CSE-Engineering Services GmbH

ERGEBNISBERICHT

Projekt:

Genehmigungsantrag zur Errichtung einer Anlage zur Verarbeitung von Kartoffeln am Standort Mehrum – Konzept gegen Eingriffe Unbefugter

Auftraggeber:

Mc Cain GmbH
Düsseldorfer Str. 13
65760 Eschborn
Deutschland

Berichtsnummer:	2024_R01635
Datum:	13.11.2024

Zusammenfassung:

In diesem Dokument wird das Grundkonzept gegen Eingriffe Unbefugter in Anlehnung an die KAS 51 dargestellt. Eingriffe Unbefugter umfassen sowohl Cyberangriffe sowie physische Eingriffe.

Autor:

Marius Bächle, M. Sc.
Process Safety Engineer

Telefon: +49 721 4706 8124
E-Mail: marius.baechle@cse-engineering.de

Unterschriften:

Marius Bächle

Natalie Schmidt, Head of Consulting

Inhaltsverzeichnis

1 Einleitung

Die Mc Cain GmbH plant eine Anlage zur Verarbeitung von Kartoffeln am Standort Mehrum. Aufgrund der im Betriebsbereich vorhandenen Mengen an gefährlichen Stoffen im Sinne der 12. BImSchV sind für die Anlage die Vorschriften der oberen Klasse anzuwenden.

Es gehört zu den Grundpflichten der Störfall-Verordnung, Eingriffe Unbefugter als Gefahrenquelle zu berücksichtigen (§ 3 Abs. 2 Nr. 3 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 Sachschänden im Sinne der Störfallverordnung vernünftigerweise ausgeschlossen werden können.

Die KAS-51[1] stellt ein Leitfaden mit Maßnahmen gegen Eingriffe Unbefugter dar. Im Folgenden werden in Anlehnung an die KAS-51 eine Ersteinschätzung der Bedrohungslage sowie geeignete Schutzmaßnahmen gegen Eingriffe Unbefugter dargestellt.

2 Eingriffe Unbefugter

Das Vorgehen zum Schutz gegen Eingriffe Unbefugter orientiert sich am Leitfaden KAS 51. Gemäß KAS 51 ist eine Sicherungsanalyse mit den Inhalten nach Tabelle 1 durchzuführen.

Tabelle 1. Anforderungen an die Sicherungsanalyse nach KAS 51

Inhalt	Details
Bedrohungsanalyse	Ersteinschätzung der Bedrohungslage
Gefahrenanalyse	Beschreibung möglicher Störfälle und Abschätzung der Auswirkungen durch Eingriffe Unbefugter
IT-Risikobeurteilung	Explizite Berücksichtigung von Gefahren durch interne/externe Vernetzung von Anlagen oder Teile des Betriebsbereiches

[1] KAS-51. Leitfaden Maßnahmen gegen Eingriffe Unbefugter, Kommission für Anlagensicherheit, November 2019.

Die einzelnen Bestandteile der Sicherungsanalyse werden nachfolgend näher erläutert.

2.1. Bedrohungsanalyse

Die Bedrohungsanalyse soll ergeben, ob eine Anlage bzw. die Umgebung hinsichtlich Eingriffen Unbefugter besonders attraktiv erscheint. Sowohl physische Eingriffe als auch Cyberangriffe sind auf folgende Motivationen zurückzuführen, woraus eine Ersteinschätzung der Bedrohungslage für die geplante Anlage abgeleitet wird:

- Eingriffe, insbesondere Cyberangriffe, können auf eine monetäre Motivation zurückzuführen sein, beispielsweise durch das Einschleusen von Ransomware zur Erpressung des Unternehmens. Aufgrund der gegenwertigen Bedrohungslage im Cyberraum ist hier von einer hohen Bedrohung auszugehen.
- Die Bedrohung durch direkte Cyberangriffe auf das OT-Netzwerk mit dem Ziel, Herstellanlagen zu manipulieren, wird hingegen als gering eingestuft. Denn im Gegensatz zu anderen Unternehmen (z.B. Rüstungsindustrie oder Energieversorgung) steht das Unternehmen aufgrund von geringerem Symbolcharakter nicht im Fokus potenzieller Angreifer.
- Eingriffe durch Insiderattacken (Mitarbeiter, Dienstleiter) erfolgen aufgrund von Verärgerung der Mitarbeiter und sind nicht auszuschließen.
- Eingriffe können aus Machtdemonstration und zur Verunsicherung der Bevölkerung durch andere Staaten oder durch Gruppen, welche den Staat in der gegenwärtigen Form ablehnen (Delegitimierung des Staates) erfolgen. Entsprechende Eingriffe zielen in der Regel auf Unternehmen ab, welche von wesentlicher Bedeutung für das Funktionieren der Gesellschaft sind. Hier liegt keine besondere Bedrohung für die geplante Anlage vor.
- Eingriffe können aus einer politischen, religiösen oder idiologischen Ablehnung der geplanten Anlage, des Unternehmens oder Unternehmensangehörigen erfolgen. Hierzu zählen auch Eingriffe von Umweltschutzorganisationen aufgrund der Ablehnung bestimmter Technologien. Es ist nicht davon auszugehen, dass eine besondere Bedrohung aufgrund einer Ablehnung der Anlage aus den genannten Gründen vorliegt.
- Terroristische Angriffe zielen darauf ab, durch möglichst katastrophale Auswirkungen politische Veränderungen zu bewirken oder die Gesellschaft zu verunsichern. Aufgrund der ländlichen Lage und des geringen Symbolcharakters der geplanten Anlage ist nicht davon auszugehen, dass die Anlage im Blickpunkt terroristischer Aktivitäten steht.

