Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IN DER PRODUKTION

Erfahrungen aus der industriellen Sicherheitsberatung

Cyber-Sicherheit in der Fabrikautomation und Prozesssteuerung – subsumiert unter dem Begriff Industrial Control Systems (ICS) – umzusetzen, ist angesichts zunehmender Vorfälle eine dringende Notwendigkeit. Viele Betreiber haben aber bislang eine rein funktionale Sicht auf ihre Maschinen oder Anlagen und stehen somit vor einer großen Herausforderung. Besonders bei kleinen und mittelständischen Unternehmen übersteigt die Einführung eines Informationssicherheitsmanagementsystems (ISMS), wie IT-Grundschutz oder ISO 27000, die internen Fähigkeiten und Kapazitäten, wenn Security bislang kein Thema war. Um sukzessive den Einstieg in das Thema Cyber-Sicherheit zu schaffen und dabei möglichst schnell signifikante Verbesserungen des Sicherheitsniveaus zu erzielen, ist unter anderem das Konzept der Kurzrevision geeignet. Hierbei werden externe Dienstleister mit einer Prüfung der Infrastruktur beauftragt. Der Aufwand bei kleineren Infrastrukturen beschränkt sich auf wenige Tage. Die bei der Prüfung identifizierten Handlungsfelder sind häufig auch ohne größere Aufwände umsetzbar. Eine gute Grundlage für die Vorgehensweise bildet die IS-Revision[1] sowie das ICS Security Kompendium[2] des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Bei der Anwendung dieses Konzepts im industriellen Umfeld ist aber dringend darauf zu achten, einen Dienstleister zu wählen, der in der jeweiligen Branche fundierte Kenntnisse besitzt. Schon nach wenigen Iterationen einer solchen Revision sind typischerweise bereits solide Voraussetzungen im Unternehmen geschaffen, um dann ein ganzheitliches Sicherheitsmanagement auf Grundlage eines ISMS zu realisieren. Auch für große Unternehmen eignet sich eine solche Revision als regelmäßige Prüfung des Sicherheitsmanagements.

Im Folgenden sind die häufigsten Mängel, die bei Revisionen im industriellen Umfeld in unterschiedlichen Branchen aufgefallen sind, dargestellt. Für die weiterführende Lektüre zu einzelnen Mängeln wird jeweils auf die entsprechenden Maßnahmen im ICS Security Kompendium des BSI verwiesen.

1 Organisation

In vielen Fällen ist keine **hinreichende Sensibilisierung** für die Bedrohungen der Cyber-Sicherheit im Unternehmen oder Betrieb vorhanden. Dies gilt sowohl für das Management (z. B. Produktionsverantwortliche) als auch auf der Arbeitsebene (z. B. Ingenieur oder Anlagenbediener). Gerade hier kann ein Revisionsbericht eine Erhöhung der Awareness herbeiführen, da die Mängel ganz konkret im eigenen Unternehmen aufgezeigt werden.

1 Informationssicherheitsrevision (IS-Revision), https://www.bsi.bund.de/is-revision
2 ICS Security Kompendium, https://www.bsi.bund.de/ICS-Security-Kompendium

Weitere Informationen im ICS Security Kompendium: Maßnahme 14 „Training des Personals“

Oftmals werden bei einer Revision Regelungslücken hinsichtlich der **Zuständigkeiten** aufgezeigt. Sehr häufig gibt es keine definierte Rolle im Unternehmen für die Gesamtverantwortung für Cyber-Sicherheit im Bereich Produktion oder auch IT. Hinzu kommen unterschiedliche Sichtweisen und Unstimmigkeiten zwischen klassischem IT-Betrieb und Produktion. Auch sind die **Kommunikationsprozesse** zwischen den wichtigen Schlüsselpositionen nicht hinreichend definiert oder umgesetzt. Dies gilt im Bereich der Security insbesondere für das Changemanagement sowie das Incident Management.

Weitere Informationen im ICS Security Kompendium: Maßnahmen 1 „Aufbau einer Security-Organisation“, 11 „Changemanagement“

Häufig sind im Unternehmen keine **Betriebsanweisungen** (Policies, Richtlinien) definiert, die das Thema Cyber-Sicherheit behandeln. Diese sind insbesondere für den Umgang mit Passwörtern, Wechseldatenträgern und privater Informationstechnik dringend zu empfehlen.

