Maak werk van cyberdreigingen voor SCADA- en IoT-systemen

Whitepaper

Tim Kenter & Hans Reterink | 4 maart 2019

Toegangspoortjes, beveiligingscamera's, maar ook verwarmingsketels en bruggen beschikken allemaal over technische besturingssystemen, zogeheten SCADA-systemen. Ze zorgen er bijvoorbeeld voor dat op afstand de toegangspoort open gaat, de verwarming wordt bediend of data van patiënten wordt gemonitord. Door de opkomst van Internet of Things (IoT) – systemen die via internet met elkaar verbonden zijn – neemt het aantal SCADA-systemen in de samenleving flink toe. Dit levert veel gemak op. Maar vaak wordt niet onderkend dat deze systemen, net zoals pc's, gehackt kunnen worden. En dus is bij de opzet van zulke systemen cyberbeveiliging meestal niet meegenomen. Ook wanneer later maatregelen worden genomen, zijn de systemen nooit echt helemaal veilig. Daar komt bij dat de ontwikkeling van wettelijke normen achterloopt, terwijl cyberbeveiliging al vanaf ontwerp en aankoop onderdeel moet zijn van de opzet. In deze whitepaper geven we u enkele inzichten en handvatten voor het omgaan met mogelijke dreigingen voor uw SCADA- en IoT-omgevingen.

Wat zijn technische systemen?

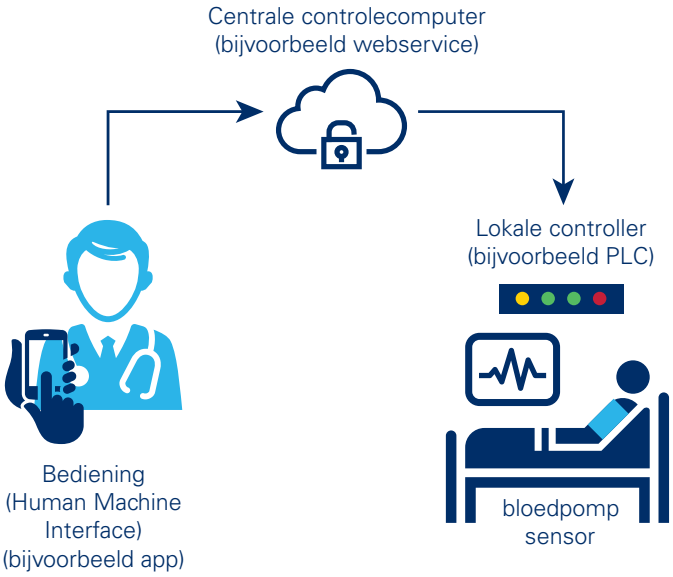
Technische systemen worden vaak aangeduid met SCADA (Supervisory Control And Data Acquisition), ICS (Industrial Control Systems) of IA (Industriële Automatisering). Deze termen hebben een iets andere lading, maar worden ook vaak door elkaar heen gebruikt. SCADA-systemen bieden gebruikers veel gemak doordat daarmee apparaten op afstand kunnen worden bestuurd. Alle besturingsinformatie komt samen in één systeem. Dit geeft een overzichtelijk beeld van het reilen en zeilen van alle onderdelen. De apparaten worden aangestuurd door zelfstandig werkende PLC's, zodat de besturing ook doorgaat als de centrale computer korte tijd niet bereikbaar is.

Met de komst van Internet of Things (IoT) is SCADA-besturing ook de huiskamer binnengekomen. IoT biedt, net als SCADA, mogelijkheden om fysieke objecten die zijn uitgerust met sensoren op afstand aan te sturen. Verlichting, centrale verwarming, muziekinstallaties en ijskasten kunnen door externe controlecomputers (bijvoorbeeld een app op een smartphone) via een internetverbinding worden bestuurd. Deze ontwikkelingen zorgen voor een kostenreductie en vergroten het gebruikersgemak enorm.

