Sicherheitsvorfallbehandlung

Problembeschreibung

Ein Sicherheitsvorfall beschreibt ein nachträgliches Ereignis, und tritt dann auf, wenn Prozesse oder Ressourcen nicht wie geplant funktionieren.
Das stellt eine Gefährdung für die OT-Sicherheit dar, wodurch große Schäden und Auswirkungen für die Firma entstehen können.

Beispiele:

- Verlust oder Diebstahl von Geräten
- Schadprogramme auf den Geräten
- Erpressung oder Nötigung mittels vertraulicher Informationen
- Ausfall des Zutrittskontrollsystem

Solche Sicherheitsvorfälle können zum Beispiel ausgelöst werden durch das Fehlverhalten von Benutzern, Administratoren oder externen Dienstleistern, das zu sicherheitskritischen Änderungen von Systemparametern führt, wie

- Verstöße gegen interne Richtlinien und Anweisungen
- unzureichende Absicherung schutzbedürftiger Räume und Gebäude
- Verletzung von Zugriffsrechten
- durchgeführte Änderungen an Software, Hardware oder Infrastruktur

Typische Folgen von Sicherheitsvorfällen:

- Schädigung von Leib oder Leben von Mitarbeitern, Kunden, Geschäftspartnern oder Besuchern
- Verlust oder Beschädigung von Eigentum der Institution (insbesondere ihrer besonders schutzbedürftigen Werte)
- Schädigung des Ansehens der Institution
- Ausspähung oder Manipulation von Informationen in elektronischer oder nicht elektronischer Form

Bedrohungen

Folgende Gefährdungen sind mit der Sicherheitsvorfallbehandlung verbunden:

- Fehlende Strukturen für den Umgang mit Sicherheitsvorfällen
- Ungeeigneter Umgang mit Sicherheitsvorfällen
- Nicht erkannte Sicherheitsvorfälle
- Zerstörung von Beweisspuren bei der Behandlung von Sicherheitsvorfällen
- Fehlerhafte oder unpassende Qualifizierung von Sicherheitsvorfällen
- Ungeeigneter Betrieb der Meldestelle
- Unzureichende Ausstattung der Meldestelle
- Nicht wirksame Eskalationskette

Behandlung von Vorfällen

Durch die Sicherheitsvorfallbehandlung lassen sich potenzielle Sicherheitsvorfälle aus verschiedenen Bereichen erkennen. Das hat zur Folge, dass Institutionen sicherheitsrelevanter Informationen ganz strukturiert sammeln können und sie eine einheitliche Bewertung haben.
Je nachdem wie ein Vorfall klassifiziert wird, erfordert dieser eine spezielle Behandlung.

Die Behandlung von Sicherheitsvorfällen ist von übergreifender Bedeutung für ein umfassendes und ganzheitliches Sicherheitsmanagement. Dies hilft dabei, dass man Schäden vermeiden und reduzieren kann.

Für einen Automatisierungsingenieur ist wichtig:

- Sicherheitsvorfälle einstufen
- die richtigen Meldestellen benachrichtigen
- Behandeln
- Dokumentieren
- Gegenmaßnahmen und Sicherheitsvorkehrungen

Zentrale Meldestelle

Es muss immer leicht sein, ein Problem oder Vorfall melden zu können. Da jeder Mitarbeiter von einem Vorfall wissen muss, ist eine zentrale Anlaufstelle wichtig. Hier es auch wichtig, dass man eine Kontaktstrategie hat, heißt also: Wer soll oder darf wen zuerst informieren? Welche nicht erlaubten Personen dürfen die Information nicht erhalten? Welche Dateien über den Sicherheitsvorfall dürfen nicht weitergegeben werden?

Notfall/Krisenstab

Aus einem Vorfall kann sich entweder ein Notfall oder eine Krise entwickeln.
Notfälle und Krisen werden durch Sonderorganisationsformen wie einen Notfall- oder Krisenstab bewältigt, welche die notwendigen Verantwortlichkeiten übertragen.
Eine Krise ist eine Art Notfall, die eine Gefahr für das Unternehmen darstellt oder die Gesundheit von Personen gefährdet. Ein Krisenstab besteht aus Vertretern unterschiedlichster Bereiche innerhalb der Aufbauorganisation in Not- und Krisenfällen. Diese werden aber nur einberufen, wenn ein Vorfall sehr belastend erscheint.
Der Notfallstab stellt alle erforderlichen Maßnahmen, die in einem Notfall auftreten, auf.
Die Institutionen haben eine zentrale Instanz, die alle Meldungen von Vorfällen bearbeitet. Diese werden dann von der zentralen Instanz qualifiziert und werden entweder als Vorfall, Notfall oder Krise an das Reaktionssystem übergeben.

Dieses Dokument orientiert sich an den Vorgaben bei Sicherheitsvorfällen des BSI-Bund. (https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/it-sicherheitsvorfall_node.html)