Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Uw ICS/SCADA- en gebouwbeheersystemen online

Zorg voor een actueel overzicht en tref maatregelen

Factsheet FS-2012-01
versie 2.2 | 6 juni 2016

Kwaadwillenden en securityonderzoekers tonen interesse in de (on)veiligheid van industriële controlesystemen. Hierbij wordt niet alleen gekeken naar 'traditionele' ICS/SCADA-systemen, maar ook naar gebouwbeheersystemen (o.a. HVAC en CCTV). Vooral deze laatste blijken vaak direct vanaf internet bereikbaar te zijn. Industriële controlesystemen vallen niet altijd binnen de reikwijdte van het securitybeleid. Veel organisaties zijn zich niet bewust van de risico's die dit met zich meebrengt. Daarnaast ontbreekt bij veel organisaties een actueel overzicht van alle systemen die met internet zijn verbonden. Hierdoor wordt niet altijd een gedegen inschatting van de risico's gemaakt en worden niet altijd de juiste maatregelen getroffen.

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.

De belangrijkste feiten

- Voor het grote publiek is een ISC/SCADA-systeem een zeer breed begrip. Ook camerabewakingssystemen (CCTV), klimaatregelsystemen (HVAC) en andere gebouwbeheer-systemen worden vaak onder deze noemer geschaard. Bij ca. 80% van de meldingen die het NCSC in het verleden heeft ontvangen inzake 'kwetsbare ICS/SCADA-systemen', bleek het te gaan om systemen in deze categorieën.
- Veel organisaties weten niet welke van hun systemen via internet bereikbaar zijn. Een deel van die onwetendheid komt omdat systemen zijn aangelegd en/of worden beheerd door derden, waarmee geen of onvoldoende afspraken zijn gemaakt over beveiliging.
- Er komt steeds meer tooling en kennis beschikbaar die het identificeren van op het internet aangesloten systemen en het zoeken op kwetsbaarheden in ICS/SCADA-systemen eenvoudiger maakt.
- Wanneer de aan internet gekoppelde ICS/SCADA-systemen onvoldoende zijn beveiligd, kunnen deze op afstand worden gemanipuleerd en/of worden overgenomen. Hiermee kan fysieke schade worden aangericht. Afhankelijk van de aard van de systemen kan dit grote gevolgen hebben voor een organisatie en haar klanten.
- Geregeld maken kwaadwillenden en securityonderzoekers hun bevindingen publiek. Organisaties kunnen hierdoor te maken krijgen met negatieve publiciteit en imagoschade. Daarnaast is het mogelijk dat de berichtgeving nieuwsgierige personen aantrekt die proberen toegang tot de systemen te verkrijgen.

Achtergrond

ICS/SCADA-systemen worden binnen vitale en (andere) industriële sectoren gebruikt voor de automatische monitoring en besturing van fysieke processen. Voor de productie, het transport en de distributie binnen onze energie- en drinkwatervoorziening wordt gebruikgemaakt van ICS/SCADA-systemen. Ook de productieprocessen van raffinaderijen, de chemische, voedingsmiddelen- en farmaceutische industrie worden (grotendeels) aangestuurd door ICS/SCADA-systemen. Daarnaast worden camerabewakingssystemen (CCTV), klimaatregelsystemen (HVAC) en andere gebouwbeheer-systemen vaak onder de noemer ICS/SCADA geschaard.

In het verleden communiceerden ICS/SCADA-systemen rechtstreeks met elkaar in een volledig gesloten netwerk en waren de systemen niet gekoppeld aan internet of andere netwerken. Tegenwoordig zijn ICS/SCADA-systemen echter vaak gekoppeld aan de kantoorautomatisering van het bedrijf en ook toegankelijk via internet.

