Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IN DER PRODUKTION

Industrial Control System Security

Top 10 Bedrohungen und Gegenmaßnahmen 2022

Systeme zur Fertigungs- und Prozessautomatisierung – zusammengefasst unter dem Begriff Industrial Control Systems (ICS, IACS) – werden in nahezu allen Infrastrukturen eingesetzt, die physische Prozesse steuern. 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 in der konventionellen IT der Fall ist. Betreiber müssen sich angesichts einer zunehmenden Häufigkeit von Vorfällen und neu entdeckten Schwachstellen dringend dieser Thematik annehmen. Das Risiko und Schadenspotenzial von sowohl nicht-zielgerichteter Schadsoftware als auch von gezielten, qualitativ hochwertigen und mit signifikantem Aufwand durchgeführten spezifischen Angriffen gegen ICS muss berücksichtigt werden. Dies gilt sowohl für Systeme, 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 bezüglich 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 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.

Bedrohungen und deren Folgen

Risiken für ein ICS resultieren aus Bedrohungen, die aufgrund existierender Schwachstellen dem ICS und damit einem Unternehmen Schaden verursachen können. Die kritischsten und am häufigsten auftretenden 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.

Top 10 Bedrohungen	Trend seit 2019
Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme	→
Infektion mit Schadsoftware über Internet und Intranet	↑
Menschliches Fehlverhalten und Sabotage	→
Kompromittierung von Extranet und Cloud-Komponenten	↗
Social Engineering und Phishing	→
(D)DoS Angriffe	→
Internet-verbundene Steuerungskomponenten	↗
Einbruch über Fernwartungszugänge	↗
Technisches Fehlverhalten und höhere Gewalt	→
Soft- und Hardwareschwachstellen in der Lieferkette	↑

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

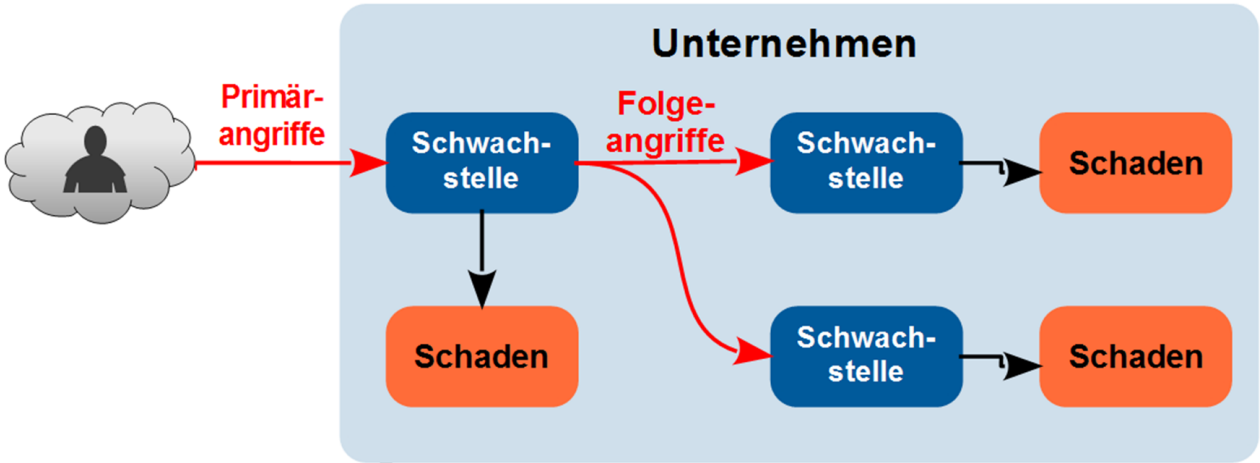

Abbildung 1: Ablauf von Primär- und Folgeangriff sowie Schadensfolgen

Zu den Folgeangriffen gehören insbesondere:

- Rechteerweiterung: Im Industrieumfeld vorhandene IT-Standardkomponenten wie Betriebssysteme, Application Server oder Datenbanken enthalten oft 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 oder grundlegende Härtungsmaßnahmen fehlen.
- 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.
- Einsatz von Ransomware: Dabei werden häufig Daten und Systeme verschlüsselt. Wenn keine Backups vorhanden sind, ist eine Wiederherstellung selten möglich. Selbst bei einer Lösegeldzahlung muss das gesamte System trotzdem neu installiert werden.

