Handlungsleitfaden zum NIS2UmsuCG für kleine und mittlere Unternehmen

Dieses Dokument dient als Orientierungshilfe für kleine und mittlere Unternehmen (KMU) und wurde im Rahmen einer Masterarbeit zum Thema „Auswirkungen der NIS-2-Richtlinie auf kleine und mittlere Unternehmen: Analyse der Anforderungen und Entwicklung von Empfehlungen“ erstellt. Als Grundlage dient der Referentenentwurf zum deutsche NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz vom 22.07.2024, welches die Anforderungen der europäischen NIS-2-Richtlinie in nationales Recht überführt.

Die NIS-2-Richtlinie und demnach das NIS2UmsuCG stellen Anforderungen an die Risikomanagementmaßnahmen aller Einrichtungen, die in deren Anwendungsbereich liegen. Dieser Handlungsleitfaden zeigt verschiedene Optionen auf die Anforderungen an die Risikomanagementmaßnahmen umzusetzen. Des Weiteren werden Registrierungs-, Unterrichtungs- und Meldepflichten gesetzlich vorgeschrieben. Dieser Handlungsleitfaden erklärt, wie diese umzusetzen sind und was dabei beachtet werden muss.

Der Handlungsleitfaden fokussiert sich auf Lösungen und Maßnahmen, die möglichst geringe Kosten verursachen, allerdings in Teilen technische Expertise voraussetzen. Für jeden Punkt besteht die Möglichkeit, dass Unternehmen die Anforderungen über Fremdbeauftragungen umsetzen lassen. Es wird davon ausgegangen, dass explizit kleine Unternehmen nicht die finanziellen Mittel besitzen, um alle Anforderungen über externe Beauftragungen abzudecken, weshalb ein Interesse an kostenloser Software und frei verfügbaren Handlungsleitfäden besteht.

Ist mein Unternehmen betroffen?

Um diese Frage zu beantworten, kann der Entscheidungsbaum in Abbildung 1 verwendet werden. Dieser bietet die Unterscheidung zwischen besonders wichtigen Einrichtungen und wichtigen Einrichtungen, da die gesetzlichen Anforderungen diese differenziert betrachten. Die Sektoren und Branchen aus den Anlagen des NIS2UmsuCG sind in Tabelle 1 und Tabelle 2 aufgeführt. Die Definitionen der Branchen sind den Anlagen des NIS2UmsuCG zu entnehmen. [1]

Die folgenden Pflichten gelten pauschal für alle Unternehmen, die vom NIS2UmsuCG betroffen sind. Zusätzliche Pflichten für besonders wichtige Einrichtungen sind als solche gekennzeichnet. Betreiber kritischer Anlagen werden gemäß des neuen Dachgesetz zur kritischen Infrastruktur (KRITIS-DachG) ermittelt und müssen weitere Anforderungen erfüllen. Der aktuelle Entwurf findet sich hier.[2]

[1] Siehe www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/nis2umsucg.html
[2] Siehe www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KRITIS-DachG.html

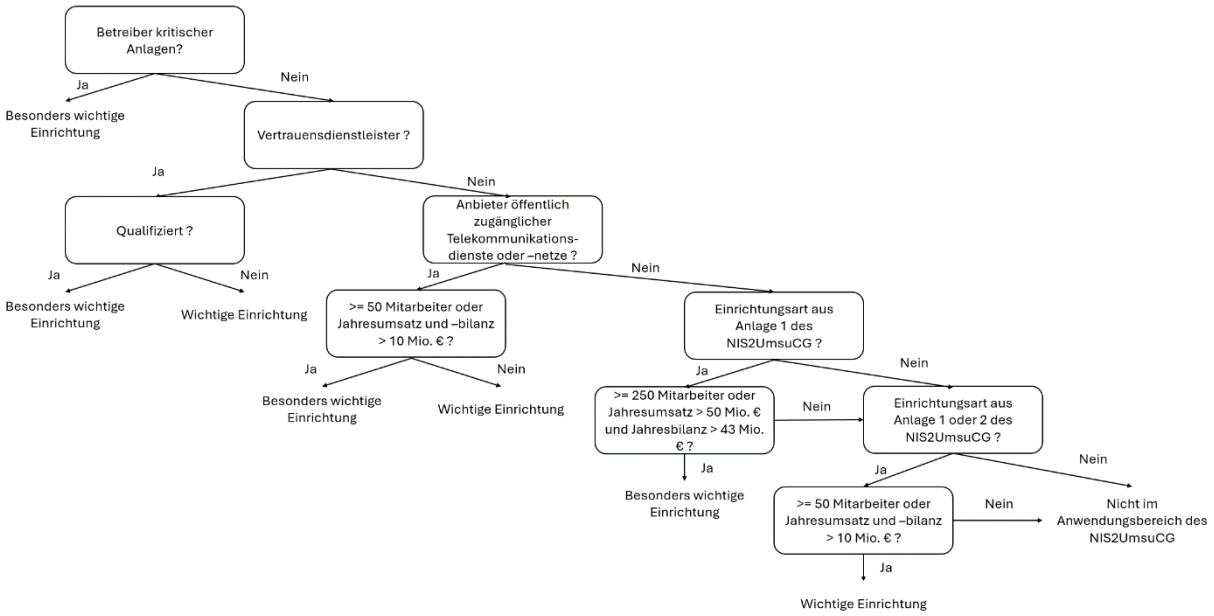

Abbildung 1: Anwendungsbereich NIS2UmsuCG

Sektor	**Branche**
Energie	Stromversorgung
	Fernwärme und -kälte
	Kraftstoff- und Heizölversorgung
	Gasversorgung
Verkehr	Luftverkehr
	Schienenverkehr
	Schifffahrt
	Straßenverkehr
Finanz- und Versicherungswesen	Bankwesen
	Finanzmarktinfrastruktur
Gesundheit	
Wasser	Trinkwasserversorgung
	Abwasserbeseitigung
Informationstechnik und Telekommunikation	
Weltraum	

Tabelle 1: Sektoren und Branchen aus Anlage 1 des NIS2UmsuCG

Sektor	**Branche**
Transport und Verkehr	Post- und Kurierdienste
Abfallwirtschaft	
Produktion, Herstellung und Handel mit chemischen Stoffen	
Produktion, Verarbeitung und Vertrieb von Lebensmitteln	
Verarbeitendes Gewerbe / Herstellung von Waren	Herstellung von Medizinprodukten und In-vitro-Diagnostika
	Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen
	Herstellung von elektrischen Ausrüstungen
	Maschinenbau

	Herstellung von Kraftwagen und Kraftwagenteilen
	Sonstiger Fahrzeugbau
Anbieter digitaler Dienste	
Forschung	

Tabelle 2: Sektoren und Branchen aus Anlage 2 des NIS2UmsuCG

Registrierungspflichten

Die Registrierung muss bis zum 01.01.2025 abgeschlossen sein. Das Registrierungsverfahren wird durch das BSI auf deren Internetseite[3] kommuniziert. Für die Registrierung werden folgende Informationen benötigt:

- Name des Unternehmens unkl. Rechtsform und Handelsregisternummer
- Anschrift
- Aktuelle Kontaktdaten (E-Mail, öffentliche IP-Adressbereiche und Telefonnummer)
- NIS2UmsuCG relevanter Sektor und / oder Branche
- Mitgliedsstaaten der EU, in denen die Dienste der obigen Sektoren und / oder Branche erbracht werden
- Zuständige Aufsichtsbehörden des Bundes und der Länder

Betreiber kritischer Anlagen müssen des Weiteren folgendes melden:

- Kritische Dienstleistung
- IP-Adressbereiche der von ihnen betriebenen kritischen Anlagen
- Anlagenkategorie
- Ermittelte Versorgungskennzahlen
- Standort der Anlagen
- Eine jederzeit erreichbare Kontaktstelle

Unterrichtungspflichten

Das BSI kann im Falle eines meldepflichtigen Sicherheitsvorfall, der im folgenden One-Pager beschrieben wird, besonders wichtige und wichtige Einrichtungen dazu verpflichten, Empfänger ihrer Dienste über jenen Sicherheitsvorfall zu unterrichten, selbst wenn die Dienste noch nicht beeinträchtigt sind, es aber sein könnten. Die sicherste und einfachste Option ist die Kommunikation des Sicherheitsvorfalls auf der Internetseite der Einrichtung.

