Anmerkungen

An dieser Stelle geht es noch nicht darum, dass Sie sich auf einer absoluten Skala bewerten können, sondern dass Sie in die Lage versetzt werden, das Risiko in ihrem Umfeld einzuschätzen und zu reduzieren.
Die Fragen beziehen sich auf Prozesse, organisatorische und technische Maßnahmen. Dabei wird, wie sich aus der Anwendung erkennen lässt, nicht der Anspruch gestellt diese Bereiche vollständig abzudecken sondern einen Einstieg zu ermöglichen.
Wir verwenden oft die Formulierung "gesichert". Dabei verstehen wir darunter, dass jedes Unternehmen für sich entscheiden muss, was als "ausreichend sicher" gilt. Es ist hilfreich, die Bemerkungszeile auszufüllen und den aktuellen "Sicherheitsstatus", also getätigte Aktionen und Lösungen, zu notieren.
Security ist ein sehr dynamisches Thema. Wir freuen uns daher jederzeit über Rückmeldungen wie Verbesserungsvorschläge, Lob, Kritik usw.

weitere Hilfestellungen

Nachfolgend einige Nennungen weiterführender Dokumente zu "Industrial Security":

1. BSI ICS Security Kompendium
https://www.bsi.bund.de/ICS-Security-Kompendium

2. BDEW Whitepaper und weitere Sicherheitsempfehlungen
http://www.bdew.de/internet.nsf/id/it-sicherheitsempfehlunge

3. Lieferantendokumentationen von Steuerungen, Maschinen und Anlagen
Fragen Sie Ihre Lieferanten nach entsprechenden Dokumentationen.

4. VDI 2182 - Informationssicherheit in der industriellen Automatisierung
http://www.vdi.de/technik/fachthemen/mess-und-automatisierungstechnik/fachbereiche/industrielle-informationstechnik/gma-fa-522-security/

Autoren

Aus der Praxis für die Praxis. Die Kollegen aus dem VDMA Arbeitskreis "Security in Produktion und Automation" arbeiten aktiv an einfach verwendbaren Dokumenten, die einen Einstieg in die produktionsnahe Security ermöglichen. Zudem kümmern wir uns um Einschätzungen zu aktuellen Sachverhalten, greifen Zukunftsthemen auf und nutzen das Netzwerk zum informellen Erfahrungsaustausch.

VDMA AK "Security in Produktion und Automation"
Sprecher: Wolfgang Bokämper, Kolbus GmbH & Co. KG

VDMA e.V.
Abteilung Informatik
Lyoner Str. 18
60528 Frankfurt am Main

Stand: 23. Oktober 2014

pks.vdma.org/security

Industrial Security - einfach anfangen.

Einleitung

Der VDMA Fragenkatalog "Industrial Security" richtet sich an Fach- und Führungskräfte von Unternehmen, welche die Security im industriellen Umfeld etablieren bzw. verbessern wollen. Er liefert Fragestellungen, die ein strukturiertes, systematisches Vorgehen zur Ermittlung und damit zur Verbesserung des aktuellen Standes der Security im Produktionsbereich ermöglichen.
Der Fragenkatalog unterstützt den einfachen Einstieg in das Thema Security und führt somit bei regelmäßiger Anwendung in kleinen, überschaubaren Schritten an Standards der "Industrial Security" heran. Der Aufwand kann dabei je nach Bedarf und Kapazität selbst gewählt werden.

Anwendung

Auf den folgenden zwei Seiten finden Sie eine überschaubare Anzahl Fragen, deren Beantwortung ihnen hilft, sich mit Gebieten der Security vertrauter zu machen.
Nehmen Sie sich **im ersten Schritt 20 Minuten Zeit**, die Fragen zu beantworten, indem Sie ein Kreuz in die entsprechende Spalte setzen und gegebenenfalls kommentieren. Sollten Sie eine Frage nicht beantworten können, so recherchieren Sie diese später. Sollten sich weitere Fragen ergeben, so notieren Sie sich diese.
Im zweiten Schritt gehen Sie einer Frage nach, deren Relevanz ihnen am höchsten erscheint. Es kann z.B. sein, dass Sie ein konkretes Problem erkennen, welches Sie beheben wollen, oder dass Sie eine Antwort auf eine nicht beantwortete Frage suchen. Sollten sich hieraus wiederum Fragen ergeben, so notieren Sie sich diese.
Diesen zweiten Schritt wiederholen Sie regelmäßig, wann immer ihre sonstige Arbeit es zulässt. Investieren Sie nur so viel Zeit, dass ihre anderen Tätigkeiten nicht zu sehr darunter leiden.

→ Es wird nicht die perfekte Lösung gesucht, sondern die kontinuierliche Verbesserung.

Wichtig: Das Ergebnis aus der Bearbeitung des Fragenkatalogs ist zu dokumentieren und die Abarbeitung regelmäßig zu wiederholen, z.B. alle drei Monate. Nur so können Sie die Verbesserung der Security ermitteln und darstellen.
Die generelle Vorgehensweise können Sie selbst bestimmen. Sie können die Betrachtungsweise aus Sicht des gesamten Unternehmens (top down), der einzelnen Abteilung oder einer einzelnen Anlage (Asset) (bottom up) starten.
Den Detailierungsgrad ihrer Auswertung werden Sie wahrscheinlich im Laufe der Zeit erhöhen wollen. Eventuell wollen Sie bei der einfachen Bewertung „zum Teil umgesetzt“ von einem Kreuz auf einen Prozentwert übergehen. Oder Sie möchten jede Frage aufteilen und nach den klassischen Schutzzielen Vertraulichkeit, Verfügbarkeit und Integrität bewerten. Sie können aber auch eigene Kriterien ansetzen wie z.B. die Gefahr von Datenverlust, Informationsverlust, Produktionsausfall, Personenschaden oder die Zeitspanne für die Wiederherstellung des Betriebs. Oder Sie ergänzen die Spalten um die Einschätzung der Kritikalität für ihr Unternehmen. Ganz wie es Ihnen sinnvoll oder notwendig erscheint.
Sie werden feststellen, dass die Menge an Erfahrungen und damit ihre Daten stetig wachsen werden und eine elektronische Bearbeitung sinnvoll wird. Aus diesem Grund bieten wir ihnen den Fragenkatalog in elektronischer Form an. Wir schlagen hierin ein Bewertungssystem vor, welches Sie nutzen oder an ihre Bedürfnisse anpassen können.

