kunden, dass 6 Begutachtungen durchgeführt wurden oder 3 Begutachtungen und 24 CPE erlangt wurden) in diesem Zeitraum erneuert werden.

Cyber-Kriminalität bezeichnet kriminelle Aktivitäten, die den Cyber-Raum als Quelle, Ziel und/oder Werkzeug nutzen.

Cyber-Raum umfasst alle durch das Internet über territoriale Grenzen hinweg weltweit erreichbaren Informationsinfrastrukturen.

Cyber-Sicherheit verfolgt den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen gegen Bedrohungen aus dem Cyber-Raum.

DoD steht für Denial of Service also die »Verweigerung eines Internetdienstes«, der eigentlich verfügbar sein sollte.

Institution wird als Oberbegriff für Behörden, Unternehmen und sonstige öffentliche oder private Organisationen verwendet.

ISACA (Information Systems Audit and Control Association) ist der Berufsverband der IT-Revisoren, IT-Sicherheitsmanager und IT-Governance-Beauftragten.

IT ist die bisher im Vordergrund stehende Informationstechnologie, die für Bürokommunikation, Verwaltung, aber auch unternehmensweite Ressourcensteuerung etc. verwendet wird.

KRITIS (Kritische Infrastrukturen) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Leitung/Management wird als Begriff für Vorstand, Geschäftsführer, Behördenleitung verwendet.

Maßnahmenziele sind für die Beurteilung relevante Aspekte und Fragestellungen der Cyber-Sicherheit. Hierzu gehören Themen des Sicherheitsmanagements genauso wie technische Aspekte.

NIST ist das National Institute of Standard and Technology mit Sitz in den USA.

OT ist die »Operational Technology«. Es handelt sich um Hard- und Software, die dazu dient, Produktionsprozesse zu steuern und zu überwachen (angelehnt an NIST).

Risikoeinschätzung wird mittels Schadenshöhe und Eintrittswahrscheinlichkeit ermittelt. Über die Risikokennzahl und somit Risikohöhe können die Gefahr für das Unternehmen und somit der zu erwartende Zeitaufwand, die Beurteilungstiefe sowie die Wahl der Stichproben bei der Durchführung des Cyber-Sicherheits-Checks bestimmt werden.

VVI bezeichnet als Abkürzung die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität.

Whistleblower (auch »Enthüller«, »Skandalaufdecker« oder »Hinweisgeber«) ist eine Person, die für die Allgemeinheit wichtige Informationen aus einem geheimen oder geschützten Zusammenhang an die Öffentlichkeit bringt.

Alle Personalbegriffe in diesem Dokument beziehen sich in gleicher Weise auf Frauen und Männer. Wird im Text die männliche Form verwendet, geschieht dies ausschließlich aus Gründen der leichteren Lesbarkeit.

6 Literaturverzeichnis

[ACS1] Allianz für Cyber-Sicherheit, Webauftritt, *www.allianz-fuer-cybersicherheit.de*

[ACS2] Allianz für Cyber-Sicherheit, »Musterbericht für den Cyber-Sicherheits-Check«, *www.allianz-fuer-cybersicherheit.de*

[BKA17] Bundeskriminalamt, Bundeslagebild Cybercrime 2017, *www.bka.de*

[BMI1] Bundesministerium des Innern, Nationaler Plan zum Schutz der Informationsinfrastrukturen in Deutschland, Umsetzungsplan KRITIS (UP-KRITIS), September 2007, *www.bmi.bund.de*

[BMI2] Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland, November 2016, *www.bmi.bund.de/cybersicherheitsstrategie*

[BMI3] Bundesministerium des Innern, Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen, Juni 2006, *www.verwaltungsvorschriften-im-internet.de*

[BMWi] Bundesministerium für Wirtschaft und Technologie, Handbuch für den Geheimschutz in der Wirtschaft, November 2004, *www.bmwi.de*

