Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IN DER PRODUKTION

Industrial Control System Security

Top 10 Bedrohungen und Gegenmaßnahmen 2016

Systeme zur Fertigungs- und Prozessautomatisierung – zusammengefasst unter dem Begriff Industrial Control Systems (ICS) – werden in nahezu allen Infrastrukturen eingesetzt, die physische Prozesse abwickeln. Dies reicht von der Energieerzeugung und -verteilung über Gas- und Wasserversorgung bis hin zur Fabrikautomation, Verkehrsleittechnik und modernem Gebäudemanagement. Solche ICS sind zunehmend denselben Cyber-Angriffen ausgesetzt, wie dies auch in der konventionellen IT der Fall ist. Die Betreiber müssen sich angesichts einer zunehmenden Häufigkeit von Vorfällen und neu entdeckten Schwachstellen dringend dieser Thematik annehmen. So muss das Risiko und Schadenspotenzial sowohl von nicht-zielgerichteter Schadsoftware als auch von gezielten, qualitativ hochwertigen und mit signifikantem Aufwand durchgeführten spezifischen Angriffen gegen ICS-Infrastrukturen berücksichtigt werden. Dies gilt sowohl für Infrastrukturen, die unmittelbar mit dem Internet verbunden sind, als auch für diejenigen, welche auf mittelbarem Wege durch Cyber-Angriffe attackiert werden können.

Im Rahmen seiner Analysen und Industriekooperationen zur Cyber-Sicherheit hat das BSI die aktuellen Bedrohungen mit der höchsten Kritikalität zusammengestellt, denen ICS derzeit ausgesetzt sind. Die identifizierten Bedrohungen werden nach dem folgenden Schema dargestellt:

1. Problembeschreibung und Ursachen: Darstellung der Ursachen und Rahmenbedingungen, die zur Existenz der Schwachstelle bzw. einer Bedrohungslage beitragen.
2. Mögliche Bedrohungsszenarien: Es werden konkrete Möglichkeiten erläutert, mit denen die zuvor genannten Rahmenbedingungen für einen Angriff missbraucht werden können.
3. Gegenmaßnahmen: Es werden Maßnahmen genannt, die derzeit als geeignet angesehen werden, um der Bedrohung entgegenzuwirken bzw. um zur Minimierung der Restrisiken beizutragen.

Im Rahmen eines solchen Übersichtsdokuments kann und soll bzgl. der Bedrohungsszenarien und Gegenmaßnahmen kein Anspruch auf Vollständigkeit erhoben werden. Die aufgeführten Szenarien sollen vielmehr die Tragweite der jeweiligen Bedrohung verdeutlichen. Die genannten Gegenmaßnahmen stellen mögliche Ansatzpunkte dar, den jeweiligen Bedrohungen zu begegnen und erlauben eine erste Einschätzung des insgesamt zur Abwehr der jeweiligen Bedrohung erforderlichen Aufwands. Ob oder welche Maßnahmen konkret geeignet sind und welche alternativen Maßnahmen möglicherweise notwendig sind, muss letztendlich am jeweiligen Anwendungsfall geprüft und im Rahmen einer Risikoanalyse bewertet werden. Dabei ist u. a. auf Wirksamkeit und Wirtschaftlichkeit zu achten. Die Vereinbarkeit mit dem operativen Betrieb sowie geltenden Echtzeit- und Safety-Anforderungen muss in jedem Fall gegeben sein. Darüber hinaus darf die Umsetzung von Sicherheitsmaßnahmen nicht zum Verlust von Garantie- oder Supportleistungen führen.

Eine erste individuelle Einschätzung des eigenen Sicherheitsniveaus und eine einfache

Bewertung der Risiken kann mit dem Selbsttest in dieser Empfehlung vorgenommen werden. Aspekte der funktionalen Sicherheit (Safety) werden hingegen explizit nicht behandelt.

Bedrohungen und deren Folgen

Bedrohungen für ein ICS resultieren aus Angriffen oder Ereignissen, die aufgrund existierender Schwachstellen dem ICS und damit einem Unternehmen Schaden verursachen können. Die kritischsten Bedrohungen für ICS sind in der folgenden Tabelle zusammengefasst.

Dabei erfolgt eine Differenzierung zwischen primären Angriffen und Folgeangriffen. Der Fokus wird dabei auf primäre Angriffe gelegt, mit denen Angreifer in industrielle Anlagen und Unternehmen eindringen, während Folgeangriffe den An- oder Zugriff auf weitere interne Systeme erlauben.

Nr. (Nr. alt)	Top 10 2016	Top 10 2014
1 (3)	Social Engineering und Phishing†	Infektion mit Schadsoftware über Internet und Intranet
2 (2)	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3 (1)	Infektion mit Schadsoftware über Internet und Intranet	Social Engineering
4 (5)	Einbruch über Fernwartungszugänge	Menschliches Fehlverhalten und Sabotage
5 (4)	Menschliches Fehlverhalten und Sabotage	Einbruch über Fernwartungszugänge
6 (6)	Internet-verbundene Steuerungskomponenten	Internet-verbundene Steuerungskomponenten
7 (7)	Technisches Fehlverhalten und höhere Gewalt	Technisches Fehlverhalten und höhere Gewalt
8 (9)	Kompromittierung von Extranet und Cloud-Komponenten	Kompromittierung von Smartphones im Produktionsumfeld
9 (10)	(D)DoS Angriffe	Kompromittierung von Extranet und Cloud-Komponenten
10 (8)	Kompromittierung von Smartphones im Produktionsumfeld	(D)DoS Angriffe

Legende: †NEU

Ausgehend von diesen primären Angriffen kann sich ein Angreifer durch Folgeangriffe sukzessive im Unternehmen ausbreiten. Folgende Skizze soll den Zusammenhang verdeutlichen:

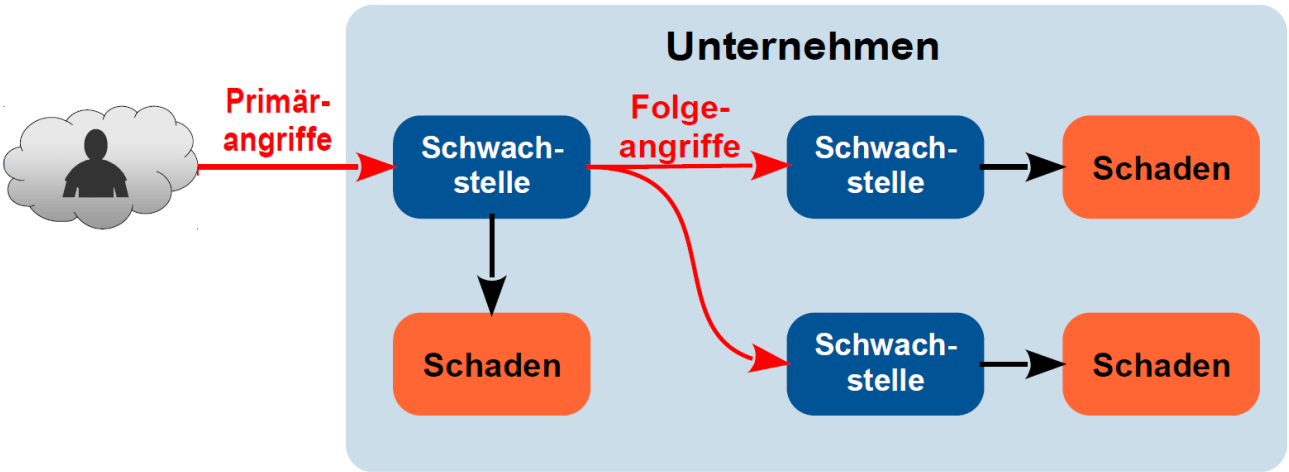

Abbildung 1: Ablauf von Primär- und Folgeangriff sowie Schadensfolgen

Zu den Folgeangriffen gehören insbesondere:

- Auslesen von Zugangsdaten zur Rechteerweiterung: Im Industrieumfeld vorhandene IT-Standardkomponenten wie Betriebssysteme, Application Server oder Datenbanken enthalten in der Regel Fehler und Schwachstellen, die von Angreifern ausgenutzt werden können.
- Unberechtigter Zugriff auf weitere interne Systeme: Insbesondere Innentäter oder Folgeangriffe nach einer Penetration von außen haben leichtes Spiel, wenn Dienste und Komponenten im Unternehmens- oder Steuerungsnetz keine hinreichenden Methoden zur Authentisierung und Autorisierung nutzen. Ein solcher Folgeangriff kann beispielsweise mittels Brute Force oder Wörterbuchangriffen auf Authentisierungsmechanismen erfolgen.
- Eingriff in die Feldbus-Kommunikation: Da die meisten Steuerungskomponenten derzeit über Klartextprotokolle und somit ungeschützt kommunizieren, ist das Mitlesen, Manipulieren oder Einspielen von Steuerbefehlen oftmals ohne größeren Aufwand möglich.
- Manipulation von Netzwerkkomponenten: Komponenten wie Router oder Firewalls können durch Angreifer manipuliert werden, um beispielsweise Sicherheitsmechanismen außer Kraft zu setzen oder Datenverkehr umzuleiten.

