enisa
European Network and Information Security Agency

Protecting Industrial Control Systems

Recommendations for Europe and Member States

Executive Summary in German

This is the executive summary in German of the ENISA report "Protecting Industrial Control Systems. Recommendations for Europe and Member States" published on the 14th of December, 2011. Full report available at: https://www.enisa.europa.eu/act/res/other-areas/ics-scada/protecting-ics-report.

Zusammenfassung

Industrielle Kontrollsysteme (Industrial Control Systems, ICS) sind Steuerungs- und Kontrollnetzwerke und -systeme, die zur Unterstützung industrieller Verfahren entwickelt wurden. Diese Systeme werden zur Überwachung und Kontrolle unterschiedlicher Verfahren und Tätigkeiten genutzt, wie in der Gas- und Stromversorgung, der Wasser- und Ölaufbereitung und im Eisenbahnverkehr. Die größte Untergruppe dieser ICS bilden dabei die sogenannten SCADA-Systeme (Supervisory Control and Data Acquisition), also Systeme zur Überwachung, Steuerung und Sammlung von Daten. In den letzten Jahren haben die ICS beträchtliche Änderungen durchlaufen und sich von proprietären, isolierten Systemen zu offenen Architekturen und Standardtechnologien gewandelt, die in hohem Maße mit anderen Unternehmensnetzwerken sowie mit dem Internet vernetzt sind. Die heutigen ICS-Produkte basieren größtenteils auf eingebetteten Standard-Systemplattformen, werden in zahlreichen unterschiedlichen Geräten eingesetzt, wie beispielsweise Routern oder Kabelmodems, und nutzen dabei häufig kommerzielle Standardsoftware. All diese Entwicklungen haben zu Kosteneinsparungen sowie einer höheren Benutzerfreundlichkeit geführt und ermöglichen es, diese Systeme auch aus der Ferne und von verschiedenen Standorten aus zu steuern. Ein entscheidender Nachteil, der sich aus der Anbindung an Intranets und offene Kommunikationsnetze ergibt, ist jedoch die erhöhte Anfälligkeit für Computernetz-basierte Angriffe.

Industrielle Steuerungssysteme stellen angesichts der zunehmenden Gefahr folgenschwerer Terroranschläge auf kritische Infrastrukturen[1] ein strategisches Kapital dar. In den letzten zehn Jahren wurde bei diesen Systemen eine beträchtliche Anzahl von Störfällen verzeichnet, darunter auch der „Stuxnet"-Angriff, der bei allen beteiligten Interessengruppen in diesem Bereich zu großen Bedenken und zu Diskussionen über die ICS-Sicherheit geführt hat.

Im April 2007 nahm der Rat die Schlussfolgerungen zu einem Europäischen Programm für den Schutz kritischer Infrastrukturen (EPCIP)[2] an. Dieser Schritt war das Ergebnis einer Reihe von Maßnahmen, die die Europäische Kommission, der Rat und der Rat (Justiz und Inneres) seit Juni 2004 vorantreiben. Der wichtigste Bestandteil von EPCIP ist die Richtlinie[3] über die

[1] ***Kommission der Europäischen Gemeinschaften.*** *Mitteilung der Kommission an den Rat und das Europäische Parlament. Schutz kritischer Infrastrukturen im Rahmen der Terrorismusbekämpfung. KOM(2004) 702 endgültig. 2004.*

[2] ***Kommission der Europäischen Gemeinschaften.*** *Mitteilung der Kommission über ein Europäisches Programm für den Schutz kritischer Infrastrukturen. KOM(2006) 786. 2006.*

[3] ***Kommission der Europäischen Gemeinschaften.*** *Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern. 2008.*

Ermittlung und Ausweisung europäischer kritischer Infrastrukturen. Daneben werden die Informationssicherheit betreffende Angelegenheiten für wichtige Infrastrukturen in Europa im Rahmen der Mitteilung über eine Digitale Agenda für Europa[4] sowie des Aktionsplans zum Schutz kritischer Informationsinfrastrukturen (CIIP)[5] behandelt.

In Anbetracht der Bedeutung dieser Problematik hat die ENISA eine Reihe von Maßnahmen auf den Weg gebracht, die darauf abzielen, die relevanten Interessenvertreter zusammenzubringen und zu einer offenen Diskussion über den Schutz der ICS anzuregen. Das maßgebliche Ziel dieses offenen Dialogs sind die Ermittlung der Hauptbedenken über die Sicherheit der ICS[6] sowie die Anerkennung und Unterstützung nationaler, europaweiter und internationaler Initiativen zur ICS-Sicherheit. Die beteiligten Interessenvertreter umfassen Anbieter von Werkzeugen und Dienstleistungen im Zusammenhang mit der ICS-Sicherheit, Hersteller und Integratoren von ICS-Soft- und Hardware, Infrastrukturbetreiber, öffentliche Einrichtungen und Normungsgremien sowie Hochschulen und Vertreter aus der Forschung und Entwicklung.