Berenschot

Een ICS/SCADA-systeem bestaat meestal uit de volgende componenten:

- Bediening (Human Machine Interface): de app of webpagina waarop het te besturen proces grafisch is weergegeven en de besturing kan worden ingeregeld en overgenomen.
- Centrale controlecomputer: een centrale server in een fabriek of een webservice op internet.
- Lokale controller (in fabrieken vaak een PLC (Programmable Logic Controller)): bestuurt een apparaat op basis van sensorwaarden. In een besturingstabel (een stack) staat welke acties moeten worden uitgevoerd bij welke sensorwaarden. Bijvoorbeeld: onder de 50°C hoeft de ventilator niet te draaien, bij 50-70°C met 100 toeren, en boven de 70°C met 800 toeren.
- Sensor: meet meestal een eigenschap die onder controle gehouden moet worden, zoals temperatuur, druk, snelheid, etc.
- Apparaat dat bestuurd moet worden: bijvoorbeeld de brander van een cv-ketel, een motortje in een camera of een medicijnenpompje.



Veiligheidsrisico's van SCADA en IoT

Hoewel SCADA en IoT het gebruikersgemak vergroten, nemen ook de veiligheidsrisico's toe. Grote SCADA-systemen zijn namelijk oorspronkelijk ontworpen als afgesloten omgevingen; veel van de huidige SCADA-systemen zijn bovendien gebouwd vóór de komst van internet. Daarnaast draaien de systemen nog regelmatig op niet bijgewerkte en verouderde besturingssystemen met verschillende veiligheidslekken en zijn de verbindingen met PLC's vaak niet beveiligd. Ook zijn software updates mogelijk zonder inlogprocedures of is het wachtwoord vanaf fabriek identiek voor alle apparaten van een bepaald type. Hoewel dit het werken met SCADA vergemakkelijkt, vergroot het ook de onveiligheid.

Doordat SCADA-systemen in het begin niet gekoppeld waren aan internet (de zogenoemde air gap) is er een vals gevoel van veiligheid ontstaan. In de loop der tijd zijn de SCADA-systemen in fabrieken gekoppeld aan kantoorautomatisering (voor bijvoorbeeld rapportages) met de bijbehorende internetverbinding. Zo werd de air gap doorbroken en werden de onbeveiligde SCADA-systemen blootgesteld aan toegang vanuit internet[1]. Deze zijn op te sporen met specifieke zoekmachines zoals SHODAN[2]. Onderzoek heeft laten zien dat in meer dan 50% van de onderzochte systemen de air gap niet blijkt te bestaan[3].

SCADA- en IoT-malware

Buiten het feit dat SCADA-systemen vaak niet gebouwd zijn om goede beveiliging te waarborgen en daarmee de air gap verdwijnt, hebben ook krachtige malware-varianten zich in hoog tempo ontwikkeld. SCADA-systemen zijn steeds vaker doelwit, nu malware-varianten steeds beter zicht krijgen op de kwetsbaarheden van deze systemen. Kwaadwillende statelijke actoren vinden dit interessant: SCADA-systemen bevinden zich namelijk vaak in vitale sectoren bij het beheren van cruciale processen. Wanneer deze actoren toegang krijgen tot dergelijke sectoren, kunnen zij maatschappelijke processen platleggen. Zo voerde de malware-variant Crashoverride in 2016 een zeer geavanceerde aanval uit waardoor het elektriciteitsnetwerk in Oekraïne voor langere tijd was uitgeschakeld.