Für Unternehmen aus den Sektoren Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, Verwaltung von IKT-Diensten und Digitale Dienste gelten weitere Pflichten. Diese müssen allen potenziell betroffenen Empfänger ihrer Dienste alle Maßnahmen und Abhilfemaßnahmen mitteilen, die die Empfänger vor der Bedrohung schützen könnte. Diese Unternehmen informieren die Empfänger ebenfalls über erhebliche Cyberbedrohungen selbst.

Die Unterrichtungspflicht gilt nur dann, wenn in Abwägung der Interessen der Einrichtung und des Empfängers die Interessen des Empfängers überwiegen.

[3] Siehe www.bsi.bund.de

Meldepflichten

Die Meldepflichten gelten für alle wichtigen und besonders wichtigen Einrichtungen. Es müssen alle erheblichen Sicherheitsvorfälle gemeldet werden. Als solcher klassifiziert sich jeder Vorfall, der einen der folgenden Punkte erfüllt oder erfüllen könnte:

- ☐ Schwerwiegende Betriebsstörung der Dienste
- ☐ Finanzieller Verlust
- ☐ Beeinträchtigt natürliche oder juristische Personen durch materielle oder immaterielle Schäden

Spezifischere Definitionen werden durch Durchführungsverordnungen erwartet, von welchen aktuell lediglich Entwürfe existieren. Der genaue Ablauf des Meldeverfahrens wird durch das BSI auf deren Internetseite veröffentlicht. Die Inhalte der Meldungen stehen bereits fest:

1. Innerhalb der ersten **24 Stunden nach Kenntnisnahme** muss eine Frühwarnung übermittelt werden:
    a. Besteht Verdacht auf rechtswidrige oder böswillige Handlungen?
    b. Sind grenzüberschreitende Auswirkungen zu erwarten?

    Übermittelt am _____ durch _____.
2. Innerhalb der ersten **72 Stunden nach Kenntnisnahme** muss eine Meldung über den erheblichen Sicherheitsvorfall erstellt werden:
    a. Die die Informationen aus der Frühmeldung aktualisiert
    b. Eine erste Bewertung des Sicherheitsvorfalls inkl. Schweregrad und die Auswirkungen enthält
    c. Soweit vorhanden Kompromittierungsindikatoren überliefert

    Übermittelt am _____ durch _____.
3. Auf Ersuchen eines CSIRT oder der zuständigen Behörde, muss **jederzeit** ein Zwischenbericht über relevante Statusaktualisierungen übermittelt werden
    Übermittelt am _____ durch _____.
    Übermittelt am _____ durch _____.
    Übermittelt am _____ durch _____.
4. Dauert der Sicherheitsvorfall länger als einen Monat an, muss **jeden Monat** ein Fortschrittsbericht übermittelt werden
    Übermittelt am _____ durch _____.
    Übermittelt am _____ durch _____.
    Übermittelt am _____ durch _____.
5. Spätestens **einen Monat nach Übermittlung der Meldung** beziehungsweise **nach abschließender Bearbeitung des andauernden Sicherheitsvorfalls** muss ein Abschlussbericht übermittelt werden. Dieser muss Folgendes enthalten:
    a. eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und Auswirkungen;
    b. Angaben zur Art der Bedrohung bzw. zugrunde liegende Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;
    c. Angabe zu den getroffenen und laufenden Abhilfemaßnahmen;
    d. wenn gegeben die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.

    Übermittelt am _____ durch _____.

Meldepflichten für Betreiber kritischer Anlagen

Die Meldepflichten gelten für alle wichtigen und besonders wichtigen Einrichtungen. Es müssen alle erheblichen Sicherheitsvorfälle gemeldet werden. Als solcher klassifiziert sich jeder Vorfall, der einen der folgenden Punkte erfüllt oder erfüllen könnte:

- ☐ Schwerwiegende Betriebsstörung der Dienste
- ☐ Finanzieller Verlust
- ☐ Beeinträchtigt natürliche oder juristische Personen durch materielle oder immaterielle Schäden

Spezifischere Definitionen werden durch Durchführungsverordnungen erwartet, von welchen aktuell lediglich Entwürfe existieren. Der genaue Ablauf des Meldeverfahrens wird durch das BSI auf deren Internetseite veröffentlicht. Die Inhalte der Meldungen stehen bereits fest:

1. Innerhalb der ersten **24 Stunden nach Kenntnisnahme** muss eine Frühwarnung übermittelt werden:
    a. Besteht Verdacht auf rechtswidrige oder böswillige Handlungen?
    b. Sind grenzüberschreitende Auswirkungen zu erwarten?
    c. Art der betroffenen Anlage
    d. Art der betroffenen Dienstleistung
    e. Auswirkungen des Sicherheitsvorfalls auf die Dienstleistung

    Übermittelt am _____ durch _____.
2. Innerhalb der ersten **72 Stunden nach Kenntnisnahme** muss eine Meldung über den erheblichen Sicherheitsvorfall erstellt werden:
    a. Die die Informationen aus der Frühmeldung aktualisiert
    b. Eine erste Bewertung des Sicherheitsvorfalls inkl. Schweregrad und die Auswirkungen enthält
    c. Soweit vorhanden Kompromittierungsindikatoren überliefert

    Übermittelt am _____ durch _____.
3. Auf Ersuchen eines CSIRT oder der zuständigen Behörde, muss **jederzeit** ein Zwischenbericht über relevante Statusaktualisierungen übermittelt werden
    Übermittelt am _____ durch _____.
    Übermittelt am _____ durch _____.
    Übermittelt am _____ durch _____.
4. Dauert der Sicherheitsvorfall länger als einen Monat an, muss **jeden Monat** ein Fortschrittsbericht übermittelt werden
    Übermittelt am _____ durch _____.
    Übermittelt am _____ durch _____.
    Übermittelt am _____ durch _____.
5. Spätestens **einen Monat nach Übermittlung der Meldung** beziehungsweise **nach abschließender Bearbeitung des andauernden Sicherheitsvorfalls** muss ein Abschlussbericht übermittelt werden. Dieser muss Folgendes enthalten:
    a. eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und Auswirkungen;
    b. Angaben zur Art der Bedrohung bzw. zugrunde liegende Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;
    c. Angabe zu den getroffenen und laufenden Abhilfemaßnahmen;
    d. wenn gegeben die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.

    Übermittelt am _____ durch _____.