VDMA Fragenkatalog Industrial Security

Datum: _____

Benennung / Bezeichnung der Anlage	

	Maßnahmen →	Fehlt	Definiert	über-wacht	nicht nötig*	Notiz / *Begründung
1.	Gibt es einen Ansprechpartner für Security, der allgemein bekannt ist? (z.B. anlagenbezogen oder unternehmensweit)					
2.	Sind die Kompetenzen des Security-Ansprechpartners klar geregelt?					
3.	Sind alle in der Anlage beteiligten programmierbaren Komponenten, inkl. Abgrenzung und Schnittstellen zu anderen Systemen, bekannt und dokumentiert?					
4.	Sind Prozesse etabliert alle programmierbaren Komponenten in der Anlage zu erfassen?					
5.	Haben alle Anwender genau die Rechte, die sie benötigen (und keine zusätzlichen)?					
6.	Sind Maßnahmen zum Zugangsschutz ergriffen worden (z.B. abschließbare Schaltschränke, Kontrollraum gesichert)?					
7.	Sind alle nicht benötigten Softwarekomponenten deaktiviert bzw. deinstalliert (z.B. Dropbox, Webserver...)?					
8.	Sind alle externen Datenzugänge, vor allem USB-Anschlüsse, gesichert (z.B. werden USB-Sticks von aktuellen Virenscannern geprüft; sind USB-Ports deaktiviert)?					
9.	Sind alle drahtgebundenen Netzwerkzugriffe gesichert (Ethernet) (z.B. Segmentierung, auch eigene Office-IT)?					
10.	Sind alle drahtlosen Netzwerkzugriffe gesichert (z.B. WLAN, Bluetooth...)?					
11.	Sind alle Laufwerke gesichert (z.B. vor Datenverlust, Know-how-Diebstahl)?					
12.	Sind alle Fernwartungszugänge technisch und organisatorisch gesichert (z.B. Firewall, NDA, Anforderungen an den Dienstleister)?					
13.	Sind Prozesse etabliert, die Fernwartung ohne Gefährdung von Mensch, Maschine und Umwelt durchzuführen (z.B. zeitliche und örtliche Begrenzung, Freischaltung)?					
14.	Sind alle zusätzlichen Verbindungen zum Internet gesichert?					
15.	Sind Prozesse etabliert, die Stände der Zusatzsoftware zu aktualisieren (z.B. Java, PDF-Reader)?					
16.	Sind Prozesse etabliert, die Stände der Automatisierungssoftware zu aktualisieren (z.B. Programmierumgebung, HMI, OPC,...)?					
17.	Sind Prozesse etabliert, die Stände der Betriebssystemsoftware zu aktualisieren (z.B. Windows)?					
18.	Sind Prozesse etabliert, die Stände der Schutzsoftware zu aktualisieren (z.B. Virensignaturen)?					
19.	Sind Prozesse etabliert, die Stände der Firmware zu aktualisieren (z.B. Steuerungsbetriebssysteme, HMI, Infrastrukturkomponenten...)?					
20.	Sind Geräte und Systeme, die nicht (mehr) aktualisiert werden können, gesichert (z.B. Windows 95/2000/XP)?					
21.	Sind alle Default-Passwörter durch individuelle Passwörter ersetzt worden (z.B. nach NERC-CIP-Vorgaben)?					
22.	Sind Prozesse etabliert, die Passwörter in geeignetem Abstand zu verändern?					
23.	Ist das Sicherheitskonzept der Maschine / der Anlage für den Betreiber umsetzbar?					
24.	Ist das Sicherheitskonzept im Gleichgewicht mit der Handhabbarkeit der Anlage (z.B. vor Manipulation von Schutzeinrichtungen)?					
25.	Ist die Sicherheitsdokumentation der Maschine / der Anlage für den Betreiber verständlich?					
26.	Erlaubt die Sicherheitsdokumentation dem Betreiber eine Bewertung der (Rest-) Risiken in seinem Umfeld?					
27.	Sind alle relevanten Mitarbeiter bezüglich der Security-Risiken und -Maßnahmen geschult (z.B. Social Engineering)?					
28.	Sind Prozesse etabliert, die Mitarbeiter bezüglich Security-Risiken und -Maßnahmen auf dem aktuellen Stand zu halten?					
29.	Sind Prozesse etabliert, regelmäßig vollständige Security-Überprüfungen der Anlage durchzuführen?					
30.	Gibt es Standardvorgehen für die Systemüberprüfung vor der Auslieferung bzw. vor der Inbetriebnahme?					
31.	Sind Prozesse bzw. Maßnahmen etabliert, um Security-Vorkommnisse zu erkennen bzw. nachzuvollziehen (z.B. Logbuchfunktionen)?					
32.	Sind Prozesse etabliert für den Fall von Security-Vorkommnissen (z.B. Desaster Recovery)?					
33.	Ist geklärt, wie mit Security-Vorfällen umgegangen wird (z.B. Melden an Dritte,)?					