Die Umsetzung von Maßnahmen gegen solche Folgeangriffe sollte im Anschluss an die Etablierung eines Basisschutzes gegen die primären Angriffe im Zuge eines sogenannten Defense-in-depth Konzepts[1] erfolgen.

Organisatorische Mängel sowie Unkenntnis oder menschliches Fehlverhalten begünstigen Angriffe und erleichtern Folgeangriffe. Außerdem erschweren sie die Erkennung von Angriffen sowie die Bereinigung und die Wiederherstellung der Systeme nach einem erfolgreichen Angriff. Die möglichen Schadensfolgen sind ebenfalls vielseitig und durchaus als äußerst kritisch zu bewerten:

- Verlust der Verfügbarkeit des ICS / Produktionseinbußen
- Datenabfluss / Verlust von Know-how (Intellectual Property)
- Herbeiführen von physischen Schäden an Anlagen
- Auslösen von Safety-Prozeduren oder Beeinträchtigung von Safety-Systemen
- Minderung der Qualität der Erzeugnisse

Die später im Dokument zugeordneten Gegenmaßnahmen bilden die erste Verteidigungslinie, deren Umsetzung die höchste Priorität haben sollte.

1 http://ics-cert.us-cert.gov/Recommended-Practices

Bewertungskriterien

Die Rangordnung der Bedrohungen ergibt sich aus einer Betrachtung von Aspekten wie beispielsweise dem Täterkreis, der Verbreitung und Ausnutzbarkeit der Schwachstellen sowie der möglichen technischen und wirtschaftlichen Folgen eines Angriffs. Zur individuellen Bewertung der Bedrohungen für ein Unternehmen können beispielsweise die folgenden Kriterien angewandt werden:

- Verbreitung: Wie verbreitet ist die potenzielle Schwachstelle in Unternehmen?
- Exposition: Wie leicht ist die Schwachstelle zu lokalisieren und zu erreichen?
- Ausnutzbarkeit: Wie einfach ist es, die Schwachstelle auszunutzen (technischer Sachverstand und benötigter Aufwand)?
- Detektion: Wie einfach ist es, eine Kompromittierung zu bemerken?

Verbreitung	Exposition	Ausnutzbarkeit	Detektion
GERING (1)	NIEDRIG (1)	SCHWIERIG (1)	EINFACH (1)
MODERAT (2)	MODERAT (2)	MODERAT (2)	MODERAT (2)
HÄUFIG (3)	HOCH (3)	EINFACH (3)	SCHWIERIG (3)

Die in diesem Dokument genannten primären Angriffsmethoden wurden anhand dieser Kriterien vorab bewertet. Grundlage hierfür sind Erfahrungen aus konkreten Sicherheitsvorfällen sowie Rückmeldungen aus der Industrie. Diese Vorabbewertung kann und sollte natürlich an die konkreten Gegebenheiten im Unternehmen individuell angepasst werden, um so zu einer eigenen Top 10 Rangliste der kritischsten Bedrohungen zu gelangen. In dieser Top 10 ergibt sich die Reihenfolge der Bedrohungen unter anderem aus den Anzahlen bekannt gewordener Vorfälle.

Um das Risiko für das eigene Unternehmen abzuschätzen, sollten einerseits die jeweiligen Gegenmaßnahmen nach technischer oder organisatorischer Umsetzbarkeit individuell bewertet werden. Diese Betrachtung sollte zusammen mit einer Kostenabschätzung der jeweiligen Maßnahme geschehen. Andererseits ist es insbesondere wichtig, für die identifizierten Bedrohungen den Business Impact, d. h. die wirtschaftlichen Auswirkungen für das Unternehmen, für den jeweiligen Fall individuell zu bewerten. Dies kann i. d. R. nur der Betreiber selbst unter Berücksichtigung der Rahmenbedingungen und möglichen Folgeangriffe durchführen.

1. Social Engineering und Phishing

Verbreitung	Exposition	Ausnutzbarkeit	Detektion
HÄUFIG (3)	HOCH (3)	EINFACH (3)	MODERAT (2)

Problembeschreibung & Ursachen

Social Engineering ist eine Methode, um durch meist nicht-technische Handlungen unberechtigten Zugang zu Informationen oder IT-Systemen zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie z. B. Neugier, Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Diese Eigenschaften dienen einem Angreifer oft als Ablenkungsstrategie, um Mitarbeiter zu einer unbedachten oder fahrlässigen Handlung zu verleiten. Ein klassisches Beispiel hierfür sind betrügerische E-Mails (Phishing-Mails). Diese verleiten Mitarbeiter dazu, Anhänge mit Schadsoftware zu öffnen oder enthalten Links zu manipulierten Webseiten.

Mögliche Bedrohungsszenarien

1. Phishing Angriffe, bei denen der Angreifer durch gefälschte Nachrichten an Zugangsdaten der Opfer gelangt oder eine Schadsoftware verteilt.
2. Nachrichten mit scheinbar harmlosen Links oder Anhängen, bei deren Öffnen Schadsoftware wie z.B. Trojaner oder Ransomware installiert wird.
3. Spear-Phishing Angriffe, bei denen ein Angreifer meist eine geringe Anzahl von Zielen angreift, bei der allerdings dann E-Mails genau an die jeweiligen Zielpersonen angepasst sind. Hierfür werden u.a. öffentliche Informationen von Unternehmenswebseiten oder aus sozialen Netzwerken genutzt.
4. Unberechtigten Zugang zu einem Gebäude kann sich der Angreifer durch sicheres und freundliches Auftreten oder durch Vorspielung falscher Tatsachen (z. B. als Techniker ausgeben) verschaffen.

Gegenmaßnahmen

1. Zielgruppenspezifisches Security-Awarenesstraining durchführen.
2. Organisatorische Maßnahmen: Erstellung und Durchsetzung von Sicherheitsrichtlinien.
   a. Informationen, die für das Unternehmen einen Wert aufweisen, identifizieren und klassifizieren.
   b. Etablieren eines Datensicherungskonzeptes
   c. Einführen von Verschwiegenheits- und/oder Datenschutzerklärungen nicht nur für die eigenen Mitarbeiter, sondern auch für Partner und Dienstleister.
   d. Richtlinien für das Vernichten von auf Papier gedruckten Informationen (z. B. Schreddern).
   e. Sichere Entsorgung von digitalen Datenträgern.
   f. Regelungen für den Umgang mit mobilen Geräten (Sichtschutzfolie, Aufbewahrung in einem Safe, usw.).
3. Etablieren von Alarmierungswegen bei Vorfällen und auch bereits bei Verdacht. Diese sollten definiert und kommuniziert werden und keine negativen Konsequenzen für die Mitarbeiter haben.
4. Nutzung von technischen Sicherheitsmechanismen zur Durchsetzung der geltenden Regelungen und zur automatischen Erkennung von Fehlverhalten oder Angriffen (z. B. Device Control oder Zutrittskontrolle).
5. Regelmäßige Datensicherungen zur Wiederherstellung von Daten und Anwendungen

Beispielsweise konnte eine Klinik, in der einige Rechner über eine E-Mail mit Ransomware infiziert worden waren, ihren Betrieb nur noch sehr eingeschränkt fortführen. So waren Datenbanken mit wichtigen Informationen nicht mehr verfügbar.

2. Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware

Verbreitung	Exposition	Ausnutzbarkeit	Detektion
HÄUFIG (3)	MODERAT (2)	MODERAT (2)	SCHWIERIG (3)

Problembeschreibung & Ursachen

Wechseldatenträger wie USB-Sticks sind sehr weit verbreitet. Mitarbeiter des Unternehmens verwenden diese häufig sowohl in Office- als auch in ICS-Netzen. Darüber hinaus werden diese oftmals mit nach Hause genommen, z. B. um dort weiter zu arbeiten oder um von dort die neueste Musik mit zur Arbeit zu nehmen. Auch führt Fremdpersonal meist eigene Wechseldatenträger mit sich. Auch der Einsatz von Notebooks mit externen Daten und Wartungssoftware, welche möglicherweise in unterschiedlichen Unternehmen durch externes Wartungspersonal zum Einsatz kommen, ist weit verbreitet und birgt vergleichbare Gefahren.

Das Sicherheitsbewusstsein beschränkt sich – bedingt durch die Historie von ICS – in vielen Fällen auf die Aspekte Verfügbarkeit und physische Sicherheit wie z. B. Safety, Zugangsbeschränkungen und Schutz vor äußeren Einflüssen. Die Auswirkungen von Schadsoftware hingegen sind den Mitarbeitern häufig nicht bewusst.

Mögliche Bedrohungsszenarien

1. USB Sticks können z. B. im Office-Netz oder im privaten Umfeld infiziert worden sein. Schadsoftware kann so ihren Weg direkt in die ICS-Netze finden.
2. Wartungsnotebooks können beim Zugriff auf das Internet, in Office-Netzen oder in der Infrastruktur des jeweiligen externen Dienstleisters infiziert werden. Sobald diese dann im ICS-Netz betrieben werden, erfolgt die Infektion der dortigen Systeme und Komponenten mit Schadcode.
3. Projektdateien oder ausführbare Anwendungen können Schadcode enthalten, der zu einer Infektion oder einem Datenabfluss führt.

Gegenmaßnahmen

1. Etablieren strikter organisatorischer Vorgaben und technischer Kontrollen bzgl. Wechseldatenträgern:
   a. Inventarisierung und Whitelisting zugelassener Wechseldatenträger.
   b. Wechseldatenträgerschleuse (Virenschutz und Datei-Whitelisting, bereitgestellt auf einem Rechner, der ein anderes Betriebssystem verwendet als die Wartungsrechner).
   c. Ausschließliche Verwendung unternehmenseigener, ggf. personalisierter Wechseldatenträger.
   d. Ausschließliche Verwendung im ICS-Netz.
   e. Physische Sperren gegen (unbefugtes) Anschließen von USB-Geräten durch z. B. Kunstharz, USB-Schlösser oder Ablöten auf Platinen.
   f. Vollverschlüsselung von Datenträgern.
2. Etablieren strikter organisatorischer Vorgaben und technischer Kontrollen bzgl. externer Wartungsnotebooks:
   a. Der Austausch von Daten erfolgt ausschließlich über Wechseldatenträger und unterliegt den zuvor genannten Kontrollen.
   b. Einrichtung von Quarantänenetzen für den Zugang externer Dienstleister.
   c. Schwachstellenscans der mitgebrachten Notebooks vor dem Zugang zum eigentlichen System.
   d. Vollverschlüsselung von Wartungsnotebooks, die beim Betreiber verwahrt werden.

3. Infektion mit Schadsoftware über Internet und Intranet

Verbreitung	Exposition	Ausnutzbarkeit	Detektion
MODERAT (2)	NIEDRIG (1)	EINFACH (3)	SCHWIERIG (3)

Problembeschreibung & Ursachen

Unternehmensnetze nutzen Standardkomponenten wie Betriebssysteme, Webserver und Datenbanken. Browser oder E-Mail Clients sind i. d. R. an das Internet angebunden. Praktisch täglich werden für diese Komponenten neue Schwachstellen[2] bekannt, die ein Angreifer für das Eindringen in das Intranet und die Infektion mit Schadsoftware ausnutzen kann. Diese Schadsoftware kann bspw. auch durch infizierte Wechseldatenträger direkt im Intranet platziert werden. Dadurch kann ein Angreifer hier mitunter an kritische Informationen gelangen.

Lange Zeit gab es keine direkte Verbindung zwischen Office-Netz und ICS-Netz (sog. Air Gap). Mit der zunehmenden Verbreitung Ethernet-basierter Netze und Protokolle im ICS-Umfeld und deren Verbindung mit Systemen im Unternehmensnetz (Fileserver, ERP-, MES-Systeme, etc.) hat sich dies jedoch in den meisten Fällen geändert. Gelingt es einem Angreifer, in das Office-Netz einzudringen oder befindet er sich bereits im Intranet, kann er sich häufig direkt oder mit einem Folgeangriff in das ICS-Netz vorarbeiten.

Die Zusammenhänge zwischen der Sicherheit im Office-Netz und der Sicherheit im ICS-Netz sind häufig nicht transparent. Den Mitarbeitern im bzw. den Verantwortlichen für das Office-Netz ist also häufig nicht bewusst, dass Kompromittierungen in diesem Bereich massive Auswirkungen auf die Sicherheit der ICS-Netze haben können.

Auch beim Zugriff aus dem ICS-Netz bzw. einem ICS-nahen Netz auf andere Netze – insbesondere dem Internet – kann sowohl ein zielgerichteter als auch ein ungezielter Angriff erfolgen.

Mögliche Bedrohungsszenarien

1. Ausnutzung von bekannten Schwachstellen oder sogenannten Zero-Day Exploits, d. h. von bislang unbekannten Angriffen, für die noch keine Erkennungsmöglichkeiten in Anti-Virenprodukten o. ä. existieren.
2. Manipulation von externen Webseiten, um z. B. einen Drive-by-Download umzusetzen und die Opfer somit ohne Nutzerinteraktion, d. h. durch einen einfachen Aufruf der Website, zu infizieren.
3. Durchführung von Angriffen auf Webseiten des Unternehmens (z. B. SQL-Injection, Cross Site Scripting, etc.).
4. Komponenten werden durch nicht-zielgerichtete Schadsoftware (z. B. Würmer) infiziert und in ihrer Funktionalität beeinträchtigt.

Gegenmaßnahmen

1. Maximale Abschottung der unterschiedlichen Netze (Segmentierung) durch Firewalls und VPN-Lösungen, um Angriffspfade zum ICS-Netz weitgehend auszuschließen. Abschottung ungeschützter / nicht-patchbarer Systeme („Secure Islands“).
2. Einsatz konventioneller Schutzmaßnahmen am Perimeter (z. B. Firewalls, Antivirensoftware) oder an den ICS (z. B. Firewalls, Application Whitelisting).
3. Beschränkung der im Unternehmen frei verfügbaren Informationen (z. B. auf Fileservern oder in Datenbanken), um einen Abfluss kritischer Informationen zu erschweren (Need-to-Know-Prinzip).
4. Regelmäßiges und zeitnahes Patchen der Betriebssysteme sowie der Anwendungen im Office- und Backend- und, wo möglich, im ICS-Netz.
5. Überwachung/Monitoring von Logfiles auf ungewöhnliche Verbindungen oder Verbindungsversuche.
6. Sämtliche im Office und ICS eingesetzten IT-Komponenten (Dienste, Rechner) sind bestmöglich zu härten.

2 Schwachstellenampel, https://www.cert-bund.de/schwachstellenampel

4. Einbruch über Fernwartungszugänge

Verbreitung	Exposition	Ausnutzbarkeit	Detektion
MODERAT (2)	MODERAT (2)	MODERAT (2)	SCHWIERIG (3)

Problembeschreibung & Ursachen

In ICS-Installationen sind externe Zugänge für Wartungszwecke weit verbreitet. Häufig existieren dabei z. B. Default-Zugänge mit Standardpasswörtern oder sogar fest kodierten Passwörtern. Externe Zugänge mittels Virtual Private Networks (VPN) sind mitunter nicht beschränkt bzgl. der erreichbaren Systeme, d. h. über einen Wartungszugang für ein bestimmtes System sind weitere Systeme zu erreichen. Zu den zentralen Ursachen zählen mangelnde Authentisierung und Autorisierung sowie flache Netzwerkhierarchien.

Zur Wartung und Programmierung von Komponenten wird häufig auf die jeweiligen Hersteller und externe Dienstleister zurückgegriffen. Dies stellt zusätzliche Herausforderungen an das Sicherheitsmanagement, da die Sicherheitskonzepte mehrerer Parteien in Einklang gebracht werden müssen.