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:

- Auslösen oder Manipulation von Safety-Prozeduren oder -Systemen
  → Schaden an Mensch und Umwelt, Produktionseinbußen
  → Herbeiführen von physischen Schäden an Anlagen
- Störung der Verfügbarkeit von Teilen oder des ganzen ICS
  → Produktionseinbußen
- Datenabfluss
  → Verlust von Know-how (Intellectual Property)
- Manipulation von Systemen oder Parametern
  → Minderung der Qualität der Erzeugnisse

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

1 https://us-cert.cisa.gov/ics/Recommended-Practices

Bewertungskriterien

Die Grundlage zur Bewertung sind Erfahrungen aus konkreten Sicherheitsvorfällen, Threat Intelligence Reports sowie Rückmeldungen aus der Industrie. Es werden die zehn häufigsten Bedrohungen beschrieben, ein Trendindikator zeigt die aktuelle Entwicklung auf. Auch bei einem gleichbleibenden oder gar fallenden Trend ist weiterhin eine Gefährdung für die IT-Sicherheit vorhanden und eine ganzheitliche Betrachtung des Unternehmens erforderlich.

Von den Bewertungskriterien der vergangen Jahre 2014 und 2016 wurde abgewichen, da das Kriterium der Verbreitung für die Bewertung des Risikos am wesentlichsten scheint. Dies liegt vor allem an dem Umstand, dass sich die vorherig herangezogene weitere Kriterien (Exposition, Ausnutzbarkeit und Detektion) nur unwesentlich ändern, während sich der Verbreitungsgrad durch die Aktivität der Tätergruppen maßgeblich ändern kann. Die Reihenfolge in diesem Dokument stellt somit kein Ranking dar.

Um die resultierende Gefährdung und das resultierende Risiko für das eigene Unternehmen abzuschätzen, sollten die jeweiligen Gegenmaßnahmen nach technischer oder organisatorischer Umsetzbarkeit für die identifizierten Bedrohungen bewertet werden. Diese Betrachtung sollte zusammen mit einer Kostenabschätzung der jeweiligen Maßnahme geschehen. Diese Kostenabschätzung sollte daraufhin mit dem Business Impact, d. h. die wirtschaftlichen Auswirkungen für das Unternehmen, für den jeweiligen Fall verglichen und bewertet werden. Dies kann i. d. R. nur der Betreiber selbst unter Berücksichtigung der Rahmenbedingungen und möglichen Folgeangriffe durchführen.

Übersicht der Änderungen

Im Vergleich zur letzten Ausgabe ist bei vielen Bedrohungen keine Veränderung hinsichtlich der Ausnutzung zu erkennen. Dies bedeutet jedoch nicht, dass sich die Gefahr durch diese reduziert hat und ihnen dadurch weniger Beachtung zu schenken ist. Insgesamt ist bei allen aufgeführten Bedrohungen von einer hohen Gefahr auszugehen.

Die Bedrohung durch Smartphones ist kein eigenständiger Punkt mehr. Dieses Kapitel ist nun Teil der Bedrohung durch Wechseldatenträger und mobile Systeme. Die wesentlichen Punkte wurden dort integriert.

Neu hinzugekommen ist die Bedrohung durch Hard- und Softwareschwachstellen in der Lieferkette. Diesem Punkt gilt es in Zukunft mehr Aufmerksamkeit zu schenken.

Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme

Problembeschreibung & Ursachen

Für die Konfiguration und Wartung von ICS-Komponenten oder den Datentransfer zwischen ICS- und Office-Netz werden häufig Notebooks, Smartphones, Tablets, Programmiergeräte oder Wechseldatenträger wie USB-Sticks eingesetzt. Bei diesen Geräten ist nicht immer klar geregelt oder für den Betreiber ersichtlich, wo diese eingesetzt werden. So ist bei Laptops oder Smartphones eine private Nutzung möglich. Auch führt Fremdpersonal meist eigene Geräte mit sich. Ebenso birgt der Einsatz von Notebooks mit externen Daten und Wartungssoftware, welche möglicherweise in unterschiedlichen Unternehmen durch externes Wartungspersonal zum Einsatz kommen, Gefahren.