Um den Interessenvertretern einen besseren Einblick in diese Thematik zu ermöglichen, hat die ENISA außerdem beschlossen, eine auf Untersuchungen und Umfragen gestützte Studie zu diesem Thema durchzuführen. Ziel dieser Studie ist es, den aktuellen Stand des Schutzes von ICS, insbesondere in Europa, aber auch im internationalen Kontext, abzubilden. Dies umfasst sowohl die Gefahren, Risiken und Herausforderungen im Zusammenhang mit dem Schutz solcher Steuerungssysteme als auch verschiedene nationale, europäische und internationale Initiativen zur ICS-Sicherheit.

Dieser abschließende Bericht stellt den Beteiligten aus dem öffentlichen sowie dem privaten Sektor sieben Empfehlungen auf dem Gebiet der industriellen Steuerungssysteme vor. Diese Empfehlungen sollen nützliche und praktische Hinweise zur Verbesserung laufender Initiativen liefern, die Zusammenarbeit verbessern, zur Entwicklung neuer Maßnahmen und bewährter Verfahren beitragen und Hindernisse beim Informationsaustausch beseitigen. Die hier enthaltenen Hinweise basieren auf den Ergebnissen einer eingehenden Analyse der Meinungen jener Sachverständigen, die an der Studie teilgenommen haben. Darüber hinaus werden auch andere wichtige Informationen berücksichtigt, die im Rahmen einer gründlichen Schreibtischstudie gewonnen wurden. Alle vorliegenden Daten wurden analysiert und haben zu rund 100 wichtigen Erkenntnissen geführt.

Im Folgenden werden die einzelnen Empfehlungen kurz vorgestellt.

---

[4] ***Kommission der Europäischen Gemeinschaften.*** *Mitteilung der Kommission: Eine Digitale Agenda für Europa. KOM(2010) 245. 2010.*

[5] ***Kommission der Europäischen Gemeinschaften.*** *Mitteilung der Kommission: Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität. KOM(2009) 149. 2009.*

[6] *Auf verschiedenen Ebenen: rechtliche und regulatorische Aspekte, organisatorische Aspekte, Aspekte der Verbreitung und Sensibilisierung, wirtschaftliche und finanzielle sowie technische Aspekte.*

Empfehlung 1: Schaffung europaweiter und nationaler Strategien für die Sicherheit von ICS. *Die Europäische Union sollte eine europaweite Strategie für europäische Maßnahmen zur ICS-Sicherheit ausarbeiten. Die einzelnen Mitgliedstaaten sollten darüber hinaus entsprechende eigenstaatliche Strategien entwickeln. Diese Strategien müssen den Vorgaben in der Richtlinie 2008/114/EG des Rates der Europäischen Union über kritische Infrastrukturen entsprechen und zur Optimierung sowohl der bestehenden Initiativen im Zusammenhang mit der ICS-Sicherheit (z. B. EuroSCSiE) als auch der nationalen und europaweiten öffentlich-privaten Partnerschaften (z. B. EP3Rs) beitragen. Die Strategien müssen für alle Interessenvertreter aus den Mitgliedstaaten als Bezugspunkte dienen, den Austausch von Initiativen begünstigen und die Forschungs- und Entwicklungsarbeit vorantreiben.*

Empfehlung 2: Ausarbeitung eines Leitfadens mit bewährten Verfahren auf dem Gebiet der ICS-Sicherheit. *Die Europäische Union sollte die Führung übernehmen und ein per Konsens beschlossenes Dokument bzw. einen Satz mehrerer Dokumente mit bewähren Verfahren auf dem Gebiet der Sicherheit erarbeiten, das Aspekte der physischen und logischen Sicherheit abdeckt und somit als Bezugspunkt für alle relevanten Interessenvertreter dient. Mithilfe dieser Unterlagen sollten alle Interessenvertreter sicherstellen können, dass optimale Sicherheitsverfahren in der Industrie zur Anwendung kommen.*

