KAS

Kommission für Anlagensicherheit

beim

Bundesministerium für

Umwelt, Naturschutz und nukleare Sicherheit

Leitfaden

Maßnahmen gegen Eingriffe Unbefugter

KAS-51

Kommission für Anlagensicherheit

KAS

Leitfaden
Maßnahmen gegen Eingriffe Unbefugter

am 14. November 2019 von der KAS verabschiedet

KAS-51

Die Kommission für Anlagensicherheit (KAS) ist eine nach § 51a Bundes-Immissionsschutzgesetz beim Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit gebildete Kommission.

Ihre Geschäftsstelle ist bei der GFI Umwelt – Gesellschaft für Infrastruktur und Umwelt mbH (GFI Umwelt) in Bonn eingerichtet.

Inhalt

1 Einleitung

Aus Anlass der Terroranschläge vom 11. September 2001 in den USA war 2001/2002 auf Bitten des BMU von der Störfallkommission (SFK) der Leitfaden SFK-GS 38 „Maßnahmen gegen Eingriffe Unbefugter“ erarbeitet worden. Angriffe über die elektronische Vernetzung der Unternehmen („Cyberattacken“) wurden auf Basis der damals gebräuchlichen Technologie für weniger gefährdend erachtet. Eine Gefährdung durch Drohnen etc. war zum Zeitpunkt der Erstellung des SFK-Leitfadens noch nicht abzusehen.

Die Kommission für Anlagensicherheit (KAS) sah vor dem Hintergrund der technologischen Entwicklungen und der geänderten Bedrohungslage die dringende Notwendigkeit, den SFK-GS-38 konzeptionell und inhaltlich grundlegend zu überarbeiten. Vor diesem Hintergrund richtete die KAS mit Beschluss vom 23./24.11.2016 einen Arbeitskreis „Eingriffe Unbefugter“ ein und bestätigte diesen Beschluss nach Wechsel der Berufungsperiode am 09.03.2018.

Der Arbeitskreis erhielt den Auftrag, eine Neufassung des SFK-GS-38 im Sinne eines umfassenden Leitfadens zu Maßnahmen gegen Eingriffe Unbefugter auf Betriebsbereiche entsprechend der Störfall-V zu erarbeiten. Hierbei sollten insbesondere veränderte und neuartige Risiken infolge der technologischen Entwicklung und der sich verändernden Bedrohungslage berücksichtigt werden. Gleichzeitig sollten die Leitsätze KAS-44 (Schutz vor cyberphysischen Angriffen) und KAS-45 (Schutz vor Drohnenangriffen), die von der KAS am 23.11.2018 vorab zur Veröffentlichung freigegeben wurden, konzeptionell in die Neufassung des SFK-GS-38 eingebunden und aktualisiert werden.

2 Zielsetzung des Leitfadens

Es gehört zu den Grundpflichten der Störfall-Verordnung (StörfallV), Eingriffe Unbefugter als Gefahrenquelle zu berücksichtigen (§ 3 Abs. 2 Nr. 3 der StörfallV). Dies hat so zu erfolgen, dass in den Betriebsbereichen vorhandene gefährliche Stoffe derart gegen durch Vorsatz ausgelöste Störungen gesichert sind, dass eine ernste Gefahr oder Sachschäden im Sinne der StörfallV vernünftigerweise ausgeschlossen werden können. Darüber hinaus gibt es Vorschriften (z. B. GefahrstoffV, Sprengstoffrecht), bestimmte Stoffe vor dem Zugriff Unbefugter zu schützen. Die Anforderungen an die

Schutzmaßnahmen müssen den Auswirkungen durch Eingriffe Unbefugter angemessen sein.

Der vorliegende Leitfaden konzentriert sich auf den Schutz vor Eingriffen Unbefugter, durch die ernste Gefahren hervorgerufen werden könnten. Dies können beispielsweise Angriffe sein oder Versuche, ein Unternehmen oder öffentliche Institutionen zu erpressen. Dazu gehören auch Gefahren durch Cyberangriffe und Drohnen. Eingriffe umfassen Zugang, Zutritt oder Zugriff.

Die Gefährdung von Menschen steht im Vordergrund, es sind aber auch Anschläge gegen die Umwelt im Sinne von § 2 Nr. 8c der StörfallV zu berücksichtigen. Es kann hierfür sinngemäß die gleiche Vorgehensweise angewendet werden.

Der Leitfaden unterscheidet zwei Bereiche von Maßnahmen. Für alle Betriebsbereiche werden kurze Hilfestellungen zur Festlegung von Basismaßnahmen zum Schutz vor Eingriffen Unbefugter formuliert (Kap. 4). Ziel dieses Teils ist die Sensibilisierung aller Betreiber für die Thematik. Die Basismaßnahmen sind dann ausreichend, wenn durch sie ein Störfall infolge Eingriffe Unbefugter vernünftigerweise ausgeschlossen werden kann. Dies wird bei Betriebsbereichen der unteren Klasse vielfach der Fall sein, sofern keine besondere Gefährdung im Sinne dieses Leitfadens vorliegt.

Die Wahrscheinlichkeit eines kriminellen Angriffs steigt, wenn hierdurch weitreichende Folgen für Mensch und Umwelt ausgelöst werden können. Über die Basismaßnahmen hinaus sind daher weitergehende Maßnahmen insbesondere dann anzuwenden, wenn eine besondere Gefährdung vorliegt.

Im Sinne dieses Leitfadens ist dies der Fall, wenn im Falle eines durch Eingriffe Unbefugter ausgelösten Ereignisses in einem Betriebsbereich

- eine ernste Gefahr für viele Menschen ausgelöst werden kann,
- Sachschäden außerhalb des Betriebsbereichs im Sinne des Anhang VI, Teil I Nr. 4b der 12. BImSchV ausgelöst werden können
- eine ernste, das Gemeinwohl beeinträchtigende Umweltschädigung ausgelöst werden kann.

Wann eine ernste Gefahr für viele Menschen ausgelöst werden kann, ist im Einzelfall zu prüfen. Ein Anhaltspunkt dafür kann die örtliche Nähe zu besonderen Schutzobjekten sein, in denen sich eine größere Zahl von Menschen aufhalten kann.

Für Anlagen, die nicht der StörfallV unterliegen, kann der Leitfaden ebenfalls sinngemäß angewendet werden, wenn im Einzelfall ein entsprechendes Gefahrenpotenzial vorliegt.

Die Anwendung dieses Leitfadens dient auch der Erfüllung der Anforderungen der Sicherheitsüberprüfungsfeststellungsverordnung (SÜFV). § 10a SÜFV stellt als lebenswichtige Einrichtungen Betriebsbereiche der oberen Klasse nach StörfallV und ihnen nach § 1 Absatz 2 StörfallV gleichgestellte Betriebsbereiche fest. Durch Erfüllung der Vorgaben dieses Leitfadens kann der Nachweis geführt werden, dass die getroffenen organisatorischen oder technischen Maßnahmen als ausreichend im Sinne von § 10a SÜFV anzusehen sind. Dies muss im Sicherheitsbericht dokumentiert werden. Damit liegt keine sicherheitsempfindliche Stelle im Sinne der SÜFV vor. Maßnahmen des vorbeugenden personellen Sabotageschutzes, wie insbesondere Sicherheitsüberprüfungen von Mitarbeitern, sind dann nicht erforderlich. Kann dieser Nachweis nicht geführt werden, ist die SÜFV zu beachten (siehe (1)).

Nicht Gegenstand des Leitfadens sind außerbetriebliche Gefahrguttransporte. Grundsätzlich gilt aber, dass für Gefahrguttransporte ähnliche Sicherungsüberlegungen anzustellen sind, wie sie hier für die stationären Anlagen angestellt werden. Zu- und Abgangswege und insbesondere deren Sicherung müssen im Einzelfall auf Schnittstellen mit dem Transportwesen untersucht und behandelt werden. Für die Entwendung von Chemikalien bzw. deren vorsätzlichen Missbrauch sind ebenfalls gesonderte Überlegungen anzustellen. (Hinweis: 1.10 ADR)

Angriffe wie Industriespionage oder Diebstahl werden ebenfalls nicht betrachtet.