[BSI1] Bundesamt für Sicherheit in der Informationstechnik, Informationssicherheitsrevision – Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz, März 2010, *www.bsi.bund.de*

[ISACA1] ISACA Germany Chapter e. V., Webauftritt, *www.isaca.de*

[ISACA2] ISACA, Transforming Cybersecurity Using COBIT 5, 2013, *www.isaca.org/cobit5*

[ISACA3] ISACA, Berufs-Ehrenkodex, 2013, *www.isaca.org*

[ISACA4] ISACA, COBIT® 5 for Information Security, *www.isaca.org/cobit5*

[ISACA5] ISACA, Responding to Targeted Cyberattacks, *www.isaca.org*

[ISACA6] ISACA, IS Auditing Standard zum kostenlosen Download unter *www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Pages/Standards-for-IS-Audit-and-Assurance-German.aspx*

[ISACA7] ISACA, Advanced Persistent Threats: How to Manage the Risk to Your Business, 2013, *www.isaca.org/apt-book*

7 Maßnahmenziele

Die nachfolgend aufgeführten Maßnahmenziele A bis N sind bei der Durchführung eines Cyber-Sicherheits-Checks verbindlich zu beurteilen. Die Reihenfolge der Maßnahmenziele ist dabei nicht als Priorisierung oder zwingende Abfolge bei der Beurteilung anzusehen, sondern dient lediglich der Strukturierung.

Zur Beurteilung eines Maßnahmenziels sind mindestens die zu dem jeweiligen Maßnahmenziel zugehörigen Basismaßnahmen heranzuziehen.

Die Stichproben für die Vor-Ort-Beurteilung sind nach einem risikoorientierten Ansatz zu prüfen. Detaillierte Hinweise zur Durchführung eines Cyber-Sicherheits-Checks finden sich in Kapitel 4.

Maßnahmenziele		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 Netzstrukturaufnahme müssen Abwehrmaßnahmen für alle internen und externen Netzübergänge sowie die entsprechenden Prozesse (wie z. B. ein Change Management) geplant und umgesetzt werden.	- 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 Server-systemen findet eine technische Schnittstellenkontrolle statt, die eine zulässige Nutzung kontrolliert und eine unzulässige Nutzung verhindert. - Zugänge mobiler IT-Geräte 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.	**BSI IT-Grundschutz-Kompendium 2/2020:** OPS.1.2.4, OPS.1.2.5, OPS.2.1, OPS.2.2, OPS.3.1, SYS.3.2.1, SYS.3.2.2, SYS.3.2.3, SYS.3.2.4, SYS.4.3, SYS.4.4, NET.1.1, NET.1.2, NET.2.1, NET.2.2, NET.3.1, NET.3.2, NET.3.3, IND.1.A16 **COBIT 2019:** DSS05.02, DSS05.03, DSS06.06 **ISO/IEC 27001:2013:** A.6.2.1, A.6.2.2, A.9.1.2, A.13.1.1, A.13.1.2, A.13.1.3 **PCI DSS 3.2.1 :** 1.1.1, 1.1.2, 1.1.4, 1.1.6, 1.1.7, 1.2.1, 1.2.3, 1.3.1, 1.3.3, 1.4, 2.2.2, 2.2.4, 2.3

Maßnahmenziele		Basismaßnahmen	Referenzen
B	**Abwehr von Schadprogrammen** Im Sinne einer gestaffelten Verteidigung gegen Angriffe durch Schadprogramme (Viren, Würmer und trojanische Pferde) muss die Abwehr über eine große Zahl von IT-Systemen einschließlich der Sicherheitsgateways verteilt werden. Der eigentliche Client als Arbeitsplatzsystem ist dabei die letzte Verteidigungslinie.	- Schutzsoftware gegen Schadprogramme kommt durchgängig zum Einsatz und wird fortlaufend aktuell gehalten. - Verteilt über die verschiedenen IT-Systeme kommen mehrere Lösungen möglichst unterschiedlicher Anbieter und Technologien zum Einsatz (gestaffelte Verteidigung). - IT-Systeme ohne angemessenen Schutz vor Schadprogrammen, sind in speziellen Netzsegmenten isoliert.	**BSI IT-Grundschutz-Kompendium 2/2020:** OPS.1.1.2, OPS.1.1.3, OPS.1.1.4, SYS.1, SYS.2, SYS.3, IND.1.A12 **COBIT 2019:** DSS05.01 **ISO/IEC 27001:2013:** A.12.2.1 **PCI DSS 3.2.1:** 5.1, 5.2