Anforderungen an Risikomanagementmaßnahmen

Während die Melde-, Registrierungs- und Unterrichtungspflichten durch organisatorische Maßnahmen mit einem sehr geringen Aufwand erfüllt werden können, benötigt es mehr Zeit und Ressourcen zur Erfüllung der Risikomanagementmaßnahmen des NIS2UmsuCG. Das Ziel dieser Maßnahmen ist wie folgt definiert:

> *„Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten.“*

Alle Maßnahmen müssen den Stand der Technik einhalten und einschlägige europäische und internationale Normen berücksichtigen, weshalb der folgende Handlungsleitfaden auf der ISO 27000er Reihe und ISO 22301, dem NIST Cybersecurity Framework (CSF) und Special Publication 800-53, dem Entwurf des technischen Regulierungsstandard der Europäischen Aufsichtsbehörde und dem aktuellen BSI-Standard 200 basiert. Um die Maßnahmen zu ordnen, werden die Funktionen des NIST Cybersecurity Framework (CSF) genutzt, welche in Abbildung 2 zu sehen sind. Der folgende Handlungsleitfaden basiert auf der Annahme eines kritischen Geschäftsprozesses, wie es bei kleinen Unternehmen der Fall ist. Mittlere Unternehmen können den Handlungsleitfaden pro kritischen Geschäftsprozess anwenden, wobei darauf geachtet werden sollte, dass die technischen Lösungen möglichst standardisiert werden, um Kosten zu sparen. Die verpflichtenden Maßnahmen werden als Checklisten mit Kästchen in den folgenden Abschnitten dargestellt.

Abbildung 2: CSF-Funktionen

Identifizieren von Risiken

Um das Thema Risikomanagementmaßnahmen gemäß NIS2UmsuCG anzugehen, wird ein Auftakt-Workshop empfohlen. Da die Maßnahmen das gesamte Unternehmen betreffen, sollte dieser von der Geschäftsleitung und den leitenden Führungskräften durchgeführt werden. In diesem Workshop sollen zuerst das Unternehmensleitbild und die Kerngeschäftsprozesse beschrieben werden. Bei den Kerngeschäftsprozessen wird eine Visualisierung empfohlen, die auf hoher Flugebene bereits einzelne Prozessschritte und Lieferanten beinhaltet, soweit zutreffend. Anhand dieser können erste Informationssicherheitsrisiken abgeleitet werden, wie z.B. Angriffe auf die Lieferkette oder Störungen von Systemen, die über das Internet erreichbar sind. Alle Ergebnisse sollten festgehalten werden, da diese im Anschluss als Grundlage der weiteren Schritte dienen. Wenn das Unternehmen mehr als einen kritischen Geschäftsprozess hat, wird empfohlen die folgenden Schritte pro Prozess durchzugehen und anschließend zu konsolidieren. Ergebnis des ersten Workshops sollte Folgendes sein:

- ☐ Unternehmensleitbild
- ☐ Auflistung der Kerngeschäftsprozesse inkl. Verantwortlichen
- ☐ Visualisierung der einzelnen Kerngeschäftsprozesse
- ☐ Liste der möglichen Informationssicherheitsrisiken pro Kerngeschäftsprozesse

Für jeden Kerngeschäftsprozess müssen die Verantwortlichen im nächsten Schritt die zugehörigen Assets identifizieren. Als Asset zählen dabei jegliche Form von benötigter Software, Hardware und Service, ohne die der Prozess nicht oder nur eingeschränkt funktionieren würden. Allgemein wird der Einsatz einer Software zur Inventarisierung empfohlen. Um NIS2UmsuCG konform zu sein, reicht allerdings eine Tabelle, die grundlegende Informationen zu den Assets enthält. Für diesen Leitfaden werden folgende Felder benötigt:

1. Software / Hardware / Service
2. Verwendungszweck
3. Asset Besitzer oder Administrator
4. Klassifizierung der Daten im Zugriff
5. Abhängig von (Verweis auf 1.)
6. Kritikalität für den Geschäftsprozess
7. Abhängigkeit von Drittanbieter (Drittanbieter dokumentieren)
8. Nutzung von Multi-Faktor-Authentifizierung
9. Return Point Objective (RPO)
10. Return Time Objective (RTO)

Bei der Klassifizierung der Daten muss eine Aussage bezüglich der Anforderungen an die Verfügbarkeit, Integrität und Vertraulichkeit der Daten getroffen werden. Die Verfügbarkeit und Integrität sollten sich mit der Kritikalität für den Geschäftsprozess decken. Des Weiteren sollten personenbezogene Daten als solche gekennzeichnet werden, um eine DSGVO konforme Verarbeitung zu gewährleisten. Die RPO und RTO werden in Abschnitt REFERENZ EINFÜGEN erklärt. Alle identifizierten Drittanbieter müssen gemäß NIS2UmsuCG hinsichtlich ihrer Sicherheit betrachtet werden, wobei die Abhängigkeit des Geschäftsprozess im Vordergrund steht.

Neben den allgemeinen Informationssicherheitsrisiken, die den gesamten Geschäftsprozess betreffen, müssen die spezifischen Risiken der einzelnen Systeme erfasst werden. Hierzu fordert das NIS2UmsuCG das Management und die Offenlegung von Schwachstellen. Zur Offenlegung von Schwachstellen können kommerzielle Schwachstellenscanner verwendet, allerdings

existieren open-source Schwachstellenscanner, die Exporte erlauben und somit mit der Asset Inventar Liste verknüpft werden können. Je nach Präferenz kann das Kommandozeilen-Tool Nmap[4] verwendet werden, welches auch für Penetrationstest verwendet wird, oder das Tool OpenVAS[5]. Für Letzteres existiert eine grafische Benutzeroberfläche über die Schwachstellenscans automatisiert und im Browser verwaltet werden können. Das Unternehmen muss einen Prozess definieren, wie mit Schwachstellen umgegangen wird. Hierzu kann beispielsweise der Common Vulnerability Scoring System (CVSS) Score herangezogen werden, der sich für jede Schwachstelle berechnen lässt.[6] Der Score geht von 0 bis 10, wodurch ein Unternehmen abhängig von der Risikobereitschaft beispielsweise alle Schwachstellen mit einem Score von unter 5 akzeptieren könnte. Alle Schwachstellen darüber müssten dann behoben werden, oder wenn die Behebung mit zu hohen Kosten verbunden ist, migriert werden. All diese Schwachstellen, die nicht behoben werden, sind als Risiko zu dokumentieren. Die Dokumentation hat wie in Abschnitt Governance beschrieben zu erfolgen. Nachdem diese Schritte abgeschlossen sind, sollte folgendes existieren:

- ☐ Prozess zur Offenlegung von Schwachstellen
- ☐ Prozess zum Schwachstellenmanagement
- ☐ Ergebnis des ersten Schwachstellenscans

Schutz der Assets

Nachdem alle relevanten Assets und ggf. Schwachstellen dieser identifiziert wurden, müssen Schutzmaßnahmen definiert werden. Das NIS2UmsuCG fordert „Schulungen im Bereich der Sicherheit in der Informationstechnik“ schätzt Erfüllungsaufwände, die als NIS2UmsuCG konform interpretiert werden. So muss jährlich eine vierstündige Schulung der Geschäftsleitung und der leitenden Führungskräfte stattfinden, wobei Schulungen durch externe Dozenten empfohlen werden. Für die Mitarbeitenden wird eine Stunde pro Jahr geschätzt. Um dies zu erfüllen, können öffentliche Schulungsunterlagen wie z.B. die des BSI verwendet werden. Eine Möglichkeit wäre die Umsetzung durch einen Artikel zum Thema Informationssicherheit pro Quartal. Zum Einstieg werden allgemeine Themen empfohlen:

- Wie erkenne ich Phishing-E-Mails und -Webseiten?[7]
- Sichere Passwörter erstellen[8]
- Passwörter verwalten mit einem Passwort-Manager[9]
- Zwei-Faktor-Authentisierung [10]

[4] Siehe https://nmap.org
[5] Siehe https://www.openvas.org/index.html
[6] Siehe https://www.first.org/cvss/v4.0/specification-document
[7] Siehe https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Wie-erkenne-ich-Phishing-in-E-Mails-und-auf-Webseiten/wie-erkenne-ich-phishing-in-e-mails-und-auf-webseiten_node.html
[8] Siehe https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html
[9] Siehe https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Passwort-Manager/passwort-manager_node.html
[10] Siehe https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html

Die Schulungen sollten verpflichtend für neue Mitarbeitende sein, um ein grundlegendes Bewusstsein zu garantieren. Um das Bewusstsein aller Mitarbeitenden zu stärken, wird eine persönliche Ansprache durch die Geschäftsleitung empfohlen, die die Risiken durch Cyberangriffe aufzeigt und Mitarbeitende sensibilisiert.