Die nachfolgende Abbildung gibt einen Überblick über das Konzept des Leitfadens zur Sicherung von Betriebsbereichen/Anlagen gegen Eingriffe Unbefugter.

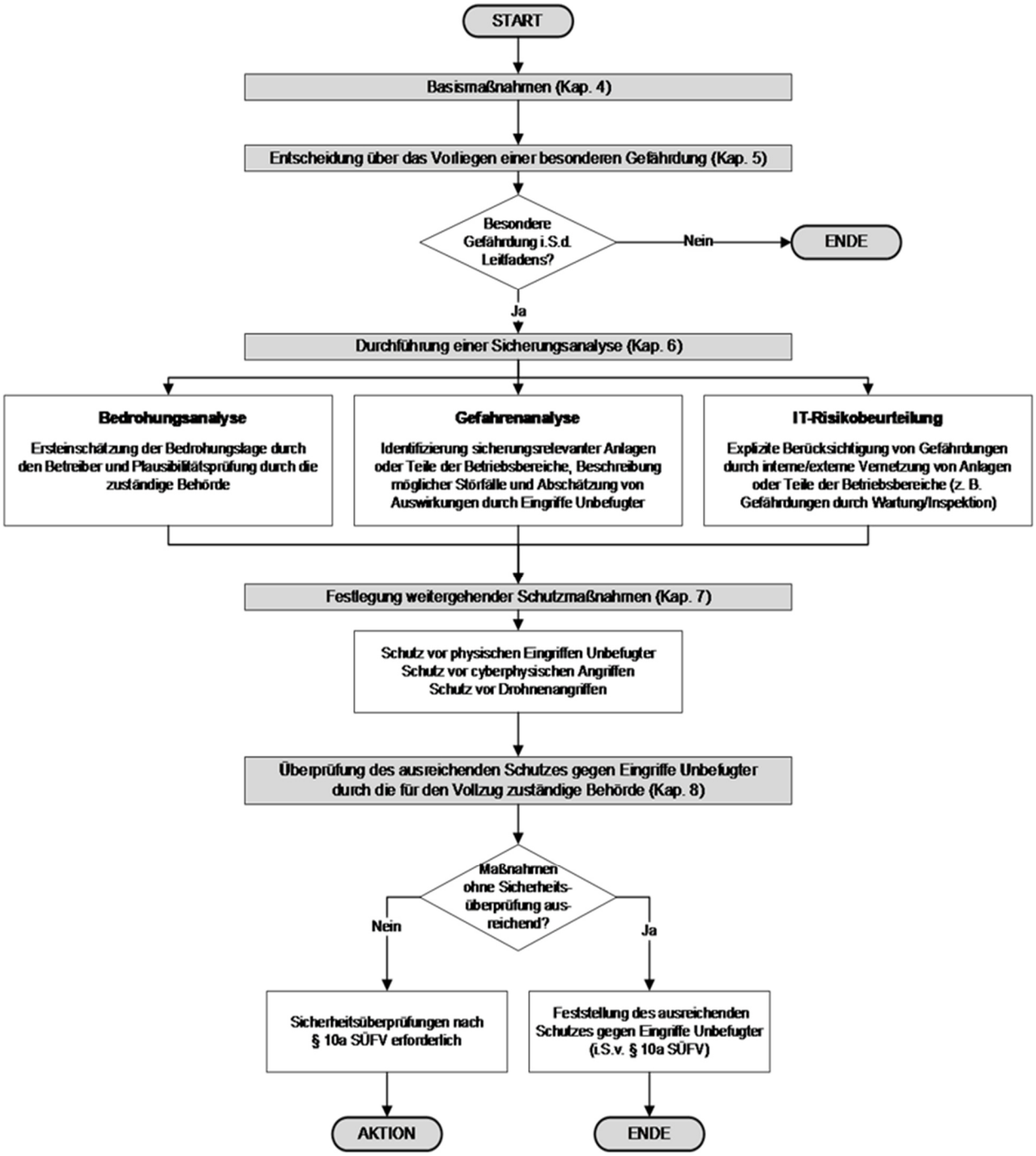

Abbildung 1: Vorgehen zur Sicherung von Betriebsbereichen und Anlagen gegen Eingriffe Unbefugter

3 Definitionen

Eine **besondere Gefährdung** im Sinne dieses Leitfadens liegt vor, wenn im Falle eines durch Eingriffe Unbefugter ausgelösten Ereignisses in einem Betriebsbereich

- eine ernste Gefahr für viele Menschen ausgelöst werden kann,
- Sachschäden außerhalb des Betriebsbereichs im Sinne des Anhang VI, Teil I Nr. 4b der 12. BImSchV ausgelöst werden können
- eine ernste, das Gemeinwohl beeinträchtigende Umweltschädigung ausgelöst werden kann.

Besondere Schutzobjekte im Sinne dieses Leitfadens sind z.B.

- Wohngebiete,
- soziale Einrichtungen, Schulen, Krankenhäuser oder
- öffentlich genutzte Gebäude (> 100 Personen gleichzeitig).

Sicherungsrelevante Anlagen, im folgenden Anlagen genannt, sind Anlagen in einem Betriebsbereich nach § 3 Abs. 5a BImSchG i. V. mit § 1 Abs. 1 und 2 StörfallV, die bei Eingriffen Unbefugter eine ernste Gefahr oder Sachschäden im Sinne der Störfall-Verordnung hervorrufen können.

Sicherheitsempfindliche Stelle ist die kleinste selbstständig handelnde Organisationseinheit innerhalb einer lebens- oder verteidigungswichtigen Einrichtung, die vor unberechtigtem Zugang geschützt ist und von der im Falle der Beeinträchtigung eine erhebliche Gefahr für die Schutzgüter „Leben oder Gesundheit großer Teile der Bevölkerung“, „öffentliche Sicherheit oder Ordnung“ sowie „Verteidigungsbereitschaft“ ausgeht (§ 1 Absatz 5 Satz 3 SÜG).

Ein **Unbefugter** im Sinne von § 3 Abs. 2 Nr. 3 der StörfallV ist hier jede Person, die Handlungen mit dem Ziel vornimmt, unmittelbar oder mittelbar einen Störfall zu verursachen. Hierbei ist es unerheblich, ob es sich um einen Mitarbeiter des Betreibers, einen von ihm Beauftragten oder einen Dritten handelt.

Als **Innentäter** werden Unbefugte im Sinne obiger Definition bezeichnet, die sich berechtigt im Betriebsbereich bzw. in der Anlage aufhalten oder zugreifen können.

Sicherungen sind alle Aktivitäten zur Verhinderung von Gefahren und Begrenzung von Auswirkungen, die durch Eingriffe Unbefugter ausgelöst werden können., Betreiber, Behörden oder sonstige Dritte können zur Sicherung beitragen. Sicherung entspricht dem Begriff „Security“ im englischen Sprachraum und ist zu unterscheiden von Sicherheit („Safety“).

Eine **Sicherungsanalyse** ist die Ermittlung und Bewertung von möglichen Eingriffen Unbefugter und der dadurch möglicherweise ausgelösten besonderen Gefahren im Sinne dieses Leitfadens unter Verwendung von systematischen Methoden. Ihre Erstellung setzt insbesondere Kenntnisse über mögliche Motivationen und Handlungsmöglichkeiten Unbefugter voraus. In der Sicherungsanalyse werden die Ergebnisse

- der Ermittlung und Beurteilung der spezifischen Gefährdungslage (Bedrohungsanalyse) mit den Ergebnissen
- der Ermittlung möglicherweise ausgelöster Gefahren im Rahmen der im Sicherheitsbericht nach StörfallV ohnehin erforderlichen Gefahrenanalyse und
- der Ermittlung und Bewertung der Auswirkungen von möglichen Cyber-Angriffen auf die Integrität und Verfügbarkeit bei einsetzten Komponenten und Systemen zur Prozess- und Sicherheitssteuerung (IT-Risikobeurteilung)

zusammengeführt. Die Sicherungsanalyse ist Voraussetzung für die Ableitung von **Sicherungszielen** und der erforderlichen **Sicherungsmaßnahmen.** Da die Sicherungsanalyse die Erfüllung von Pflichten der StörfallV nachweisen soll, wird empfohlen, das Ergebnis der Sicherungsanalyse als Bestandteil des Sicherheitsberichts nach § 9 StörfallV zu dokumentieren und regelmäßig zu überprüfen und fortzuschreiben.