2.2. Gefahrenanalyse

Die Gefahrenanalyse soll ergeben, ob Cyberangriffe in der Anlage zu einer besonderen Gefährdung im Sinne der KAS 51 führen können. Dabei soll auch ermittelt werden, von welchen Anlagen / Teilen des Betriebsbereichs eine Gefahr ausgeht und welche Anlagen / Teile des Betriebsbereichs daher besonders sicherungsrelevant sind.

Die Gefahrenanalyse kann erst abschließend durchgeführt werden, wenn die gesamte Netzwerkinfrastruktur, Netzwerkarchitektur und alle Mess-, Regel- und Steuereinrichtungen bekannt sind. Zum derzeitigen Planungsstand sind diese Informationen nicht bekannt und werden zu einem späteren Zeitpunkt in das Gesamtkonzept integriert.

Dem späteren Sicherheitsbericht wird das umfassende Konzept nach KAS-51 beigefügt.

2.3. IT-Risikobeurteilung

Zur Absicherung der Anlage gegen Eingriffe Unbefugter werden folgende Maßnahmen in Anlehnung an die KAS 51 in der Anlage umgesetzt.

Tabelle 2. Schutzmaßnahmen gegen Eingriffe Unbefugter

Aspekt	**Vorkehrungen**
Assetmanagement und Netzwerkpläne	- Asset-Register und eine Netzwerk-Architektur liegen vor. - Alle relevanten Assets sind in der Assetliste und in der Netzwerk-Architektur aufgeführt.
Festlegung Verantwortlichkeit	- Verantwortlichkeiten für die Maßnahmen zum Schutz vor Eingriffen Unbefugter werden zugewiesen. - Maßnahmen zum Schutz vor Eingriffen Unbefugter werden dokumentiert und regelmäßig überprüft.
Zugangs- und Zutrittsmanagement	- Maßnahmen zur Begrenzung des physischen Zugangs (zu Anlagen, Gefahrstoffen, Komponenten, Steuerungen, Computern) und des Zutritts auf das Gelände werden festgelegt. - Schlüsselmanagement wird definiert.

Aspekt	Vorkehrungen
Zugriffsmanagement auf Prozesssteuerung/Sicherheitssteuerung	- Segmentierung von IT/OT-Systemen sowie der sicherheitsgerichteten Steuerungen - Kommunikation zwischen Komponenten und unterschiedlichen Netzwerksegmenten wird auf ein Minimum beschränkt. - Absicherung von Fernzugriffen wird umgesetzt. - Änderung voreingestellter Passwörter und Änderung der Passwörter in regelmäßigen Intervallen. - Nutzung personalisierter Accounts für den Zugriff auf das Prozessleitsystem und sicherheitsgerichteten Steuerungen
Schutz vor Schadsoftware	- Viren-Scanner im Prozessleitsystem werden stets aktuell gehalten. - Fortlaufende Aktualisierung von Hersteller-Updates (Patch-Management) wird vorgenommen. - Virenscan von Wechseldatenträgern vor Einbringung in potentielle Angriffsziele wird durchgeführt.
Fremdpersonal, fremdvergebene Dienstleistungen	- Regelungen zum Schutz vor Eingriffen Unbefugter wird in die generelle Unterweisung und Einweisung zu den betrieblichen Gefahrenquellen eingebunden. - Überwachung der fremdvergebenen Arbeiten in geeignetem Umfang wird vorgenommen.
Reaktion auf Schwachstellen und IT-Bedrohungen	- Schwachstellen werden über geeignete Informationsquellen regelmäßig erfasst. - Sicherheitsupdates werden regelmäßig durchgeführt.
Schulungskonzept	- Schulungskonzept gegen Eingriffe Unbefugter und zur IT-Sicherheit (Umgang mit Wechseldatenträgern, Umgang mit Auffälligkeiten und möglichen Manipulationen) wird erstellt.
Maßnahmen nach IT-Sicherheitsvorfällen	- Vorgaben zur Wiederherstellung des sicheren Anlagenzustands (der IT-Sicherheit) nach Vorfällen wird definiert. - Schulung und Training der Maßnahmen, sofern technisch möglich, werden regelmäßig durchgeführt.