Mögliche Bedrohungsszenarien

1. Wechseldatenträger 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.
4. Diebstahl oder Verlust von mobilen Systemen (wie z. B. Smartphones) mit sensiblen Informationen (z. B. Passworte oder vorkonfigurierte Zugänge ins ICS-Netz).

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 Entfernung der Anschlüsse.
   f. Vollverschlüsselung von Datenträgern.
2. Etablieren strikter organisatorischer Vorgaben und technischer Kontrollen bzgl. externer Wartungsnotebooks, Smartphones, Tablets, usw. :
   a. Beschränkung des Zugriffs bzw. Beschränkung des Einsatzes
   b. Der Austausch von Daten erfolgt ausschließlich über Wechseldatenträger und unterliegt den zuvor genannten Kontrollen.
   c. Einrichtung von Quarantänenetzen für den Zugang externer Dienstleister.
   d. Virenscans der mitgebrachten Geräte vor dem Zugang zum eigentlichen System.
   e. Vollverschlüsselung von Wartungsnotebooks, die beim Betreiber verwahrt werden.
   f. Einschränkung und Kontrolle der Software/Apps.

Infektion mit Schadsoftware über Internet und Intranet

Problembeschreibung & Ursachen

Unternehmensnetze nutzen Standardkomponenten wie Betriebssysteme, Webserver und Datenbanken. Browser oder E-Mail Clients und sind i. d. R. an das Internet angebunden. Täglich werden in diesen Komponenten neue Schwachstellen bekannt, die ein Angreifer für das Eindringen in das Intranet und die Infektion mit Schadsoftware ausnutzen kann. Diese Schadsoftware kann bspw. auch durch einen Innentäter im Intranet platziert werden.

Die Ausbreitung wird zudem durch die zunehmende Verbreitung Ethernet-basierter Netze und Protokolle im ICS-Umfeld und deren Verbindung mit Systemen im Unternehmensnetz (Fileserver, ERP-, MES-Systeme, etc.) erleichtert. 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. Diese Zusammenhänge sind den Mitarbeitenden nicht immer bewusst.

Auch beim Zugriff aus dem ICS-Netz bzw. einem ICS-nahen Netz auf andere Netze – insbesondere dem Internet – kann eine direkte Infektion der Systeme mit Schadsoftware erfolgen.

Mögliche Bedrohungsszenarien

1. Infektion von Systemen über Software zur Bürokommunikation z.B. als Anhang einer E-Mail oder eines manipulierten Office-Dokument
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. Beispielsweise, wenn das Surfen im Internet über Systeme in einer Leitwarte oder andere Bedienstationen möglich ist.
3. Undokumentierte oder ungeschützte Verbindungen zwischen Unternehmensnetz und ICS-Netz.
4. Durchführung von Angriffen auf extern bereitgestellte Dienste des Unternehmens (z. B. Webseiten durch z. B. SQL-Injection, Cross Site Scripting, etc.).
5. ICS-Komponenten enthalten bekannte Schwachstellen, die von Schadsoftware zur Manipulation ausgenutzt werden können.
6. Installation von privater Hardware (z.B. WLAN-Router fürs Smartphone, Gaming-PC, Spielekonsole) durch das Personal, die mit Schadsoftware infiziert ist oder Infektionswege ermöglicht (siehe auch Menschliches Fehlverhalten und Sabotage).

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 (sogenannte „Secure Islands“).
2. Einsatz konventioneller Schutzmaßnahmen am Perimeter (z. B. Firewalls, Antivirensoftware, Intrusion Detection Systems) oder an den ICS (z. B. Firewalls, Application Allowlisting).
3. Beschränkung der im Unternehmen offen zugänglichen 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 Backendnetz und, wo möglich, im ICS-Netz.
5. Überwachung/Monitoring des Netzwerks und der Systeme auf ungewöhnliche Verbindungen und Transfervolumina, Verbindungsversuche und Aktivitäten durch netz- und hostbasiertes IDS.
6. Sämtliche im Office und ICS eingesetzten IT-Komponenten (Dienste, Rechner) sind bestmöglich zu härten.