Assets sind im Betriebsbereich eingesetzte Komponenten und Software (etwa Sensoren, Netzwerk-Switch, Kameras, etc.) und Systeme (PLS, Engineering Workstations, etc.) und deren Konfiguration.

Eine **Schwachstelle** ist ein sicherheitsrelevanter Fehler eines Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen. Vgl. Quelle: **(2)**

Eine **Bedrohung** ist ganz allgemein ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände, Umwelt oder Gesundheit. Vgl. Quelle: **(2)**

Eine **IT-Bedrohung** ist ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer bzw. Benutzer der Informationen ein Schaden entstehen kann. Vgl. Quelle: (3)

Als **Gefährdung** wird eine ernste Gefahr bezeichnet, die für ein konkretes Schutzgut wie Vermögen, Wissen, Gegenstände, Umwelt oder Gesundheit besteht, aber noch nicht eingetreten ist.

Eine **IT-Gefährdung** ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirken kann. Eine IT-Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt. Vgl. Quelle: **(2)**

Mit **Zugang** wird die Nutzung von IT-Systemen, System-Komponenten und Netzen bezeichnet. Zugangsberechti-gungen erlauben somit einer Person, bestimmte Ressourcen wie IT-Systeme oder System-Komponenten und Netze zu nutzen. Quelle: **(2)**

Mit **Zugriff** wird die Nutzung von Informationen oder Daten bezeichnet. Über Zugriffsberechtigungen wird geregelt, welche Personen im Rahmen ihrer Funktionen oder welche IT-Anwendungen bevollmächtigt sind, Informationen, Daten oder auch IT-Anwendungen zu nutzen oder Transaktionen auszuführen. Quelle: **(2)**

Mit **Zutritt** wird das Betreten von abgegrenzten Bereichen wie z. B. Räumen oder geschützten Arealen in einem Gelände bezeichnet. Zutrittsberechtigungen erlauben somit Personen, bestimmte Umgebungen zu betreten, also beispielsweise ein Gelände, ein Gebäude oder definierte Räume eines Gebäudes. Quelle: **(2)**

Schadsoftware wird mit dem Ziel entwickelt unerwünschte und meistens schädliche Funktionen auszuführen. Im Sprachgebrauch synonyme Begriffe sind Schadprogramme oder Malware. Quelle: **(2)**

Die **zuständige Behörde** für den Vollzug der StörfallV ist die nach Landesrecht für die Genehmigung und Überwachung zuständige Behörde.

4 Basismaßnahmen

Die Basismaßnahmen sind von allen Betreibern von Betriebsbereichen umzusetzen.

Festlegung von Verantwortlichkeiten

- Verantwortlichkeit für die Maßnahmen zum Schutz vor Eingriffen Unbefugter muss eindeutig zugewiesen sein.
- Effektive Maßnahmen zum Schutz vor Eingriffen Unbefugter festlegen und dokumentieren.
- Regelmäßige Überprüfung der Maßnahmen.
- Vertraulichkeit bezüglich der getroffenen Schutzmaßnahmen sicherstellen.

Zugangs- und Zutrittsmanagement und -überwachung

- Physischer Zugang (zu Anlagen, Gefahrstoffen, Komponenten, Steuerungen, Computern) und der Zutritt auf das Gelände sind geeignet zu begrenzen.
- Geeignete Dokumentation des Zutritts zu sensiblen Bereichen.
- Schlüsselmanagement („Hierarchiestufen“ für Schutzbereiche und Zugangsberechtigungen) festlegen und Schlüssel regelmäßig kontrollieren.
- Bei Personal- und Funktionswechseln Vergabe der Berechtigungen überprüfen.
- Überwachung von Verboten und Geboten sicherstellen.

Zugriffsmanagement auf Prozesssteuerung/Sicherheitssteuerung

- IT-/OT-Systeme (Operational Technology Systems) sind in geeigneter Form zu trennen (Segmentieren).
- Voreingestellte Passwörter (Default) müssen geändert werden und Maßnahmen gegen Mißbrauch festgelegt werden (siehe Quelle (3)).
- Sicherheitsrelevante Veränderungen an der Anlagensteuerung über „Vier-Augen-Prinzip“ (unabhängige Prüfinstanz) absichern.
- Für besonders relevante Eingriffe: Absicherung durch technische Maßnahmen (z. B. Schlüsselschalter mit entsprechender Berechtigung)

- Prozesssteuerung/Sicherheitssteuerung sind vor dem Einsatz auf Schadsoftware zu überprüfen.
- Es ist sicherzustellen, dass externe Speichermedien und Hardwarekomponenten (z. B. Laptop des Servicetechnikers) ausreichend vor der Infektion mit Schadsoftware geschützt sind.[1]

Manipulationserkennung und –schutz

- Die Anlagen selbst sind so zu sichern, dass ein Störfall ohne interne Kenntnisse und/oder technische Hilfsmittel durch Unbefugte nicht ausgelöst werden kann.
- Frühzeitige Erkennung bzw. Verhinderung von Manipulationen an Systemen (z. B. Maßnahmen zum Schutz vor bzw. zur Erkennung von Schadsoftware, Maßnahmen gegen Fehlbedienung)
- Dies gilt auch für Maßnahmen zum physischen Schutz (Integritätsüberwachung der Zäune und Schlösser, Zutrittsschutz, ggf. Kameraüberwachung)

Regelungen für Fremdpersonal und fremdvergebene Dienstleistungen

- Regelungen zum Schutz vor Eingriffen Unbefugter in die generelle Unterweisung und Einweisung zu den betrieblichen Gefahrenquellen einbinden.
- Überwachung der fremdvergebenen Arbeiten in geeignetem Umfang durch unabhängiges oder eigenes Personal.
- Vertragliche Regelung mit Dienstleistern zur Integrität der Daten sowie zur Vertraulichkeit der Arbeitsergebnisse und der übergebenen Dokumentation treffen.

Sensibilisierung/Schulung eigener Mitarbeiter

- Zielgruppenorientiertes und risikobasiertes Schulungskonzept gegen Eingriffe Unbefugter und zur IT-Sicherheit umsetzen.
- Motivation zur Meldung von Abweichungen bzgl. des physischen Schutzes und der IT-Sicherheit fördern. Die Meldung sollte über ein betriebliches Meldesystem sichergestellt werden.

Reaktion auf neue Schwachstellen und IT-Bedrohungen

- Es sind grundlegende Maßnahmen zu treffen, um auf kritische Schwachstellen und IT-Bedrohungen reagieren zu können, z. B. durch das Installieren von sicherheitsrelevanten Aktualisierungen (z. B. Fehlerbehebungen). Um die Wirksamkeit der getroffenen Maßnahmen dauerhaft sicherzustellen, sollten diese auf gegenseitige Wechselwirkung und mögliche Beinflussung überprüft werden.

5 Entscheidung über das Vorliegen einer besonderen Gefährdung

Sofern dem Betreiber oder der zuständigen Behörde **im Einzelfall** Informationen vorliegen, dass von dem Betriebsbereich durch Eingriffe Unbefugter eine besondere Gefährdung im Sinne dieses Leitfadens ausgehen kann, ist eine Sicherungsanalyse gemäß Kap. 6 durchzuführen. Als Ergebnis können ggf. über die Basismaßnahmen gemäß Kap. 4 hinaus weitergehende Schutzmaßnahmen erforderlich sein. Der Umfang der weitergehenden Schutzmaßnahmen gemäß Kap. 7 ist dann aufgrund der Ergebnisse einer Sicherungsanalyse gemäß Kap. 6 festzulegen.