Eine weitere organisatorische Schutzmaßnahme bilden die Vorschriften für Zugriffsberechtigungen. Mitarbeitende sollten basierend auf ihrer aktuellen Tätigkeit ausschließlich Zugriff auf die nötigen Systeme haben (Least-Privilege-Prinzip). Innerhalb der Systeme sollten lediglich die Informationen zugänglich sein, die für die Tätigkeit relevant sind (Need-to-know-Prinzip). Während bei kleinen Unternehmen die Zuständigkeiten ggf. verschwimmen, wächst die Bedeutung dieser Prinzipien mit der Größe des Unternehmens, weshalb sie frühzeitig eingeführt werden sollen. Folgende Dokumente sollten gepflegt werden:

- ☐ Richtlinie zur Schulung aller Mitarbeitenden (Frequenz, Aufwand)
- ☐ Richtlinie für Zugriffsberechtigungen (Least-Privilege- und Need-to-know-Prinzip)
- ☐ Dokumentation durchgeführter Schulungen

Die folgenden technischen Schutzmaßnahmen werden im NIS2UmsuCG als „grundlegende Verfahren im Bereich der Cyberhygiene“ verstanden und bilden einen Basis Schutz gegen die meisten Cyberbedrohungen. An vorderster Stelle steht der physische Zugriff auf Server und Anlagen. Diese müssen durch Absperrungen und Zugangskontrollen gesichert sein, damit niemand unbefugtes die Hardware beschädigen oder manipulieren kann. Es werden elektronische Zugangskontrollen empfohlen, da hierüber auch der Zutritt von externen Dienstleistern protokolliert werden kann, sollte es zu einem Vorfall kommen. Mit den Zugangskontrollen geht die Erstellung eines Prozesses zur Zutrittsvergabe einher. Hierzu kann eine einfache Liste mit vergebenen Chipkarten gepflegt werden, die die Karten Personen zuordnet. Dies ermöglicht es ebenfalls Chips bei einem Verlust zu sperren, was bei konventionellen Schlössern einen Austausch nach sich ziehen würde.

Neben der physischen Trennung des Unternehmensgeländes von der Umwelt, sollte auch eine logische Trennung auf Netzwerkebene vom Internet vorhanden sein. Hierzu wird eine Firewall benötigt, die den Übergang vom internen Netzwerk zum Internet schützt. Diese kann ebenfalls genutzt werden, wenn es auf dem Unternehmensgelände unterschiedliche Zonen gibt. So sollten Server, aber auch Fertigungsanlagen durch ein restriktives Firewall Regelwerk geschützt werden. Wie genau die Trennung auszusehen hat, sollte in einer Richtlinie zur Netzwerksegmentierung festgehalten werden. Empfohlen wird so restriktiv wie möglich zu starten und ausschließlich benötigte Verbindungen zu öffnen (Whitelisting-Ansatz). Für Unternehmen mit Fertigungsanlagen wird empfohlen diese vollständig von allen anderen Bereichen zu trennen, da diese i.d.R. keine eigenen Schutzmaßnahmen aufweisen.

Als nächstes sollte eine Richtlinie zur regelmäßigen Installation von Patches und Updates verfasst werden, die die Asset Besitzer bzw. Systemadministratoren dazu verpflichtet Patches und Updates einzuspielen. Um Fehler und Versäumnis vorzubeugen, wird die Aktivierung automatischer Updates empfohlen, solange hiervon keine betrieblichen Störungen erwartet werden. Halbjährige Stichproben können das Bewusstsein fördern sowie die Erfüllung der Richtlinie verifizieren.

Das NIS2UmsuCG fordert des Weiteren „Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung“, welche in Form einer Richtlinie festgehalten werden sollten. Grundsätzlich sollten alle Daten verschlüsselt gespeichert werden, weshalb die standardmäßige Verschlüsselung von Speichermedien empfohlen wird. Des Weiteren sollten

lediglich jene Protokolle genutzt werden, die die verschlüsselte Übertragung von Daten ermöglichen. Demnach sollte anstatt HTTP für Webseiten HTTPS und für Dateiübertragungen SFTP anstatt FTP verwendet werden. Dasselbe Prinzip gilt für alle weiteren verwendeten Protokolle, wobei es besonders wichtig ist bei den Daten, die das Unternehmensnetz verlassen. Auch bei dem Einkauf und der Entwicklung von Systemen muss hierauf geachtet werden. Es wird geraten sich an die Empfehlungen des BSIs zu halten, welche in der Technischen Richtlinie (TR) „02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen“[11] vorzufinden sind. Die aktuellen Empfehlungen sind in Abbildung 3 zu sehen.

Blockchiffre	MAC	RSA	DH $\mathbb{F}_p$	ECDH	ECDSA
128	128	3000	3000	250	250

Abbildung 3: Empfohlene Schlüssellängen für verschiedene kryptographische Verfahren

Als letzte Schutzmaßnahme benötigt es ein Backup-Management sowie Wiederherstellungsprozesse. Diese werden vom NIS2UmsuCG explizit als Maßnahme zur Aufrechterhaltung des Betriebs gefordert. Ohne Backups ist es für ein Unternehmen nicht möglich nach einem Cyberangriff, bei dem Daten verschlüsselt oder gelöscht wurden, die Geschäftsprozesse wieder zum Laufen zu bekommen. Auch bei Hardwareausfällen sind Unternehmen auf Backups angewiesen. Deshalb werden unterschiedlichen Optionen beschrieben, die Abhängig von der Unternehmenslandschaft sind.

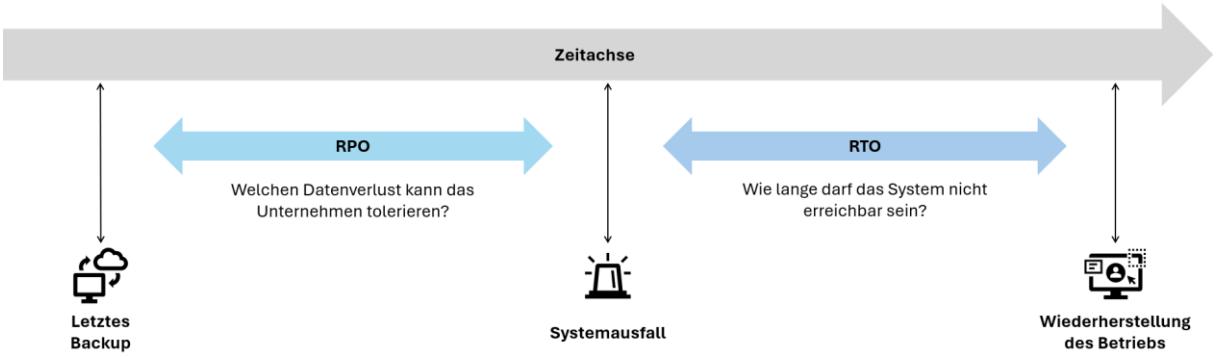

Abbildung 4: RPO und RTO

Zuerst sollten in jedem Fall der Umfang der Daten und Systeme festgelegt werden, für die Sicherungen erstellt werden müssen. Dabei handelt es sich mindestens um alle Komponenten des NIS2UmsuCG relevanten Geschäftsprozesses. Darüber hinaus wird empfohlen das Konzept auf alle Assets des Unternehmens auszuweiten. Für die relevanten Assets sollten das Return-Point-Objective (RPO), also der maximal tolerierbare Datenverlust, sowie das Return-Time-Objective (RTO) als Teil des Asset Inventars festgelegt werden. Die Begriffe werden in Abbildung 4 veranschaulicht. Abhängig von den RPO- und RTO-Werten bedarf es unterschiedliche Lösungen, wobei pauschal niedrigere Werte zu erhöhten Kosten führen. Um Geld zu sparen, sollte ebenfalls definiert werden, wie viele Backups wie lange vorgehalten werden müssen und