Mögliche Bedrohungsszenarien

1. Direkter Angriff auf einen Wartungszugang, z. B. mittels
   a. Brute Force Attacke auf passwortgeschützte Zugänge,
   b. Wiederverwendung eines zuvor aufgezeichneten Tokens,
   c. Web-spezifischer Angriffe (z.B. Injection oder CSRF) auf Zugänge, die zu Wartungszwecken genutzt werden.
2. Indirekter Angriff über die IT-Systeme des Dienstleisters, für den der externe Zugang geschaffen wurde, z. B.
   a. Trojaner, welcher den Zugang direkt auf dem externen Wartungsrechner ausnutzt,
   b. Diebstahl eines Passworts, Zertifikats oder eines sonstigen Tokens bzw. sonstige Beschaffung benötigter Zugangsdaten wie z. B. durch Bestechung / Erpressung eines Mitarbeiters mit einer derartigen Berechtigung,
   c. Verwendung gestohlener Notebooks, auf denen eine Software für den externen Zugriff konfiguriert ist.

Gegenmaßnahmen

1. Standardnutzer/-passwörter eines Herstellers (Auslieferungszustand) sind zu sperren/löschen (Abnahmeprotokoll).
2. Nutzung von hinreichend sicheren Authentisierungsverfahren wie z. B. Pre-Shared-Keys, Zertifikate, Hardwaretoken, Einmalpasswörter und Mehr-Faktor-Authentisierung durch Besitz und Wissen.
3. Schutz des Übertragungsweges durch Verschlüsselung, z.B. mit SSL/TLS.
4. Hinreichend granulare Segmentierung der Netze zur Minimierung der „Reichweite“ von Fernzugängen.
5. Einrichtung von Zugriffspunkten für Fernwartung in einer demilitarisierten Zone (DMZ), sodass sich Dienstleister statt ins ICS-Netz zunächst in eine DMZ verbinden und von dort ausschließlich den benötigten Zugriff auf das Zielsystem erhalten.
6. Fernzugänge müssen immer über eine Firewall geführt werden, die den Zugang zum Zielsystem erteilt und überwacht. Dabei werden ausschließlich die zur Wartung erforderlichen IP-Adressen, Ports und Systeme freigegeben.
7. Freischaltung von Fernzugängen durch internes Personal nur für die Dauer und den Zweck der Fernwartung.
8. Protokollierung von Fernzugriffen zur Gewährleistung der Nachvollziehbarkeit. Durch ergänzende Prozesse ist sicherzustellen, dass diese Logdaten ausgewertet und archiviert werden.
9. Alle Zugänge sind zu personalisieren, d. h. Verzicht auf Funktionskonten, die von mehreren Personen benutzt werden. Es wird nur eine Anmeldung pro Nutzer zur selben Zeit zugelassen.
10. Durchführung von Audits für solche Systeme / Zugänge.

5. Menschliches Fehlverhalten und Sabotage

Verbreitung	Exposition	Ausnutzbarkeit	Detektion
MODERAT (2)	MODERAT (2)	SCHWIERIG (1)	SCHWIERIG (3)

Problembeschreibung & Ursachen

Das im Umfeld eines ICS tätige Personal nimmt eine besondere Stellung bzgl. der Sicherheit ein. Dies gilt sowohl für eigene Mitarbeiter als auch sämtliches externes Personal z. B. für Wartung oder Konstruktion – unabhängig davon, ob diese Zutritt zu den Anlagen haben oder aus der Ferne arbeiten. Sicherheit kann niemals ausschließlich durch technische Maßnahmen gewährleistet werden, sondern bedarf auch immer organisatorischer Regelungen.

Mögliche Bedrohungsszenarien

1. Fehlkonfiguration sicherheitsrelevanter Komponenten (z. B. Firewall) oder Netzwerk-Komponenten, aber auch von ICS-Komponenten.
2. Insbesondere beim unkoordinierten Einspielen von Updates oder Patches kann es zu Problemen in der Funktionsweise von einzelnen Komponenten und deren Zusammenspiel kommen.
3. Seiteneffekte vorsätzlicher Handlungen sind zu berücksichtigen (Beschädigung von Geräten und Installationen, Platzierung von Abhörgeräten, etc.).
4. Kompromittierung von Systemen durch nicht genehmigte Soft- und Hardware. Darunter fallen z. B. Spiele, Digitalkameras, Smartphones oder andere USB-Geräte der Bediener.
5. Erstellung nicht freigegebener Konfigurationen für Infrastruktur- und Sicherheitskomponenten (z. B. Hinzufügen einer Firewall-Regel, damit ein nicht autorisierter Zugriff von außen über mobile Endgeräte möglich ist).

Oben genannte Szenarien können grundsätzlich sowohl durch Spionage und Sabotage als auch durch Fahrlässigkeit oder sonstiges menschliches Versagen und Fehlverhalten ausgelöst werden. Solche Vorfälle können insbesondere dazu führen, dass aufgrund organisatorischer Mängel eine signifikante Beeinträchtigung der Verfügbarkeit eintritt. Viele Kompromittierungen sind nur aufgrund solcher Mängel möglich.

Gegenmaßnahmen

1. Etablieren des „Need-to-Know“-Prinzips: Kenntnis von Systemdetails, Passwörtern, etc. sowie Zugriff auf sensible Daten nur wenn erforderlich.
2. Schaffung der Rahmenbedingungen für engagierte, qualifizierte und vernetzte Mitarbeiter zur Gewährleistung der Kompetenz der Bediener und Administratoren für funktionale als auch für sicherheitsspezifische Komponenten. Qualifizierungs- und Fortbildungsprogramme sind genau wie Sensibilisierungsmaßnahmen nachhaltig zu gestalten und verpflichtend vorzusehen.
3. Deaktivieren des Internetzugangs für Steuerungssysteme und produktionsnahe Systeme sowie Bereitstellung von Komponenten für ICS-fremde Aufgaben, die den Bedienern z. B. für Office, E-Mail, ERP etc. zur Verfügung stehen, hinreichend abgesichert und in einem anderen Netz eingebunden sind.
4. Etablierung von standardisierten Prozessen für Neueinstellungen bzw. aus dem Unternehmen ausscheidende Mitarbeiter sowie für extern Beauftragte (Hersteller, Dienstleister).
5. Geeignete Vorgaben („Policies & Procedures“) für den Umgang der Mitarbeiter mit technischen Systemen (z. B. Handhabung von Wechseldatenträgern, Kommunikationsverhalten bei E-Mail und in Sozialen Netzen, Passwort-Richtlinien, Installation individueller Software, etc.).
6. Etablieren geeigneter Policies insbesondere für kritische Prozesse im ICS-Netz: Beispielsweise Vorgaben bzgl. Sicherheits- und Konfigurationsmanagement, welche die Einbindung von Sicherheitsexperten und anderen relevanten Rollen regeln, sodass Änderungen oder Aktualisierungen ausschließlich nach erfolgter Abstimmung mit diesen erfolgen. Wichtig ist dabei, sämtliche Festlegungen zu dokumentieren und möglichst flankierende Vorkehrungen (z.B. Vieraugenprinzip) zu treffen.
7. Automatische Überwachung von Systemzuständen und -konfigurationen.
8. Sichere Hinterlegung von Projekten und Konfigurationen.

6. Internet-verbundene Steuerungskomponenten

Verbreitung	Exposition	Ausnutzbarkeit	Detektion
NIEDRIG (1)	MODERAT (2)	MODERAT (2)	SCHWIERIG (3)

Problembeschreibung & Ursachen

Oftmals werden ICS-Komponenten wie Speicherprogrammierbare Steuerungen entgegen den Empfehlungen der Hersteller direkt mit dem Internet verbunden. Solche Steuerungen verfügen jedoch oft nicht über ein hinreichendes Sicherheitsniveau, welches in der klassischen IT vorhanden ist. Zudem ist bei Bekanntwerden von Schwachstellen in diesen Steuerungen ein (zeitnahes) Einspielen von Patches nicht möglich, sodass zwingend flankierende Sicherheitsmechanismen umzusetzen sind.

Mögliche Bedrohungsszenarien

1. Auffinden von Steuerungskomponenten durch allgemeine Suchmaschinen („google dorks“), spezielle Suchmaschinen wie Shodan oder eigene Internetscans.
2. Direkter Zugriff auf ungeschützte Komponenten oder Verwendung von öffentlich verfügbaren Standardpasswörtern, um eine unberechtigte Bedienung und Manipulation vorzunehmen.
3. Ausnutzung von Schwachstellen in den erreichbaren Diensten wie z.B. Webschnittstelle (WWW), FTP, SNMP oder TELNET, um Zugriff auf die Komponenten zu erlangen oder deren Verfügbarkeit zu beeinträchtigen.

Gegenmaßnahmen

1. Keine direkte Verbindung von Steuerungskomponenten mit dem Internet.
2. Härtung der Konfiguration der Steuerungskomponenten (Abschalten nicht benötigter Dienste, Ändern von Standardpasswörtern, etc.).
3. Einsatz flankierender Maßnahmen wie z.B. Firewalls und VPN-Lösungen.
4. Zeitnahes Aktualisieren (Updates/Patchen) betroffener Produkte sofern möglich.

7. Technisches Fehlverhalten und höhere Gewalt

Verbreitung	Exposition	Ausnutzbarkeit	Detektion
MODERAT (2)	HOCH (3)	SCHWIERIG (1)	EINFACH (1)

Problembeschreibung & Ursachen

Software-Fehler in sicherheitsspezifischen Komponenten und ICS-Komponenten, die zu unvorhergesehenem Fehlverhalten führen können, lassen sich ebenso wenig ausschließen, wie mögliche Hardwaredefekte und Netzwerkausfälle. Insbesondere Hardwaredefekte treten in einigen Anwendungsszenarien angesichts der dort vorzufindenden Betriebsumgebungen (Schmutz, Temperatur, etc.) mit einer erhöhten Wahrscheinlichkeit auf, sofern keine entsprechende Vorsorge getroffen wurde.

Mögliche Bedrohungsszenarien

1. Defekt von Komponenten, z. B. Ausfall von Festplatten oder Switches, Kabelbruch, etc. zur Laufzeit, die zu einem sofortigen Ausfall führen.
2. Sowohl Hardwaredefekte als auch Fehler in Softwarekomponenten können lange unbemerkt bleiben und erst dann zum Problem werden, wenn z. B. Systeme neu gestartet werden oder eine bestimmte Randbedingung eintritt.
3. Softwarefehler können zum Ausfall eines Systems führen. So kann etwa ein Update des Betriebssystems bei einer zentralen Sicherheitskomponente dazu führen, dass das System nach einem erforderlichen Neustart nicht mehr korrekt funktioniert.

Solche Vorfälle können insbesondere dazu führen, dass aufgrund organisatorischer Mängel eine signifikante Beeinträchtigung der Verfügbarkeit eintritt.

Gegenmaßnahmen

1. Aufbau eines Notfallmanagements, welches Aspekte wie mögliche Gegenmaßnahmen, Prozeduren zur Systemwiederherstellung, alternative Kommunikationsmöglichkeiten und die Durchführung von Übungen beinhaltet.
2. Vorhalten von Tausch- oder Ersatzgeräten.
3. Vorhalten und Nutzung von Test- und Staging-Systemen, auf denen Patches, Updates und neue Softwarekomponenten eingehend getestet werden, bevor diese auf Produktivsystemen aufgespielt werden.
4. Nutzung von standardisierten Schnittstellen, die keine eigene Entwicklung des Herstellers sind. Dies verringert das Risiko unerkannter Lücken.
5. Redundante Auslegung von wichtigen Komponenten.
6. Bei der Auswahl der eingesetzten Systeme und Komponenten sind – gemäß des identifizierten Schutzbedarfs – hinreichende Mindestanforderungen zu stellen und durchzusetzen. Wichtige Aspekte in diesem Kontext sind:
   a. Vertrauenswürdigkeit und Verlässlichkeit der Hersteller,
   b. Robustheit der Produkte,
   c. Vorhandensein geeigneter Sicherheitsmechanismen (z. B. sichere Authentisierung),
   d. langfristige Verfügbarkeit bzgl. Ersatzteile, Updates und Wartung,
   e. zeitnahe Verfügbarkeit von Patches,
   f. offene Migrationspfade,
   g. Verzicht auf nicht benötigte Produktfunktionen.

Eine solide Basis für diese und weitere Aspekte liefert z. B. ein Whitepaper des BDEW[3].

3 https://www.bdew.de/internet.nsf/id/232E01B4E0C52139C1257A5D00429968/$file/OE-BDEW-Whitepaper_Secure_Systems%20V1.1%202015.pdf

8. Kompromittierung von Extranet und Cloud-Komponenten

Verbreitung	Exposition	Ausnutzbarkeit	Detektion
GERING (1)	NIEDRIG (1)	SCHWIERIG (1)	SCHWIERIG (3)

Problembeschreibung & Ursachen

Der in der konventionellen IT verbreitete Trend zum Outsourcing von IT-Komponenten hält mittlerweile auch in ICS Einzug. Häufig handelt es sich dabei nicht um Komponenten, die unmittelbar reale Prozesse steuern, da durch Latenzzeiten beispielsweise Echtzeitanforderungen i.d.R. nicht eingehalten werden können. Jedoch gibt es immer mehr Anbieter für extern betriebene Softwarekomponenten im Bereich Datenerfassung und -verarbeitung auf Historians, zur Berechnung von komplexen Modellen für die Konfiguration von Maschinen oder der Optimierung von Herstellungsprozessen (Big Data). Auch sicherheitsspezifische Komponenten werden mitunter als Cloud-basierte Lösung angeboten. So platzieren Anbieter von Fernwartungslösungen die Clientsysteme für den Remote-Zugriff in der Cloud, mit der sich der Wartungstechniker Zugriff auf die jeweiligen Komponenten verschaffen kann.

Derzeit sind solche Lösungen insbesondere für kleine und mittelständische Unternehmen (KMU) interessant, da der eigenverantwortliche Betrieb häufig nicht wirtschaftlich ist, während die Cloud kostengünstig Vorteile wie Skalierbarkeit, Redundanz und Pay-per-use ermöglicht. Solche Cloud-Lösungen führen allerdings dazu, dass der Anlagenbetreiber nur noch eine sehr eingeschränkte Kontrolle über die Sicherheit dieser Komponenten hat, diese aber sehr wohl unmittelbar mit der lokalen Produktion vernetzt sein können.

Mögliche Bedrohungsszenarien

1. Störung oder Unterbrechung der Kommunikation zwischen der lokalen Produktion und den ausgelagerten (Cloud-)Komponenten, z.B. durch Denial of Service Angriffe. Durch Kaskadeneffekte kann hierdurch die Produktion auch lokal beeinträchtigt werden.
2. Ausnutzung von Implementierungsfehlern oder unzureichenden Sicherheitsmechanismen, um Zugriff auf extern gespeicherte Daten zu bekommen (Datendiebstahl, Löschung).
3. Bei unzureichender Trennung der Mandanten eines Cloud-Anbieters können auch Angriffe auf fremde Cloud-Dienste zu einer Beeinträchtigung führen (Kollateralschaden).

Gegenmaßnahmen

1. Vertragliche Verpflichtung der Betreiber externer Komponenten zu einem hinreichenden Sicherheitsniveau, z.B. mittels Service Level Agreement (SLA).
2. Nutzung vertrauenswürdiger und möglichst auch zertifizierter Anbieter.
3. Betrieb einer Private Cloud, um die Kontrolle zu behalten und um Prozess-Know-how zu schützen.
4. Nutzung von hinreichend starken kryptographischen Mechanismen (Verschlüsselung, Integritätsschutz) zur Absicherung der in der Cloud gespeicherten Daten.
5. Nutzung von Virtual Private Networks (VPN), um die Anbindung zwischen lokaler Produktion und externen Komponenten zu sichern.

9. (D)DoS Angriffe

Verbreitung	Exposition	Ausnutzbarkeit	Detektion
MODERAT (2)	MODERAT (2)	MODERAT (2)	EINFACH (1)

Problembeschreibung & Ursachen

Die Kommunikation zwischen den Komponenten eines ICS kann sowohl über drahtgebundene als auch über drahtlose Verbindungen erfolgen. Werden diese Verbindungen gestört, können beispielsweise Mess- und Steuerdaten nicht mehr übertragen werden. Eine andere Möglichkeit besteht in der Überlastung einer Komponente durch eine sehr hohe Anzahl von Anfragen, sodass keine fristgerechte Antwort mehr ausgeliefert werden kann. In diesem Fall spricht man von einem (Distributed) Denial of Service ((D)DoS), also einem – ggf. auf mehrere Angreifer verteilten – Herbeiführen eines Funktionsausfalls.