In der Regel wird das mögliche Schadensausmaß bei **Betriebsbereichen der oberen Klasse** infolge der definitionsgemäß höheren Störfallstoffmenge so weitreichend sein, dass die weitergehenden Schutzmaßnahmen erforderlich sind. Jedoch kann auch bei Betriebsbereichen der oberen Klasse aufgrund spezifischer Rahmenbedingungen ein größeres Schadensausmaß unwahrscheinlich werden und damit nur einige Maßnahmen nach Kap. 7 umzusetzen sind. Im Einzelfall sind die spezifischen Rahmenbedingungen

[1] Es ist sicherzustellen, dass ein Gerät mit einem aktiven Malwareschutz mit aktueller Malwaresignaturdatenbank ausgestattet ist oder das Gerät ist vor der Nutzung auf Schadsoftware zu überprüfen.

auf der Grundlage einer Sicherungsanalyse gemäß Kap. 6 von Betreiber und Behörde gemeinsam zu betrachten und zu bewerten.

6 Sicherungsanalyse

Die Sicherungsanalyse ist die Ermittlung und Bewertung von möglichen Eingriffen Unbefugter und der dadurch ausgelösten Gefahren. Ihre Erstellung setzt insbesondere Kenntnisse über mögliche Motivationen (Bedrohungsanalyse) und Handlungsmöglichkeiten Unbefugter (Gefahrenanalyse) voraus.

Aus der Sicherungsanalyse können Sicherungsziele und erforderliche Sicherungsmaßnahmen abgeleitet werden.

Insbesondere sollen Betreiber prüfen, ob die jeweiligen Unternehmen und Betriebsbereiche ein herausgehobenes Ziel darstellen können (Bedrohungsanalyse, siehe Kap. 6.1) und ob Eingriffe Unbefugter zu einer besonderen Gefährdung im Sinne dieses Leitfadens führen könnten (Gefahrenanalyse, siehe Kap. 6.2 und IT-Risikoanalyse, Kap. 6.3). Nicht alle Unternehmen und Betriebsbereiche sind aber in gleichem Maße als Ziele für kriminelle Angriffe anzusehen. Generell sind IT-/OT-Systeme in einem Betriebsbereich attraktiv für Cyber-Angriffe. Das gilt insbesondere für Sicherheitssteuerungen, Prozessleitsysteme und Netzwerkkomponenten.

Es ist dem Betreiber freigestellt, andere Vorgehensweisen als die im Folgenden beschriebenen zu wählen. Sie sollen jedoch das gleiche Schutzniveau gewährleisten.

Besonders wichtig ist neben den möglichen sicherheitstechnischen und organisatorischen Verbesserungen vor allem die gute und intensive Zusammenarbeit zwischen Betreibern und Sicherheits- und Gefahrenabwehrbehörden. Soweit zum Schutz vor Eingriffen Unbefugter behördliche Unterstützung erforderlich ist, sollte der Betreiber den Kontakt zur zuständigen Behörde aufnehmen.

6.1 Bedrohungsanalyse

Im Kern kommt es darauf an zu prüfen, inwieweit die Anlagen bzw. die Umgebung für den Eingriff Unbefugter besonders „attraktiv“ erscheinen. Dazu ist eine Bewertung erforderlich, in der insbesondere die folgenden Aspekte zu berücksichtigen sind:

- Einschätzung der Bedrohungslage durch den Betreiber (z. B. allgemeine Sicherheitslage, Größe und Zusammensetzung der Belegschaft, Qualität der Sicherheitsorganisation, geografische Lage und Anbindung, Art und Ausmaß möglicher Auswirkungen, gesellschaftliche Position von Angehörigen der Unternehmensleitung, Symbolcharakter des Unternehmens bzw. der Anlage, Art der Vertriebsverbindungen und Auslandsaktivitäten)
- Plausibilitätsprüfung der Einschätzung der Bedrohungslage durch die zuständige Behörde.

6.2 Identifizierung der sicherungsrelevanten Anlagen / Teile des Betriebsbereichs (Gefahrenanalyse)

Die Gefahrenanalyse soll ergeben, ob Eingriffe Unbefugter zu einer besonderen Gefährdung im Sinne dieses Leitfadens führen könnten. Dabei soll auch ermittelt werden, von welchen Anlagen / Teilen des Betriebsbereichs eine Gefahr ausgeht und welche daher besonders sicherungsrelevant sind.

Wesentliche Elemente der Gefahrenanalyse können dem Sicherheitsbericht entnommen werden. Von Bedeutung sind insbesondere folgende Informationen:

- Beschreibung der Störfälle gemäß § 3 Abs. 1 und 3 StörfallV.
- Abschätzung der Auswirkungen von Störfällen. Diese Angaben sind für Betriebsbereiche der oberen Klasse ohnehin notwendig im Rahmen der den Gefahrenabwehrbehörden gemäß § 10 Abs. 1 Nr. 2 StörfallV zur Verfügung zu stellenden Informationen.

Bei der Bewertung ist darauf zu achten, dass durch Eingriffe Unbefugter gegebenenfalls passive Sicherheitseinrichtungen zerstört werden könnten, deren Versagen sonst ausgeschlossen wird.

6.3 IT-Risikobeurteilung

Gefährdungen im IT-Bereich sind zeitlich nicht konstant; ständig werden neue IT-Gefährdungen identifiziert; neue IT-Bedrohungen können etwa auf vorhandene Schwachstellen einwirken bzw. es werden neue Schwachstellen bekannt, auf die

vorhandene IT-Bedrohungen einwirken können. Daher muss die Gefährdungslage ständig beobachtet[2] werden.

Dementsprechend ist die gesamte IT-Risikobeurteilung regelmäßig und anlassbezogen zu wiederholen, damit sichergestellt ist, dass umgesetzte Schutzmaßnahmen weiterhin bekannte Risiken effektiv mindern und neue IT-Gefährdungen berücksichtigt werden. Das Intervall zwischen den Beurteilungen sollte nicht länger als 2 Jahre sein. Auslöser für eine vorzeitige Überprüfung können unter Anderem sein:

- bekannt werden von IT-Gefährdungen, die die Integrität und Verfügbarkeit der sicherheitstechnischen Einrichtungen beeinträchtigen können
- Integration neuer oder Austausch bestehender Komponenten oder Systeme

Der Betreiber muss das Intervall und die Auslöser geeignet festlegen und begründen.

Die IT-Risikobeurteilung

- erfasst Schwachstellen aus Sicht der IT-Sicherheit für alle im Betriebsbereich eingesetzten Assets.
- erfasst IT-Gefährdungen aus Sicht der IT-Sicherheit. IT-Gefährdungen sind IT-Bedrohungen, die von extern oder intern über Schwachstellen auf Komponenten und Systeme einwirken können.
- identifiziert die möglichen Auswirkungen der IT-Gefährdungen auf die Integrität und Verfügbarkeit der sicherheitstechnischen Funktionen (nach DIN EN 61511) (Auswirkungsanalyse) und
- bewertet diese anhand der Wahrscheinlichkeit des Ausnutzens der IT-Schwachstelle.

Mit der IT-Risikobeurteilung wird die Effektivität der vorhandenen Schutzmaßnahmen in Bezug auf die aktuellen IT-Gefährdungen bewertet. Sofern die vorhandenen Schutzmaßnahmen die identifizierten Risiken nicht effektiv mindern, sind zur effektiven

[2] Siehe etwa CERT Bund. Verfügbar unter https://www.cert-bund.de/wid

Minderung geeignete Anpassungen an den vorhandenen Maßnahmen durchzuführen oder geeignete Maßnahmen zu implementieren.

Für Details zur IT-Risikobeurteilung siehe Anhang 2.

7 Weitergehende Schutzmaßnahmen

7.1 Umgang mit verschiedenen Auslösern

7.1.1 Schutz vor physischen Eingriffen Unbefugter, die sich gewaltsam Zutritt verschaffen (Außentäter)

Zum Schutz vor Außentätern dient primär die Zutrittssicherung (siehe Basismaßnahmen, Kap. 4). In Kap. 6.2 identifizierte sicherungsrelevante Anlagen, die durch Außentäter potentiell gefährdet sind, sollten zusätzlich gegen Zutritt und Angriffe von außen gesichert werden (z. B. speziell gesicherte Räume, Anfahrschutz, etc.). Es sollte auch geprüft werden, ob die örtliche Lage solcher Anlagen geheimhaltungsbedürftig ist (siehe Kap. 7.2.4).