[11] Siehe https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

welche Daten ausgeklammert werden können. Greifbar wird dies bei Backups, die in der Cloud gespeichert werden, da eine Verrechnung auf Gigabyte-Ebene stattfinden kann. Die hat den Vorteil, dass Kosten mit der Größe des Unternehmens skalieren, Anschaffungskosten wegfallen und keine eigenen Backupsysteme betreut werden müssen. Aus technischer Sicht sind Backups in der Cloud insofern vorteilhaft, dass diese viele Probleme eigener Backupsysteme lösen. Kommt es zum Beispiel zu Schäden der Betriebsstätte wie Feuer oder Überschwemmungen wären die primären Daten auf Servern, Anlagen und Desktops genauso betroffen wie die des Backupsystems. Bei mittleren Unternehmen mit mehr als einem Standort könnten die Backups über die Standorte verteilt werden, allerdings müssten diese in unterschiedlichen Gefahrengebieten liegen und die Orchestrierung von Backups wäre mit hohen finanziellen Aufwänden verbunden. Des Weiteren müsste sichergestellt werden, dass die Backups Ransomware sicher abgelegt werden, was die Verwendung zusätzlicher Software erfordert. Ansonsten würden die Backups zusammen mit den primären Daten verschlüsselt werden und wären ebenfalls nutzlos. Der einzige Vorteil lokaler Backups ist die Geschwindigkeit der Wiederherstellung von Daten, da diese bei der Cloud an den Durchsatz der Internetanbindung des Unternehmens gebunden ist. Wenn Cloud-Speicher genutzt wird, müssen die oben genannten Punkte vertraglich adressiert werden, um die Backups angemessen zu schützen. Ebenso müssen die Daten verschlüsselt gespeichert werden, wie oben beschrieben. All dies wird von großen Cloud-Providern bereits angeboten, weshalb Standardlösungen genutzt werden können.

Hindernisse sind bei der Anbindung von Anlagen zu erwarten, grade wenn diese nicht direkt mit dem Internet kommunizieren können oder sollen. Hier müsste ein sogenannter Forwarder konfiguriert werden. Beim Backup-Management sollte regelmäßig geprüft werden, ob die definierten Wiederherstellungsprozesse funktionieren und die vorgegebenen RPO- und RTO-Werte einhalten können. Kommt es zu Abweichungen, muss entschieden werden, ob in ein besseres Backup-Management investiert werden soll, oder die höheren RPO und RTO-Werte hinsichtlich der Kosten akzeptiert werden können. Abhängig von der Branche, in der das Unternehmen tätig ist, müssen die branchenspezifischen Gesetze beachtet werden, die z.B. die Archivierung bestimmter Daten fordert. Demnach dürfen die Daten nie verloren gehen, oder müssen zu einem späteren Zeitpunkt wieder erhoben werden können.

Folgendes sollte zum Schutz der Assets existieren:

- ☐ Richtlinie zur Physischen Sicherheit
- ☐ Prozess zur Zutrittsvergabe
- ☐ Richtlinie zur Netzwerksegmentierung
- ☐ Restriktives Firewall Regelwerk auf Basis von White-Listing
- ☐ Richtlinie zum Einspielen von Patches und Updates
- ☐ Richtlinie zur Nutzung von Kryptografie und Verschlüsselung
- ☐ Richtlinie zum Backup-Management
- ☐ Wiederherstellungsprozesse
- ☐ Optional: Richtlinie zum Betrieb von Anlagen

Erkennen von Cyberangriffen

Um Cyberangriffe frühzeitig eindämmen oder verhindern zu können, muss man in der Lage sein, Angriffe erkennen zu können. Das NIS2UmsuC fordert den Einsatz von Systemen zur Angriffserkennung ausschließlich von Betreibern kritischer Anlagen. Dennoch sollten grundlegende Maßnahmen zur Erkennung von Cyberangriffe im Interesse aller Unternehmen

sein, da sie zur Aufrechterhaltung des Betriebs beitragen. Die Systeme zur Angriffserkennung können auf Netzwerk-, Endgerät- oder Applikationsebene betrieben werden.

Sollte wie oben empfohlen eine Firewall für den Übergang zwischen dem internen Unternehmensnetz und dem Internet installiert sein, kann auf dieser die IDS/IPS Funktionalität aktiviert werden. Bei einem Intrusion Detection System (IDS) handelt es sich um ein System auf der Firewall, welches den gesamten Netzwerkverkehr überwacht und bekannte Angriffsmuster erkennen kann. Wenn man diesem System die Erlaubnis gibt bösartigen Netzwerkverkehr automatisch zu blockieren, handelt es sich um ein Intrusion Prevention System (IPS). Diese Funktionalitäten sind i.d.R. mit Lizenzkosten verbunden, arbeiten dafür allerdings transparent. Des Weiteren besteht der einzige zusätzliche Aufwand für das Unternehmen darin, Patche einzuspielen, da die Systeme sich automatisch die neusten Angriffsmuster und Anzeichen bösartigen Netzwerkverkehrs ziehen.

Da Laptops auch außerhalb des Unternehmensnetzes genutzt werden und Anlagen auch über Viren auf USB-Sticks angegriffen werden können, wird ebenfalls empfohlen Maßnahmen auf Ebene der Endgeräte zu ergreifen. Hier könnten Antivirus Programme, Endpoint Detection and Response (EDR) Tools oder Systemhärtungen verwendet werden. Antivirus Programme bilden sogenannte Signaturen von Dateien und gleichen diese mit einer Datenbank von Schadprogrammen ab. EDR-Tools basieren auf maschinellem Lernen und können typische Angriffsmuster erkennen, wodurch sie auch potentiell neue Schadprogramme erkennen können. Für Systeme, für die weder Antivirus noch EDR-Lösungen existieren, wie Anlagen oder Internet of Things (IoT) Geräte, wird zur Systemhärtung geraten. Dabei wird das System so konfiguriert, dass ausschließlich freigegebene Programme ausgeführt werden können.

Um Cyberangriffe erkennen zu können, lohnt sich die Anbindung eines Security Information and Event Management (SIEM) Systems. Dieses wertet alle vorhandenen Logs aus und weist auf verdächtiges oder bösartiges Verhalten hin. An ein SIEM können auch Applikationen angebunden werden, wodurch z.B. Brute-Force Attacken auf Passwörter einzelner User erkannt werden können. Bei einer solchen Attacke probiert ein Angreifer alle möglichen Passwörter aus, was durch eine überproportional große Menger fehlgeschlagener Anmeldeversuche leicht zu erkennen und abzustellen ist.

