DITS.center e.V.

ICS-S Industrial Control System Security

Industrie 4.0 und das „Internet of Things (IoT)“ fördern die Vernetzung von Systemen zur Prozessteuerung und der Fabrikautomation. Der Entwurf, die Entwicklung und der Betrieb robuster und sicherer Systeme münden in neuen Herausforderungen, die besser unternehmensübergreifend behandelt werden. Die Förderung von KMU Netzwerken ist das Ziel.

Die IT-Landschaft von Fertigungs- und Prozessautomatisierungsunternehmen gliedert sich in die Komponenten Office IT und das Industrial Control System (ICS). ICS kontrolliert die physischen Prozesse und ist in den meisten produzierenden Unternehmen ein integraler Bestandteil der Wertschöpfungskette. ICS besteht aus einer Vielzahl von IT Komponenten in allen Ebenen der Automatisierungspyramide mit diversen angreifbaren Schnittstellen.

In der Office IT stehen bereits ausgefeilte und reife Sicherheitsmechanismen, Prozesse sowie Regularien (z.B. Passwortpolicy, Endpointsecurity, Firewalls, Absicherung mobiler Systeme) zur Verfügung. Der Reifegrad bzgl. Informationssicherheit bei heterogenen und über Jahrzehnte gewachsenen Automatisierungssystemen und -netzwerken ist indes noch stark verbesserungswürdig. Den handelnden Verantwortlichen fehlt es oft an Erfahrung zum Thema Informationssicherheit – den IT-Sicherheitsexperten sind dagegen die besonderen Rahmenbedingungen der Automatisierer wie z.B. Echtzeit, Safety, Firmware, Maschinensteuerungs-Software o.ä. wenig geläufig.

Für ICS Komponenten existiert kein Standard zur Gefahrenabwehr, obwohl gravierende wirtschaftliche Schäden, Verletzungsgefahr und der Versorgungsausfall drohen. Der systematische Ausschluss von Gefahren erfordert Schulung, Maßnahmen in der Entwicklung und im Betrieb. Der Austausch zwischen Anwendern (Produktionsbetrieben), IT-Experten und hoheitlichen Einrichtungen (BSI) ist erforderlich, um sowohl das spezielle Branchen Know-How als auch das Sicherheitsverständnis zu integrieren

ICS-S baut über Förderung und Forschung ein Netzwerk auf, welches nachhaltig Lösungen im Sicherheitsumfeld der Mechatronik erarbeitet und markt- und anwendungsnah umsetzt.

Treiber der ICS-S Netzwerkaktivität sind die sich andauernd ändernden Anforderungen und der daraus resultierende Handlungsbedarf. Industrie 4.0 vergrößert mit den neuen Zielen und Technologien das Gefahrenpotential. Verschärfte Anforderungen aus dem IT-Sicherheitsgesetz, sowie die Internationale Normenreihe IEC 62443 über industrielle Kommunikationsnetze sind zu berücksichtigen.

In der Vergangenheit konnte die Firmware der Automatisierungstechnik von den Entwicklern als proprietäre Lösung, außerhalb allgemein gültiger Standards, entwickelt und betrieben werden. Heute sind Transparenz und die nachvollziehbare Einhaltung von Standards und Normen verbindlich. Es besteht die Notwendigkeit zur Anpassung von Produkten und zur Aufstellung neuer Standards für die Entwickler und Betreiber.

Sowohl der Verlust an Daten, als auch der Angriff auf Prozesse und Anlagen im Bereich Produktion, Versorgung und Verteilung definieren Bedrohungen mit gravierenden wirtschaftlichen und gesellschaftlichen Auswirkungen. Die Sensibilisierung für das Thema sowohl in der Entwicklung von Komponenten, der Produktion als auch im Management auf Betreiberseite wird im Rahmen der Initiative ICS-S gefördert. Die Praktiker und Anwender werden durch ein Informationsforum für Prozesse, Methoden und auch Maßnahmen zur Erkennung von Angriffen und der Abwehr unterstützt und gefördert.

Die Komplexität der möglichen Angriffe in den Bereichen Automatisierung, Digitalisierung, Industrie 4.0 und im Internet der Dinge ist vielfältig. Insbesondere die mittelständischen Hersteller und Betreiber von Automatisierungstechnik sind durchwegs mit identischen Fragen gefordert. Es besteht die Gefahr, dass ICS-S den Wettbewerb zwischen Großindustrie und Mittelstand nachhaltig zum Nachteil des Mittelstands beeinflussen kann. Es ist nur vernünftig, die Effektivität und Effizienz der Maßnahmen und die Wettbewerbsfähigkeit durch gemeinschaftliches und koordiniertes Handeln zu sichern bzw. zu steigern. Folgende konkrete Maßnahmen sind im Rahmen des Projekts ICS-S vorgesehen:

- Systematischen Aufarbeitung der Problemkreise (Use-cases)
- Analyse von Bedrohungsszenarien und Fallbeispielen
- Analyse gesetzlicher Rahmenbedingungen, Datenschutz u.a.
- Zusammenarbeit mit Forschungseinrichtungen
- Zusammenarbeit mit Behörden (BSI) im Bereich IT-Security
- Zusammenarbeit mit Sicherheitsbehörden zur Schaffung von Lagebildern
- Zusammenarbeit mit Systemintegratoren
- Einbindung von Software-, Hardwareware- und Beratungsfirmen
- Durchführung von Projekten zu Einzelfragen und -themen
- Durchführung von Informationsveranstaltungen und Schulungen
- Aufbau und Pflege internetbasierten Wissensplattform
- Aufzeigen von Lösungswegen
- Förderung von Kooperationen.

Technologie	Software, Viren, Digitalisierung, IT und Cyber Security, IEC 62443, zivile Sicherheit, Datenschutz, Datensicherheit.
Märkte	Produktionstechnik, Automatisierungstechnik, Prozesstechnik, Software, Firmware.
Anmerkungen	Industrial Control System, Industrie 4.0, Internet of Things, Vernetzung, KMU, Mittelstand, Synergie, Kooperation.