Menschliches Fehlverhalten und Sabotage

Problembeschreibung & Ursachen

Das im ICS-Umfeld tätige Personal nimmt eine besondere Stellung bzgl. der Sicherheit ein. Dies gilt sowohl für eigene Mitarbeitende 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 immer gelebter 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. Bei Hardware sind dies z. B. Spielekonsolen, Digitalkameras, Smartphones, WLAN-Router oder andere USB-Geräte des Personals.
5. Erstellung nicht freigegebener Konfigurationen für Infrastruktur- und Sicherheitskomponenten (z. B. Hinzufügen einer Firewall-Regel, damit 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 Mitarbeitende zur Gewährleistung der Kompetenz zur Bedienung und Administration funktionaler als auch für sicherheitsspezifischer 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 getrennten 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 Mitarbeitende sowie für extern beauftragte Personen (z. B. von Herstellern oder Dienstleistern).
5. Geeignete Vorgaben („Policies & Procedures“) für den Umgang der Mitarbeitenden 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.

Kompromittierung von Extranet und Cloud-Komponenten

Problembeschreibung & Ursachen

Der in der konventionellen IT verbreitete Trend zum Outsourcing von IT-Komponenten oder Applikationen ist auch bei ICS vorzufinden. 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, Digitaler Zwilling). Auch sicherheitsspezifische Komponenten werden mitunter als Cloud-basierte Lösung angeboten. Beispielsweise 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 und damit verbundene Detektionsmöglichkeiten einer Kompromittierung hat. Die Komponenten können jedoch sehr wohl unmittelbar mit der lokalen Produktion vernetzt sein.

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 lokal beeinträchtigt werden.
2. Bei einer zu starken und einseitigen Abhängigkeit von Cloudbasierten Dienstleistungen können die Auswirkungen eines Ausfalls standortübergreifend Infrastrukturen und deren Produktion gefährden.
3. Ausnutzung von Implementierungsfehlern oder unzureichenden Sicherheitsmechanismen, um Zugriff auf extern gespeicherte Daten zu bekommen (Datendiebstahl, Löschung).
4. Bei unzureichender Trennung der Mandanten eines Cloud-Anbieters können 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.

Social Engineering und Phishing

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, Mitarbeitende zu einer unbedachten oder fahrlässigen Handlung zu verleiten. Ein klassisches Beispiel hierfür sind betrügerische E-Mails (Phishing-Mails). Diese verleiten Mitarbeitende dazu, Anhänge mit Schadsoftware zu öffnen oder enthalten Links zu manipulierten Webseiten. Diese Bedrohung steht in engem Zusammenhang mit Infektion mit Schadsoftware über Internet und Intranet .

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 Personen angreift, bei denen 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 Vorspiegelung falscher Tatsachen (z. B. als Techniker ausgeben) verschaffen.

Gegenmaßnahmen

1. Regelmäßig 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 Mitarbeitende, 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 Mitarbeitenden haben.
4. Nutzung von technischen Sicherheitsmechanismen zur Durchsetzung der geltenden Regelungen und zur automatischen Erkennung von Fehlverhalten oder Angriffen (z. B. Device Control, Netzwerksegmentierung oder Zutrittskontrolle).
5. Regelmäßige Datensicherungen zur Wiederherstellung von Daten und Anwendungen

(D)DoS Angriffe

Problembeschreibung & Ursachen

Bei Denial-of-Service-Angriffen wird die Kommunikationsverbindung überlastet oder gestört bzw. der empfangende Server mit Anfragen überlastet. In der Folge ist kein oder ein verzögerter Datenaustausch möglich. Dieses Risiko besteht vor allem bei internetverbundenen Systemen. Im Falle von Fernzugriffen kann diese Schnittstelle überlastet werden, was eine weitere Überwachung oder Steuerung verhindert. Mess- und Steuerdaten können dann nicht mehr übertragen werden.

Bei drahtlosen Schnittstellen ist dies ebenfalls möglich, in dem das Funkspektrum gestört wird.