Mögliche Bedrohungsszenarien

1. (D)DoS-Angriffe auf die Internetanbindung zentraler oder entfernter Komponenten: Dies kann u. a. durch Botnetze erfolgen, die ein Angreifer z. B. anmieten kann. Darüber hinaus werden in diesem Kontext zunehmend Angreifergruppen im Kontext „Hacktivismus“ relevant, wie z. B. Anonymous.
2. DoS-Angriffe auf die Schnittstellen einzelner Komponenten: Hierbei wird die Verarbeitungslogik einer Komponente durch bestimmte Nachrichten gestört und zum Absturz gebracht. Dies kann u. a. Steuergeräte oder zentrale Komponenten (z. B. Datenbanken oder Applikationsserver) betreffen.
3. Angriffe auf drahtlose Anbindungen wie WLAN oder Mobilfunknetze (GSM, UMTS, LTE). Dies kann z. B. erfolgen durch:
   a. den Einsatz von Störsendern, welche die entsprechenden Frequenzbereiche stören oder überlagern,
   b. den Einsatz von Fake Base Stations, d. h. gefälschten Basisstationen, die die angegriffenen Systeme zum Verbinden mit einem falschen Funknetz verleiten,
   c. das Versenden spezieller Datenpakete, die zum Abbruch vorhandener Verbindungen führen.

Gegenmaßnahmen

1. Strikte Konfiguration und Härtung von Netzzugängen und Kommunikationskanälen (z. B. GSM-Netze).
2. Zur Unterstützung Betroffener bei der Notfallplanung und Abwehr von DDoS-Angriffen hat das BSI auf den Webseiten der Allianz für Cyber-Sicherheit ein Dokument zur DDoS-Mitigation[4] bereitgestellt.
3. Nutzung dedizierter, kabelgebundener Verbindungen für kritische Funktionen.
4. Falls anwendbar: Einrichtung von Intrusion Detection Systemen (IDS) zur Detektion von Angriffen und Alarmierung über alternative Kanäle.
5. Redundante Anbindung von Komponenten unter Verwendung unterschiedlicher Protokolle bzw. Kommunikationswege.

4 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_002.pdf

10. Kompromittierung von Smartphones im Produktionsumfeld

Verbreitung	Exposition	Ausnutzbarkeit	Detektion
GERING (1)	NIEDRIG (1)	SCHWIERIG (1)	SCHWIERIG (3)

Problembeschreibung & Ursachen

Die Anzeige sowie die Veränderung von Betriebs- oder Produktionsparametern auf einem Smartphone oder Tablet wird bei immer mehr ICS-Komponenten als zusätzliche Produkteigenschaft beworben und eingesetzt. Dies stellt einen Sonderfall eines Fernwartungszugangs dar, bei dem durch den Einsatz von Smartphones eine zusätzliche Angriffsfläche hinzugefügt wird.

Mögliche Bedrohungsszenarien

1. Diebstahl oder Verlust von Smartphones.
2. Angriff auf das Smartphone durch zusätzliche Programme, die unzureichend gesicherte Informationen auf dem Gerät auslesen.
3. Angriff auf den Kommunikationskanal des Smartphones mit der ICS-Komponente:
   a. Kommunikation mit dem ICS protokollieren.
   b. Replay-Angriffe durch Wiedereinspielen aufgezeichneter Kommunikation.
   c. Reverse Engineering der verwendeten Applikation oder des verwendeten Protokolls.
   d. Man-in-the-Middle-Angriffe.

Gegenmaßnahmen

1. Beschränkung des Zugriffs von Smartphones auf ICS-Systeme auf den lesenden Zugriff. Eine Modifikation von Betriebs- oder Produktionsparametern sollte nicht möglich sein.
2. Einsatz von Produkten oder Nutzung von Bordmitteln des Betriebssystems für Zugriffsschutz, Schutz vor Schadsoftware und Fernlöschfunktionen (Mobile Device Management).
3. An Smartphones dürfen keine unerlaubten oder sicherheitskritischen Manipulationen (Jailbreak, Rooting) vorgenommen werden.
4. Smartphone-Applikationen müssen aus einer zertifizierten Quelle (App-Store) bezogen werden. Im Idealfall erfolgt die zentrale Prüfung und Verteilung von Apps durch die IT.
5. Nutzen von verschlüsselten Verbindungen (VPN).
6. Abwägen, ob der Nutzen des Smartphone-Einsatzes die Risiken aufwiegt.
7. Keine Verwendung von Apps zum direkten Zugriff auf ICS. Nur indirekter verschlüsselter Zugriff über einen gesicherten Terminalserver, der die benötigten Programme bereitstellt.

Ergänzende Sicherheitsmaßnahmen

Basismaßnahmen

An dieser Stelle soll betont werden, dass die beschriebenen Best Practices nur den Einstieg in einen geordneten IT-Sicherheitsprozess innerhalb eines ICS bzw. eines ganzen Unternehmens ermöglichen sollen. Ziel sollte es sein, ein funktionierendes Informationssicherheitsmanagement auf Basis etablierter Standards, die sowohl allgemein bzgl. IT-Sicherheit als auch spezifisch zur ICS-Sicherheit Vorgaben enthalten, aufzubauen. Beispielhaft seien genannt:

- IT-Grundschutz auf Basis von ISO 27001[5],
- ISO/IEC 27000-Reihe[6],
- VDI/VDE 2182[7],
- IEC 62443[8].

Ein hierauf aufbauendes Informationssicherheitsmanagementsystem (ISMS) für den Betrieb eines ICS sollte als Teil des übergeordneten Managementsystems eines Unternehmens verstanden werden. Es berücksichtigt auch die spezifischen Risiken von ICS und hat zum Ziel, die Informationssicherheit dauerhaft zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Bei der Etablierung eines ISMS sollte vor allem auf die folgenden elementaren Maßnahmen geachtet werden. Diese dienen dazu, einen Überblick über die eigenen Systeme und die Infrastruktur zu erhalten, Verantwortlichkeiten zu definieren und sich der bestehenden Risiken bewusst zu werden. Eine Maßnahmenumsetzung zu einem möglichst frühen Zeitpunkt ist sinnvoll, damit die weitere Planung möglichst ganzheitlich und kosteneffizient erfolgen kann.

- Aufbau einer Sicherheitsorganisation: Diese übergreifende Aufgabe dient dazu, dass sicherheitsrelevante Rollen und die damit verbundenen Verantwortlichkeiten für die IT-Sicherheit von ICS-Komponenten definiert werden. Diese Sicherheitsverantwortung tragen nicht nur die Personen, die diese Rollen einnehmen. Dieser Verantwortung müssen sich alle Mitarbeiter eines Unternehmens bewusst werden und nachkommen. Die Sicherheit von ICS sollte ein selbstverständlicher Teil des Betriebskonzepts sein.
- Erstellen und Pflegen der Dokumentation: Dokumente und Informationen zur IT-Sicherheit von ICS-Komponenten (z. B. Risiko- und Schwachstellenanalysen, Netzpläne, Netzmanagement, Konfiguration, Security-Programm und -Organisation) sollten erstellt, gepflegt und ausreichend vor unbefugtem Zugriff geschützt werden und ggf. in Vorgaben für Dienstleister und Lieferanten enthalten sein. Diese Dokumentation ermöglicht es, Inkompatibilitäten und Inkonsistenzen von Software in spezifischen Versionen sowie Konfigurationen zu vermeiden und von Schwachstellen betroffene Anlagenteile zu identifizieren. Insbesondere physische und logische Netzpläne ermöglichen ein stringentes Management der Infrastruktur und der darin enthaltenen Komponenten.
- Risikomanagement: Eine der wichtigsten Aufgaben stellt das Risikomanagement dar. Im Rahmen dieses sollten sämtliche funktionalen als auch sicherheitsspezifischen Ressourcen eines ICS in Betracht gezogen werden. Diese werden systematisch analysiert und bewertet. Ziel dabei ist es, Schwachstellen zu identifizieren, zu priorisieren und geeignete Maßnahmen – sowohl technische als auch organisatorische – abzuleiten. Nur dadurch kann ein Unternehmen sein Sicherheitsniveau bzw. die Restrisiken fundiert einschätzen.