Maßnahmenziele		Basismaßnahmen	Referenzen
C	**Inventarisierung der IT-Systeme** Zur Planung und anschließenden Umsetzung von Abwehrmaßnahmen auf den eingesetzten IT-Systemen ist eine vollständige Inventarisierung der eingesetzten IT-Systeme notwendig. Mithilfe dieses Inventarverzeichnisses ist insbesondere zu klären, welche verschiedenen Systemtypen in der Organisation im Einsatz sind.	- Bestand an Hard- und Software ist vollständig inventarisiert und wird fortlaufend aktualisiert. - Versionen und Patchstände von Betriebssystemen und Anwendungen werden regelmäßig aufgenommen. - Es existieren automatisierte Verfahren zur Erkennung nicht autorisierter IT-Systeme und Anwendungen.	**BSI IT-Grundschutz-Kompendium 2/2020:** ORP.1, SYS.1.5.A10, IND.1.A4, IND.1.A5, CON.4, CON.5, OPS.1.1.6, ORP.1.A7, ORP.1.A8 **COBIT 2019:** APO01.07, BAI03.04, BAI09.01, BAI09.03, BAI09.05 **ISO/IEC 27001:2013:** A.8.1.1, A.8.1.2, A.8.1.3, A.8.1.4 **PCI DSS 3.2.1:** 2.4, 9.7, 11.1, 12.3.3, 12.3.4

Maßnahmenziele		Basismaßnahmen	Referenzen
D	**Vermeidung von ausnutzbaren Sicherheitslücken** Um das Risiko erfolgreicher Cyber-Angriffe zu minimieren, müssen ausnutzbare Sicherheitslücken konsequent vermieden werden. Vorhandene Sicherheitsmechanismen von Betriebssystemen sollten daher genutzt werden. Verfügbare Sicherheitsaktualisierungen von genutzter Software müssen zeitnah getestet und anschließend installiert werden. Ein wirksamer Change-Management-Prozess sollte etabliert werden.	- Ein effizienter Prozess zum Schwachstellen- und Patchmanagement ist etabliert. - Im Rahmen der Softwareplanung wird die Nutzung stärkerer Abwehrmechanismen in aktuellerer Software gefördert. - Bekannte Sicherheitslücken werden kurzfristig durch Workarounds und bereitgestellte Sicherheitsaktualisierungen geschlossen. - Betriebssysteme, Serverdienste und Anwendungen werden vor Inbetriebnahme gehärtet. - Ein Prozess zur sicheren Softwareentwicklung ist etabliert. - Bei der Beschaffung neuer Hard- und Software werden Sicherheitsanforderungen berücksichtigt.	**BSI IT-Grundschutz-Kompendium 2/2020:** ISMS.1, OPS.1.1.2, OPS.1.1.3, OPS.1.1.4, OPS.1.1.6, SYS.1, SYS.2, SYS.3, APP.1, APP.2 APP.3, APP.4, APP.5, IND.1.A17, NET.3.2.A11, **COBIT 2019:** APO12.01, BAI02.01, BAI10.02, BAI10.03, BAI10.05, DSS05.03, DSS05.07 **ISO/IEC 27001:2013:** A.9.4.4, A.12.1.2, A.12.5.1, A.12.6.1, A.14.1.1, A.14.2.2, A.14.2.3, A.14.2.4 **PCI DSS 3.2.1:** 2.2, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7