Die beobachtete Häufigkeit und Bandbreite von DoS-Angriffen steigt jährlich. Der Trend bewegt sich von einfachen Varianten mit hohen Bandbreiten bis hin zu ambitionierten und intelligenten Formen, die auf die Anwendung zugeschnitten sind. Angreifer berücksichtigen hier die Anwendung und die Infrastruktur und reagieren auch auf Gegenmaßnahmen.

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.
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 (z. B. WLAN, LoRaWAN) oder Mobilfunknetze (z.B. GSM, LTE, 5G). Dies kann z. B. erfolgen durch:
   a. den Einsatz von Störsendern (Jamming), welche die entsprechenden Frequenzbereiche überlagern,
   b. den Einsatz von Fake Base Stations, d. h. gefälschten Basisstationen, welche die angegriffenen Systeme zum Verbinden mit einem falschen Funknetz verleiten,
   c. das Versenden spezieller Datenpakete, die zum Abbruch vorhandener Verbindungen führen.
4. DoS-Angriffe mittels Ransomware[2] [3] (z. B. Trickbot).

Gegenmaßnahmen

1. Strikte Konfiguration und Härtung von Netzzugängen und Kommunikationskanälen.
2. Nutzung dedizierter, kabelgebundener Verbindungen für kritische Funktionen.
3. Falls anwendbar: Einrichtung von Intrusion Detection Systemen (IDS) zur Erkennung von Angriffen und Alarmierung über alternative Kanäle.
4. Redundante Anbindung von Komponenten unter Verwendung unterschiedlicher Protokolle bzw. Kommunikationswege.

Darüber hinaus hat das BSI zur Unterstützung Betroffener bei der Notfallplanung und Abwehr von DDoS-Angriffen auf den Webseiten der Allianz für Cyber-Sicherheit ein Dokument zur DDoS-Mitigation[4] bereitgestellt. Ein Abgleich der eigenen Gegenmaßnahmen sollte vorgenommen werden.

2 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf
3 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf
4 https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_002.html

Internet-verbundene Steuerungskomponenten

Problembeschreibung & Ursachen

Es werden immer wieder ICS-Komponenten wie Speicherprogrammierbare Steuerungen oder Gebäudeleittechnikkomponenten entgegen den Empfehlungen der Hersteller direkt mit dem Internet verbunden und sind dann über Suchmaschinen leicht findbar. Solche Steuerungen verfügen jedoch oft nicht über ein hinreichendes Sicherheitsniveau. Zudem ist bei Bekanntwerden von Schwachstellen in Steuerungen ein (zeitnahes) Einspielen von Patches meist nicht möglich.

Mögliche Bedrohungsszenarien

1. Auffinden von Steuerungskomponenten durch allgemeine Suchmaschinen („google dorks“), spezielle Suchmaschinen wie Shodan[5] 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. Oft sind auch auch ICS-Protokolle (z.B. Modbus oder Bacnet) direkt erreichbar. Da sie meist keine oder nur schwache Authentisierungsfunktionen besitzen, können Angreifer direkt Steuerbefehle auf die nachgelagerten Komponenten schicken.

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. Konsequentes Anwenden von Defense-in-Depth Prinzipien für alle ICS-Komponenten.
4. Einsatz flankierender Maßnahmen wie z.B. Firewalls und VPN-Lösungen.
5. Zeitnahes Aktualisieren (Updates/Patchen) betroffener Produkte - sofern möglich.

5 https://www.shodan.io/

Einbruch über Fernwartungszugänge

Problembeschreibung & Ursachen

In ICS-Installationen sind externe Zugänge für Wartungszwecke weit verbreitet. Häufig existieren dabei u. A. Default-Zugänge mit Standardpasswörtern oder gelegentlich 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 kann auf weitere Systeme zugegriffen werden. Unzureichende oder mangelnde Authentisierung und Autorisierung sowie flache Netzwerkhierarchien erleichtern den Einbruch.

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-spezifische 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 Mitarbeitenden mit einer derartigen Berechtigung oder einen Innentäter,
   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 TLS[6].
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.

6 https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html

Technisches Fehlverhalten und höhere Gewalt

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.