Es wird davon ausgegangen, dass die wenigsten Unternehmen die Ressourcen besitzen, um ein SIEM-System zu konfigurieren sowie kontinuierlich zu Monitoren. Aus diesem Grund wird die Beauftragung von Dienstleistern zur Anbindung von Systemen, Monitoring und Alarmierung empfohlen. Unter Umständen lassen sich Synergien erzeugen, indem die Antivirus- bzw. die EDR-Lösung zusammen mit der SIEM-Lösung erworben wird. Die SIEM-Lösung wird dabei als Optimum angesehen. Besitzt ein Unternehmen hierfür nicht die finanziellen Mittel, sollte eine Risiko basierte Entscheidung getroffen und dokumentiert werden. Mögliche Ergebnisse sind der Entfall einzelner Komponenten, wie z.B. dem SIEM oder eines EDR-Tools.

Betreiber Kritischer Anlagen sollten mindestens einen der folgenden Punkte erfüllen:

- ☐ Nutzung einer Firewall mit aktivierter IDS/IPS Funktionalität
- ☐ Ein Antivirus Programm auf allen relevanten Systemen
- ☐ Die Nutzung einer EDR-Lösungen auf allen relevanten Systemen
- ☐ Die Anbindung von Systemen und Applikationen an ein SIEM mit konfigurierten Alarmierungen

Reaktion auf Cyberangriffe

Trotz der vorhandenen Schutzmaßnahmen und der frühzeitigen Erkennung von Cyberangriffen, können diese nicht ausgeschlossen werden. Das NIS2UmsuCG fordert deshalb Maßnahmen zur Bewältigung von Sicherheitsvorfällen. Bei einem erheblichen Sicherheitsvorfall kann es dazu kommen, dass alle IT-Systeme nicht mehr erreichbar sind und die kritischen Geschäftsprozesse der Unternehmen zum Erliegen kommen. In diesem Moment beginnt in jedem Unternehmen die Chaos Phase, in der keiner weiß, was genau passiert ist und was getan werden muss. Um diese Phase möglichst kurz zu halten und schnell in einen Notbetrieb übergehen zu können, braucht es ein IT-Notfallmanagement sowie einen Krisenstab. Diese sollten nach einem Notfallhandbuch arbeiten, welches durch die Chaos Phase bis zum Notbetrieb führt.

Der Krisenstab eines KMUs sollte mindestens folgende Rollen abdecken:

- Leitung des Stabs
- Vertreter der IT
- Vertreter der Personalabteilung
- Vertreter der Gebäudeverwaltung
- Zuständiger für die Notfall und Krisen Kommunikation
- Protokollierung

Speziell bei kleinen Unternehmen kann eine Person ebenfalls mehrere Rollen abdecken. Es wird dennoch empfohlen die Rollen separat zu besetzen, da jede Rolle ihren respektiven Bereich koordinieren muss. So sollte der Vertreter der IT sich auf die Wiederherstellung der Systeme konzentrieren und nicht gleichzeitig die interne und externe Kommunikation gestalten. Die Vertreter der Personalabteilung und Gebäudeverwaltung besitzen die Fach- und Sachkenntnis über die jeweiligen Ressourcen und werden benötigt für bauliche oder organisatorische Maßnahmen. Bei der Notfall und Krisen Kommunikation muss darauf geachtet werden, dass alle gesetzlichen Anforderungen, wie die Meldepflichten gemäß NIS2UmsuCG oder der DSGVO, sowie vertragliche Verpflichtungen eingehalten werden. Es wird empfohlen den One-Pager zur Meldepflicht um alle Unternehmens spezifischen Verpflichtungen zu erweitern. Nach Möglichkeit sollte eine Person Protokoll führen, da somit immer klar ist, was bereits umgesetzt wurde und was noch ausstehend ist. Des Weiteren kann das Protokoll im Nachhinein genutzt werden, um das Notfallhandbuch zu verbessern und aus dem Vorfall zu lernen. Es sollte eine interne Möglichkeit geben, um erhebliche Sicherheitsvorfälle zu melden und damit das Notfallmanagement einzuleiten. Diese sollte in den Schulungsunterlagen enthalten sein.

Die Vorlage eines Notfallhandbuchs bietet einen Ausgangspunkt, der durch Unternehmen erweitert werden kann. Der Einschätzungsbogen sollte einen initialen Überblick über den Sicherheitsvorfall geben. Soweit angemessen, können bereits Teile der definierten Sofortmaßnahmen ergriffen werden. Alle Sofortmaßnahmen sollten vorab mit der Geschäftsleitung abgestimmt werden, damit der Krisenstab ohne Verzögerungen agieren kann. Allgemein sollte die unten bereitgestellte Vorlage eines Notfallhandbuchs an die Spezifika des Unternehmens adaptiert werden. Es sollten ebenfalls alle kritischen Systeme gelistet werden, wobei am besten die Liste aus dem Abschnitt Identifizieren von Risiken genutzt wird.

Um auf Cyberangriffe reagieren zu können, sollte Folgendes existieren und gepflegt werden:

- ☐ Definition eines Krisenstabs
- ☐ Ein Notfallhandbuch inkl. Einem Verantwortlichen für dessen Pflege
- ☐ Definierter Prozess zur Einberufung des Krisenstabs

- ☐ Kommunikation des Prozesses zur internen Meldung erheblicher Sicherheitsvorfälle
- ☐ Sofortmaßnahmen, die mit der Geschäftsleitung abgestimmt sind

Wiederherstellung des Normalbetriebs

Spätestens nachdem das Notfallmanagement einen Notbetrieb etabliert hat, sollen mit der Wiederherstellung aller betroffenen Systeme und somit des Normalbetriebs begonnen werden. Für diesen Schritt muss das oben geforderte Backup-Management bereits umgesetzt sein! Bei der Wiederherstellung werden ebenfalls regelmäßige Tests der dokumentierten Wiederherstellungsprozesse belohnt, da diese nun benötigt werden. Ohne Backups können die Systeme nicht wiederhergestellt werden, sondern müssen neu aufgesetzt und konfiguriert werden, was erheblich mehr Zeit und Aufwand bedeutet.

Da die Ressourcen der IT während der Wiederherstellungsphase limitiert sind, sollte vorab eine Reihenfolge definiert werden, in der die Systeme wiederhergestellt werden. Neben der Kritikalität (z.B. anhand der RTOs gemessen) sollte ebenfalls die Abhängigkeit von weiteren Systemen berücksichtigt werden. Wenn ein Unternehmen mehrere, voneinander unabhängige Geschäftsprozesse besitzt, müssen die Geschäftsprozesse ebenfalls untereinander priorisiert werden.

Wenn es sich bei dem erheblichen Sicherheitsvorfall um einen Cyberangriff handelt, müssen vor der Wiederherstellung die Backups überprüft werden. Hierbei muss die Integrität der Backups sichergestellt werden, da sich die Schadprogramme, die den Ausfall erzwungen haben, in den Backups befinden können. Hierfür sollte ebenfalls ein Prozess definiert werden, damit die Arbeit auf möglichst viele Personen aufgeteilt werden kann.

Wenn das Unternehmen Cloud-Dienste nutzt, sollte die Betroffenheit dieser Dienste eruiert werden. Hierfür sollten ebenfalls Kontaktdaten der gewählten Cloud-Provider dokumentiert werden. Wenn lokale- und Cloud-Dienste voneinander abhängig sind, ist die Orchestrierung der Wiederherstellung in der korrekten Reihenfolge besonders wichtig. Dasselbe gilt, wenn das Unternehmen seine Backups in der Cloud gespeichert hat, da beim Wiedereinspielen dieser die Bandbreite des Internetanschlusses des Unternehmens zum limitierenden Faktor wird und mit eingeplant werden muss.