Maßnahmenziele		Basismaßnahmen	Referenzen
E	**Sichere Interaktion mit dem Internet** Alle Vorgänge, bei denen Daten und Dienste aus dem Internet abgefragt und verarbeitet werden, sind mit geeigneten Maßnahmen abzusichern. Die jeweilige Stärke der eingesetzten Schutzmechanismen muss dem Schutzbedarf der auf dem jeweiligen IT-System verarbeiteten Daten sowie den einem Angreifer zur Verfügung stehenden möglichen Weiterleitungs-mechanismen gerecht werden.	- Der Browser inklusive aller Erweiterungen (Flash, Java, ActiveX usw.) verfügt über starke Sicherheitseigenschaften und ist bei einem hohen Cyber-Sicherheits-Risiko besonders abgeschottet (z. B. Sandbox). - Eingehender E-Mail-Verkehr wird zentral auf Bedrohungen, wie Schadprogramme und Phishing-Angriffe, untersucht. - Für die Darstellung von Dokumenten aus externen Quellen werden sichere Darstellungsoptionen verwendet. - Unerwünschte aktive Inhalte werden zentral gefiltert. - Apps und andere Internetanwendungen sind durch geeignete Schutzmechanismen abgesichert. - Es existieren verbindliche Vorgaben zur sicheren Nutzung von Cloud-Services und anderen Diensten im Internet.	**BSI IT-Grundschutz-Kompendium 2/2020:** CON.7.A8, CON.7.A14, OPS.1.2.4.A7, NET.1.2.A13, ORP.4.A22, ORP.4.A23 **COBIT 2019:** BAI10.02, BAI10.03, BAI10.05, DSS05.01 **ISO/IEC 27001:2013:** A.13.2.1, A.13.2.2, A.13.2.3, A.13.2.4 **PCI DSS 3.2.1:** 1.1, 1.4, 4.1, 6.6, A1

Maßnahmenziele		Basismaßnahmen	Referenzen
F	**Logdatenerfassung und -auswertung** Oftmals bleiben Sicherheitsvorfälle unerkannt, weil kurzfristig kein sichtbarer oder offensichtlicher Schaden eintritt. Mithilfe eines gut getarnten und hinreichend vorsichtigen Vorgehens ist es Angreifern aber u. U. möglich, über längere Zeiträume die Kontrolle über Zielsysteme zu übernehmen, ohne dass diese Angriffe unmittelbar aufgrund singulärer Ereignisse detektiert werden. Daher ist es notwendig, ebenfalls Verfahren zur Aufdeckung von nicht offensichtlichen Sicherheitsvorfällen und langfristig angelegten Angriffen zu entwickeln.	- Relevante Logdaten werden zusätzlich zur Umsetzung einschlägiger gesetzlicher, regulatorischer und organisatorischer Anforderungen auch mit dem Ziel der Angriffsdetektion erfasst und regelmäßig ausgewertet. - Die Nutzung privilegierter Konten und administrativer Zugriffe wird fortlaufend überwacht. - Logdaten sind angemessen vor Manipulation und Zerstörung geschützt, z. B. durch Auslagerung auf zentrale Log-Management-Server.	**BSI IT-Grundschutz-Kompendium 2/2020:** OPS.1.1.5, DER.1.A6, DER.1.A7, DER.1.A8, DER.1.A9, DER.1.A10, DER.1.A11, DER.1.A12, DER.1.A13, DER.1.A14, DER.1.A15, DER.1.A16, DER.1.A17, DER.1.A18, IND.1.A10, IND.1.A15 **COBIT 2019:** APO11.04, DSS05.04, DSS05.07 **ISO/IEC 27001:2013:** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4 **PCI DSS 3.2.1:** 10.1, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.4, 10.5, 10.6

Maßnahmenziele		Basismaßnahmen	Referenzen
G	**Sicherstellung eines aktuellen Informationsstands** Die Fähigkeit zur Planung wirksamer Cyber-Sicherheits-Maßnahmen wird im Wesentlichen durch die Qualität und den Umfang des eigenen Informationsstands bestimmt. Daher muss die Versorgung mit aktuellen und fachlich verlässlichen Informationen zur Cyber-Sicherheit sichergestellt werden.	- Aktuelle Informationen zur Cyber-Sicherheit werden fortlaufend aus verlässlichen Quellen bezogen und ausgewertet. - Cyber-Sicherheits-Maßnahmen werden regelmäßig auf der Basis vorhandener Informationen hinsichtlich ihrer Wirksamkeit überprüft und angepasst.	**BSI IT-Grundschutz-Kompendium 2/2020:** ISMS.1 IND.1.A1, ORP.4.A4 **COBIT 2019:** APO12.01, APO13.02, DSS04.02, DSS05.01 **ISO/IEC 27001:2013:** A.6.1.1, A.6.1.2, A.6.1.4, A.16.1.3 **PCI DSS 3.2.1:** 6.1, 6.2

Maßnahmenziele		Basismaßnahmen	Referenzen
H	**Bewältigung von Sicherheitsvorfällen/ Notfällen** Geeignete Prozesse und Verfahren zur Bewältigung von Sicherheitsvorfällen sind zu etablieren und zu üben, um eine schnelle und angemessene Bewältigung von Sicherheitsvorfällen und damit die Aufrecht-erhaltung des Geschäftsbetriebs sicherzustellen.	- Es existieren etablierte Prozesse und Verfahren zur schnellen und angemessenen Bewältigung von Sicherheitsvorfällen. - Die Bewältigung von Sicherheitsvorfällen wird regelmäßig geübt. - Abgeschlossene Sicherheits-vorfälle werden hinsichtlich der Ursachen und möglicher Konsequenzen ausgewertet. - Sicherheitsvorfälle werden zur Strafverfolgung und Lagebild-erstellung an die zuständigen Behörden gemeldet.	**BSI IT-Grundschutz-Kompendium 2/2020:** IND.1.A13, IND.2.7.A5, NET.2.1.A8, NET.2.2.A4, NET.3.2.A12, ORP.1.A10, OPS.1.1.2.A2, OPS.2.1.A14, DER.2.1.A1, DER.2.1.A2, DER.2.1.A3, DER.2.1.A4, DER.2.1.A5, DER.2.1.A6, DER.2.1.A7, DER.2.1.A8, DER.2.1.A9, DER.2.1.A10, DER.2.1.A11, DER.2.1.A13, DER.2.1.A14 **COBIT 2019:** APO12.06, DSS02.02, DSS02.04, DSS04.03 **ISO/IEC 27001:2013:** A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.17.1.1, A.17.1.2, A17.1.3, A.17.2.1 **PCI DSS 3.2.1:** 11.1.2, 12.5.3, 12.10, A1.4

Maßnahmenziele		Basismaßnahmen	Referenzen
I	**Sichere Authentisierung** Zur sicheren Authentisierung von Benutzern sollten komplexe Passwörter und/oder Multifaktor-Authentisierungsverfahren genutzt werden. Authentisierungsdaten für Bereiche unterschiedlichen Schutzbedarfs sollten voneinander getrennt werden.	- Der Zugang zu kritischen Ressourcen wird durch den Einsatz von Multifaktor-Authentisierungsverfahren abgesichert. - Authentisierungsdaten für Bereiche unterschiedlichen Schutzbedarfs sind voneinander getrennt, z. B. Konten von Administratoren und anderen Nutzern. - Es werden nur sichere Authentisierungsprotokolle eingesetzt. - Authentisierungsdaten wie z. B. Passwort-Hashes oder private Schlüssel werden angemessen geschützt.	**BSI IT-Grundschutz-Kompendium 2/2020:** ORP.4.A9, ORP.4.A10, ORP.4.A12, ORP.4.A13, ORP.4.A21 **COBIT 2019:** DSS05.04, DSS06.03 **ISO/IEC 27001:2013:** A.9.1.1, A.9.1.2, A.9.2.4, A9.3.1, A.9.4.2, A.9.4.3, A.9.4.4 **PCI DSS 3.2.1:** 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.8

