Brockmann & Büchner

IT-Sicherheit im Unternehmen

KRITIS als Chance nutzen

Brockmann & Büchner PartG
Unternehmensberatung
Hohe Bleichen 8
20354 Hamburg

Telefon: +49 (0) 40 59 4666 93
Mail: kontakt@2bic.de

Der Krieg in der Ukraine zeigt, dass Kriege nicht mehr nur in Schützengraben ausgetragen werden. Im virtuellen Raum werden immer ausgefeiltere Angriffsvektoren genutzt, mit dem Ziel weitreichende Auswirkungen für Unternehmen und ganze Volkswirtschaften herbeizuführen.

Das Bundesamt für Sicherheit in der Informationstechnik (kurz: BSI) bietet grundsätzlich jedem Unternehmen, das erste Maßnahmen für mehr Cyber-Sicherheit umsetzen möchte, Empfehlungen und Unterstützung an (siehe bsi.bund.de).
Für Unternehmen, die zu der kritischen Infrastruktur in Deutschland gehören, bleibt es jedoch nicht nur bei Empfehlungen.

Diese KRITIS-Unternehmen tragen nach Ansicht der Bundesregierung eine relevante Verantwortung im staatlichen Gemeinwesen, da sie die Grundversorgung der Bevölkerung mit Gütern und Dienstleistungen gewährleisten. Mit den gesetzlichen Vorgaben werden damit besondere IT-Sicherheitsanforderungen an Betreiber in den Branchen Energie, Transport und Verkehr, Gesundheit, Ernährung und Wasserversorgung gestellt, die über definierten Schwellenwerten liegen.

Hierzu hat die Bundesrepublik Deutschland 2015 das IT-Sicherheitsgesetz und die KRITIS-Verordnung 1.0 erlassen.

Mit Inkrafttreten des erneuerten IT-Sicherheitsgesetztes (IT-SiG2.0) im Jahr 2021 wurden die Schwellwerte, die definieren welche Unternehmen zu den Betreibern kritischer Infrastrukturen gehören, heruntergesetzt und ausgeweitet. Dies bewirkt, dass neue gesetzliche Pflichten auf Unternehmen zukommen, die erstmals über den Schwellwerten liegen. Betreiber dieser Unternehmen müssen sich von diesem Zeitpunkt an mit Themen wie der §8a-Prüfung, Risiko Assessments, Maßnahmenumsetzung, Nachweisen und Co. auseinandersetzen. Betroffene Unternehmen müssen nun technische und organisatorische Maßnahmen zur langfristigen Reduzierung von Informationssicherheitsrisiken gemäß dem „Stand der Technik“ definieren, umsetzen und deren Umsetzung regelmäßig gegenüber dem BSI nachweisen.

Gleichzeitig steigt auch die Zahl der möglichen Bedrohungsszenarien (z.B. Social Engineering), die jedes Unternehmen – unabhängig von gesetzlichen Anforderungen – betreffen.

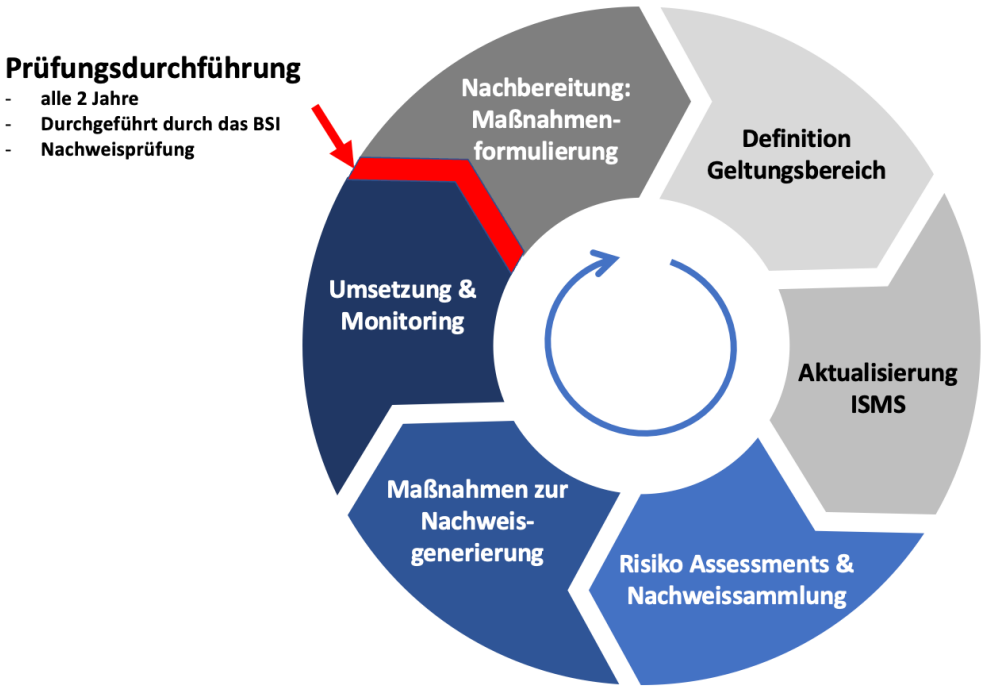
Es empfiehlt sich daher, dass auch nicht-KRITIS-Unternehmen die gesetzlichen Vorgaben als Leitplanken nutzen, um entsprechende Maßnahmen und Strukturen einzuführen, die das Unternehmen in Bezug auf Informationssicherheit für die Zukunft rüsten.