Wanneer ICS/SCADA-systemen met internet worden verbonden, bijvoorbeeld om beheer op afstand mogelijk te maken, worden niet altijd de juiste beveiligingsmaatregelen getroffen. De beveiliging van ICS/SCADA-systemen maakt niet altijd onderdeel uit van securitybeleid. Men is zich enerzijds onvoldoende bewust van de risico's die internetkoppeling met zich meebrengt. Anderzijds ontbreekt bij veel organisaties een actueel overzicht van alle systemen die met internet verbonden zijn. Het maken van een gedegen inschatting van de risico's en het treffen van de juiste maatregelen is dan niet mogelijk.

Het vinden van online ICS/SCADA-systemen

De beschikbaarheid van laagdrempelige, en over het algemeen ook gratis, zoekmachines en andere hulpmiddelen reduceert de benodigde tijd en kennis om aan internet gekoppelde systemen te identificeren. Volgens berichtgeving in de media zou toegang tot ICS/SCADA-systemen ook worden verkocht op ondergrondse fora.[1]

SHODAN is een zoekmachine die vaak gebruik wordt om mogelijk kwetsbare systemen te vinden. Bekende netwerkscanners als Nmap[2] of Nessus[3] kunnen ook worden gebruikt. Daarnaast biedt de vrij verkrijgbare tool Metasploit[4] mogelijkheden om gericht te zoeken op ICS/SCADA-gerelateerde kwetsbaarheden in systemen.

Wat kan er gebeuren?

In 2014 vond een succesvolle hack plaats bij een Duitse staalfabriek. De aanvallers wisten door middel van spearphishing toegang te verkrijgen tot de ICS/SCADA-systemen. Zij zorgden er vervolgens voor dat controlecomponenten van de fabriek niet meer werkten, waardoor een hoogoven niet gecontroleerd kon worden uitgeschakeld. Dit leidde tot schade aan de apparatuur.[5]

Wanneer uw aan internet gekoppelde ICS/SCADA-systemen onvoldoende zijn beveiligd, kunnen deze op afstand worden gemanipuleerd en worden overgenomen. Als de centrale bediening direct via internet beschikbaar is, is er geen specifieke kennis nodig. Digitaal vandalisme, zoals willekeurig systemen of programma's aan- of uitzetten, is dan zeer eenvoudig. Ook kan toegang worden verkregen tot (proces)informatie. Hoe ernstig de gevolgen hiervan zijn wordt mede bepaald door de aard van het proces en of er aanvullende beveiliging aanwezig is.

Geregeld maken kwaadwillenden en securityonderzoekers hun bevindingen publiek via sociale media zoals Twitter, op openbare websites zoals Pastebin of door journalisten te informeren. Dit kan leiden tot negatieve publiciteit en imagoschade voor de betreffende organisatie. Belangrijker is echter dat de kans op misbruik van de openbaargemaakte kwetsbaarheden toeneemt.

Wat kunt u doen?

Op de volgende pagina vindt u een checklist met maatregelen. Zorg er in de eerste plaats voor dat u een actueel overzicht heeft van alle systemen in uw organisatie die met internet (en het interne netwerk) verbonden zijn. Stel bij elk systeem de vraag of toegang via internet noodzakelijk is. Kijk niet alleen naar 'wel of geen internetconnectie' maar ook naar welke poorten en services actief zijn.

Controleer de juistheid van het overzicht regelmatig, scan periodiek welke systemen (in uw publieke IP-range) op internet te vinden zijn, en vergelijk dit met het overzicht dat u zelf bijhoudt. U kunt dit zelf nagaan met behulp van de eerdergenoemde zoekmachines en tools. U kunt dit ook onderdeel laten uitmaken van een periodieke penetratietest.

Het NCSC adviseert nadrukkelijk om ICS/SCADA-systemen of elke andere vorm van procesmonitoring en/of –besturing niet

Zoeken met SHODAN

SHODAN is een zoekmachine, maar wel een speciale. Daar waar andere zoekmachines indexeren op basis van de inhoud van de webpagina, indexeert SHODAN op basis van de banner-informatie van systemen. Als u weet welke zoektermen u moet kiezen, zijn mogelijk kwetsbare systemen snel te vinden. SHODAN biedt bovendien een aantal filteropties (bijvoorbeeld op land, IP-adres, poortnummer et cetera) om nog gerichter te kunnen zoeken.