Maßnahmenziele		Basismaßnahmen	Referenzen
J	**Gewährleistung der Verfügbarkeit notwendiger Ressourcen** Zur wirksamen Abwehr von Bedrohungen der Cyber-Sicherheit sollten ausreichend eigene finanzielle und personelle Ressourcen bereitgestellt und bei Bedarf auf qualifizierte externe Dienstleister zurückgegriffen werden.	- Finanzielle und personelle Ressourcen zur Abwehr von Bedrohungen der Cyber-Sicherheit stehen ausreichend zur Verfügung. - Bei Bedarf werden qualifizierte und zuverlässige externe Dienstleister eingebunden. - Datensicherungen und Wiederherstellungstests müssen regelmäßig durchgeführt werden.	**BSI IT-Grundschutz-Kompendium 2/2020:** ISMS.1.A1, ISMS.1.A2, ISMS.1.A3, ISMS.1.A4, ISMS.1.A5, ISMS.1.A6, ISMS.1.A8, ISMS.1.A15, OPS.1.1.2.A9, OPS.1.1.2.A10 **COBIT 2019:** APO07.01, APO10.02, APO14.01, APO14.10, DSS4.07 **ISO/IEC 27001:2013:** A.6.1.1, A.2.1.2, A.7.2.1 **PCI DSS 3.2.1:** 6.4.5.4, 12.10.1
Maßnahmenziele		**Basismaßnahmen**	**Referenzen**
K	**Sensibilisierung und Schulung von Mitarbeitern** Auch das eigene Personal muss in den Mittelpunkt einer Cyber-Sicherheitsstrategie gerückt werden. Sämtliche technischen Vorkehrungen können durch menschliche Fehler oder bewusste Fehlhandlungen unwirksam werden.	- Anwender und IT-Personal werden zielgruppenorientiert regelmäßig für die Gefahren eines Cyber-Angriffs sensibilisiert und hinsichtlich des korrekten Verhaltens geschult. - IT-Personal und Management sind mit ihren Rollen und Verantwortlichkeiten vertraut. - Es ist eine klare Rollentrennung vorhanden. Eine Konzentration zu vieler Zuständigkeiten in einer Rolle wird vermieden.	**BSI IT-Grundschutz-Kompendium 2/2020:** ISMS.1.A8, ISMS.1.A9, ISMS.1.A14, ORP.1.A1, ORP.1.A2, ORP.1.A6, OPS.1.1.2.A10 **COBIT 2019:** APO07.02, APO07.03, APO13.02, DSS05.01, DSS05.04, DSS06.03 **ISO/IEC 27001:2013:** A.6.1.1, A.7.2.2, A8.1.2 **PCI DSS 3.2.1:** 6.4.2, 7.1, 7.2, 12.6

Maßnahmenziele		Basismaßnahmen	Referenzen
L	**Sichere Nutzung sozialer Netze** Die Sensibilisierung von Mitarbeitern muss insbesondere das Verhalten in sozialen Netzen in Form verbindlicher Vorgaben (Social Media Guidelines) und Aufklärungsmaßnahmen umfassen.	- Es existieren verbindliche Vorgaben (Social Media Guidelines) hinsichtlich des sicheren und seriösen Auftritts der Organisation sowie der beruflichen Profile der Beschäftigten in sozialen Netzwerken. - Mitarbeiter werden regelmäßig hinsichtlich der Risiken und des korrekten Verhaltens in sozialen Netzwerken sensibilisiert. - Direkte Schnittstellen zwischen sozialen Netzwerken und der organisationseigenen Infrastruktur, sofern vorhanden, sind angemessen abgesichert.	**BSI IT-Grundschutz-Kompendium 2/2020:** APP.1.4.A2, CON.9.A1, CON.9.A2, CON.9.A3, CON.9.A4 **COBIT 2019:** APO07.03 **ISO/IEC 27001:2013:** A.7.2.2, A.8.1.3, A.8.2.3, A.13.2.1, A.13.2.2, A.13.2.3 **PCI DSS 3.2.1:** n. a.