Weitere Informationen im ICS Security Kompendium: Maßnahmen 55 „Passwortverteilung und -management, Passwort-Richtlinien“, 66 „Umgang mit Wechseldatenträgern“

2 Netzwerk

Grundvoraussetzung für ein solides Sicherheitsmanagement ist ein **Netzplan**. Dieser ist in der Praxis häufig entweder unvollständig, veraltet oder erst gar nicht vorhanden. Auch Abhängigkeiten zwischen Systemen sind hierbei häufig nicht dokumentiert. Ohne diese Grundlage lassen sich aber weder Maßnahmen planen, noch mögliche Auswirkungen von Angriffen bewerten. Gerade historisch gewachsene Fernzugriffsmöglichkeiten sind in Netzplänen häufig nicht berücksichtigt, obgleich diese als mögliches Einfallstor als besonders kritisch einzustufen sind.

Weitere Informationen im ICS Security Kompendium: Maßnahmen 4 „Netzplan“, 5 „Liste der IT-Systeme und installierten Anwendungen“

Flache Netzwerkhierarchien und fehlende **Segmentierung der Netze** erleichtern einem Angreifer oder einer Schadsoftware, sich im Unternehmen auszubreiten („lateral movement“). Die Bildung geeigneter Teilnetze und die technische Absicherung an den Netzübergängen ist für eine hinreichende Absicherung jedoch zwingend erforderlich. So sollte besonders der Zugriff aus dem Office-Netz in die Produktion besonders restriktiv geregelt werden.

Weitere Informationen im ICS Security Kompendium: Maßnahmen 32 „Netzsegmentierung“, 38 „Einsatz von Firewalls“, 41 „Geeignete logische Trennung und VLAN“, 33 „Absichern der elektronischen externen Schnittstellen“

Zugangspunkte für einen **Fernzugriff** sind häufig unzureichend umgesetzt. Oftmals werden diese Systeme nicht gepflegt oder befinden sich in einer unsicheren Konfiguration. Gerade moderne Fernwartungslösungen enthalten jedoch eine Vielzahl sinnvoller Schutzfunktionen, die in der Praxis mit einem gewissen Maß an Fachkenntnissen gut umgesetzt werden könnten.

Weitere Informationen im ICS Security Kompendium: Maßnahmen 29 „Sichere Fernwartung“, 58 „Einsatz geeigneter kryptographischer Verfahren“

Häufig ist ein uneingeschränkter **Zugriff auf das Internet aus der Produktion** heraus möglich. Dies erhöht nicht nur die Wahrscheinlichkeit einer erfolgreichen Kompromittierung über manipulierte E-Mails oder infizierte Webseiten. Der Angreifer erhält damit zugleich die Möglichkeit, mit seiner Infrastruktur (Command and Control Server) Kontakt aufzunehmen, um weitere Anweisungen oder zusätzliche Schadmodule nachzuladen und gestohlene Daten nach außen zu schleusen.

Weitere Informationen im ICS Security Kompendium: Maßnahme 51 „Zugriff auf das Internet innerhalb des ICS-Netzwerks“

Infrastrukturen in der Produktion unterliegen zudem nicht selten keiner hinreichenden **Erfassung und Auswertung von Kommunikationsdaten und lokalen Ereignissen** (Logging). Ohne diese Sammlung und Auswertung von Informationen über den ein- und ausgehenden Datenverkehr ist aber weder eine Erkennung erfolgreicher Kompromittierungen noch eine Aufbereitung/Forensik möglich.

Weitere Informationen im ICS Security Kompendium: Maßnahmen 73 „Logging / Monitoring“, 42 „Implementierung von Intrusion-Detection- bzw. Intrusion-Prevention-Systemen“

3 Komponenten

Oftmals ist bei Komponenten, wie etwa Bedienterminals, SPSen oder Engineering Workstations, keine **sichere Standardkonfiguration** vorhanden. So werden beispielsweise Dienste über das Netzwerk betrieben, die nicht benötigt werden und somit eine unnötige Angriffsfläche bieten. Auch vorhandene Sicherheitsmechanismen werden häufig nicht genutzt oder sind falsch konfiguriert.

