Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Generalsekretariat

Nationales Zentrum für Cybersicherheit NCSC
www.ncsc.admin.ch

NCSC

Massnahmen zum Schutz von Industriellen Kontrollsystemen (ICS)

Inhaltsverzeichnis

1 Einleitung 3
2 Zusammenfassung 3
3 Massnahmen zum Schutz von Industriellen Kontrollsystemen (ICS) 4
3.1 Asset Datenbank für Geräte 4
3.2 Umgang mit Software 4
3.3 Sichere Konfigurationen 5
3.4 Robuste Netzwerkarchitektur 5
3.5 Mehrstufiger Malwareschutz 6
3.6 Authentisierung und Autorisierung 7
3.7 Zentrale Logauswertung 8
3.8 Physischer Schutz 8
3.9 Backup und Recovery Prozeduren 9
3.10 Security Incident Management Prozesse 9
3.11 Sicherheitskultur etablieren 10

1 Einleitung

Kontroll- oder Steuerungssysteme bestehen aus einem oder mehreren Geräten, welche das Verhalten von anderen Geräten oder Systemen steuern, regeln und/oder überwachen. In der industriellen Produktion ist der Begriff «Industrielle Kontrollsysteme» (engl. Industrial Control Systems, ICS) geläufig. Industrielle Kontroll- und Steuerungssysteme finden seit einiger Zeit vermehrt auch ausserhalb der produzierenden Industrie Anwendung, zum Beispiel bei der Hausautomation oder der Verkehrsregelung. Im Prinzip kann man bei jedem System, welches einen physischen Prozess regelt und/oder überwacht von einem Industriellen Kontrollsystem sprechen. Die meisten Grundregeln für den Schutz solcher Systeme finden auch ausserhalb der industriellen Produktion Anwendung. Aus diesem Grund werden Industrielle Kontrollsysteme in diesem Artikel allgemein als «ICS» bezeichnet.

SANS[1], ein Sicherheitsinstitut aus den USA, hat 20 Schlüsselelemente[2] publiziert, wie IT-Infrastrukturen generell geschützt werden können. Diese Elemente können teilweise auch auf ICS angewendet werden. Weitere Empfehlungen sind vom US-amerikanischen Industrial Control Systems Cyber Emergency Response Team (ICS-CERT[3]) sowie vom National Institute of Standards and Technology (NIST[4]) herausgegeben worden.

Die folgenden Empfehlungen basieren auf diesen Dokumenten.

2 Zusammenfassung

Die detaillierte Anleitung finden Sie auf den hinteren Seiten dieses Dokumentes

11 Massnahmen zum Schutz von Industriellen Kontrollsystemen (ICS)

1. Asset Datenbank für alle Geräte erstellen und pflegen
2. Life Cycle und Patchmanagement für Software etablieren
3. Sichere Konfigurationen definieren und verwenden
4. Robuste Netzwerkarchitekturen planen und bauen
5. Mehrstufigen Malwareschutz implementieren
6. Authentisierung und Autorisierung
7. Zentrale Logauswertung aufbauen
8. Physischen Schutz gewährleisten
9. Backup und Recovery durchführen und regelmässig testen
10. Security Incident Management Prozesse etablieren und üben
11. Sicherheitskultur etablieren

1 SANS: http://www.sans.org

2 SANS Top 20 Critical Security Controls: http://www.sans.org/critical-security-controls/

3 ICS CERT: http://ics-cert.us-cert.gov/

4 NIST: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

3 Massnahmen zum Schutz von Industriellen Kontrollsystemen (ICS)

Die aufgeführten Massnahmen sollten in einen übergeordneten Sicherheitsprozess eingebettet sein, welcher sicherstellt, dass die Massnahmen angewendet, regelmässig geprüft und kontinuierlich verbessert werden. Weiter sollte der Betreiber einer Anlage seine aktuelle Bedrohungslage kennen, diese regelmässig überprüfen und die Erkenntnisse in die Implementierung und Verbesserung der Sicherheitsmassnahmen einfliessen lassen. Dazu ist eine enge Zusammenarbeit zwischen Risikomanagement, Engineering und Betrieb von grosser Bedeutung.

Meistens lässt sich die Sicherheit nicht mit einer einmaligen Aktion erhöhen. Es handelt sich um einen kontinuierlichen Prozess, der niemals enden sollte. Setzen Sie sich realistische, erreichbare Ziele und arbeiten Sie zuerst die Punkte ab, die mit einem relativ geringen Aufwand die Sicherheit spürbar erhöhen. Beispielsweise können Sie zuerst alle Standardpasswörter ändern und von aussen erreichbare Steuerungsinterfaces schützen.