Betreiber, die erstmalig von der KRITIS-Verordnung betroffen sind, stehen nun zwar vor einer neuen Herausforderung, jedoch lässt der Gesetzgeber bei der Umsetzung der Anforderungen auch Freiräume zu. Hiermit kann die Erfüllung der gesetzlichen Anforderungen in Einklang mit den Unternehmenszielen gebracht werden. Bereits in der Prüfungsvorbereitung existieren relevante Stellhebel, die signifikante Auswirkungen auf den Aufwand zur Erfüllung der gesetzlichen Anforderungen haben.
Wir kennen diese Stellhebel und helfen Ihnen bei der richtigen Nutzung, um den Aufwand mit Augenmaß zu reduzieren.

Die §8a-Prüfung
Der §8a des BSI-Gesetzes verpflichtet KRITIS-Betreiber dazu, alle 2 Jahre eine Prüfung durchzuführen, um den Status Quo bei der Umsetzung der IT-Sicherheit gemäß „Stand der Technik“ nachzuweisen. Hiermit soll die Sicherstellung der kritischen Dienstleistung entlang der relevanten Schutzziele (Auswahl aus Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit) gewährleistet werden.
Bei der Prüfung handelt es sich um eine Nachweisprüfung, die eigenständig gegenüber dem zertifizierten §8a-Prüfer und dem BSI erbracht werden muss. Der Nachweis erfolgt durch Dokumentationsprüfung und örtliche Begehung. Insbesondere Dokumentnachweise sind mit Planung im Voraus vorzubereiten.

Prüfungsroadmap

Die Roadmap der Vorbereitung auf die §8a-Prüfung sieht vor, dass (KRITIS-)Unternehmen ihre kritische Dienstleistung, sowie Prozesse, Systeme und Komponenten zur Erbringung der kritischen Dienstleistung erfassen und anhand dessen den Geltungsbereich definieren. Das Ergebnis wird in einem s.g. Geltungsbereichsdokument festgehalten, das als Basis für die spätere Prüfung dient. In den folgenden Schritten werden diese Prozesse, Systeme und Komponenten hinsichtlich der Risiken für die kritische Dienstleistung analysiert. Auf Basis der Risiken werden dann Maßnahmen abgeleitet, welche die KRITIS-relevanten Prozesse, Systeme und Komponenten dem Stand der Technik mit Augenmaß annähern.
Ziel ist es, mit jedem Prüfzyklus die Informationssicherheit zu steigern und kontinuierlich weiterzuentwickeln. Hierzu müssen alle relevanten Risiken identifiziert, bewertet und mit Maßnahmen behandelt werden. Deren Wirksamkeit muss anschließend zum nächsten Prüfzyklus hin überprüft und nachgewiesen werden.