Maßnahmenziele		Basismaßnahmen	Referenzen
M	**Durchführung von Penetrationstests** Es sollten regelmäßige Penetrationstests von qualifizierten und erfahrenen Personen, die nicht an der Planung oder Implementierung der zu beurteilenden IT-Systeme beteiligt waren, durchgeführt werden.	- Um die technische Maßnahmenwirksamkeit zu prüfen und zu bestätigen, werden regelmäßig Penetrationstests von qualifizierten Personen durchgeführt. - Umfang und Intensität der Penetrationstests sind der Cyber-Sicherheits-Risiko-einschätzung angemessen. - Die Ergebnisse von Penetrationstests werden konsequent zur Reduzierung von Risiken genutzt.	**BSI IT-Grundschutz-Kompendium 2/2020:** OPS.1.1.6.A14 **COBIT 2019:** APO12.01, APO13.02, DSS05.02 **ISO/IEC 27001:2013:** A.14.2.8, A.18.2.1, A.18.2.3 **PCI DSS 3.2.1:** 11.3, A3.2.4

Maßnahmenziele		Basismaßnahmen	Referenzen
N	**Sicherer Umgang mit Cloud-Anwendungen** Es sollten regelmäßig die genutzten Cloud-Anwendungen überprüft werden und einem Freigabeprozess unterliegen. Nicht zulässige Cloud-Anwendungen sollten gesperrt, erlaubte durch geeignete Sicherheitsmaßnahmen geschützt werden.	- Es existieren verbindliche Vorgaben hinsichtlich der Speicherung, Verwendung und Verarbeitung von Daten in Cloud-Anwendungen. - Anwendbare Sicherheitsstandards und vertragliche Anforderungen werden gegenüber dem Cloud Service Provider durchgesetzt. - Cloud-Dienste werden fachgerecht provisioniert, administriert und überwacht. - Mitarbeiter werden regelmäßig hinsichtlich der Risiken und des korrekten Umgangs mit Cloud-Anwendungen sensibilisiert. - Direkte Schnittstellen zwischen Cloud-Anwendungen und der organisationseigenen Infrastruktur, sofern vorhanden, sind angemessen abgesichert.	**BSI-Standard 200-2 V1.0:** Kapitel 10.1.1, insbesondere 10.1.3 **BSI IT-Grundschutz-Kompendium 2/2020:** OPS.2.1.A1, OPS.2.1.A3, OPS.2.1.A4, OPS.2.1.A5, OPS.2.1.A6, OPS.2.1.A7, OPS.2.1.A8, OPS.2.1.A9, OPS.2.1.A10, OPS.2.1.A11, OPS.2.1.A12, OPS.2.1.A13, OPS.2.1.A15 **COBIT 2019:** APO07.03, APO09.01, APO09.02, APO09.03, DSS01.02, DSS01.03, DSS05.02, DSS06.03 **ISO/IEC 27001:2013:** A.15.1.1, A15.1.2, A15.1.3, A15.2.1, A15.2.2, A.18.2.1, A.18.2.2, A.18.2.3 **PCI DSS 3.2.1:** 2.6, 12.8, A1

ISACA Germany Chapter e. V.
Storkower Straße 158
D-10407 Berlin

www.isaca.de
info@isaca.de