5 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
6 https://www.iso.org
7 http://www.vdi.de/uploads/tx_vdirili/pdf/9875774.pdf
8 http://webstore.iec.ch/preview/info_iec62443-1-1%7Bed1.0%7Den.pdf

- Notfallmanagement und Wiederanlaufprozeduren: Nach einem Vorfall müssen für eine Weiterführung des Betriebs Prozesse definiert sein, die eine geordnete Wiederinbetriebnahme ermöglichen. Für den sicheren und unterbrechungsfreien Betrieb ist es notwendig, dass das Service- und Wartungspersonal sowie Administratoren alle Funktionen des ICS kennen und diese bedienen können. Sämtliche für den Betrieb bzw. die Inbetriebnahme erforderlichen Dokumente in Form von Administrations- und Benutzerhandbüchern müssen verfügbar und für die zuständigen und berechtigten Mitarbeiter zugänglich sein.
- Schwachstellenreduzierung: Da sich die Bedrohungen stetig verändern und weiterentwickeln, sind regelmäßig Maßnahmen notwendig, um potenzielle Angriffe abzuwehren. Dazu gehören neben Mitarbeiterschulung und dem Abonnieren von Sicherheitsbenachrichtungen (beispielsweise von Komponentenherstellern oder der Allianz für Cyber-Sicherheit) auch eine aktive Suche nach Sicherheitslücken. Diese Maßnahmen müssen regelmäßig durchgeführt werden.
- Erkennung von Angriffen und angemessene Reaktionen: Zu Detektion und Nachvollziehbarkeit von Angriffen müssen IT- und ICS-spezifische Prozeduren sowie interne und externe Benachrichtigungswege definiert werden.[9]

Die Rolle des Unternehmens-Managements

Das Management eines Unternehmens ist in der Pflicht, die Vorgaben bzgl. Cyber-Sicherheit klar darzustellen und an alle Beteiligten in geeigneter Weise zu kommunizieren. Es müssen geeignete Kontrollmechanismen etabliert werden, um die Erfüllung dieser Erwartungen nachzuhalten. Wichtig ist, dass Cyber-Sicherheit nicht als nebenläufiges Ziel erachtet wird, welches implizit im Rahmen der Umsetzung funktionaler Anforderungen zu erfüllen ist. Vielmehr ist Cyber-Sicherheit Teil der kritischen Aspekte bei der Erbringung der Unternehmensziele. Neben wirtschaftlichen Gründen ist das Management nicht zuletzt angesichts einer möglichen persönlichen Haftung der Gesellschafter oder des Managements zur Gewährleistung eines hinreichenden Sicherheitsniveaus verpflichtet. Insgesamt liegt Cyber-Sicherheit somit durchaus auch im Eigeninteresse des Managements, weshalb insbesondere die notwendigen personellen und monetären Ressourcen zur Verfügung gestellt werden sollten.

Damit das Management die Rahmenbedingungen für ein hinreichendes Niveau bzgl. Cyber-Sicherheit schaffen kann, muss eine geeignete Unterstützung seitens der Fachseite erfolgen. Dies beinhaltet die Sensibilisierung bzgl. der Auswirkungen von potenziellen Sicherheitsvorfällen sowie die Versorgung mit zielgruppengerechten Informationen zum aktuellen Stand der Umsetzung der Cyber-Sicherheit. Im Rahmen strategischer Planungen ist das Management frühzeitig in alle wichtigen Entscheidungen einzubinden. Dabei müssen jeweils verbleibende Restrisiken sowie Fälle von akutem Handlungsbedarf aufgezeigt werden. Die Fachseite muss sich dessen bewusst sein, dass Sicherheit durchaus auch im Interesse des Managements liegt – es müssen aber die jeweiligen Entscheidungsgrundlagen transparent gemacht werden, damit das Management entsprechend handeln kann.

Maßnahmen gegen Folgeangriffe

Zur Absicherung gegen mögliche Folgeangriffe gibt es eine Reihe weiterer geeigneter Maßnahmen. Hierzu gehören u.a. die physische Absicherung der Infrastruktur gegen unbefugten lokalen Zugriff, Erfassung und Auswertung von Logdaten sowie die Härtung von IT- und ICS-Komponenten. Diese und weitere Maßnahmen sind im ICS Security Kompendium des BSI detailliert dargestellt. Auch solche Maßnahmen sollten unbedingt umgesetzt werden. Fatal ist die verbreitete Auffassung, dass einzelne Sicherheitsmaßnahmen oder Sicherheitsprodukte genügen, um ein hinreichendes Sicherheitsniveau zu erzielen. Zielführend ist vielmehr die Umset-

9 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/meldestelle.html

zung des sog. Defense-in-depth Ansatzes, also eines mehrschichtigen Sicherheitskonzepts, in dem die ausgewählten Sicherheitsmechanismen geeignete Redundanzen bilden und sich gegenseitig unterstützen.

Self Check

Der folgende Fragenkatalog dient zur Selbsteinschätzung des Sicherheitsniveaus im eigenen Unternehmen. In kleinen und mittelständischen Unternehmen (KMU) kann die Beantwortung der Fragen mit Bezug auf das gesamte Unternehmen vorgenommen werden. In größeren Unternehmen empfiehlt sich die Beschränkung auf einzelne Teile wie z.B. eine einzelne Produktionslinie. Beantworten Sie diese Fragen möglichst nicht allein, sondern in Gesprächen mit den Verantwortlichen für IT und Produktion.

Bewerten Sie bitte für jede der einzelnen Maßnahmen, ob diese für das Unternehmen bzw. den betrachteten Teil jeweils nicht, teilweise oder vollständig umgesetzt sind. Im jeweiligen Feld ist eine Punktzahl notiert. Addieren Sie die erzielten Punktzahlen pro Abschnitt und tragen Sie die Summe in der Zeile mit der jeweiligen Überschrift ein. Die folgende Abbildung zeigt dies beispielhaft. Sollte eine Sicherheitsmaßnahme nicht erforderlich sein, notieren Sie bitte die volle Punktzahl. Dies ist beispielsweise unter Punkt 4 der Fall, wenn es im gesamten Unternehmen keine Fernwartungszugänge gibt. Am Ende werden sämtliche erzielten Punkte addiert und in der letzten Zeile ebenfalls in die Skala eingetragen.

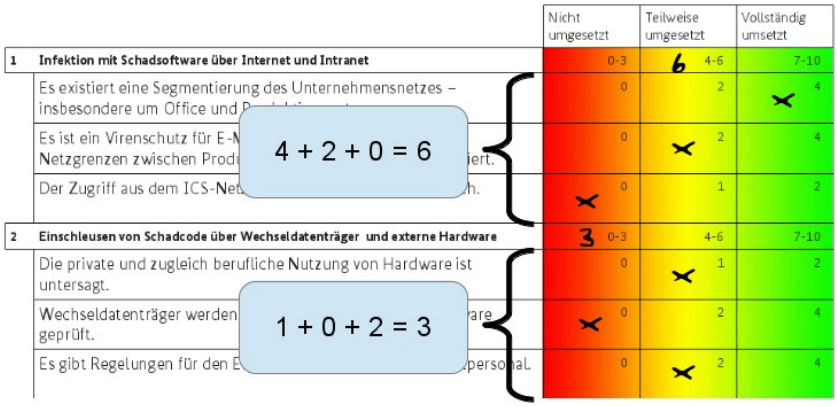

Abbildung 2: Beispiel für einen ausgefüllten Self-Check-Bogen

Im Ergebnis erhalten Sie eine erste Selbsteinschätzung darüber, wie gut Sie gegen die kritischsten Bedrohungen für den Bereich Industrial Control Systems bzw. Industrial IT aufgestellt sind. Dieser Selbsttest dient nur als erste Orientierungshilfe bei der Bewertung der Sicherheit einer Anlage oder eines Unternehmens. Er kann und darf eine ganzheitliche Betrachtung der Cyber-Sicherheit nicht ersetzen. Auch der erzielte Gesamtwert ist daher mit Vorsicht zu interpretieren. Es gilt folgende Empfehlung in Abhängigkeit der erreichten Punktzahl:

- 0-25: Das aktuelle Lagebild auf www.allianz-fuer-cybersicherheit.de und die Top 10 Bedrohungen und Gegenmaßnahmen für ICS verdeutlichen, wieso Sie jetzt handeln sollten.
- 26-50: Es sind schon einige Sicherheitsmechanismen implementiert. Es besteht jedoch Handlungsbedarf hinsichtlich elementarer Maßnahmen, die in den vorliegenden Top 10 aufgeführt sind.
- 51-75: Führen Sie eine Risikoanalyse durch, um zu analysieren, gegen welche Bedrohungen sie am dringendsten die Sicherheitsmechanismen verbessern müssen.
- 76-100: Ihr Unternehmen geht bereits verantwortungsvoll mit IT-Sicherheit um. Dies bedeutet aber keinesfalls einen verlässlichen Schutz gegen Cyber-Angriffe. Sie sollten den Weg zu einem systematischen und ganzheitlichen Ansatz wie IT-Grundschutz oder IEC 62443 verfolgen. Auf diesem Weg unterstützt sie das ICS Security Kompendium des BSI.