3.1 Asset Datenbank für Geräte

Massnahme	Führen Sie eine Datenbank, in welcher alle Elemente der Steuerung, von Umsystemen, aber auch von normalen Endgeräten verzeichnet sind.
Begründung	Ohne zu wissen, welche Elemente geschützt werden müssen und welche Elemente vertrauenswürdig sind, ist ein effektiver und effizienter Schutz unmöglich.
Implementierungshinweise	Es gibt verschiedene technische Hilfsmittel, wie dieses Ziel erreicht werden kann. Mit einem netzbasierten Inventarisierungstool lässt sich ein erster Überblick gewinnen. Bei aktiven Scannern ist jedoch grosse Vorsicht geboten. Viele ICS sind nicht darauf vorbereitet, unerwarteten Netzwerkverkehr zu erhalten, was zu einer Fehlfunktion führen kann. Unbekannte Geräte, die sich neu mit dem Netz verbinden, sollten einen Alarm auslösen. Dies kann auf den MAC-Adressen der Geräte basieren. Obwohl eine MAC-Adresse leicht gefälscht werden kann, entfaltet diese Massnahme bereits eine ansehnliche Detektionswirkung.

3.2 Umgang mit Software

Massnahme	Führen Sie eine Datenbank, in welcher alle Software-Elemente verzeichnet sind. Dies ist auch die Basis für ein gutes Patch-, Release und Life Cycle Management. Machen Sie – wo immer möglich – ein Whitelisting, insbesondere auf allen kritischen Geräten, so dass nur bekannte Software ausgeführt wird.
Begründung	Die Asset Datenbank für Software liefert die Basis für ein Change-, Patch- und Release Management.

	Viele Angriffe, insbesondere gezielte Angriffe, werden via schwach geschützte Systeme mit hohen Rechten durchgeführt (z. B. Administrations- oder Entwicklergeräte). Wird dieser Angriffspfad erschwert, ist der Aufwand für einen erfolgreichen Angriff wesentlich höher. Generell ist das Life Cycle Management bei ICS aufgrund ihrer sehr langen Lebensdauer von grosser Wichtigkeit.
Implementierungshinweise	Die initiale Erstellung der Datenbank kann mit technischen Hilfsmitteln (Software Inventory Tools) erleichtert werden. Das Patch Management bei ICS ist sehr heikel und kann (aus Gewährleistungsgründen) meist nur in Zusammenarbeit mit dem Lieferanten erfolgen. Das heisst, dass in der Regel längere Zeitfenster vorhanden sind, während denen ein System angreifbar ist. Das Risiko kann durch ein Whitelisting von ausführbaren Anwendungen reduziert werden. Bei fast jedem Angriff muss auf dem angegriffenen Gerät Software gestartet werden. Ein Whitelisting soll erreichen, dass nur noch zugelassene Programme ausgeführt werden können.

3.3 Sichere Konfigurationen

Massnahme	Sichere Konfigurationen.
Begründung	Häufig nutzen Angreifer schwache Passwörter oder Standardpasswörter aus.
Implementierungshinweise	Administrationsoberflächen sollten nie direkt vom Internet her erreichbar sein. Falls dies nötig ist, muss eine Einschränkung in Bezug auf die erlaubten IP-Adressen bestehen. Sicherheitsrichtlinien und Härtungsanweisungen seitens der Hersteller sind unbedingt zu befolgen. Bietet das ICS die Möglichkeit, Software zu signieren und bei einer Veränderung der eingesetzten Software einen Alarm auszulösen, ist diese Möglichkeit unbedingt zu nutzen. Konfigurationen sollen auch darauf hin geprüft werden, dass keine schwachen Passwörter und keine Standardpasswörter vorhanden sind.

3.4 Robuste Netzwerkarchitektur

Massnahme	Robuste Netzwerkarchitektur mit voneinander abgeschotteten Netzwerkzonen.