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.
4. Bei Klimaveränderungen oder Extremwetterereignissen, wie Hitzewellen oder Flutereignisse, können bisherige Schutzmaßnahmen oder Planungen (z.B. hinsichtlich Kühlung) nicht ausreichend sein und zu Ausfällen führen.

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, offengelegten Schnittstellen, die keine eigene Entwicklung eines einzigen 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.
7. Regelmäßige Überprüfung der Maßnahmen hinsichtlich der Eignung und Rahmenbedingungen

Eine solide Basis für diese und weitere Aspekte liefert z. B. ein Whitepaper des BDEW[7].

7 https://www.bdew.de/service/anwendungshilfen/whitepaper-anforderungen-sichere-steuerungs-telekommunikationssysteme/

Soft- und Hardwareschwachstellen in der Lieferkette

Problembeschreibung & Ursachen

Lieferketten sind mitunter sehr komplexe Gebilde mit einem hohen Grad an Vernetzung, innerhalb derer Hersteller oft zugleich auch Kunden sind. Schwachstellen können daher Auswirkungen auf alle Teile der Lieferkette haben. Schwachstellen in Hard- und Software sind neben Fehlkonfigurationen der Ausgangspunkt vieler Sicherheitsprobleme (auch der in diesem Dokument genannten). Durch die Integration von Bibliotheken oder externem Quellcode (von Drittanbietern) steigen die Abhängigkeiten zwischen unterschiedlichen Herstellern.

Updates zur Beseitigung von Schwachstellen müssen von allen an der Lieferkette Beteiligten in ihre Produkte eingepflegt werden. Je nach Länge dieser Lieferkette braucht es Zeit, bis alle Beteiligten über die Schwachstelle informiert sind, tätig werden und die Kunden benachrichtigt sind.

Mögliche Bedrohungsszenarien

1. Von jedem Teil der Lieferkette kann eine Bedrohung ausgehen. Je früher in der Kette verwundbarer Code vorhanden ist, desto mehr Produkte sind betroffen und desto schwieriger ist es, die eigene Betroffenheit festzustellen. Es gibt auch Beispiele, wo gezielt Schadfunktionen bzw. Schwachstellen von Angreifern eingebaut wurden.
2. Die entstehenden Fehler können unterschiedliche Auswirkungen haben. Diese reichen von falschen Berechnungen über zu weit reichende Zugriffsrechte bis hin zur Möglichkeit der Ausführung von beliebigen Code. Dies betrifft nicht nur Primärangriffe, sondern ist „vielfach essentiell“ für Folgeangriffe.
3. Nicht alle Hersteller reagieren auf Meldungen zu Schwachstellen. Dies betrifft auch Informationskanäle des Herstellers zur Benachrichtigung seiner Kunden zu Schwachstellen, Updates oder Workarounds. Angreifer nutzen Phishing Mails mit vermeintlichen Informationen zu Patches, um Schadcode zu verteilen.
4. Es befinden sich Schachstellen in einer externe Bibliothek, die keine Updates mehr erhält oder der Hersteller nicht mehr am Markt tätig ist.

Gegenmaßnahmen

1. Es sollte ein Asset-Management vorhanden sein. Dabei sollten auch Informationsquellen hinterlegt sein, die Informationen zu Security-Advisories und Updates bereitstellen. Dazu zählen auch Kontaktinformationen von Herstellern, Integratoren und anderen beteiligten Dienstleistern.
2. Beim Bezug von Updates und Bibliotheken sollte auf vertrauenswürdige Quellen zurückgegriffen werden. Die Integrität sollte vor dem Einsatz validiert werden.
3. Es sollte ein Prozess zum Schwachstellenmanagement etabliert werden.[8] In diesem werden eingehende Security-Meldungen koordiniert, bewertet und die Integration der Updates in Komponenten und Anlagen geplant und durchgeführt.

8 https://www.bsi.bund.de/casf/

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[9],
- ISO/IEC 27000-Reihe[10],
- VDI/VDE 2182[11],
- IEC 62443[12].

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 Mitarbeitenden 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 durchgängiges 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.