Im Zuge der Beantwortung der Fragen haben Sie möglicherweise bereits Diskussionen mit Kollegen darüber begonnen, was für eine Verbesserung der Sicherheit nötig und sinnvoll wäre. Dies ist eine gute Gelegenheit, die als Anlass für weitere Schritte genutzt werden sollte. Die in der Selbsteinschätzung erzielten Ergebnisse eignen sich auch dazu, das Thema Sicherheit im Unternehmen allgemein und speziell in der Produktion mit dem Management zu diskutieren.

		Nicht umgesetzt	Teilweise umgesetzt	Vollständig umgesetzt
1	**Social Engineering und Phishing**	0-3	4-6	7-10
	Es existieren regelmäßige Fortbildungs- und Sensibilisierungsmaßnahmen für alle Beschäftigten zur IT-Sicherheit.	0	2	4
	Vorgaben (Policies) regeln den Umgang der Mitarbeiter/innen mit technischen Systemen. Deren Einhaltung wird kontrolliert.	0	2	4
	Technische Sicherheitsmechanismen forcieren die Einhaltung von Policies.	0	1	2
2	**Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware**	0-3	4-6	7-10
	Die private und zugleich berufliche Nutzung von Hardware ist untersagt.	0	1	2
	Wechseldatenträger werden vor Verwendung auf Schadsoftware geprüft.	0	2	4
	Es gibt Regelungen für den Einsatz von Hardware durch Drittpersonal.	0	2	4
3	**Infektion mit Schadsoftware über Internet und Intranet**	0-3	4-6	7-10
	Es existiert eine Segmentierung des Unternehmensnetzes – insbesondere um Office- und ICS-Netz zu trennen.	0	2	4
	Es ist ein Virenschutz für E-Mail, Fileserver, PCs sowie an den Netzgrenzen zwischen ICS und anderen Netzen etabliert.	0	2	4
	Der Zugriff aus dem ICS-Netz in das Internet ist nicht möglich.	0	1	2
4	**Einbruch über Fernwartungszugänge**	0-3	4-6	7-10
	Sämtliche Fernzugriffe erfordern eine Authentisierung und sind verschlüsselt.	0	2	4
	Der Fernzugriff erfolgt feingranular, d.h. nur auf die jeweilige Komponente statt pro Subnetz.	0	1	3
	Es gibt Vorgaben für die Sicherheit der fernwartenden Rechner (z.B. aktueller Virenschutz).	0	1	3
5	**Menschliches Fehlverhalten und Sabotage**	0-3	4-6	7-10
	Es ist das „Need-to-Know“-Prinzip etabliert, sodass sensible Informationen nicht unnötig weit verbreitet sind.	0	2	4
	Es gelten hinreichende Vorgaben bzgl. Sicherheits- und Konfigurationsmanagement.	0	1	3
	Technische Maßnahmen überwachen die aktuellen Systemkonfigurationen und -zustände.	0	1	3

		Nicht umgesetzt	Teilweise umgesetzt	Vollständig umgesetzt
6	**Internet-verbundene Steuerungskomponenten**	0-3	4-6	7-10
	Es gibt keine direkte Verbindung von Steuerungskomponenten mit dem Internet.	0	2	4
	Härtung der Konfiguration der Steuerungskomponenten (Abschalten nicht benötigter Dienste, Ändern von Standardpasswörtern, ...).	0	1	3
	Es kommen flankierende Maßnahmen wie z.B. Firewalls und VPN-Lösungen zum Einsatz.	0	1	3
7	**Technisches Fehlverhalten und höhere Gewalt**	0-3	4-6	7-10
	Bei der Auswahl von Komponenten werden Sicherheitsaspekte berücksichtigt (z. B. auf Grundlage von ISA99 oder BDEW Whitepaper).	0	2	4
	Wichtige IT-Systeme sind redundant ausgelegt und verteilt aufgebaut.	0	1	3
	Es sind Prozeduren für die Reaktion auf Ausfälle/Notsituationen definiert.	0	1	3
8	**Kompromittierung von Extranet und Cloud-Komponenten**	0-3	4-6	7-10
	Betreiber externer Komponenten sind zur Einhaltung eines hinreichenden Sicherheitsniveaus, z.B. mittels SLA verpflichtet.	0	2	4
	Es erfolgt die Nutzung vertrauenswürdiger und möglichst auch zertifizierter Anbieter.	0	1	3
	Der Betrieb erfolgt in Form einer Private Cloud oder unter Gewährleistung einer strikten Mandantentrennung.	0	1	3
9	**(D)DoS Angriffe**	0-3	4-6	7-10
	Es sind Mechanismen zur Detektion und Alarmierung bei signifikanten Änderungen im Netzverkehr etabliert.	0	2	4
	Externe Anbindungen kritischer Systeme sind redundant über unterschiedliche Kommunikationstechnologien ausgelegt.	0	1	3
	In der Notfallplanung sind das Vorgehen und die relevanten externen Kontakte bei DDoS-Angriffen dokumentiert.	0	1	3
10	**Kompromittierung von Smartphones im Produktionsumfeld**	0-3	4-6	7-10
	Es erfolgt lediglich ein lesender Zugriff auf ICS-Systeme, jedoch keine Modifikation von Betriebs- oder Produktionsparametern.	0	2	4
	Die verwendeten Smartphones sind in einer möglichst sicheren Basiskonfiguration (insbesondere kein Jailbreak/Rooting).	0	1	3
	Smartphone-Applikationen müssen aus einer zertifizierten Quelle (App-Store) bezogen werden.	0	1	3
	GESAMTPUNKTZAHL			(0-100 Punkte)

Einer Vielzahl von Risiken und Bedrohungen kann nicht durch die Umsetzung technischer Maßnahmen, sondern vielmehr durch die Kombination von organisatorischen Regelungen und technischen Maßnahmen minimiert werden.

Die in diesem Dokument vorgeschlagenen Gegenmaßnahmen sind grundsätzlich geeignet, die identifizierten Bedrohungen in ihren Eintrittswahrscheinlichkeiten sowie ihren Auswirkungen hinreichend einzugrenzen. Wichtig für das Sicherheitsverständnis aller Beteiligten ist aber, dass stets gewisse Restrisiken verbleiben.

Weiterführende Informationen zur Sicherheit in der Fabrikautomation und Prozesssteuerung liefert das kostenfrei verfügbare ICS Security Kompendium des BSI. Darin sind u. a. Maßnahmen beschrieben, die neben den hier betrachteten primären Angriffen auch zum Schutz vor Folgeangriffen im Sinne eines Defense-in-depth Ansatzes angewandt werden sollten. Das ICS Security Kompendium sowie weitere Publikationen und Hilfsmittel sind auf der Webseite des BSI verfügbar:

https://www.bsi.bund.de/ICS

Bei weiteren Fragen zur Sicherheit in Industrial Control Systems steht das BSI unter der E-Mail-Adresse

ics-sec@bsi.bund.de

zur Verfügung. Hier erhalten Sie auch weitere Informationen zu Themen wie Mitarbeitersensibilisierung, Sicherheitsmanagement, technischen Anforderungen und einer Vielzahl weiterer Themen im Zusammenhang mit Industrial Control Systems.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an info@cyber-allianz.de gesendet werden.