Auch gilt dies für die Grenzen der internen Netze des Betriebsbereichs zu externen. Innerhalb des Betriebsbereichs sind IT-Bereiche unterschiedlichen Sicherheitsniveaus voneinander zu trennen. Grenzen beziehen sich nicht nur auf Vernetzung, sondern auch auf den Transport von Wechseldatenträgern.

Industrieparks (insbesondere Chemieparks) stellen wegen der Vielzahl rechtlich selbständiger Betreiber besondere Anforderungen an die Schutzmaßnahmen gegen Eingriffe Unbefugter. Die Angreifbarkeit gefährlicher Anlagen kann hier in der Regel nur durch eine einheitliche Überwachung minimiert werden (gemeinsamer Werkszaun und Werkschutz).

7.1.2 Schutz vor unbefugten Eingriffen durch Innentäter

Ein Risiko kann insbesondere auch von sogenannten Innentätern ausgehen. Hierunter werden Mitarbeiter des eigenen Unternehmens bzw. von Fremdfirmen verstanden, die sich befugt im Bereich sicherungsrelevanter Anlagen aufhalten (oder sich die Befugnis

erschlichen haben) und unbefugte Eingriffe vornehmen. Sie können über gute Kenntnis der entsprechenden Anlagen verfügen und dies in krimineller Absicht nutzen wollen.

Neben den allgemeinen Maßnahmen insbesondere gegen Fehlbedienungen (siehe Basismaßnahmen, Kap. 4) kommen verschiedene weitergehende, z. T. auch präventive Schutzmaßnahmen in Betracht. Diese sind vor allem dem Bereich der Personalführung und -fürsorge zuzuordnen (Erzeugung einer Identifikation mit dem Unternehmen, Motivation, sensibler Umgang mit belastenden Personalmaßnahmen, Schulung der Vorgesetzten etc.). Darüber hinaus sollte eine allgemeine Sensibilisierung aller Mitarbeiter gegenüber dieser Gefährdung durch Innentäter geschaffen werden. Eine Beratung durch Psychologen kann ggf. sinnvoll sein.

Hinsichtlich der Angriffspfade (Kap. 7.1.1 und 7.1.2) kommt der qualitativen und quantitativen personellen und technischen Ausstattung des Personals mit Sicherungsaufgaben (z. B. Werkschutz) besondere Bedeutung zu.

7.2 Sicherungsmaßnahmen

7.2.1 Einführung eines Sicherungsmanagements

Zur Umsetzung der Sicherungsziele und der sich daraus ergebenden Maßnahmen wird ein Sicherungsmanagement empfohlen, das Teil des Sicherheitsmanagements nach Anhang III Störfall-Verordnung sein sollte. Zum Sicherheitsmanagementsystem werden Hinweise in KAS-19 gegeben. Bei Integration des Sicherungsmanagements in ein Sicherheitsmanagement nach Anhang III Störfall-Verordnung sind die einzelnen Maßnahmen in geeigneter Weise in die Systematik des Anhangs III einzufügen, so dass ein einheitliches Managementsystem im Sinne des Anhangs III erhalten bleibt. Die zuständige Behörde bezieht im Rahmen ihrer Überwachung nach § 16 Störfall-Verordnung die Überprüfung der Sicherungsmanagement-Bausteine mit ein.

Im Sicherungsmanagement sollten Maßnahmen definiert werden, um auf Cyber-Angriffe effektiv reagieren zu können. Darüber hinaus sollen hier die erforderlichen und umsetzbaren Maßnahmen zum Schutz vor Drohnenangriffen dargestellt werden.

Zum Aufbau und Unterhalt eines Sicherungsmanagements werden Hinweise in Anlage 1 gegeben.

Es wird empfohlen, die Maßnahmen im Hinblick auf die Gefährdungslage zu staffeln („keine Gefährdung“ bis „Unbefugte in den Betriebsbereich eingedrungen“). Ferner sollte berücksichtigt werden, dass die Gefährdungslage sich durch interne und externe Entwicklungen u. U. sehr kurzfristig verändern kann und somit kontinuierlich beobachtet werden sollte.

7.2.2 Schutz vor cyberphysischen Angriffen

Generell ist der Betreiber des Betriebsbereichs dafür verantwortlich, das Risiko durch cyberphysische Angriffe zu bewerten und ggf. notwendige technische und organisatorische Gegenmaßnahmen zu ergreifen. Dabei sind die schnelle technologische Entwicklung und die daraus resultierenden Veränderungen der Rahmenbedingungen und der möglichen Gegenmaßnahmen in diesem Bereich zu berücksichtigen (siehe Anhang 2).

7.2.3 Schutz vor Drohnenangriffen

Generell ist der Betreiber des Betriebsbereichs dafür verantwortlich, das Risiko durch Drohnenangriffe zu bewerten und ggf. notwendige technische und organisatorische Gegenmaßnahmen zu ergreifen. Dabei sind die schnelle technologische Entwicklung und die daraus resultierenden Veränderungen der Rahmenbedingungen und der möglichen Gegenmaßnahmen in diesem Bereich zu berücksichtigen (siehe Anhang 3).

7.2.4 Geheimhaltung von Unterlagen

Die Geheimhaltung von Unterlagen bedarf einer sorgfältigen Abwägung. Jegliche Information, die einem Unbefugten den Eingriff erleichtert oder ihn dazu animieren könnte, muss geschützt werden. Gleichzeitig muss sichergestellt sein, dass alle Informationen, die zur Bekämpfung eines Störfalls benötigt werden, jederzeit verfügbar sind. Es ist zu beachten, dass die Information Betroffener über sie betreffende Risiken nicht nur ein Freiheitsrecht darstellt, sondern auch ein Element der Störfallvorsorge ist.

Zum Schutz der öffentlichen Sicherheit sind im Sinne des § 11 Absatz 6 der StörfallV insbesondere die Teile des Sicherheitsberichts der Öffentlichkeit nicht zugänglich zu machen, aus denen Schlüsse über die Auslösung möglicher Störfallszenarien gezogen werden können.

Zu den Informationen, die nicht im Sicherheitsbericht veröffentlicht werden dürfen, gehören weiterhin etwa Details zur Anbindung des Betriebsbereiches an IT-/OT-Systeme (z. B. an den Industriepark oder an das Internet, zur IT Netzwerkkonfiguration innerhalb des Betriebsbereiches, zur Fernwartungslösung und deren Anbindung ans Internet, zu den verwendeten OT Netzwerkkomponenten, zu den verwendeten Prozess- und Sicherheitssteuerungen, Engineering Workstations sowie deren Konfiguration und die Ergebnisse von Penetrationstests).

Dagegen dürfen Angaben zu den Auswirkungen möglicher Störfälle nicht geheim gehalten werden; sie bilden die Grundlage für die Maßnahmen zum Schutz der Nachbarschaft, die in der Information der Öffentlichkeit gemäß §§ 8a und 11 der StörfallV dargestellt werden. Das genaue Vorgehen ist mit der zuständigen Behörde abzustimmen.

8 Notwendigkeit für Sicherheitsüberprüfungen (§ 10a SÜFV) für Betriebsbereiche der oberen Klasse

Ob die getroffenen organisatorischen oder technischen Maßnahmen ausreichend sind, um den Betrieb gegen Eingriffe Unbefugter zu schützen, beurteilt die zuständige Behörde aufgrund der Einschätzung des Betreibers. Diese kann aus dem Sicherheitsbericht ersehen, ob der Betreiber seine Pflicht nach § 3 Absatz 2 Nummer 3 in Verbindung mit § 9 Absatz 1 Nummer 2 der Störfall-Verordnung erfüllt hat. Der Sicherheitsbericht dient dem Betreiber insoweit als Rechtssicherheitsnachweis.

Die zuständige Behörde überprüft in diesem Zusammenhang die Sicherungsanalyse und die Qualität der Umsetzung der Basismaßnahmen gemäß Kap. 4. und die darüber hinaus getroffenen Maßnahmen gemäß Kap. 7.

