Industrial Control System Security

Top 10 Bedrohungen für Automatisierungs-, Prozesssteuerungs- und -leitsysteme und Gegenmaßnahmen mit Produkten von INSYS icom

INSYS icom
Industrielle Datenkommunikation

25.05.2013

Top 10 Bedrohungen im Überblick lt. BSI [1)]

Nr.	Bedrohung	Erläuterung
1	Unberechtigte Nutzung von Fernwartungszugängen	Wartungszugänge sind bewusst geschaffene Öffnungen des ICS-Netzes nach außen, die häufig jedoch nicht hinreichend abgesichert sind.
2	Online-Angriffe über Office- / Enterprise-Netze	Office-IT ist i.d.R. auf vielen Wegen mit dem Internet verbunden. Meist bestehen auch Netzwerkverbindungen vom Office- ins ICS-Netz, sodass Angreifer über diesen Weg eindringen können.
3	Angriffe auf eingesetzte Standardkomponenten im ICS-Netz	IT-Standardkomponenten (commercial off-the-shelf, COTS) wie Betriebssysteme, Application Server oder Datenbanken enthalten in der Regel Fehler und Schwachstellen, die von Angreifern ausgenutzt werden. Kommen diese Standardkomponenten auch im ICS-Netz zum Einsatz, so erhöht dies das Risiko eines erfolgreichen Angriffs auf die ICS-Systeme.
4	(D)DoS Angriffe	Durch (Distributed) Denial of Service Angriffe können Netzwerkverbindungen und benötigte Ressourcen beeinträchtigt und Systeme zum Absturz gebracht werden, z.B. um die Funktionsfähigkeit eines ICS zu stören.
5	Menschliches Fehlverhalten und Sabotage	Vorsätzliche Handlungen – ganz gleich ob durch interne oder externe Täter – sind eine massive Bedrohung für sämtliche Schutzziele. Daneben sind Fahrlässigkeit und menschliches Versagen eine große Bedrohung insbesondere bzgl. der Schutzziele Vertraulichkeit und Verfügbarkeit.
6	Einschleusen von Schadcode über Wechseldatenträger und externe Hardware	Der Einsatz von Wechseldatenträgern und mobilen IT-Komponenten externer Mitarbeiter stellt stets eine große Gefahr bzgl. Malware-Infektionen dar. Dieser Aspekt kam z.B. bei Stuxnet zum Tragen.
7	Lesen und Schreiben von Nachrichten im ICS-Netz	Da die meisten Steuerungskomponenten derzeit über Klartextprotokolle und somit ungeschützt kommunizieren, ist das Mitlesen und Einspielen von Steuerbefehlen oftmals ohne größeren Aufwand möglich.
8	Unberechtigter Zugriff auf Ressourcen	Insbesondere Innentäter oder Folgeangriffe nach einer Penetration von außen haben leichtes Spiel, wenn Dienste und Komponenten im Prozessnetz keine bzw. unsichere Methoden zur Authentisierung und Autorisierung implementieren.
9	Angriffe auf Netzwerkkomponenten	Netzwerkkomponenten können durch Angreifer manipuliert werden, um z.B. Man-in-the-MiddleAngriffe durchzuführen oder um Sniffing zu erleichtern.
10	Technisches Fehlverhalten und höhere Gewalt	Ausfälle durch extreme Umwelteinflüsse oder technische Defekte sind immer möglich – Risiko und Schadenspotential können hier lediglich minimiert werden.

1) Quelle: BSI-A-CS 004 | Version 1.00 vom 12.04.2012 Weblink

Maßnahmen durch INSYS SECURITY INSIDE

Nr.	Bedrohung	Maßnahme
1	Unberechtigte Nutzung von Fernwartungszugängen	▪ VPN ▪ Netzsegmentierung ▪ Firewalls ▪ Authentisierung ▪ Autorisierung ▪ Blacklisting ▪ Whitelisting ▪ Schlüsselschalter-Funktion
2	Online-Angriffe über Office- / Enterprise-Netze	▪ Netzsegmentierung ▪ Firewalls ▪ Authentisierung ▪ Autorisierung ▪ VPN
3	Angriffe auf eingesetzte Standardkomponenten im ICS-Netz	▪ Remote-Firmewareupdate ▪ Keine Standard-Officekomponenten ▪ Individuell für INSYS ausgewählte Linux-Komponenten
4	(D)DoS Angriffe	▪ Redundante Verbindungen
5	Menschliches Fehlverhalten und Sabotage	▪ Zugriff auf Webinterface deaktivierbar ▪ RADIUS-Server ▪ Whitelisting ▪ Blacklisting ▪ Intuitive Konfiguration „keep it simple and secure“ ▪ Schlüsselschalter-Funktion ▪ Sensibilisierung (Policies & Procedures) ▪ Geräte und Dienste „Made in Germany“ und „Designed by INSYS“ ▪ Nur notwendige Dienste werden installiert ▪ Nur notwendige Dienste laufen
	Fortsetzung s. nächste Seite	

Maßnahmen durch INSYS SECURITY INSIDE, Fortsetzung

Nr.	Bedrohung	Maßnahme
6	Einschleusen von Schadcode über Wechseldatenträger und externe Hardware	▪ Netzsegmentierung ▪ Port-based Security
7	Lesen und Schreiben von Nachrichten im ICS-Netz	▪ Netzsegmentierung ▪ Secure Islands ▪ Remote-Modi deaktivieren ▪ VPN
8	Unberechtigter Zugriff auf Ressourcen	▪ VPN ▪ INSYS Connectivity Service ▪ Firewalls ▪ Authentisierung ▪ Autorisierung ▪ Netzsegmentierung ▪ Schlüsselschalter-Funktion ▪ Port-based Security ▪ Whitelisting ▪ Blacklisting
9	Angriffe auf Netzwerkkomponenten	▪ Logfiles überwachen ▪ Meldungsversand ▪ Nur notwendige Dienste werden installiert ▪ Nur notwendige Dienste laufen
10	Technisches Fehlverhalten und höhere Gewalt	▪ Redundante Verbindungen ▪ Rudundante Geräte ▪ Backup der Konfiguration

- Setzen Sie Produkte von INSYS icom mit INSYS SECURITY INSIDE ein.
- Nutzen Sie die wie immer technisch fundierte Beratung unserer Mitarbeiter:
- Telefon +49 941 58692-0 oder E-mail insys@insys-tec.de - Wir beraten Sie gerne und kompetent!