10 ICS-Sicherheitsmaßnahmen für KMUs

1x1 der ICS-Sicherheit

Ing. DI (FH) Herbert Dirnberger, MA, CISM, Cyber Security Austria

Der effektive Einsatz von Technologien und Prozessen sind entscheidende Faktoren, um qualitativ hochwertige Produkte und innovative Dienstleistungen als Unternehmen anbieten zu können. Durch den Einsatz entstehen auch Risiken, exemplarisch durch die Konvergenz von IT und Automatisierungstechnik. Auch mittelständische Unternehmen bilden da keine Ausnahme. Zu den typischen Risiken, die auf Industrial Control Systeme von kleinen und mittelständischen Firmen einwirken können, gehören neben den direkten monetären Schäden auch Qualitätsminderung der Produkte oder Dienstleistungen, die Überlastung von Personal, Rechtsstreitigkeiten sowie Reputations- und Know-how-Verluste.

Im Folgenden werden zehn Sicherheitsmaßnahmen für Industrial Control Systeme (ICS) dargestellt, die speziell auf die Anforderungen von kleinen und mittelständischen Unternehmen (KMU) abgestimmt sind. Zugrunde liegt der „Baseline"-Ansatz, der die Risiken möglichst minimiert. Wichtig ist, dass die Komposition dieser Maßnahmen für jedes KMU speziell betrachtet und durch weitere Maßnahmen ergänzt werden sollte. Der Vorteil der vorgestellten Maßnahmen ist ihre einfache Anwendung und die Einbeziehung der Organisation zur Risikobehandlung. Die Maßnahmen wirken oft gegen mehrere Risiken und sind Grundbausteine, um langfristig eine Sicherheitskultur im Unternehmen zu bilden.

Sensibilisieren und Bewusstsein schaffen, Management einbinden

Der erste Erfolgsbaustein, um Risiken zu vermeiden oder zu mindern, ist es, das Management zu sensibilisieren und zu integrieren sowie bei allen Mitarbeitern ein Sicherheitsbewusstsein zu schaffen. Die Förderung und Bereitstellung von Sicherheit ist eine elementare Aufgabe des Managements und wird erst im Zuge eines offenen Informationsaustausches zwischen den handelnden Organisationseinheiten ermöglicht.

Verantwortung definieren

Damit Sicherheit im Unternehmen und für die ICS gebildet werden kann, muss die Organisation diese Aufgabe auch funktionell vergeben. Typische Rollen, die diese Aufgabe wahrnehmen können, sind Sicherheitsbeauftragte, Servicekoordinatoren, aber auch Administratoren und Techniker. Wichtig ist, dass die Verantwortung über die Sicherheit im ganzen Unternehmen bekannt ist und entsprechend unterstützt wird.

Budget und Ressourcen bereitstellen

Ohne entsprechendes Budget und Ressourcen sind auch ICS-Sicherheitsmaßnahmen nicht umsetzbar. Vor allem bei Neuinvestitionen sind entsprechende Mittel für künftige Maßnahmen einzuplanen und bereitzustellen. Zu knapp bemessene Ressourcen behindern in jedem Fall die Entwicklung der Sicherheit. Allerdings wirken zu viele Mittel auch kontraproduktiv. Dann werden oft unpassende Maßnahmen eingesetzt.

Zugangskontrollen und -schutz installieren

Viele Risiken entstehen dadurch, dass die Zugänge zu den Systemen nicht gesichert sind und keine Kontrolle über Zugriff, Verwaltung und Datenhaltung besteht. Physikalisch können nicht befugte Zugänge durch Pförtner, Zäune, Schranken, Zugangskontrollsysteme, versperrbare Türen oder Schaltschränke verhindert werden. In diesem Kontext muss auch auf IT-Systemen und ICS die Authentifizierung und Autorisierung von Benutzern geklärt werden. Nach Möglichkeit sollten keine Standardkennwörter der Hersteller verwendet und Administratorkonten nicht für klassische Bedienaufgaben herangezogen werden. Kritisch sind auch Zugänge für betriebsfremde Personen über Fernwartungen. Oft kommen ungesicherte Remote-Zugänge via Modem oder Router und ungesicherte physikalische Zugänge zum Einsatz.