Ook IoT-omgevingen zijn niet veilig. De Mirai-malware bijvoorbeeld nestelt zich in slecht beveiligde IoT-devices zoals IP-camera's door gebruik te maken van standaard wachtwoorden van leveranciers. Daarna gaat de malware op zoek naar andere IoT-devices die het kan besmetten. Als een device is besmet, wordt de informatie ervan verstuurd naar verzamelservers op internet. Zo wordt een zogenaamd botnet met tientallen miljoenen apparaten (bots) gecreëerd. Deze botnets worden vervolgens gebruikt om DDoS-aanvallen op websites uit te voeren. Door het grote aantal besmette devices hebben sommige botnets een hoge slagkracht. De eigenaar merkt daar meestal niet zoveel van, hooguit dat het IoT-device soms langzamer werkt dan normaal en veel internetverkeer veroorzaakt.

1 https://www.securityweek.com/air-gap-or-not-why-icsscada-networks-are-risk
2 https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/factsheets/beveiligingsrisicos/1/Uw%2BICS%2BSCADA%2B%2Ben%2Bgebouwbeheersystemen%2Bonline.pdf
3 https://www.tofinosecurity.com/blog/1-ics-and-scada-security-myth-protection-air-gap

Normenkader

Om vitale processen te beschermen, zijn verschillende wetten en normen opgesteld. Zo zijn er internationaal verschillende normenkaders voor het gebruik van SCADA-systemen. Denk aan de internationale standaarden ISA-99 en ISA-112, maar ook de algemene informatiebeveiligingsnormen ISO 27001 en ISO 27002, de Amerikaanse norm NIST 800-82 en de Europese handreikingen van ENISA bieden handvatten voor de beveiliging van SCADA- systemen[4],[5],[6]. Een actueel en coherent normenkader in de Nederlandse context ontbreekt echter nog. Er bestaan weliswaar normenkaders voor het Rijk (BIR), gemeenten (BIG) en waterschappen (BIWA), maar daarin zijn geen specifieke normen voor concrete beveiliging van SCADA-systemen opgenomen. De BIR en BIG kunnen wel een basis bieden voor algemene informatiebeveiliging. In 2019 zullen deze normenkaders worden opgevolgd door de Baseline Informatiebeveiliging Overheid (BIO), waarin wel rekening gehouden wordt met statelijke actoren in het hoogste BasisBeveiligingsNiveau 3. De BIO is gebaseerd op de norm ISO 27002 en koppelt verantwoordelijken aan de 114 beheersmaatregelen van deze norm. Deze richt zich vooral op processen, verantwoordelijkheden en bescherming van informatie. Er is geen specifieke aandacht voor SCADA-systemen en de risico's die deze met zich meebrengen: risico's in de 'echte' fysieke wereld waar juistheid en beschikbaarheid van stuurinformatie veel belangrijker zijn.

In enkele specifieke Nederlandse normen is SCADA wel als concept meegenomen, zoals de BIWA. De BIWA stelt dat procesautomatisering, waaronder ICS/SCADA-systemen, ondersteunend is aan nagenoeg alle beveiligingsprocessen. "De eisen die aan ICT-voorzieningen gesteld worden, zijn hierdoor zeer ingrijpend en bepalen voor een significant deel de inrichting van het ICT-landschap."[7]. Ook het Nationaal Cyber Security Centrum (NCSC) heeft specifiek aandacht besteed aan beveiligingsmaatregelen voor SCADA-systemen.

Zo stelde het NCSC in 2015 de Checklist beveiliging van ICS/SCADA-systemen: Tref organisatorische en technische maatregelen op[8]. Dit is echter geen verplichte norm.

Kortom, er bestaan maar zeer beperkt dwingende normen voor beveiliging van SCADA-systemen tegen cyberdreigingen. De internationale normen en Nederlandse checklists zijn natuurlijk nuttig, maar toepassing in de praktijk is afhankelijk van inzicht en op vrijwillige basis.