Weitere Informationen im ICS Security Kompendium: Maßnahmen 24 „Verzicht auf überflüssige Produktfunktionen“, 48 „Entfernen von unnötiger Software und Diensten“, 49 „Anpassung der Standard-Einstellungen“

In nahezu sämtlichen Unternehmen finden sich im Produktionsumfeld **Standardpasswörter**. Diese können von einem Angreifer genutzt werden, um ohne weiteren Aufwand einen Vollzugriff zu erlangen. Besonders kritisch sind Standardpasswörter, wenn sie zu Benutzerkonten gehören, die den Verantwortlichen nicht bekannt sind oder die sich nicht ändern/deaktivieren lassen, da der Hersteller diese fest einprogrammiert hat.

Weitere Informationen im ICS Security Kompendium: Maßnahmen 25 „Individuelle Zugangsdaten“, 46 „Standard-Benutzerkonten und -Passwörter“, 47 „Individuelle Benutzerkonten“

USB-Sticks und andere Wechseldatenträger werden häufig unkontrolliert eingesetzt. Einerseits fehlt das Problembewusstsein bei den Mitarbeitern, andererseits sind keine physischen oder technischen Maßnahmen zur Absicherung umgesetzt. Dies erhöht besonders die Gefahr einer Infektion mit nicht-zielgerichteter Schadsoftware massiv.

Weitere Informationen im ICS Security Kompendium: Maßnahmen 66 „Umgang mit Wechseldatenträgern“, 67 „Wechseldatenträgerschleuse (Quarantäne-PC)“

Veraltete **Patchlevel** stellen in der Produktion weniger ein Problem dar, sondern mit Blick auf das primäre Ziel der meist ständigen Verfügbarkeit der Maschinen eher eine Tatsache. Die Philosophie des „Wir können keine Softwareupdates einspielen“ gilt häufig nicht nur für den eigentlichen Produktionsprozess, sondern auch für externe Komponenten. Fernzugriffslösungen und Engineering Workstations nicht zu patchen, führt zu unnötigen und höchst kritischen Angriffsmöglichkeiten sowie einem hohen Potential für Kollateralschäden durch nicht-zielgerichtete Schadsoftware.

Weitere Informationen im ICS Security Kompendium: Maßnahme 26 „Aktivierte Sicherheitsmechanismen und aktueller Patchstand“, 52 „Umgang mit Patches“

Die **Geräte für den Fernzugriff und Wartung vor Ort** unterliegen oftmals keiner strengen Reglementierung. Mitunter verwenden die eigenen Mitarbeiter private Geräte, die über kein hinreichendes Sicherheitsniveau verfügen. Über die von Drittfirmen genutzten Clients besteht keine Kontrollmöglichkeit, sodass hier zumindest eine vertragliche Regelung hinsichtlich eines

Basisschutzes getroffen werden sollte. Ein an das eigene Unternehmens- oder Produktionsnetz angeschlossene Gerät sollte mindestens über ein aktuelles Patchlevel und einen tagesaktuellen Virenschutz verfügen.

Weitere Informationen im ICS Security Kompendium: Maßnahme 68 „Einsatz von Notebooks zu Wartungszwecken“

Die aufgeführten Mängel gehören aufgrund ihrer weiten Verbreitung und den damit verbundenen Risiken zu den Aspekten, die jeder Betreiber berücksichtigen sollte. Angesichts der Effektivität einer Kurzrevision sind zudem Anlagenbetreiber dazu angehalten, dieses Mittel für den Einstieg in das Thema ICS Security zu nutzen. Auch bei Unternehmen mit einem fortgeschrittenen Sicherheitsmanagement kann eine Revision ein wichtiges Element sein. Für die Vorgehensweise eignet sich als Orientierungshilfe u. a. die IS-Revision[3] des BSI sowie der Cyber-Sicherheits-Check[4].

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.

3 Informationssicherheitsrevision (IS-Revision), https://www.bsi.bund.de/is-revision
4 Cyber-Sicherheits-Check, https://www.allianz-fuer-cybersicherheit.de/dok/6644004