9 https://www.bsi.bund.de/grundschutz/
10 https://www.iso.org
11 https://www.vdi.de/uploads/tx_vdirili/pdf/9875774.pdf
12 https://webstore.iec.ch/preview/info_iec62443-1-1{ed1.0}en.pdf

- Business-Continuity-Management (BCM): Ziel des BCM ist es sicherzustellen, dass der Geschäftsbetrieb selbst bei massiven Schadensereignissen nicht unterbrochen wird (Prävention) oder nach einem Ausfall in angemessener Zeit fortgeführt werden kann (Reaktion). Das BCM umfasst organisatorische, technische, bauliche und personelle Maßnahmen. Institutionen können hierzu teilweise auf vorhandene Sicherheitsmaßnahmen weiterer Managementsysteme, wie dem ISMS, zurückgreifen oder erweitern diese gegebenenfalls.
- Schwachstellenreduzierung: Da sich die Bedrohungen stetig verändern und weiterentwickeln, sind regelmäßig Maßnahmen notwendig, um potenzielle Angriffe abzuwehren. Dazu gehören neben Schulung 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.[13]

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 durch die 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[14] des BSI detailliert dargestellt. Auch solche Maßnahmen sollten unbedingt umgesetzt werden. Fatal ist die verbreitete Auffassung, dass einzelne Sicherheitsmaßnahmen oder Sicherheitsprodukte ge-

13 https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Service/Meldungen/meldungen_node.html
14 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/Allgemeine-Empfehlungen/allgemeine-empfehlungen_node.html

nügten, um ein hinreichendes Sicherheitsniveau zu erzielen. Zielführend ist vielmehr die Umsetzung 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.

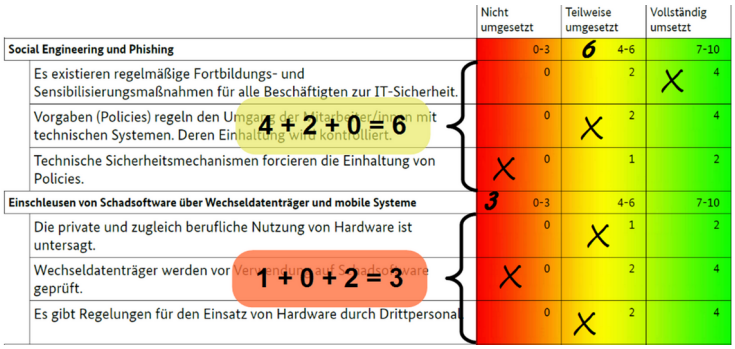

Abbildung 2: Beispiel für einen ausgefüllten Self-Check-Bogen

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 Abbildung zeigt dies beispielhaft. Sollte eine Sicherheitsmaßnahme nicht erforderlich sein, notieren Sie bitte die volle Punktzahl. Dies ist beispielsweise unter dem Punkt "Einbruch über Fernwartungszugänge" 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.

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 umsetzt
Social Engineering und Phishing	0-3	4-6	7-10
Es existieren regelmäßige Fortbildungs- und Sensibilisierungs-maßnahmen für alle Beschäftigten zur IT-Sicherheit.	0	2	4
Vorgaben (Policies) regeln den Umgang der Mitarbeitenden mit technischen Systemen. Deren Einhaltung wird kontrolliert.	0	2	4
Technische Sicherheitsmechanismen forcieren die Einhaltung von Policies.	0	1	2
Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme	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
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
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
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 umsetzt
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
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
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
(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
Soft- und Hardwareschwachstellen in der Lieferkette	0-3	4-6	7-10
Es gibt eine zentrale Asset-/Geräteverwaltung?	0	2	4
Informationen zu Schwachstellen werden von regelmäßig in kurzen Abständen von Herstellern oder Integratoren bezogen und ausgewertet.	0	1	3
Bereitgestellte Updates werden in Wartungsprozesse eingeplant und eingespielt.	0	1	3
GESAMTPUNKTZAHL			(0-100 Punkte)

Eine Vielzahl von Risiken und Bedrohungen kann nicht durch die Umsetzung technischer Maßnahmen alleine, 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. Auch wenn die Eintrittswahrscheinlichkeit gering erscheint, ist eine Auseinandersetzung mit den Restrisiken und das Üben, was bei deren Eintritt zu tun ist, empfohlen.

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 Mitarbeitendensensibilisierung, 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.