SHODAN, te vinden via www.shodan.io, biedt gratis en zonder registratie beperkte zoekmogelijkheden. Wanneer u zich registreert krijgt u extra zoekmogelijkheden en tegen betaling zijn nog geavanceerdere opties mogelijk. Als u SHODAN gebruikt met de filteroptie op IP-adressen van uw eigen organisatie, krijgt u snel een overzicht welke systemen van u online te vinden zijn. Let erop dat zoektermen worden bewaard waardoor u hoog in de lijst populaire zoektermen kunt voorkomen. De vindbaarheid door zoekmachines kunt u verkleinen door, waar mogelijk, de banner-informatie die uw systemen vrijgeven te beperken.

SHODAN wordt nog steeds uitgebreid. Inmiddels worden meerdere specifieke poorten en protocollen voor ICS/SCADA-systemen geïndexeerd.

[1] http://www.infosecisland.com/blogview/24608-SCADA-Systems-Offered-for-Sale-in-the-Underground-Economy.html
[2] www.nmap.org
[3] www.tenable.com
[4] www.metasploit.com
[5] Zie het jaarrapport 2014 van het Duitse Federaal Bureau voor Informatiebeveiliging (BSI): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lageberichte2014.pdf?__blob=publicationFile

met internet te verbinden. Indien er toch toegang van buiten noodzakelijk is, zorg dan dat dit veilig ingericht wordt. Regel dit bij voorkeur via een daarvoor ingerichte VPN-verbinding.[6]

Wees erop bedacht dat er ook mogelijkheden voor toegang op afstand kunnen zijn die geen gebruik maken van de IP-range van uw organisatie. Denk aan leveranciers en gebruikers die zelf in- en uitbelverbindingen, wifi-accesspoints of ADSL-lijnen aanleggen voor aanleg, beheer en/of onderhoud van hun producten en diensten. Maak ook met externe leveranciers afspraken over de beveiligingseisen die aan de gebruikte systemen gesteld worden.

Checklist beveiliging online ICS/SCADA-systemen

1. Stel een overzicht op van alle systemen en netwerkkoppelpunten in uw organisatie die met internet verbonden zijn.
   Het gaat hierbij om alle systemen die vanaf internet te benaderen zijn. Vraag ook bij uw leveranciers en onderhoudspartijen welke koppelingen ze in gebruik hebben. Bedenk dat als een leverancier service op afstand verleent, er een koppeling aanwezig moet zijn. Vergeet daarnaast ook de ouderwetse inbelverbinding of GPRS-modems niet. Doe ook navraag bij uw inkoopafdeling, zij kunnen u wellicht helpen met het inventariseren van de afspraken met leveranciers.

2. Stel bij elk systeem de vraag of toegang via internet noodzakelijk is. Maak een inschatting van de risico's van deze koppeling, en definieer passende beveiligingsmaatregelen.
   Kijk niet alleen naar de vraag of er een koppeling met internet is, maar ook naar welke poorten en services actief zijn. Regel toegang bij voorkeur via een daarvoor ingerichte VPN-verbinding waarmee de verbinding alleen op uw initiatief geactiveerd kan worden.

3. Toets uw overzicht aan de praktijk. Dit kunt u bijvoorbeeld doen met behulp van zoekmachine SHODAN of diverse scantools.
   In de praktijk blijken er vaak meer koppelingen te zijn dan men vooraf dacht. Toetsing is daarom noodzakelijk. Maak deze toetsing een onderdeel van uw periodieke penetratietest. Onderzoek de filterregels van uw firewalls en andere beveiligingsapparatuur. Kijk naar de van buiten naar binnen toegestane verkeerstromen en vergelijk deze met uw overzicht.