Begründung	ICS sollten möglichst in abgeschotteten Netzwerken ohne direkten Internetzugang betrieben werden. Dies hält die Angriffsfläche möglichst gering und den Aufwand für das Überwinden der verbleibenden Grenze möglichst hoch. Das Netz der Büroautomation und das Netz der ICS sollten, wenn möglich, komplett getrennt sein. Ist dies nicht möglich, muss ein entsprechendes Zonenkonzept die Kommunikation steuern.
Implementierungshinweise	Müssen Elemente vom Internet her erreichbar sein, muss der Zugang besonders geschützt werden. Der Einsatz von VPN-Technologien mit einer 2-Faktor Authentisierung (z. B. mit einem One Time Password Token und einem PIN) ist sehr zu empfehlen. Ebenso sollten nur einzelne IP-Adressen gezielt für die Wartung freigeschaltet werden. Dasselbe gilt für die interne Segmentierung: Ist ein Zugriff aus dem normalen Netzwerk ins ICS Netz notwendig, muss dieser über einen dedizierten Punkt gehen, wo eine Authentisierung und ein Monitoring erfolgen. Die Netzwerke sollten mit dedizierten auf ICS-Protokolle spezialisierten Netzwerk-basierten Intrusion Detection Systemen (IDS) überwacht werden. Netzwerkprotokolle sollten wo immer möglich in verschlüsselter Form realisiert werden. Gibt es keine entsprechende Protokollvariante, kann der Netzwerkverkehr in einen Tunnel eingepackt werden. Besonders beim Zugriff auf webbasierte Administrationsinterfaces sollte immer SSL/TLS verwendet werden. Wenn Daten aus der Produktionsumgebung regelmässig in das Büronetzwerk übertragen werden sollen (z. B. für Statistik), können diese via einen optischen Isolator (Datendiode) ausgeleitet werden, welcher Kommunikation in nur eine Richtung zulässt. So wird verhindert, dass durch diese Leitung Schadcode vom Büronetzwerk zu den Kontrollsystemen gelangt.

3.5 Mehrstufiger Malwareschutz

Massnahme	Mehrstufiger Malware-Schutz.
Begründung	ICS, welche auf handelsüblichen Betriebssystemen aufsetzen, sind gegenüber Malware exponiert, insbesondere, weil sie (aus Gründen von Herstellervorschriften, Validierungen, Produktionssicherheit) oft auf einem alten Patch-Level gehalten werden müssen. Oft wird Malware eingesetzt, um Hilfssysteme, Administrationsgeräte oder Datenbankserver zu übernehmen, welche mit ICS verbunden sind. Alte Plattformen von ICS, welche auf Windows-basierten Betriebssystemen aufsetzen, sind bezüglich Malware-Angriffe besonders gefährdet.

Implementierungshinweise	Generell ist ein guter Malware-Schutz zentral für das korrekte Funktionieren jedes ICS. Oft ist es weder möglich noch sinnvoll, Malwareschutzprodukte auf kritischen ICS zu installieren. Administrationsgeräte und normale Windows Server sollten jedoch über einen aktuellen Virenschutz verfügen. Der Schutz vor Malware sollte auf mehreren Stufen erfolgen, so dass Malware, die auf der einen Stufe nicht erkannt wird, auf einer anderen Stufe detektiert werden kann. Darüber hinaus sollte das Netzwerk auf verdächtige Datenströme, welche auf Malware-Infektionen hindeuten, überwacht werden. Es ist sehr sinnvoll dafür zu sorgen, dass sich keine der beteiligten Systeme direkt mit dem Internet verbinden dürfen, sondern dass nur eingeschränkte Punkt-zu-Punkt Verbindungen via einen Proxy Server zugelassen werden.

3.6 Authentisierung und Autorisierung

Massnahme	Sichere Authentisierung und Autorisierung von allen beteiligten Personen und Systemen.
Begründung	Auf die Authentisierung und die Rechtevergabe sollte grosser Wert gelegt werden, da Mängel in diesem Bereich von Angreifern sehr rasch und einfach ausgenutzt werden können.
Implementierungshinweise	Wo immer möglich, sollte eine Authentisierung verlangt und die Autorisierung nach dem Prinzip der minimalen Rechtevergabe umgesetzt werden. Verschiedene ICS und/oder ICS-Protokolle unterstützen keine oder nur eine rudimentäre Authentisierung. In diesem Fall sind kompensierende Massnahmen zu ergreifen, wie z. B. eine Authentisierung an der Grenze zum Netzwerk mit den ICS. Stellen Sie sicher, dass keine Standard-User-Accounts mit den Standardpasswörtern existieren. Alle Passwörter sollten so stark wie möglich gewählt werden und für exponierte Administrationsoberflächen sollte eine 2-Faktor-Authentisierung zum Einsatz kommen. Die Benutzer – insbesondere auch Wartungsfirmen – sollten nur die Rechte erhalten, die sie zum Ausführen der jeweiligen Aufgabe effektiv benötigen.