Empfehlung 3: Erstellung von Vorlagen für ICS-Sicherheitspläne. *Die im Rahmen der unterschiedlichen nationalen ICS-Sicherheitsstrategien vorgesehenen Aufgaben sollten die Erstellung sowohl einer operativen als auch einer infrastrukturbezogenen Vorlage für einen ICS-Sicherheitsplan berücksichtigen, die die Sicherheitsexperten dann an die jeweilige Situation anpassen können. Diese Pläne sollten sowohl den Bereich der operativen wie auch der physischen Sicherheit abdecken und technische Aspekte, Schulungs- und Sensibilisierungsmaßnahmen, die Verwaltung von Sicherheitsaspekten mit entsprechenden Rollen und Zuständigkeiten sowie Maßnahmen zu betrieblichen Auswirkungen und zum Krisenmanagement berücksichtigen. Diese Vorlagen sollten die mit der Ausarbeitung von Sicherheitsplänen verbundenen Kosten deutlich senken und die Einführung umfassender Sicherheitsmaßnahmen in der Industrie beschleunigen können.*

Empfehlung 4: Förderung des Sensibilisierungs- und Schulungsaspekts. *Aufgrund ihrer Mitwirkung an den nationalen ICS-Sicherheitsstrategien sollten die Mitgliedstaaten verstärkt Maßnahmen zur Verbreitung solcher Systeme sowie zur Sensibilisierung hierfür unterstützen, indem sie hochkarätige Veranstaltungen organisieren, an denen alle Arten von Interessenvertretern teilnehmen. Besonderes Augenmerk sollte dabei auf die Einbindung der oberen Führungsebene gelegt werden. Schulungs- und Sensibilisierungsprogramme und -veranstaltungen sollten für alle Arten von Endnutzern entwickelt werden.*

Empfehlung 5: Schaffung einer gemeinsamen Testgrundlage oder alternativ eines Rahmens für eine ICS-Sicherheitszertifizierung. *Die gemeinsame ICS-Strategie sollte zur Schaffung gemeinsamer Testgrundlagen auf europäischer Ebene in Form einer öffentlich-privaten Partnerschaft führen, in deren Rahmen Tests mit dem Ziel durchgeführt werden können, durch die Interaktion verschiedener Systeme bedingte Sicherheitsverletzungen zu vermeiden. Mithilfe einer gemeinsamen Testgrundlage können alle Interessenvertreter potenzielle Störfälle in*

einem kontrollierten Umfeld leichter erkennen. Auf diese Weise werden die Integrität und Vertrauenswürdigkeit zertifizierter Lösungen verbessert.

Alternativ kann auch ein Modell für einen Sicherheitsrahmen für ICS aufgestellt werden, der sich auf aktuelle Bemühungen auf diesem Gebiet stützt, beispielsweise gemeinsame Kriterien oder FIPS. In den Mitgliedstaaten bereits bestehende Zertifizierungsbehörden wären in diesem Szenario für das in diesem Rahmen festgelegte Zertifizierungsverfahren zuständig.

Empfehlung 6: Schaffung nationaler ICS-Notfallkapazitäten im Falle von computerinduzierten Störfällen. *Gemäß den nationalen Strategien für die ICS-Sicherheit sollten gemeinsam mit einer angemessenen Anzahl von öffentlichen und privaten Computernotfallteams (Computer Emergency Response Team, CERT) Notfallkapazitäten für die Reaktion auf ICS-bezogene Computerstörfälle eingerichtet werden. Diese ICS-Notfallkapazitäten sollten dazu beitragen, dass die Interessenvertreter immer eine zentrale Plattform haben, über die sie Informationen austauschen und bekannt machen, Maßnahmen koordinieren und ein wirksames Risikomanagement in ICS-Infrastrukturen anbieten können. Bei den grenzübergreifenden Herausforderungen sollten die Mitgliedstaaten auf europäischer Ebene zusammenarbeiten, beispielsweise im Rahmen einer ICS-Sicherheitsplattform wie EuroSCSiE für den Informationsaustausch.*

Empfehlung 7: Förderung der Forschung auf dem Gebiet der ICS-Sicherheit zur Optimierung bestehender Forschungsprogramme. *Die nationalen wie die gemeinsamen ICS-Sicherheitsstrategien sollten die Förderung der Forschungsarbeit vorsehen, um sowohl gegenwärtige als auch künftige Bedrohungen und Herausforderungen im Zusammenhang mit der ICS-Sicherheit wirksam angehen zu können. Hierzu zählen unter anderem die Integration von ICS und IKT, Altsysteme und unsichere Ausrüstung, zielgerichtete Angriffe oder auch Probleme im Zusammenhang mit Smart Grids. Umgesetzt werden sollte diese Empfehlung durch die Optimierung bestehender europäischer und nationaler Forschungsprogramme, wie des Europäischen Rahmenprogramms.*

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu