Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Checklist beveiliging van ICS/SCADA-systemen

Tref organisatorische én technische maatregelen

Factsheet FS-2012-02
versie 1.2 | 22 december 2015

Kwaadwillenden en securityonderzoekers tonen interesse in de (on)veiligheid van industriële controlesystemen (ICS/SCADA-systemen). Systemen die direct vanaf het internet bereikbaar zijn liggen in het bijzonder onder vuur. ICS/SCADA-systemen kennen echter meer aandachtspunten. Met behulp van deze factsheet kunt u bepalen of uw ICS/SCADA-systemen afdoende zijn beveiligd. Deze maatregelen worden als good practice beschouwd.

Achtergrond

Het toepassingsgebied van ICS/SCADA-systemen is breed en varieert van eenvoudige tot kritieke systemen en processen. Het is aan de eigenaren om te bepalen welk beveiligingsniveau en diepgang van maatregelen passend zijn. Voor deze bepaling is risicoanalyse noodzakelijk.

Uitgangspunten

In de checklist worden organisatorische en technische maatregelen onderscheiden. Elke maatregel wordt kort toegelicht inclusief referenties naar meer achtergrondinformatie en implementatietips. De checklist omvat maatregelen tegen de meest voorkomende kwetsbaarheden en beveiligingsproblemen.

Doelgroep

Eigenaren en beheerders van ICS/SCADA-systemen en gebouwbeheersystemen.

Samenwerking

Deze factsheet is tot stand gekomen in samenwerking met vertegenwoordigers van de vitale infrastructuur en andere NCSC-partners.

Checklist organisatorische maatregelen

1. De organisatie beschikt over een securitybeleid dat ook van toepassing is op de ICS/SCADA-systemen.
   Veel organisaties hebben wel een securitybeleid, maar ICS/SCADA-systemen vallen niet altijd binnen de reikwijdte van dit beleid. U kunt kiezen voor één beleid voor alle systemen waarbij rekening wordt gehouden met de verschillen tussen de kantoor- en procesomgeving. U kunt ook kiezen voor twee aparte documenten. Een goed beleid draagt bij aan het treffen van de juiste beveiligingsmaatregelen tegen reële risico's.
   Referenties: ISO-2700x [1], hoofdstuk 2.1 van [2], hoofdstuk 4 van [22], hoofdstuk 4.2 van [5], ISA99/IEC62443 [23], hoofdstuk 2 van [24].

2. Het senior management heeft zijn commitment uitgesproken m.b.t. de beveiliging van ICS/SCADA-systemen en handelt hier ook naar.
   Cybersecurity is een gedeelde verantwoordelijkheid van alle medewerkers binnen een organisatie en in het bijzonder van leidinggevenden. Zorg voor heldere afspraken met het senior management over het belang van de beveiliging van ICS/SCADA-systemen, de inzet van de benodigde resources en het budget om maatregelen te treffen waar nodig.
   Referenties: hoofdstuk 4.2 van [5], hoofdstuk 1 van [24].

3. Risicomanagement wordt toegepast op alle bedrijfsprocessen, inclusief de voor de primaire processen verantwoordelijke ICS/SCADA-systemen. Incidentmanagement, inclusief managementrapportage, is ook ingericht voor de ICS/SCADA-systemen.
   Met risicomanagement kunt u het benodigde beveiligingsniveau vaststellen en daarbij passende maatregelen vaststellen.
   Referenties: hoofdstuk 2.12 en 2.18 van [2], [3], hoofdstuk 6.1 van [5], [16], [18], hoofdstuk 3 van [24].

Checklist organisatorische maatregelen (vervolg)

4. Periodiek vindt een EDP-audit plaats waarin ook de beveiliging van ICS/SCADA-systemen wordt beoordeeld.
   Het is raadzaam om naast de audit periodiek self-assessments en penetratietesten uit te (laten) voeren.
   Referenties: hoofdstuk 2.16 van [2], [4], [11], hoofdstuk 11 van [24].

5. Er worden beveiligingseisen gesteld die de totale cyclus van ontwikkeling, aanschaf, beheer, onderhoud en vervanging van ICS/SCADA-systemen (hard- en software) afdekken en toepassing van de eisen is gewaarborgd.
   Ook de werkzaamheden die derden uitvoeren en ingekochte producten en diensten moeten aan de beveiligingseisen voldoen. Het is noodzakelijk hiervoor bindende afspraken te maken.
   Referenties: deel 2-4 van [5], [6], [20], hoofdstuk 6 van [24].

6. Periodiek volgen alle medewerkers, ook de medewerkers die met ICS/SCADA-systemen werken, een security-awarenesstraining.
   De mens is een belangrijke schakel in de informatiebeveiliging. Zonder voldoende bewustwording kan elke (technische) maatregel falen. Toets periodiek het awarenessniveau van de medewerkers.
   Referenties: hoofdstuk 2.11 van [2], [10], [19], hoofdstuk 2, 7 en 15 van [24].

7. Wees helder over rollen, taken en verantwoordelijkheden. Maak een team verantwoordelijk voor de beveiliging van ICS/SCADA-systemen. Laat deze medewerkers periodiek aanvullende securitytrainingen volgen. Zorg ook voor betrokkenheid en ondersteuning van de IT-afdeling.
   Eigenaarschap van ICS/SCADA-security is belangrijk. Het moet helder zijn wie waarvoor verantwoordelijk is. Om dit eigenaarschap goed in te kunnen vullen, dienen medewerkers ook over de nodige kennis en vaardigheden beschikken.
   Referenties: hoofdstuk 4.2 van [5], hoofdstuk 2, 7 en 15 van [24].

Checklist technische en operationele maatregelen

1. De ICS/SCADA-systemen maken gebruik van een aparte netwerkinfrastructuur. Deze netwerkinfrastructuur is gescheiden van andere netwerken. De scheiding kan fysiek of logisch zijn ingericht.
   Door gebruik te maken van een aparte netwerkinfrastructuur wordt voorkomen dat (ver)storingen en beveiligingsincidenten in andere netwerken (bijvoorbeeld het standaard kantoornetwerk) direct invloed hebben op de ICS/SCADA-systemen. Wanneer netwerken niet van elkaar zijn gescheiden kan een kwetsbaarheid in het kantoornetwerk bovendien worden misbruikt om toegang te verkrijgen tot de ICS/SCADA-systemen.
   Referenties: [17], [23], hoofdstuk 8 van [24].

2. Beperk koppelingen van ICS/SCADA-systemen met internet en andere netwerken.
   Elke koppeling vormt een potentieel risico. Stel periodiek (minimaal één keer per jaar) een overzicht op van alle koppelingen van uw systemen met internet en andere netwerken. Voer een risicoanalyse uit voor deze koppelingen om de juiste maatregelen te kunnen bepalen. Maak gebruik van beveiligingsapparatuur zoals firewalls, proxyservers en datadiodes en een bijbehorend beleid.
   Er kan een valide reden voor een koppeling zijn, denk bijvoorbeeld aan snelle storingsanalyse, beheer of procesmonitoring. Laat informatie-uitwisseling tussen verschillende netwerken via een apart netwerksegment (DMZ) verlopen. Zorg ervoor dat toegang op afstand alleen plaatsvindt via een centrale beveiligde voorziening en gebruik hierbij tweefactorauthenticatie.
   Referenties: hoofdstuk 2.15 van [2], hoofdstuk 5.8 en 6.3 van [5], Configuring remote access [9], [12], [25].

3. Er is een wachtwoordbeleid opgesteld en er zijn maatregelen getroffen om dit beleid af te dwingen. Onderdeel van dit beleid zijn minimaal:
   - complexiteit van wachtwoorden;
   - wijzigingsfrequentie;
   - wijziging van default accounts en wachtwoorden, inclusief een waarborg voor het verwijderen van dergelijke accounts;
   - eisen ten aanzien van beheeraccounts.

   Wachtwoordbeleid is een groot aandachtspunt bij ICS/SCADA-systemen. Het is echter niet altijd mogelijk om gebruikersaccounts/wachtwoorden te gebruiken. In dergelijke gevallen zullen aanvullende maatregelen, zoals fysieke toegangsbeperkingen, noodzakelijk zijn.
   Referenties: hoofdstuk 2.15 van [2], hoofdstuk 6.3 van [5], hoofdstuk 4.2 van [7].

4. Er is een beleid voor het gebruik van (verwijderbare) media (zoals USB-sticks, harddisks en CD-roms) en er zijn technische maatregelen getroffen om dit beleid af te dwingen.
   Veel virus- en malwareinfecties op ICS/SCADA-systemen worden veroorzaakt door gebruik van besmette opslagmedia. Neem dit beleid expliciet mee in awarenesscampagnes.
   Referentie: hoofdstuk 2.13 van [2], hoofdstuk 6.2 van [5].

Checklist technische en operationele maatregelen (vervolg)

5. De ICS/SCADA-infrastructuren en -systemen zijn volgens principes van 'defense in depth' beveiligd:
   - Stel systemen zo min mogelijk bloot aan andere netwerkinfrastructuren.
   - Pas hardening toe: schakel overbodige functies en ongebruikte services uit, verwijder niet gebruikte of onnodige gebruikersaccounts en wijzig standaardwachtwoorden.
   - Zorg dat het toevoegen en wijzigen van systemen en configuraties een gedocumenteerd en gecontroleerd proces is.
   - Pas indien mogelijk antivirussoftware en whitelisting van applicaties toe.
   - Breng een scheiding aan tussen beheer- en gebruikersfuncties en het bijbehorende netwerkverkeer.

   Net als standaard ICT-applicaties zijn ook veel ICS/SCADA-applicaties gevoelig voor manipulatie van de invoer. Het hoofdstuk 'Uitvoeringsdomein Webapplicaties' van de ICT-Beveiligingsrichtlijnen voor webapplicaties – Verdieping geeft een uitgebreide beschrijving van deze problemen [8].
   Referenties: hoofdstuk 2.8 van [2], hoofdstuk 4 van [7], [13], hoofdstuk 8 van [24].

6. Richt patchmanagement in: definieer een patchbeleid en blijf op de hoogte van kwetsbaarheden, securitypatches en workarounds van al uw systeemcomponenten.
   Kwetsbaarheden in software zijn een belangrijke oorzaak van veel beveiligingsproblemen. Leveranciers van ICS/SCADA-systemen maken steeds meer gebruik van standaardsoftware, -systemen en -protocollen. Daarmee worden ook de bijbehorende beveiligingsproblemen geïntroduceerd. Standaard tooling en exploitkits zijn dan makkelijker toepasbaar. Het is daarom noodzakelijk dat alle gebruikte software up-to-date is.
   Onderhoud van systemen, inclusief securitypatches, kan onderdeel zijn van onderhoudscontracten. Het doorvoeren van securitypatches kan ook onderdeel zijn van releasemanagement van een bedrijf en dient daarnaast altijd in overleg met de systeemleverancier te gebeuren.
   Referenties: [14], hoofdstuk 14 van [24].

7. Er is een beleid voor het aansluiten van mobiele apparatuur, zoals laptops, tablets, smartphones, op de bedrijfsnetwerken en er zijn technische maatregelen getroffen om dit beleid af te dwingen.
   Besmette apparatuur die aangesloten wordt op de ICS/SCADA-netwerkinfrastructuur kan virus- en malwareinfecties veroorzaken. Veel leveranciers maken gebruik van laptops voor servicewerkzaamheden. Daarom is een totaalverbod in de praktijk niet altijd mogelijk. Zorg dan op zijn minst dat het aan te sluiten systeem altijd wordt gescand voordat het aangesloten wordt. U kunt ook overwegen de externe leverancier alleen gebruik te laten maken van laptops die onder beheer van uw eigen organisatie blijven (en deze laptops op locatie bewaren).
   Referentie: hoofdstuk 2.13 van [2].

8. Richt technische middelen in om aanvallen te detecteren. Onderdeel daarvan is een, bij voorkeur centrale, logging-faciliteit. Hierdoor is bij incidenten beter te achterhalen wat er heeft plaatsgevonden. Voer ook proactief controle uit op deze logging. Maak daarnaast gebruik van een Intrusion Detection Systeem (IDS) voor het detecteren van aanvallen.
   Ook in het geval van aangifte na een hackpoging is het hebben van goede logfiles een goed hulpmiddel. Vanwege het voorspelbare systeemgedrag van veel procesomgevingen kan een IDS goed worden gebruikt voor het detecteren van aanvallen.
   Referenties: hoofdstuk 2.16 van [2], [15], hoofdstuk 9 van [24].

9. Zorg voor passende fysieke toegangsbeveiliging tot systemen en locaties.
   Veel ICS/SCADA-systemen strekken zich uit over een groter gebied. Plaatselijk fysieke toegang tot een ICS/SCADA-systeem kan tot gevolg hebben dat meerdere of alle systemen in het ICS/SCADA-netwerk toegankelijk zijn. Ook hier geldt dat de zwakste schakel de sterkte van de beveiligingsketen bepaalt.
   Referentie: hoofdstuk 2.4 van [2], hoofdstuk 12 van [24].

10. Neem maatregelen om de integriteit van uw configuraties te kunnen garanderen.
    - Documenteer configuraties, instellingen en connecties en registreer aangebrachte wijzigingen.
    - Controleer periodiek de daadwerkelijke instellingen/configuraties met de documentatie en onderzoek eventuele verschillen.
    - Richt changemanagement. Controleer de integriteit van de software bij implementatie op operationele systemen, bijvoorbeeld door wijzigingen vooraf te testen in een testomgeving met simulatiemogelijkheden (FAT).
    - Zorg dat u zeker weet dat de configuratie die in de FAT getest (en akkoord bevonden) wordt, ook zo geïmplementeerd wordt in de productieomgeving (SAT).

    In veel configuraties van ICS/SCADA-systemen vindt geen authenticatie plaats voor het aanbrengen van systeemwijzigingen. Voorbeelden hiervan zijn mogelijkheden tot het downloaden van nieuwe software of firmware. De mogelijkheden om dit te beveiligen zijn sterk systeem- en configuratie-afhankelijk.
    Referenties: hoofdstuk 2.15 van [2], hoofdstuk 4.1 van [7], hoofdstuk 4 van [24].

Referentielijst

[1] ISO 27000-serie: NEN-ISO/IEC 27001 Information Security management systems. Meer informatie via www.nen.nl
[2] DHS, ICS-Cert: Catalog of Control Systems Security: Recommendations for Standards Developers
[3] DHS, ICS-Cert: Developing an Industrial Control Systems Cybersecurity Incident Response Capability
[4] DHS, ICS-Cert: Cyber Security Assessments of Industrial Control Systems
[5] National Institute of Standards and Technology (NIST): Guide to Industrial Control Systems (ICS) Security
[6] DHS, ICS-Cert: Cyber Security Procurement Language for Control Systems
[7] DHS, ICS-Cert: Common Cyber Security Vulnerabilities in Industrial Control Systems.
[8] NCSC.NL : ICT-Beveiligingsrichtlijnen voor webapplicaties
[9] DHS, ICS-Cert: Configuring and Managing Remote Access for Industrial Control Systems
[10] DHS, ICS-Cert: Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Systems Environments (draft)
[11] CPNI.UK Cyber security assessments of industrial control systems - A good practice guide
[12] US-Cert: Backdoors and Holes in Network Perimeters: A Case Study for Improving Your Control System Security
[13] DHS ICS-Cert: Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies
[14] DHS ICS-Cert: Recommended Practice for Patch Management of Control Systems
[15] DHS ICS-Cert: Creating Cyber Forensics Plans for Control Systems
[16] CPNI.UK : Good practice guide: 1 understand the business risk
[17] CPNI.UK : Good practice guide: 2 Implement secure architecture
[18] CPNI.UK : Good practice guide: 3 Establish response capabilities
[19] CPNI.UK : Good practice guide: 4 Improve awareness and skills
[20] CPNI.UK : Good practice guide: 5 Manage third party risk
[21] CPNI.UK : Good practice guide: 6 Engage projects
[22] CPNI.UK : Good practice guide: 7 Establish ongoing governance
[23] ISA99/IEC62443 : Standard for Industrial Automation and Control Systems Security
[24] Swedish Civil Contingencies Agency (MSB): Guide to Increased Security in Industrial Information and Control Systems
[25] NCSC Factsheet 2012-01 'Uw ICS/SCADA- en gebouwbeheersystemen online'

Uitgave van **Nationaal Cyber Security Centrum**
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
www.ncsc.nl | info@ncsc.nl | T 070-751 55 55 |
Publicatienr: FS-2012-02 1.2 | Aan deze informatie kunnen geen rechten worden ontleend.