Zur Wiederherstellung der Backups bedarf es folgende Dokumente:

- ☐ Anleitung für den Wiederherstellungsprozess
- ☐ Definierte Reihenfolge zur Wiederherstellung der Systeme eines Geschäftsprozesses
- ☐ Priorisierung der Geschäftsprozesse untereinander
- ☐ Prozess zur Integritätsprüfung von Backups
- ☐ Optional: Vorgehen zur Wiederherstellung von Cloud-Diensten und Cloud-Backups

Governance

Zuletzt fordert das NIS2UmsuCG Konzepte für Risikoanalysen und die Sicherheit in der Informationstechnik. Diese sollten mit dem Unternehmensleitbild einher gehen. Bezüglich der Sicherheit in der Informationstechnik fordert das NIS2UmsuCG explizit „Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen“. Dies wird in Teilen durch das Schwachstellenmanagement erfüllt, welches oben gefordert wird. Um den Absatz vollständig zu adressieren, sollte ein Dokument mit allen Basisanforderungen formuliert werden, unabhängig

davon, ob das System selbst entwickelt oder eingekauft wird. Die Anforderungen sollten sich an den oben geforderten Richtlinien, wie z.B. den Einsatz von Kryptographie und Verschlüsselungen, aber auch an allgemeine, gesetzliche Vorgaben halten, wie die Verarbeitung personenbezogener Daten. Ist das System und die verarbeiteten Daten besonders schützenswert, sollten die Basisanforderungen erweitert werden. Beispiele könnten die Implementierung von Multi-Faktor-Authentifizierung oder die Hochverfügbarkeit von Systemen sein. Ebenfalls kann das Unternehmen spezifische Anforderungen stellen, wenn z.B. ein SIEM verwendet wird und die Anbindung des Systems gewünscht ist. Im Idealfall werden die allgemeinen Anforderungen so geschrieben, dass aus der Einstufung des Systems sich spezifisch technische und organisatorische Anforderungen ergeben. Können die Anforderungen aus wirtschaftlichen Gründen nicht erfüllt werden, muss eine Risiko basierte Entscheidung getroffen werden.

Für die Risikoanalyse sollte ein Prozess erstellt werden, wie Risiken analysiert werden und was alles für eine Risiko basierte Entscheidung benötigt wird. Alle Entscheidungen müssen dokumentiert werden, um die Risikoexposition des gesamten Unternehmens zusammenfassen zu können. Die Dokumentation kann Anfangs über eine einfache Tabelle erfolgen, die folgende Informationen enthält:

- Eine **Risiko ID**, um auf die Einträge referenzieren zu können
- Eine **Beschreibung**, die die Bedrohung sowie den potenziellen Schadensfall erklärt
- Die **Eintrittswahrscheinlichkeit** des Risikoszenarios. Da die Szenarien meist sehr spezifisch und abhängig vom Unternehmenskontext sind, wird eine Abstufung in gering, mittel und hoch empfohlen. Die Stufen sollten entsprechend definiert werden
- Die **Auswirkungen**, die das Eintreten eines Risikoszenarios auf das Unternehmen haben würde. Es wird eine Abstufung in gering, mittel und hoch empfohlen. Die Stufen sollten entsprechend definiert werden
- Eine **Risikobewertung**, die sich aus der Eintrittswahrscheinlichkeit und den Auswirkungen zusammensetzt. Hierzu wird die Matrix in Abbildung 5 empfohlen, die Risiken in akzeptabel, diskutabel und kritisch kategorisiert. Für kritische Risiken müssen umgehend Maßnahmen ergriffen werden, um die Eintrittswahrscheinlichkeit oder Auswirkung zu verringern. Diskutable Risiken bilden den Bereich ab, in dem geprüft werden muss, ob die Reduktion des Risikos wirtschaftlich ist. Gemäß Paragraph 31 des NIS2UmsuCG sollten diese Risiken durch Betreiber kritischer Anlagen ebenfalls adressiert werden
- Die **Maßnahmen**, die ergriffen werden, um das Risiko abhängig von der Risikobewertung zu managen
- Die **Kosten**, die mit den Maßnahmen verbunden sind
- Den **Verantwortlichen**, der sich um die Umsetzung der Maßnahmen kümmert
- Den **Status**, in dem sich die Umsetzung der Maßnahmen befindet

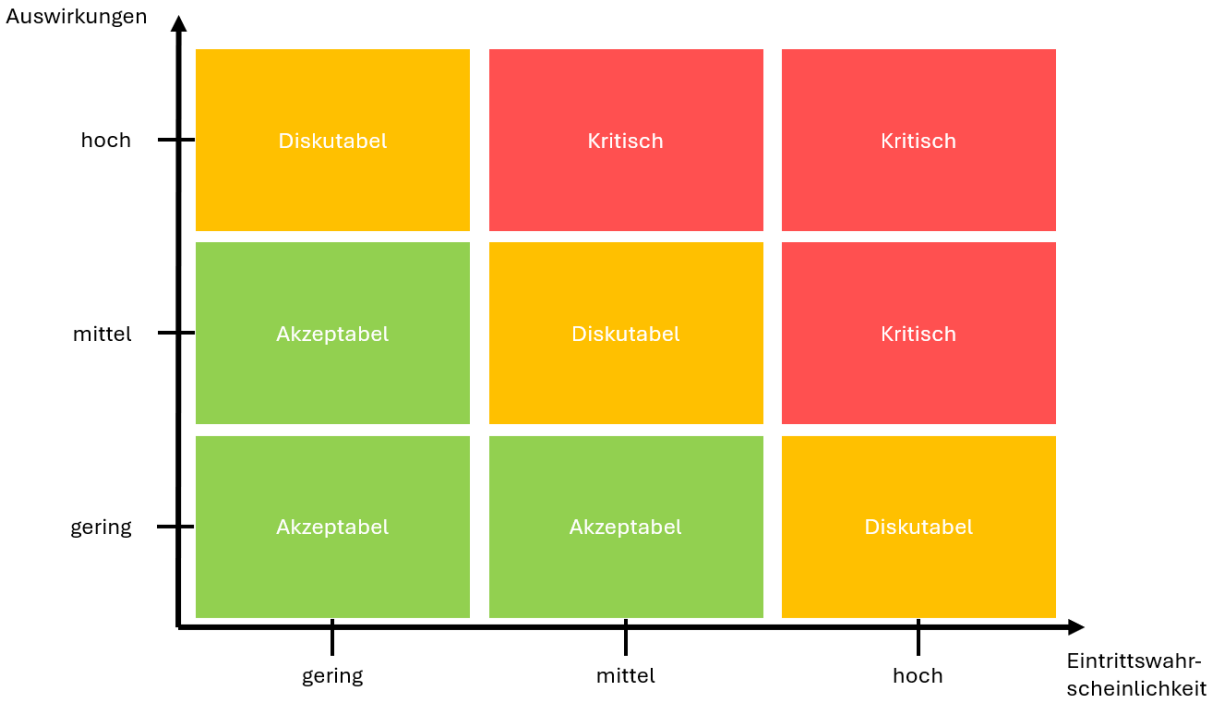

Abbildung 5: Matrix zur Risikobewertung

Die Prozessbeschreibung der Risikoanalyse sollte ebenfalls beinhalten, dass die Risiken bei signifikanten Änderungen des Geschäftsprozesses aktualisiert werden falls nötig. Allgemein sollten alle Maßnahmen, die zur Mitigation von Risiken genutzt werden, gemäß NIS2UmsuCG regelmäßig getestet werden. Hierzu zählen ebenfalls Standardprozesse wie die Erstellung und das Wiedereinspielen von Backups, aber auch Prozess spezifische Maßnahmen.