Definition des Geltungsbereiches (GBD)

Um sich zunächst einen Überblick über die aktuelle Lage des Unternehmens und das Ausmaß der notwendigen und beeinflussbaren Elemente zu verschaffen, werden die Rahmenbedingungen des Unternehmens, die bestehenden Anforderungen, die Unternehmensstruktur sowie der Status Quo der Informationssicherheit und die IT Governance des Unternehmens betrachtet.
Anschließend werden die kritischen Dienstleistungen identifiziert und beschrieben, sowie die dafür unmittelbar notwendigen Prozesse ermittelt. Schließlich können die für diese Prozesse notwendigen Systeme und Anlagen (mit Blick auf Anlagenkategorien KRITIS-V) identifiziert und nachvollziehbar für Dritte beschrieben werden.
Ziel ist die Auswahl eines kleinen, aber gezielten Geltungsbereiches, der sich eng an den KRITIS-Anforderungen, den eigenen Anlagen und Strukturen sowie den eigenen Schutzzielen orientiert.
Bei den Schutzzielen ist zudem zu definieren, welche Schutzziele als relevant angesehen werden und ob sich diese von denen der KRITIS-Verordnung, nämlich hauptsächlich dem Schutzziel der Verfügbarkeit, abgrenzen lassen. Dies dient schließlich zur Definition der Prüfungsgrundlage.

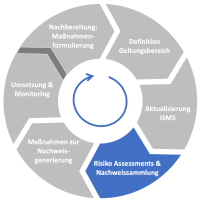
Mit Abschluss der Definition des Geltungsbereiches erfolgt die Anmeldung der Anlagen gemäß KRITIS-Verordnung beim BSI.
Die Verantwortung für die Anmeldung liegt hierbei beim Unternehmen. Auf Basis des Prüftermins kann ein Zeitplan erstellt werden, der regelmäßig zu überwachen ist. Anschließend wird ein zertifizierter Prüfer ausgewählt und auch mit diesem der Zeitplan für die Prüfung abgestimmt.

Das Informationssicherheits-Management System (ISMS)

Eine wichtige Grundlage beim Aufbau der Informationssicherheit ist die Aufstellung von Verfahren und Regeln zur Steuerung und Aufrechterhaltung der Informationssicherheit. Dies wird im Rahmen eines Informationssicherheits-Managementsystems (ISMS) definiert und festgehalten.
Allgemein bietet ein ISMS gemäß der DIN EN ISO/IEC 27001 die Grundlage zur Spezifikation von Standards für die Informationssicherheit. Ein solches Managementsystem nach Stand der Technik ist für KRITIS-Betreiber verpflichtend.
Wenn noch kein ISMS vorhanden ist, ist der Aufbau eines Kern-ISMS für den KRITIS-relevanten Teil (zuvor definierter Geltungsbereich) umzusetzen. Hierzu sind im ersten Schritt die Verantwortlichkeiten zu definieren und konkrete verantwortliche Personen zu benennen. Anschließend sind die entsprechenden Prozesse zu definieren. Dabei kommt es oft vor, dass die Strukturen gemäß ISMS in der Praxis bereits grundsätzlich gelebt werden. Sie müssen jedoch dokumentiert und standardisiert werden.
Wenn bereits ein ISMS vorhanden ist, wird geprüft, ob es den Geltungsbereich abdeckt und wird bei Bedarf entsprechend angepasst.

Ein frühzeitiger Beginn der Vorbereitung ist zudem wichtig, da zunächst die Implementierung des Kern-ISMS erfolgen muss, um die entsprechenden Nachweise zu identifizieren oder zu erstellen.

Durchführung von Risiko Assessments & Erfassung vorhandener Nachweise



Nachdem das ISMS als Grundlage implementiert wurde, werden Risiko Assessments für die Systeme aus dem Geltungsbereich durchgeführt, um vorhandene Nachweise zu erfassen. Risk Assessments werden hierbei durch Interviews mit den Fachverantwortlichen entlang einem definierten Anforderungskatalog durchgeführt. Das Ziel ist es hierbei den Erfüllungsgrad der BSI-Anforderungen zu ermitteln und bei nicht umgesetzten Anforderungen potenzielle Risiken zu bewerten. Bei diesem Vorgehen werden automatisch die notwendigen Nachweise für die §8a-Prüfung identifiziert bzw. generiert.

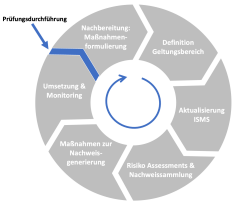
Maßnahmen und Aktivitäten definieren

Im nächsten Schritt können anhand der identifizierten Risiken passende Maßnahmen abgeleitet werden. Diese sollten risikoorientiert priorisiert werden. Die notwendigen Aktivitäten zur Umsetzung der Maßnahmen müssen dann definiert werden, um die fehlenden Nachweise zu erhalten bzw. um die Sicherheitslücken zu schließen

Umsetzung planen, umsetzen & monitoren

Wie Sie die Maßnahmen planen, koordinieren, umsetzen und monitoren, können Sie in einem weiteren Whitepaper nachlesen. Hier werden die Erfolgsfaktoren für die Umsetzung von IT-Security-Maßnahmen vorgestellt, die erfahrungsgemäß die optimale Planung, Durchführung und Dokumentation erzielen.