Die Notwendigkeit von Sicherheitsüberprüfungen gemäß SÜG i.V.m. § 10a SÜFV ist vor dem Hintergrund der umgesetzten organisatorischen und technischen Maßnahmen hinsichtlich der erreichten Risikoreduzierung zu bewerten (siehe (1)).

9 Literaturverzeichnis

1. **Bundesministerium für Wirtschaft und Energie.** *Leitfaden - Vorbeugender personeller Sabotageschutz im nichtöffentlichen Bereich; Satellitendatensicherheit.* Berlin : s.n., 2018.

2. **Bundesamt für Sicherheit in der Informationstechnik.** *IT-Grundschutz Kompendium.* Bonn : s.n., 2019.

3. **Informationstechnik, Bundesamt für Sicherheit in der.** *IT-Grundschutz-Kompendium Baustein ORP.4.A8.* Bonn : s.n., 2019.

4. **Kommission für Anlagensicherheit.** *Empfehlungen für Abstände zwischen Betriebsbereichen nach derStörfall-Verordnung und schutzbedürftigen Gebieten im Rahmen der Bauleitplanung — Umsetzung § 50 BImSchG.* Bonn : s.n., 2010.

Anhang 1

Sicherungsmanagement

Managementsysteme haben sich in der Vergangenheit als Instrument zur systematischen Handhabung und Überprüfung von Unternehmensabläufen bewährt. Insbesondere im Zusammenhang mit Unternehmenssicherheit ist eine ständige systematische Steigerung von Effizienz und Transparenz der Prozesse von größter Bedeutung. Die Vorgehensweise und die zusätzlichen Elemente eines Managementsystems zur Sicherung des Unternehmens sollen im Folgenden kurz skizziert werden. Unternehmen sollten solche Systeme verbindlich einführen.

Unternehmenspolitik

In einer Selbstverpflichtungserklärung (Sicherungspolitik) macht das Unternehmen sein Verhältnis zu Sicherheit und Sicherung deutlich. Das Unternehmen verpflichtet sich, zusammen mit seinen Angestellten und seinen von ihm beauftragten Auftragnehmern dafür sorgen zu wollen, dass ständig eine sichere Arbeitsumgebung gewährleistet wird, in der die Investitionsgüter und die Betriebe gegen das Risiko von Verletzungen, Verlusten und Zerstörung durch Eingriffe Unbefugter geschützt und deren etwaigen Folgen für die Nachbarschaft und die Umwelt begrenzt werden. Weiter erklärt das Unternehmen seine Verpflichtung, die angesprochenen Sicherheitsmaßnahmen auf dem Stand der Technik zu halten und das Sicherungsmanagementsystem regelmäßig zu überprüfen.

Dokumentation

Um ein Managementsystem prüfbar und überwachbar zu machen, ist es notwendig, einen Soll/Ist- Vergleich vornehmen zu können. Für ein Sicherungs-Managementsystem stellt dies eine Herausforderung dar, da zum einen eine Soll–Beschreibung vorhanden sein sollte, andererseits diese aber nicht dazu führen darf, dass durch die Art der Beschreibung das eigentliche Ziel - nämlich den Eingriff Unbefugter zu verhindern - durch eine zu detaillierte Darstellung aller organisatorischen und technischen Sicherungseinrichtungen in Frage gestellt wird.

Details der konkreten organisatorischen und technischen Maßnahmen sollten daher gegen den Zugriff aller Personen, die dieses Wissen nicht unmittelbar benötigen,

geschützt werden und nicht öffentlich zugänglich aufbewahrt werden. Bei einer Überprüfung des Sicherungsmanagementsystems durch die zuständigen Behörden sind die entsprechenden Unterlagen zu sichten und das Ergebnis der Prüfung ist zu dokumentieren.

Grundsätzliche Aussagen zur Offenlegung von Sicherheits- bzw. Sicherungsunterlagen enthält Kap. 7.2.4 des Leitfadens.

Organisation und Verantwortlichkeit

Zur Verantwortung des Unternehmens gehört, dass Vorgehensweisen entwickelt werden müssen, die sicherstellen, dass die Sicherungsrisiken identifiziert (siehe Kapitel 6.1, 6.2, 6.3) werden und ihnen mit Sicherungsmaßnahmen begegnet wird (siehe Kapitel 4 und 7). Für Sicherungsvorfälle wird ein Prozess eingeführt, der dafür sorgt, dass das Management unverzüglich unterrichtet wird.

Kommunikation und Schulung

Über Sicherungsvorfälle und Erfahrungen mit Sicherungstechnik wird mit anderen ein Informationsaustausch betrieben, um sicherzustellen, dass der jeweils aktuelle Stand der Sicherungstechnik bei den eigenen Maßnahmen eingehalten wird. Durch regelmäßige Schulung ist dafür zu sorgen, dass fachkompetentes Personal beschäftigt wird und dass das Personal sich der aktuellen Sicherungsrisiken bewusst ist. Dies wird durch regelmäßige Unterweisung zur Schulung des Bewusstseins für Sicherungsrisiken und ein spezielles Trainingsprogramm für das Personal mit Sicherungsaufgaben geleistet.

Festlegung der Sicherungsprozesse

Alle Unternehmensprozesse, in denen die Sicherung eine Rolle spielt, müssen festgelegt, dokumentiert und geplant sein. Hierbei sind insbesondere folgende Prozesse zu berücksichtigen:

- **Kontraktorenüberwachung**

  Kontraktoren, die mit dem Unternehmen geschäftlich verbunden sind, müssen sich den Sicherungsregeln und -prozeduren des Unternehmens anschließen und auch diesen Regeln entsprechende eigene Überwachungen (Audits) durchführen.

- **Planung und Errichtung von Anlagen**

  Bei der Planung und Errichtung von Anlagen ist die Beachtung der Sicherungsanforderungen ein wesentliches Element. Die Beachtung der Sicherungsziele muss entsprechend dokumentiert werden.

- **Veränderungsmanagement**

  Die Auswirkungen von zeitweiligen oder andauernden Veränderungen auf die Sicherungslage müssen genau geprüft, gesteuert und dokumentiert werden. Um auf Veränderungen der Sicherungslage ohne Verzug reagieren zu können, sind Maßnahmenkataloge für die unterschiedlichen Niveaus von Gefährdungslagen vorzuhalten.

- **Notfallmanagement**

  Ausrüstung, Installation und Personal für die Bewältigung von Sicherungsnotfällen ist zu identifizieren und verfügbar zu halten. Für die Bewältigung von Notfällen ist eine Krisenabwehrorganisation bereitzuhalten. Eine Kernbesetzung sollte vorab festgelegt werden. Die Zusammensetzung kann jedoch je nach Situation unterschiedlich sein.

- **Zusammenarbeit mit Behörden und Interessensvertretern**

  Ein offener Dialog mit Behörden und Interessenvertretungen stellt sicher, dass die möglicherweise in den Anlagen auftretenden Sicherungsprobleme identifiziert und die Risiken minimiert werden können. Die Besorgnisse der Allgemeinheit sollen ernst genommen und geeignet berücksichtigt werden.

Betrieb und Wartung der Sicherungseinrichtungen

Sicherungseinrichtungen müssen so betrieben und gewartet werden, dass sie sich stets auf dem Stand der Technik befinden und immer einsatzbereit sind.

Überwachungsmaßnahmen

In Übereinstimmung mit der Unternehmenspolitik wird in regelmäßig wiederkehrenden Untersuchungen des Sicherungsmanagements der Status untersucht und festgehalten.

Es werden regelmäßige und anlassbezogene interne Audits durchgeführt. Kap. 4 und 7 dieses Leitfadens enthalten zu prüfende Elemente.

Korrektur- und Vorbeugungsmaßnahmen

Sicherungsvorfälle werden festgehalten, berichtet und je nach Schweregrad bzw. entsprechendem Potential umfassend untersucht. Die Vorfalluntersuchungen werden dokumentiert und die notwendigen präventiven Maßnahmen festgehalten.