Allgemein sollte die Einhaltung aller im Zuge dieses Handlungsleitfadens definierter Maßnahmen überprüft werden, um die kontinuierliche Erfüllung der Anforderungen des NIS2UmsuCG zu gewährleisten. Hierbei kann es sich um eine interne Überprüfung handelt, allerdings wird eine externe Überprüfung empfohlen. Um die getroffenen Maßnahmen als Werbung zu nutzen, würde es sich lohnen, eine Zertifizierung des mit diesem Leitfaden erstellten Informationssicherheitsmanagementsystem (ISMS) anzustreben. Für die gängigen Zertifizierungen (ISO27001, TISAX, etc.) müssen jeweils bestimmte Themen ergänzt werden, die der Informationssicherheit allerdings nur zuträglich wären. Da große Unternehmen, die vom NIS2UmsuCG betroffen sind, die Sicherheit ihrer Lieferkette sicherstellen müssen, kann eine Zertifizierung als Wettbewerbsvorteil angesehen werden.

Allgemeine Hinweise

Für die Kommunikation innerhalb des Unternehmens fordert das NIS2UmsuCG “gesicherte Sprach-, Video- und Textkommunikation” sowie ein Notfallkommunikationssystem. Diese Anforderungen können und werden wahrscheinlich bereits über Standardlösungen umgesetzt. Für die Notfallkommunikation ist darauf zu achten, dass sie für alle zugänglich ist, auch wenn beispielsweise die Endgeräte des Unternehmens durch einen Cyberangriff unbrauchbar sind.

Das BSI schätzt den Aufwand zur Erstellung der Richtlinien und deren initiale Implementierung auf rund 963 Stunden und 21.000 Euro Sachkosten für ein mittleres Unternehmen. Dieselben Aufwände sollen für die jährliche Aufrechterhaltung des geschaffenen Standards eingerechnet werden, was eine doppelte Belastung im ersten Jahr von rund 1926 Stunden und 42.000 Euro

Sachkosten bedeutet. Die jährlichen Aufwände basieren auf Neuanschaffungen von Hardware und Software sowie die Zeit die benötigt wird, um alle entstehen den Risiken zu adressieren sowie die bestehenden Risiken zu pflegen. Änderungen der Organisationsstruktur sowie der Kritikalität von Systemen sind ebenfalls mit Aufwand verbunden. Speziell in den ersten Jahren sind viele Lessons Learned zu erwarten sowie 78 einige technische Durchführungsverordnungen, die in die eigenen Richtlinien und Prozesse eingepflegt werden müssen.

Zur Orientierung kann aktuell der Entwurf für kleine Unternehmen, die als Finanzunter nehmen klassifiziert sind, genutzt werden. Dieser ist im "Final report on draft RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework" enthalten und kann von der Webseite der Europäische Aufsichtsbehörde für das Versiche rungswesen und die betriebliche Altersversorgung (EIOPA) abgerufen werden.[12] Artikel 28 und Folgende beschreiben ein vereinfachtes Risikomanagement Framework, welches zur Ergänzung dieses Handlungsleitfaden genutzt werden kann. Der Entwurf ist im Di gital Operational Resilience Act explizit gefordert worden und ist demnach NIS-2 und NIS2UmsuCG konform.

Verstöße gegen die Meldepflicht sowie die Anforderungen an die Risikomanagementmaß nahmen können mit Geldbußen geahndet werden. Dabei ist der Höchstbetrag für für wichtige Einrichtungen gemäß NIS2UmsuCG mindestens 7.000.000 Euro oder 1,4% des Umsatzes des vorangegangenen Geschäftsjahres, je nachdem welcher Betrag höher ist. Für besonders wichtige Einrichtungen sind die Werte respektive 10.000.000 Euro oder 2% des Umsatzes. Des Weiteren kann die zuständige Behörde bei besonders wichtigen Einrichtungen Vor-Ort-Kontrollen durchführen, Schwachstellenscans auf öffentliche IP-Adressen starten, Informationen anfordern zur Bewertung der ergriffenen Risikomaßnahmen sowie Nachweise für die Umsetzung der definierten Cybersicherheitskonzepte.

Kommt ein Unternehmen den Anordnungen des BSI trotz Fristsetzung nicht nach, kann dies dazu führen, dass Zertifizierungen oder Genehmigungen für Teile oder der gesamten von der besonders wichtigen Einrichtung erbrachten Dienste oder Tätigkeiten vorübergehend ausgesetzt werden. Des Weiteren kann das BSI unzuverlässigen Geschäftsleitungen die Ausübung der Tätigkeit, zu den sie berufen sind, vorübergehend untersagen. Dies ist solange zulässig, bis die Einrichtung den Anordnungen nachkommt.

[12] Siehe https://www.eiopa.europa.eu/publications/set-rules-under-dora-ict-and-third-party-risk-management-and-incident-classification_en?prefLang=de

Vorlage eines Notfallhandbuchs

Verantwortlicher des Notfallhandbuchs: <Person>

Letzte Änderung: <Datum>, durch <Person>

Wichtige Kontakte

Rolle	**Telefonnummer**
Leitung des Krisenstabs	
Verantwortlicher IT	
Verantwortlicher Personal	
Verantwortlicher Gebäudeverwaltung	
Verantwortlicher Kommunikation	
Zentrale Anlaufstelle der Behörde	
Kontakt bei der Bank	
Kontakt bei der Versicherung	
Kontakt bei dem Cloud-Provider	
Kontakt Vertragspartner 1	
Kontakt Vertragspartner 2	
…	

Wichtige Systeme

Applikation	**Gerät**	**Ansprechpartner**	**Telefonnummer**

Einschätzungsbogen

Technische Situation

- Welche kritischen Geschäftsprozesse sind betroffen?
- Welche IT-System sind betroffen?
- Was sind die Symptome?
- Welche Kommunikationskanäle stehen zur Verfügung?
- Was ist der Zustand der Backups?
- …

Bereits ergriffene Maßnahmen

- Gibt es bereits technische Maßnahmen?
- Gibt es bereits organisatorische Maßnahmen?
- Wer wurde bereits informiert (Behörden, Dienstleister, …)?
- …

Auswirkungen des Vorfalls

- Besteht Gefahr für Leib und Leben?
- Wie sind die kritischen Geschäftsprozesse beeinflusst?
- Gibt es Auswirkungen auf Dritte (Kunden, Dienstleister, …)?
- Ist der Angriff noch in Gange / verschlimmert sich die Situation weiterhin?

- Welche Schäden sind bereits eingetreten?
- ...

Sofortmaßnahmen

Die hier beschriebenen Maßnahmen sind vorab mit der Geschäftsleitung abgestimmt und dürfen im Falle eines erheblichen Sicherheitsvorfalls für die potentiell betroffenen Systeme ergriffen werden:

- Trennung der Verbindung zum Internet
- Trennung der physischen Netzwerkanbindung
- Eingrenzen der Netzwerkanbindung durch Firewalls
- Ausschalten von Systemen (Um Verbreitung zu verhindern)
- Trennung des Netzwerks (Switches abschalten)
- Sicherung der Backup-Systeme
- Löschen gefährlicher Dateien

Wiederherstellung von Backups

Dieser Abschnitt muss vom Unternehmen selbst verfasst werden, da die Wiederherstellungsprozesse je nach verwendeter Technologie und Applikationslandschaft variieren können. In jedem Fall ist es wichtig, dass bei einem Cyberangriff Integritätschecks der Backups stattfinden, bevor diese wiederhergestellt werden.