KAS

Kommission für Anlagensicherheit

beim
Bundesministerium für
Umwelt, Naturschutz, Bau und Reaktorsicherheit

Leitsätze der Kommission für Anlagensicherheit zum Schutz vor cyberphysischen Angriffen

KAS-44

Kommission für Anlagensicherheit

KAS

Leitsätze der

Kommission für Anlagensicherheit zum

Schutz vor cyberphysischen Angriffen

am 23. November 2017 von der KAS verabschiedet

KAS-44

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

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

Anmerkung:

1 *Einleitung*

Betriebsbereiche nach Störfall-Verordnung (12. BImSchV) und die in diesen Bereichen vorhandenen IT- und OT-Systeme[1] und Anlagen werden zunehmend intern und nach außen informationstechnisch vernetzt. Diese Netze und Systeme sind grundsätzlich als Angriffspunkte nach § 3 Absatz 2 Nummer 3 der Störfall-Verordnung (StörfallV) zu betrachten, da vorsätzliche Störungen des bestimmungsgemäßen Betriebs, die über Netze oder IT-Systeme ausgelöst werden, nicht ausgeschlossen werden können. Damit stellen sich IT-Sicherheitsfragen zum Eingriff Unbefugter auf Betriebsbereiche (IT-Security[1]) über derartig vernetzte Systeme und ihre Auswirkungen. Betrachtet werden an dieser Stelle ausschließlich diejenigen Angriffe über IT-Systeme, die sicherheitstechnische Relevanz (Safety) haben. Maßnahmen zur Gewährleistung der IT-Security sollen im Sicherheitsmanagementsystem, basierend auf dem Sicherheitskonzept gem. § 8 Absatz 1 der StörfallV, dokumentiert und umgesetzt werden.

Die Integration der IT-Security 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.

2 *Leitsatz 1: IT-Security ist Führungsaufgabe*

Die Leitung der Organisation ist für die IT-Security in der Organisation verantwortlich.

Die Leitung der Organisation erstellt eine IT-Security-Richtlinie für die Organisation. Die IT-Security-Richtlinie ist regelmäßig an veränderte interne und externe Rahmenbedingungen anzupassen.

In der IT-Security-Richtlinie legt die Leitung die IT-Security-Ziele der Organisation in Abhängigkeit von der Strategie der Organisation und von relevanten gesetzlichen Anforderungen fest.

Zur Erreichung der IT-Security-Ziele schafft die Leitung geeignete Organisationsstrukturen und Prozesse.

---

[1] 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-Security.

Die Leitung stellt die notwendigen Ressourcen zur Erreichung der IT-Security-Ziele bereit.

3 *Leitsatz 2: Sensibilisierung und Unterweisung*

Die Leitung kommuniziert die IT-Security-Richtlinie an alle Mitarbeiter und alle Dritte, welche die IT-Security der Organisation unmittelbar beeinflussen können.

Die Leitung führt geeignete Maßnahmen zur zielgruppenspezifischen Sensibilisierung der Mitarbeiter und Dritter bezüglich der Risiken, die sich aus Cyberangriffen[2] auf Betriebsbereiche und deren Auswirkungen auf die funktionale Sicherheit auf die Organisation ergeben können, durch.

Zur Etablierung der betrieblichen Security-Kultur werden alle Mitarbeiter und Dritte regelmäßig in den Maßnahmen zur Erreichung der Sicherheitsziele geschult und unterwiesen. Dritte können im Rahmen der üblichen Sicherheitseinweisung unterrichtet werden.

Die Effektivität der Maßnahmen wird regelmäßig überprüft.

4 *Leitsatz 3: Asset Register und Netzwerkarchitektur*

Nach § 3 Absatz 2 Nr. 3 der StörfallV hat der Betreiber bei der Festlegung von Vorkehrungen zur Verhinderung von Störfällen Eingriffe Unbefugter zu berücksichtigen. Relevant im Sinne der IT-Security 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 Dokumentation.

---

[2] Unter Cyberangriffen wird jeder unbefugte Zugriff oder jede unbefugte Veränderung auf/von IT-Systemen verstanden.

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 sind bei der Darstellung der Kommunikationsbeziehungen zu berücksichtigen.

Das Asset Register und das Netzwerkarchitekturbild sind bei Änderungen im Betriebsbereich, insbesondere bei strukturellen Änderungen, umgehend zu aktualisieren.

5 *Leitsatz 4: IT-Security bei der Errichtung von Anlagen*

IT-Security 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-Security werden in der Konzeptphase vom Betreiber in Abhängigkeit von der IT-Security-Richtlinie der Organisation formuliert und in den folgenden Phasen vom Systemintegrator[3] detailliert und umgesetzt.

Die Erfüllung der Anforderungen an die IT-Security 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.

6 *Leitsatz 5: Risikomanagement beim Betrieb von Anlagen*

Zur dauerhaften Gewährleistung der IT-Security ist ein Risikomanagement (angelehnt z. B. an ISO 27005) aufzubauen.

Kern des Risikomanagements ist die Risikobeurteilung bestehend aus Risikoidentifizierung, Risikoanalyse und Risikobewertung.

Grundlage für die Risikoidentifizierung sind, auf der Basis des Asset-Registers, die aktuell vorhandenen Gefährdungen für den Betriebsbereich.

Mit der Risikobeurteilung wird die Effektivität der vorhandenen Schutzmaßnahmen in Bezug auf die aktuellen Risiken bewertet. Sofern die vorhandenen Schutzmaßnahmen

---

[3] Der Systemintegrator ist verantwortlich für die Errichtung der Anlage.

die aktuellen Risiken nicht effektiv mindern sind geeignete Maßnahmen zur effektiven Minderung zu implementieren.

Die Risikobeurteilung muss regelmäßig wiederholt werden, da ständig neue Schwachstellen bei vorhandenen Assets entdeckt und neue Angriffswege erfunden werden. Sollten neue, höchst kritische Schwachstellen bekannt werden, für die bereits neue Angriffswege bekannt gemacht wurden, so ist die Risikobeurteilung für die betroffenen Assets umgehend zu wiederholen.

7 *Leitsatz 6: Erkennung von IT-Securityvorfällen*

Nach § 3 Absatz 1 der StörfallV haben Betreiber erforderliche technische und organisatorische Schutzvorkehrungen zu treffen um Störfälle zu verhindern. Die rechtzeitige Detektion von IT-Securityvorfällen ist Grundvoraussetzung für die Einleitung von wirksamen Gegenmaßnahmen.

Darüber hinaus kann die Analyse von IT-Securityvorfällen 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-Securityvorfällen zu ergreifen.

8 *Leitsatz 7: Maßnahmen nach IT-Securityvorfällen*

Im Sicherheitsmanagementsystem sind geeignete Maßnahmen zur Wiederherstellung der IT-Security nach IT-Securityvorfällen 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.

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