Anhang 2

IT-Sicherheit

Die folgenden Anforderungen sind als Ergänzung zu den Basismaßnahmen (Kapitel 4 dieses Leitfadens) zu verstehen, um eine höhere Resilienz gegen Cyberangriffe zu erzeugen. Sie basieren auf den Anforderungen des BSI IT-Grundschutz-Kompendiums. Quelle (2)

Die Integration der Informationssicherheit im Sicherheitsmanagementsystem kann in Anlehnung an die ISO-27000-Normenreihe erfolgen. Die folgenden Leitsätze konkretisieren die Anforderung zur Anwendung auf Betriebsbereiche im Sinne des § 3 Absatz 5a des BImSchG.

Zu den Anforderungen werden Kontrollfragen formuliert. Diese sollen helfen, die Anforderungen umzusetzen, das Verständnis zu verbessern und die Umsetzung zu überprüfen, sind jedoch nicht abschließend.

IT-Security ist Führungsaufgabe

- Die Leitung der Organisation ist für die IT-Sicherheit in der Organisation verantwortlich.
- Die Leitung der Organisation erstellt eine IT-Sicherheit-Richtlinie für die Organisation. Die IT-Sicherheit-Richtlinie ist regelmäßig an veränderte interne und externe Rahmenbedingungen anzupassen.
- In der IT-Sicherheit-Richtlinie legt die Leitung die IT-Sicherheit-Ziele der Organisation in Abhängigkeit von der Strategie der Organisation und von relevanten gesetzlichen Anforderungen fest.
- Zur Erreichung der IT-Sicherheit-Ziele schafft die Leitung geeignete Organisationsstrukturen und Prozesse.
- Die Leitung stellt die notwendigen Ressourcen zur Erreichung der IT-Sicherheit-Ziele bereit.

Kontrollfragen:

- *Wer ist als Verantwortlicher (Person/Abteilung) festgelegt?*

- *Wie sind für IT-Sicherheit zuständige Mitarbeiter in die Unternehmensstruktur eingebunden?*
- *Gibt es Richtlinien/Vorgaben zur IT-Sicherheit?*
- *Welche Ressourcen stehen für IT-Sicherheit zur Verfügung?*

Sensibilisierung und Unterweisung

- Die Leitung kommuniziert die IT-Sicherheit-Richtlinie an alle Mitarbeiter und alle berechtigten Dritten, welche die IT-Sicherheit der Organisation unmittelbar beeinflussen können.
- OT-Systeme: Operational Technology Systems, d. h. Systeme der Betriebstechnik
- In der Folge werden unter IT-Systemen sowohl IT- als auch OT-Systeme verstanden. Gleiches gilt für IT-Sicherheit.
- Die Leitung führt geeignete Maßnahmen zur zielgruppenspezifischen Sensibilisierung der Mitarbeiter bezüglich der Risiken durch, die sich aus Cyberangriffen auf Betriebsbereiche ergeben und sich auf die funktionale Sicherheit der Organisation auswirken können.
- Zur Etablierung der betrieblichen Security-Kultur werden alle Mitarbeiter und Dritte regelmäßig in den Maßnahmen zur Erreichung der Sicherheitsziele geschult und unterwiesen. Dritte werden im Rahmen der üblichen Sicherheitseinweisung unterrichtet.
- Die Effektivität der Maßnahmen wird regelmäßig überprüft.

Kontrollfragen:

- *Wie werden Mitarbeiter und Dienstleister hinsichtlich IT-Sicherheit sensibilisiert?*
- *Wie wird die Effektivität und Aktualität der Sensibilisierungsmaßnahmen geprüft?*

Asset Register und Netzwerkarchitektur

- Relevant im Sinne der IT-Sicherheit sind solche Teile und Komponenten von Anlagen (Assets), deren Manipulation durch einen Cyberkriminellen eine

mittelbare oder unmittelbare Auswirkung auf die funktionale Sicherheit der Anlage hat. Assets können sein:

  - sicherheitsrelevante Anlagenteile, Komponenten, Bauteile;
  - sicherheitsrelevante Software;
  - alle Netzwerk-Ein- und -Ausgangspunkte zu anderen Netzwerken;
  - alle IT-Systeme außerhalb des Produktionsbereiches, von denen eine Kommunikationsbeziehung in den Produktionsbereich aufgebaut werden kann;
  - alle den Betriebsbereich betreffende sicherheitsrelevante Dokumentationen.

- Zur Erfassung aller Assets ist es zweckmäßig ein Asset Register anzulegen. Für jedes Asset ist ein Verantwortlicher und der Schutzbedarf des Assets für den Betriebsprozess festzulegen.
- Zur Darstellung der Kommunikationsbeziehungen zwischen den Assets ist ein Netzwerk-Architekturbild anzufertigen. Sämtliche Übertragungsprotokolle sollten bei der Darstellung der Kommunikationsbeziehungen berücksichtigt werden.
- Das Asset Register und das Netzwerk-Architekturbild sind bei Änderungen im Betriebsbereich, insbesondere bei strukturellen Änderungen, umgehend zu aktualisieren.
- Die erlaubte Kommunikation zwischen Komponenten und unterschiedlichen Netzwerksegmenten sollte auf das funktional notwendige Minimum reduziert werden.

Kontrollfragen:

- *Gibt es ein aktuelles Register (Datenbank, Tabelle, o. Ä.) der Assets des Betriebsbereichs?*
- *Gibt es einen aktuellen Netzwerkplan des Betriebsbereichs?*
- *Wie wird die Aktualität von Asset Registern und Netzwerkplänen gewährleistet?*
- *Welche Maßnahmen werden getroffen, um den Einsatz nicht erfasster bzw. unberechtigter Assets zu vermeiden?*
- *Welche Maßnahmen werden ergriffen, um die Kommunikation (innerhalb und nach außen) auf das notwendige Minimum zu beschränken?*

IT-Sicherheit bei der Errichtung von Anlagen

- IT-Sicherheit ist integraler Bestandteil aller Errichtungsphasen von Anlagen und ihre Integration in den Betriebsbereich bis zur Inbetriebnahme durch den Betreiber. Sie ist integraler Bestandteil der Systemfunktionen eines Betriebsbereiches.
- Anforderungen an die IT-Sicherheit werden in der Konzeptphase vom Betreiber in Abhängigkeit von der IT-Sicherheit-Richtlinie der Organisation formuliert und in den folgenden Phasen vom Systemintegrator detailliert und umgesetzt.
- Unter Cyberangriffen wird jeder unbefugte Zugriff oder jede unbefugte Veränderung auf/von IT-Systemen verstanden.
- Die Erfüllung der Anforderungen an die IT-Sicherheit wird zum Ende jeder Errichtungsphase vom Systemintegrator in Zusammenarbeit mit dem Betreiber verifiziert und validiert. Vor der Inbetriebnahme erfolgt die abschließende IT-Securityabnahme durch den Betreiber.

Kontrollfragen:

- *Wurden/werden bei der Beschaffung/Planung von Anlagen, Komponenten usw.Vorgaben zur IT-Sicherheit gemacht?*
- *Wurden/werden diesen Vorgaben vor der Inbetriebnahme überprüft?*

Reaktion auf neue Schwachstellen und Bedrohungen

- Es sind Konzepte und Abläufe festzulegen, wie auf neue Schwachstellen und IT-Bedrohungen reagiert wird. Dazu gehören u. A. der Umgang mit Updates und der Schutz vor Schadsoftware.

Kontrollfragen:

- *Über welche Wege werden Informationen zu neuen Schwachstellen und IT-Bedrohungen erfasst, die den Betriebsbereich betreffen?*
- *Wie wird auf neue Schwachstellen reagiert?*
- *Gibt es Vorgaben bezüglich der Reaktion auf neue Schwachstellen und IT-Bedrohungen (z.B. Patch- und Updatemanagement)?*
- *In welchem zeitlichen Rahmen werden Schutzmaßnahmen ergriffen?*

Erkennung von IT-Sicherheitsvorfällen

- Die rechtzeitige Detektion von IT-Sicherheitsvorfällen ist Grundvoraussetzung für die Einleitung von wirksamen Gegenmaßnahmen.
- Darüber hinaus kann die Analyse von IT-Sicherheitsvorfällen dazu dienen, geeignete Maßnahmen zur zukünftigen Vermeidung derartiger Vorfälle treffen zu können. Die Erkenntnisse fließen in das Risikomanagement ein.
- Im Sicherheitsmanagementsystem sind daher geeignete Maßnahmen zur effizienten Erkennung und Meldung von IT-Sicherheitsvorfällen zu ergreifen.