Prüfungsdurchführung



Die Grundmenge der zu prüfenden Systeme wird durch das eingereichte Geltungsbereichsdokument definiert. Dieses Geltungsbereichsdokument wird im ersten Schritt durch die Prüfer auf Nachvollziehbarkeit und ausreichende Breite des Geltungsbereichs untersucht. Hieraus werden die zu prüfenden Systeme abgeleitet und die Anfrage zur Einreichung der Nachweise wird an den KRITIS-Betreiber übermittelt. Anschließend wird das ISMS und eine Auswahl der Vorgaben auf Systemebene anhand der bereitgestellten Nachweise geprüft. Die Umsetzung dieser Vorgaben wird anschließend durch eine Vor-Ort-Prüfung hinsichtlich ihrer Wirksamkeit geprüft.
Besonders bei großen Unternehmen mit mehreren Standorten ist die Besichtigung aller Systeme oft nicht gewinnbringend, da einheitliche Vorgaben für mehrere Standorte gelten und eine Stichprobe somit repräsentativ ist.
Aus diesem Grund muss im Voraus geprüft werden, ob der Nachweis durch eine Stichprobe angemessen ist.

Umgang mit Feststellungen und Definition von Maßnahmen

Ergebnis der Prüfung ist ein Prüfbericht mit Feststellungen zu Schwachstellen und resultierenden Risiken. Hierzu müssen passende Maßnahmen durch den KRITIS-Betreiber aufgestellt werden und mit einem Fälligkeitsdatum versehen werden. Bei einer sorgfältigen Durchführung der Risiko Assessments sind diese Maßnahmen bereits definiert und befinden sich zum Zeitpunkt der Prüfung in Umsetzung. Der Prüfbericht ist zusammen mit der Liste der Maßnahmen rechtzeitig beim BSI einzureichen.

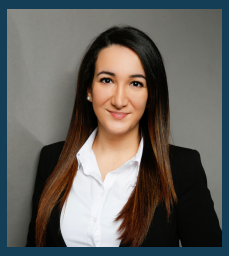
Nach der Prüfung ist vor der Prüfung

Die Prüfungsergebnisse bilden die Basis für die weiteren Aktivitäten bis zum Beginn der nächsten Prüfung, die ca. 1,5 Jahre nach Abschluss der letzten Prüfung beginnt. So wird bei jeder Prüfung auch die Weiterentwicklung des ISMS und die wirksame Umsetzung der Maßnahmen überwacht. Allen Beteiligten ist von Beginn an transparent zu kommunizieren, dass die Umsetzung der KRITIS-Verordnung kein einmaliges Projekt, sondern ein kontinuierlicher Prozess ist.

Kraft auf die Strecke bei Informationssicherheit

Brockmann & Büchner PartG hat bereits große Konzerne mit komplexer Technik- und Prozesslandschaft auf die §8a-Prüfung vorbereitet, diese begleitet und die Umsetzung von mehr als 400 KRITIS-Maßnahmen koordiniert.
Wir unterstützen Sie bei der Definition und Beschreibung des richtigen Geltungsbereiches und der Implementierung eines passenden ISMS zur strukturierten Erfassung und Behandlung von Risiken.
Wir verfügen über übergreifendes Fachwissen, Erfahrung zur Vorbereitung und Begleitung der Nachweisprüfung und stehen Ihnen entlang des gesamten Prozesses zur Seite.
Gemeinsam bringen wir beim Thema Informationssicherheit Kraft auf die Strecke!

Autoren



Sarah Tok

ist Managementberaterin bei Brockmann & Büchner mit Spezialisierung auf IT-Sicherheits- und Transformationsthemen.
E-Mail: tok@2bic.de

Jan Albert

Ist Teamleiter bei Brockmann & Büchner mit Spezialisierung auf IT-Sicherheits- und Projektmanagementthemen
E-Mail: albert@2bic.de

Quellen sowie weitere Informationen zum Nachlesen:

[1] https://www.bsi.bund.de/DE/Home/home_node.html
[2] https://www.bsi.bund.de/DE/Das-BSI/Auftrag/BSI-Gesetz/bsi-gesetz_node.html