3.7 Zentrale Log-Auswertung

Massnahme	Logs aller Systeme sollten zentral gesammelt, ausgewertet und aufbewahrt werden.
Begründung	Erst mit der Sammlung aller Logs lassen sich Zusammenhänge von einzelnen Ereignissen verstehen und Angriffe erkennen.
Implementierungshinweise	Für jede Systemklasse, unabhängig ob es sich um ein ICS, ein Administrationsgerät oder ein Umsystem handelt, ist festzulegen, welche Ereignisse aufgezeichnet werden. Die aufgezeichneten Daten sollten möglichst lange aufbewahrt werden. Erfolgreiche Angriffe werden manchmal erst nach Monaten oder Jahren entdeckt und lassen sich oft nur mit Hilfe von Logs nachvollziehen. Definieren Sie eine Baseline von Ereignissen, welche ein normales und störungsfreies Funktionieren repräsentiert. Abweichungen, Fehler und unerwartetes Verhalten sind immer abzuklären.

3.8 Physischer Schutz

Massnahme	ICS und damit direkt oder indirekt verbundene Umsysteme sind gegen unerlaubten physischen Zugriff zu schützen.
Begründung	In der Regel ist der physische Zugangsschutz zu ICS sehr hoch. Beachten Sie jedoch auch Umsysteme und Fernwartungslokalitäten sowie abgesetzte, fernadministrierte Anlagen. Durch physischen Zugang zu einem Anschluss lassen sich meist Sicherheitsmassnahmen auf Netzwerkebene umgehen.
Implementierungshinweise	Die Suche nach Schwachstellen in dem bestehenden, physischen Schutz der ICS erweitern auf Umsysteme und Administrationssysteme, sowie auf allfällige Systeme, welche sich an entfernten Standorten befinden. Jede physische Schnittstelle bietet einen erleichterten Zugriff auf das Netzwerk.

3.9 Backup- und Recovery-Prozesse

Massnahme	Backup- und Recovery-Vorgänge sind zu definieren und regelmässig zu testen. Dies gilt sowohl für die eigentlichen ICS als auch für damit verbundene Umsysteme. Die Backup-Dateien sind regelmässig auf ihre Integrität hin zu prüfen.
Begründung	Oft werden Backups nicht getestet. Im Krisenfall stehen zwar Backup-Dateien zur Verfügung, diese können aber unter Umständen nicht gelesen oder nicht ohne Weiteres eingespielt werden.
Implementierungshinweise	Die Backup-Daten müssen an einem sicheren Ort, in einer gewissen Entfernung zum gesicherten System, gespeichert werden. Backups sollten nicht nur Daten umfassen, sondern auch Konfigurationsdateien. Das Zurückspielen von Backups sollte mindestens einmal im Jahr, besser halbjährlich geübt werden. Die Backup-Dateien sind regelmässig auf ihre Integrität hin zu prüfen. Dazu sollten für alle Backup-Dateien kryptographische Hashwerte gerechnet und aufbewahrt werden.

3.10 Security Incident Management-Prozesse

Massnahme	Für einen Zwischenfall sind vorbereitete und geübte Prozesse definiert. Dieser umfasst sowohl die Erkennung, die Reaktion als auch die Prävention.
Begründung	Richtiges und entschiedenes Reagieren bei einem Zwischenfall kann den Schaden in der Regel stark reduzieren.
Implementierungshinweise	Die ICS sind in den normalen Security Incident Response-Prozess einzubinden. Sicherheitsvorfälle lassen sich nicht immer auf den ersten Blick erkennen. Deshalb ist unerklärbares Verhalten eines ICS immer abzuklären. Nach einem Sicherheitsvorfall ist immer eine Analyse über die Ursachen durchzuführen. Massnahmen zur zukünftigen Vermeidung sind zu definieren. So lässt sich eine kontinuierliche Verbesserung erreichen.

3.11 Sicherheitskultur etablieren

Massnahme	Schaffen einer Sicherheitskultur mit entsprechenden Verantwortlichkeiten und Abläufen, welche explizit auch ICS beinhalten.
Begründung	Die Sicherheit ist in alle Geschäftsprozesse zu integrieren. Notwendige Massnahmen und die Risikolandschaft sollten über ein internes Kontrollsystem direkt und unverfälscht der Geschäftsleitung berichtet werden können. Die Geschäftsleitung muss über die speziellen Risiken und Eigenschaften von Industriellen Kontrollsystemen informiert sein.
Implementierungshinweise	Die Sicherheitsprozesse sollten in die normalen Geschäftsprozesse und Kontrollkreisläufe eingebettet werden. Das Funktionieren und das Erreichen der Ziele sollten auf technischer und organisatorischer Ebene regelmässig überprüft und wo nötig Verbesserungen geplant und umgesetzt werden. Das Durchführen der Prüfungen und die Kommunikation der Ergebnisse an die Geschäftsleitung ist einem möglichst unabhängigen Rollenträger mit den notwendigen Ressourcen und Befugnissen zu übertragen. Die Verantwortlichkeit bleibt immer bei der Geschäftsleitung.