Kontrollfragen:

- *Welche Maßnahmen gibt es, um IT-Sicherheitsvorfälle zu erkennen?*
- *Welche Gegenmaßnahmen werden ergriffen?*

Maßnahmen nach IT-Sicherheitsvorfällen

- Im Sicherheitsmanagementsystem sind geeignete Maßnahmen zur Wiederherstellung der IT-Sicherheit nach Vorfällen festzulegen.
- Die Mitarbeiter werden in der Ausführung der Maßnahmen geschult.
- Sofern technisch möglich werden die Maßnahmen trainiert.
- Die Wirksamkeit der Maßnahmen wird regelmäßig im Rahmen des Risikomanagements überprüft.

Kontrollfragen:

- *Gibt es ein dezidirteres Desaster-/Recoverymanagement?*
- *Gibt es Backups und werden diese regelmäßig überprüft?*

Anhang 3

Hinweise zu Drohnenangriffen auf Betriebsbereiche nach StörfallV

1. Rahmenbedingungen

Die technische Entwicklung von Drohnen verläuft aktuell überaus dynamisch. So werden Drohnen zunehmend leistungsfähiger, insbesondere hinsichtlich Navigation, Handhabung, Flugeigenschaften, möglicher Traglasten, Einsatzdauer und Reichweite. Diese Eigenschaften ermöglichen ein breites Spektrum an Nutzungsmöglichkeiten für kommerzielle Anwender. Zudem sind Drohnen im gesellschaftlichen Mainstream angekommen; ihre private Nutzung geht folglich weit über den klassischen Modellflug hinaus.

Mit der wachsenden Leistungsfähigkeit von Drohnen steigt auch die Gefahr für Betriebsbereiche nach StörfallV (12. BImSchV) aufgrund einer missbräuchlichen oder fahrlässigen Nutzung. Die Anwesenheit einer Drohne in der räumlichen Nähe eines Betriebsbereichs stellt neben einem luftrechtlichen Verstoß (laut § 21b Nr. 3 LuftV muss ein seitlicher Abstand von 100 m zu Industrieanlagen eingehalten werden) auch eine konkrete Gefahr gem. § 3 Abs. 2 Nr. 3 StörfallV dar, die durch das Inkrafttreten der sogenannten „Drohnenverordnung“ (Verordnung zur Regelung des Betriebs von unbemannten Fluggeräten vom 30.03.2017) nicht hinreichend verhindert werden kann.

Damit ist jede Annäherung einer Drohne an einen Betriebsbereichals potentiell gefährlich anzusehen, soweit nicht der Betreiber der Anlage dem Betrieb ausdrücklich zugestimmt hat. Es sind folgende Szenarien denkbar:

a) Zufälliges (unbeabsichtigtes) Überfliegen eines Betriebsbereiches durch eine Drohne.

b) Ausspähen eines Betriebsbereiches mit dem Ziel der Planung einer späteren Straftat oder eines späteren Angriffes.

c) Unmittelbarer Angriff einer oder mehrerer Drohnen auf einen Betriebsbereich.

Für keines dieser Szenarien lassen sich derzeit ausreichende technische oder organisatorische Gegenmaßnahmen ableiten.

Maßnahmen gemäß StörfallV sind vom Betreiber nach dem Stand der Sicherheitstechnik zu treffen. Bei der Ermittlung des Standes der Sicherheitstechnik sind die schnelle technologische Entwicklung und ggf. die Veränderung der Rahmenbedingungen in diesem Bereich zu berücksichtigen.

Die Maßnahmen sind zu dokumentieren.

2. Maßnahmen

2.1 Grundlegende Maßnahmen

Der Betreiber des Betriebsbereichs ist dafür verantwortlich, das Risiko durch Drohnenangriffe zu bewerten und ggf. notwendige technische und organisatorische Maßnahmen zur Risikominderung zu ergreifen. Diese Maßnahmen müssen Verhaltensregeln für Beschäftigte beim Erkennen und Bewerten von Drohnenanflügen sowie zur Abwehr von Drohnenangriffen beinhalten.

Der Betreiber veranlasst die Sensibilisierung seiner Mitarbeiter und ggf. weiterer Personen, die im Betriebsbereich tätig sind, über die Gefahren durch Drohnen. Hierzu können z. B. Schulungen durchgeführt werden, die auf die getroffenen Maßnahmen (passive oder aktive) eingehen und auch das Erkennen von Drohnenangriffen berücksichtigen.

2.2 Passive Maßnahmen

Passive Maßnahmen sind solche, die präventiv und unabhängig von einem konkreten Drohnenangriff getroffen werden können. Voraussetzung zum Ergreifen von passiven Maßnahmen ist die Ermittlung und Dokumentation aller sicherheitsrelevanten Anlagenteile, die durch Drohnen empfindlich gestört werden können.

Maßnahmen, die einen unmittelbaren Anflug auf sicherheitsrelevante Anlagenteile wirksam verhindern können, sind z. B.

a) Einhausung,

b) Sichtschutz,

c) Schutz von Öffnungen, wie z. B. offenen Fenstern, gegen Durchflug,

d) Schutznetze gegen Anflug auf außenliegende Anlagenteile.

2.3 Aktive Maßnahmen

Aktive Maßnahmen sind solche, die zum Erkennen und Verifizieren sowie Abwehren eines konkreten Drohnenanflugs getroffen werden.

Unter aktiver Erkennung und Verifizierung sind insbesondere Systeme zur Detektion mittels

a) Funkaufklärung,

b) Radar,

c) Optik und Infrarot sowie

d) Akustik

zu verstehen, deren Sensordaten in einer gemeinsamen Plattform fusioniert werden, um den Standort der Drohne und ihre Anflugrichtung/-geschwindigkeit für einen Bediener zu visualisieren sowie ggf. die Position des Steuerers darzustellen.

Der Betreiber prüft regelmäßig, ob Einrichtungen zum Erkennen von Drohnenanflügen notwendig, verfügbar und geeignet sind.

Ist ein Erkennungssystem installiert, sind für den Fall des Erkennens eines Drohnenanflugs vom Betreiber organisatorische, z. B. Meldeverfahren, und ggf. ergänzende technische Maßnahmen, zu treffen. Zur Bewertung eines evtl. Drohnenangriffes ist eine Kurz-/Schnellsicherheitanalyse durchzuführen. Die Bewertungsaspekte sind vom Betreiber des Betriebsbereiches bereits in der Planungsphase der Anlage mit zu berücksichtigen. Die Beschäftigen sind entsprechend zu unterweisen.

Abwehrmaßnahmen sind aktiv, wenn mit technischen Mitteln oder sonstigem mechanischen Einwirken der Flug der Drohne beeinflusst, beeinträchtigt oder unterbrochen wird.

Die rechtliche Lage bezüglich erforderlicher Maßnahmen zur Detektion und Abwehr sind durch den Betreiber jeweils auf den aktuellen Stand der Technik zu prüfen. Die rechtliche Einordnung der aktiven Maßnahmen zur Drohnenabwehr ist gegenwärtig nicht geklärt.

Mitglieder des Arbeitskreises:

Ursula Fischbach

Stephan Gebhard

Dirk Hablawetz

Rainer Hoss

Klaus Jochem

Christian Jochum

Stephan Kurth

Katharina Löwe

Jens Mehrfeld

Jürgen Schmidt

Joachim Schmidt

Cornelia Sedello

Linda Söllenböhmer

Annette Stumpf

GFI Umwelt – Gesellschaft für Infrastruktur und Umwelt mbH
Geschäftsstelle der Kommission für Anlagensicherheit

Königswinterer Str. 827
D-53227 Bonn

Telefon 49-(0)228-90 87 34-0
Telefax 49-(0)228-90 87 34-9
E-Mail kas@gfi-umwelt.de
Internet www.kas-bmu.de