Beveiliging van SCADA- en IoT-systemen

De literatuur noemt drie verschillende kwaliteitsaspecten waar rekening mee gehouden dient te worden om informatiesystemen te beveiligen: beschikbaarheid, integriteit en vertrouwelijkheid (Confidentiality, Integrity en Availability (CIA). De elementen van de CIA-driehoek zijn ontwikkeld om het beleid rondom technische veiligheid in een omgeving te sturen[9]. Voor SCADA- en IoT-systemen geldt dat vooral integriteit en beschikbaarheid van belang zijn om veiligheid te garanderen. Wanneer metingen uit uw systemen niet overeenkomen met de werkelijkheid, kan de sturing van het gehele proces worden veranderd, gebaseerd op incorrecte metingen. Daarnaast dienen uw SCADA-systemen altijd beschikbaar te zijn. Deze systemen sturen namelijk centrale bedrijfsprocessen aan in uw organisatie. Vertrouwelijkheid geldt niet of nauwelijks voor SCADA en IoT, maar is wel een cruciaal onderdeel voor andere IT-systemen waarin veel overheidsinformatie, persoonsgegevens en bedrijfsgegevens worden verwerkt.

4 https://www.isa.org/isa99/
5 https://dutchitchannel.nl/535307/top-tips-om-het-meeste-uit-een-scada-beveiliging-te-halen.html
6 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
7 https://www.uvw.nl/wp-content/uploads/2013/10/Baseline-Informatiebeveiliging-waterschappen-2013.pdf
8 https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/factsheets/checklist-beveiliging-van-ics-scada-systemen/1/FS2012%2B02%2BChecklist%2Bbeveiliging%2Bvan%2BICS%2BSCADA%2Bsystemen.pdf
9 https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Om tot een goede beveiliging van SCADA- en IoT-systemen te komen, zijn drie zaken belangrijk: wettelijke kaders, awareness en organisatie.

Wettelijke kaders

De beveiliging van SCADA- en IoT-systemen moet worden voorzien van wettelijke kaders waarin een aantal zaken specifiek worden benoemd. Goede encryptie van netwerkverkeer, sterke passwords en solide updateprocedures zouden minimaal verplicht moeten zijn.

Awareness

Daarnaast moeten de betrokken medewerkers bekend zijn met mogelijke kwetsbaarheden en daarnaar handelen. Dat kan ook inhouden dat zij bedacht zijn op een goede scheiding van de kantoorautomatisering (KA) en industriële automatisering (IA, SCADA).

Organisatie

Ook dient een organisatie te worden ingericht om zowel preventief als in de respons kwetsbaarheden te identificeren, de juiste maatregelen te nemen en adequaat te kunnen reageren als er toch een cyberaanval plaatsvindt. Een goed veiligheids- en compliance beleid is van belang om het handelen van werkgever en werknemers duidelijk te structureren binnen de organisatie. Een onderdeel van het beleid is training en oefening; die zorgen voor vaardigheden en onderling vertrouwen dat nodig is wanneer er echt een cyberaanval plaatsvindt.

Conclusie

Van waterkeringen voor droge voeten tot aan de verwarmingsketel in huis, SCADA-systemen bevinden zich overal. Met de komst van nieuwe ontwikkelingen zoals IoT komen SCADA-systemen letterlijk overal voor. Ze vergroten het gemak voor iedereen, maar ook de digitale kwetsbaarheden. Daarom is het nodig om zowel wettelijke normen aan te passen als awareness bij individuele personen en organisaties te vergroten om dit aspect mee te nemen in de aankoop en het ontwerp van systemen. Richt uw organisatie zo in dat de juiste maatregelen worden genomen wanneer een cyberincident plaatsvindt. Ieder op zijn eigen niveau: bij de aanschaf van een medicijnenpomp tot aan de encryptie van communicatieprotocollen in de fabriek en het ontwerpen van een cyberweerbare organisatie.

Tim Kenter en Hans Reterink zijn adviseur bij Berenschot

Berenschot Groep B.V.
Europalaan 40, 3526 KS Utrecht
Postbus 8039, 3503 RA Utrecht
030 2 916 916
www.berenschot.nl
/berenschot