Backup erstellen und Recovery prüfen

Bei einer typischen Laufzeit von 15 bis 25 Jahren wird es bei fast allen ICS zu technischen Defekten, Fehlbedienungen, aber auch zu Energieausfällen oder ähnlichem kommen. Um die Systeme nach Ausfällen wieder in Betrieb nehmen zu können, sind Sicherungen von Betriebssystemen, Anwenderprogrammen, Parametern und aktuellen Daten notwendig. Erschwerend kommt bei heterogenen Umgebungen hinzu, dass manche Ersatzhardware nicht mehr verfügbar ist. Ein weiterer Aspekt ist, dass bei großen Systemen ein gemeinsamer Wiederherstellungszeitpunkt nicht festgelegt werden kann und eine Sicherung des Systems wiederum die Verfügbarkeit beeinträchtigt. Eine entscheidende Rolle kommt den Wiederherstellungstests zu, da diese präventiv prüfen, ob die Backup-Maßnahmen wirksam sind.

Dokumentation laufend überarbeiten

In allen Phasen des Lebenszyklus eines ICS wie Errichtung des Systems, Inbetriebnahme, Betrieb, Service, aber auch bei Störungen und in Notfällen ist eine gut strukturierte, leicht zugängliche und aktuelle Dokumentation notwendig. Kombiniert mit Backup und Recovery mindert eine gute Dokumentation viele Risiken. Ein Beispiel: Eine ordnungsgemäße Versionsverwaltung ist eine der stärksten Maßnahmen, wenn die Integrität von Daten durch Malware kompromittiert wird. Die Dokumentation von Patch- und Change-Management-Prozessen ist ein wichtiges Element für weitere Serviceaktivitäten.

Segmentierung durchführen

Durch den Ersatz von Feldbussen wie Industrial Ethernet, aber auch durch die Migration von ICS in Unternehmensnetze, ist ein weiterer Schutz der ICS notwendig. Beispielsweise sind ältere Betriebssysteme nicht für den Einsatz in Netzwerken geeignet, aber auch Systemdienste von Steuerungen sollten nicht allen Mitarbeitern im Unternehmen zugänglich sein. Spezielle Patch-Strategien oder bekannte Schwachstellen, die behoben werden sollen, erfordern eine klassische Segmentierung des Netzwerkes durch Firewalls, Router, VLAN, Datendioden oder Ähnliches. Eine begleitende, sehr wirksame Folge der Segmentierung ist, dass generell die Komplexität im gesamten Unternehmen sinkt.

Anti-Malwareschutz einsetzen

Trotz der technischen Maßnahmen wie Segmentierung und sicherer Authentifizierung besteht die Gefahr, dass Systeme durch Malware wie Viren, Trojaner oder Ähnliches kompromittiert werden. Da nicht immer alle Maßnahmen aus der klassischen IT wie Patch-Management oder Virenscanner eingesetzt werden können, sind auch alternative Maßnahmen wie Application Whitelistening, Write Blocker, CIFS-Scanning, aber auch Isolation der Systeme einsetzbar.

Komplexität reduzieren

Komplexe, empfindliche und nicht-lineare Systeme lassen sich nur schwer beherrschen. Maßnahmen wie Secure by Design, Hardening, Application Whitelistening usw. können die Komplexität verringern und in Folge die Robustheit erhöhen. Allgemein ist es ein wirksames Mittel zur Erhöhung der Widerstandsfähigkeit, wenn man die Ein- und Ausgangsparameter begrenzt.

Integration von ICS-Sicherheit im Managementsystem durchführen

Alle vorgestellten Maßnahmen werden oft von organisatorischen Maßnahmen wie Richtlinien, Standards, Messungen und laufenden Prozessverbesserungen begleitet. Dabei darf man das vorhandene Managementsystem nicht vergessen und sollte Arbeitsweisungen für die Bedienung von ICS-Systemen mit den bestehenden IT-Richtlinien abgleichen. ■