4. Bepaal voor elk koppelpunt of de beveiliging past bij de risico's voor achterliggende systemen in geval van ongeautoriseerde toegang en bediening.
   Maak bij voorkeur gebruik van beveiligingsapparatuur zoals firewalls en proxyservers voor uw koppelpunten. Vertrouw niet op de fabrieksinstellingen van uw apparatuur. Regelmatig blijkt dat deze problemen bevatten (zoals standaardwachtwoorden).

5. Maak duidelijke afspraken met leveranciers over toegang op afstand.
   Denk hierbij aan afspraken over het soort gebruik (welke handelingen mogen er via de koppeling uitgevoerd worden), het beveiligingsniveau en het rapporteren van incidenten.

6. Monitor de beveiliging van uw koppelpunten.
   Log de toegang tot uw koppelpunten, en kijk deze logs na op ongewone activiteiten. Dit zijn bijvoorbeeld veel mislukte inlogpogingen, of het inloggen op ongewone tijdstippen. Zorg dat uw software en systemen altijd up-to-date zijn.

7. Doorloop ook de uitgebreide 'Checklist beveiliging van ICS/SCADA-systemen' van het NCSC.[7]
   De bereikbaarheid vanaf internet is niet het enige potentiële beveiligingsprobleem voor ICS/SCADA-systemen. De checklist helpt u om te bepalen of de ICS/SCADA-systemen voldoende beveiligd zijn op basis van maatregelen die als good practice worden beschouwd.

[6] Meer informatie over het veilig inrichten van toegang op afstand vindt u bijvoorbeeld op de website van CPNI.UK: http://www.cpni.gov.uk/documents/publications/2011/2011022-remote_access_for_ics_gpg.pdf?epslanguage=en-gb

[7] https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/checklist-beveiliging-van-ics-scada-systemen.html

Responsible disclosure

Het is belangrijk dat kwetsbaarheden op verantwoorde wijze bij uw organisatie kunnen worden gemeld en dat deze correct worden afgehandeld. Richt een beleid in voor responsible disclosure en maak dit beleid publiekelijk kenbaar, zodat melders weten waar ze terechtkunnen met hun ontdekkingen.[8]

Wat als het toch misgaat?

U hebt al het mogelijke gedaan om uw systemen te beveiligen, maar toch gaat het mis. Hoe kunt u zich daarop voorbereiden?

- Tref voorbereidingen voor mogelijke persvragen of meldingen van onderzoekers. Ook als systemen bewust met internet verbonden zijn, kan men securitygerelateerde vragen stellen. Informeer voorlichters en telefonisten daarom hoe om te gaan met persvragen of meldingen.
- Zorg dat de WHOIS-contactinformatie over de bij u gebruikte IP-range op orde is. U bent zo voor eventuele melders makkelijker te vinden.[9]

Tot slot

Er zijn veel goede Engelstalige publicaties beschikbaar over het beveiligen van ICS/SCADA-systemen. Aan te bevelen zijn de volgende websites en publicaties:

- Control Systems Security Program (CSSP) van het Amerikaanse DHS en ICS-CERT:
https://ics-cert.us-cert.gov/
- Centre for the Protection of National Infrastructure (UK):
http://www.cpni.gov.uk/advice/cyber/Security-for-Industrial-Control-Systems/
- International Society of Automation (ISA):
https://www.isa.org/isa99/
- National Institute of Standards and Technology (NIST):
http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
- Swedish Civil Contingencies Agency (MSB):
https://www.msb.se/en/Tools/News/Guide-to-Increased-Security-in-Industrial-Information-and-Control-Systems/

[8] Meer informatie over het opstellen van een beleid voor responsible disclosure vindt u in de Leidraad Responsible Disclosure van het NCSC:
https://www.ncsc.nl/actueel/Responsible+Disclosure+Leidraad

[9] Houd er rekening mee dat u via de WHOIS-database niet alleen voor melders, maar ook voor eventuele kwaadwillenden makkelijker vindbaar bent. Doorloop deze checklist daarom periodiek om te toetsen of de beveiliging van uw ICS/SCADA-systemen nog steeds op orde is.

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-2012-01 2.2 | Aan deze informatie kunnen geen rechten worden ontleend.