ONBEWUST ONVEILIG

Eric Luiijf is principal consultant bescherming vitale infrastructuur bij TNO en is als expert beveiliging procescontrolesystemen en Smart Grids verbonden aan het Nederlandse Centre for Protection of National Infrastructure (CPNI.NL). Eric is bereikbaar via eric.luiijf@tno.nl en eric.luiijf@cpni.nl

Uw organisatie of bedrijf heeft een risicoanalyse van de eigen ICT-faciliteiten en -diensten uitgevoerd, informatiebeveiligingsmaatregelen getroffen en houdt nieuwe dreigingen in de gaten. U denkt het ICT-risico volledig te beheersen. De kans is dan groot dat uw organisatie of bedrijf, net zoals zo vele andere organisaties en bedrijven, onbewust onveilig is. Dit artikel gaat in op enkele recente incidenten en de onderliggende oorzaken. Een gedegen oplossing vereist de samenwerking van de hele keten van aanbieders, opdrachtgevers, inkopers en opleidingen.

U bent verantwoordelijk voor de informatiebeveiliging in organisatie of bedrijf. Na een risicoanalyse, het treffen van maatregelen en het continu in de gaten houden van nieuwe dreigingen bent u in een beheerste fase terecht gekomen. Bent u niet iets vergeten?
U bent facilitair manager of hoofd technische dienst. Om de haverklap moest u vroeger 's nachts de regenjas over de pyjama aan trekken om te reageren op een storingsmelding via de semafoon. Tegenwoordig hoeft u alleen de tablet aan te zetten en het reservecircuit in te schakelen.
U bent onderhoudsmonteur van een bedrijf in luchtbehandelingen of gebouwbeheersing. Vroeger reed u heel Nederland en Vlaanderen af om diep de kelders in te duiken van organisaties en bedrijven. Nu, telewerkend, controleren u en uw collega's de werking van de systemen. Volgens afspraak is het wachtwoord NL_organisatie resp. BE_organisatie. De klanten zijn blij, de onderhoudskosten zijn door onderhoud op afstand met 30% gedaald.

Monitoring en besturing van steeds meer technische apparatuur, zowel lokaal als op afstand, gaat met computers, de zogenaamde procescontrolesystemen. Iedereen denkt dan aan de besturingssystemen van onze vitale sectoren zoals onze energie- en drinkwatervoorzieningen, wissels en seinen van trein en metro, raffinaderijen, containeroverslag, bagagebanden en afvulinstallaties van zuivelproducten. Dergelijke procescontrolesystemen in vitale infrastructuren en andere sectoren in binnen- en buitenland zijn in de afgelopen jaren ten prooi gevallen aan hackers en malware (virussen, wormen en Trojans). Incidenten die in de media terecht zijn gekomen omvatten nucleaire centrales, elektriciteitsnetwerken, gas- en oliewinning, trein- en tramwissels, chemische fabrieken en havensystemen. De publiek gemaakte incidenten vormen slechts een klein topje van de ijsberg.

Minder gauw wordt gedacht aan besturingssystemen van riolering, straatverlichting, pomp-, sluis- en brugbedieningen, gebouwbeheersing, luchtbehandeling, liften en toegangsbeveiligingssystemen. Geheel buiten de ICT-afdeling om, wordt de bediening van deze apparatuur door een installatiebedrijf gekoppeld met publieke netwerken zoals het internet. Dat geeft de mogelijkheid van bediening op afstand en/of "onderhoud of afstand". Onderhoudskosten worden zo aanzienlijk gedrukt en het aantal manuren om monteurs te begeleiden is ook lager. Bij oplevering of derde partij onderhoud worden eenvoudige wachtwoorden gebruikt.

> De bediening van deze apparatuur wordt door een installatiebedrijf gekoppeld met het internet

Niemand in de hele keten van fabrikant tot eindgebruiker maakt zich druk om beveiliging: de hele keten is onbewust onveilig.

Recente incidenten laten zien dat systeemeigenaren als gemeenten, organisaties en bedrijven geen flauw benul hebben van het risico. De verantwoordelijkheid hiervoor ligt op papier bij de systeemeigenaar. Echter inkopers, fabrikanten, systeemleveranciers, systeemintegrators, installatie- en onderhoudsbedrijven en opleidingen treffen ook blaam dat de informatiebeveiliging onvoldoende geborgd is. Wat incidenten steeds zichtbaarder maken is dat, bij gebrek aan kennis en beveiligingsbewustzijn, de bediening van vitale fysieke processen zonder na te denken over enige vorm van informatiebeveiliging gekoppeld wordt met publieke telecommunicatienetwerken zoals mobiele netwerken of het internet. Het grootste probleem ligt bij de verantwoordelijken voor het proces die denken aan de meest efficiënte en gebruiksvriendelijke besturing van de processen als airconditioning, riolering, straatverlichting zonder zich ook maar een moment af te vragen of het wel veilig is. Dit artikel legt uit wat er in Nederland al aan de beveiliging van procescontrolesystemen gebeurt.

Daarna wordt aangegeven waar de kern van het probleem zit en hoe dit aangepakt kan worden.

Incidenten

Op 14 februari jongstleden liet het TV-programma Een Vandaag zien dat de verwarming in een pand van het Leger des Heils vanaf het internet was te regelen [1]. De toegang was simpel. Er was geen wachtwoord nodig. Ook technische systemen van gemeenten zijn gekoppeld aan het Internet. Systemen van de Gemeente Veere bleken voorzien te zijn van het wachtwoord Veere. Dat kwam prominent in beeld omdat het twee weken en een aantal telefoontjes duurde voordat de installateur/externe onderhoudspartij aangaf actie te gaan nemen. De burgemeester vertelde dat de gemeente uiteindelijk "de stekker uit het systeem getrokken had". Niet direct in beeld waren de bediensystemen bij een aantal andere gemeenten die met eenzelfde 'gemeentewachtwoord' bloot aan het internet aangetroffen zijn. Ook de pompen van een zwemparadijs waren via het internet te manipuleren [9].

Nederlandse aanpak

Dat informatiebeveiligingsproblemen met procescontrolesystemen zich in steeds sterkere mate voor zullen doen, is iets waar deskundigen al tien jaar voor waarschuwen. Begin 2006 schreven TNO/KEMA een rapport voor de overheid over de organisatorische en technische aspecten van de onveiligheid van SCADA-systemen [2]. Sindsdien wordt er hard gewerkt aan het nog strakker op orde brengen van de beveiliging van de procescontrolesystemen in onze vitale sectoren. Dit binnen het thematische kader van het Informatieknooppunt Cybercrime van het Nederlandse Centre for Protection of the National Infrastructure (CPNI.NL). Een voorbeeld hiervan is de start van het programma 'Nationale Roadmap voor veilige procescontrolesystemen', waaronder diverse activiteiten zijn en worden ontplooid.

De verwarming in een pand van het Leger des Heils was te regelen vanaf het internet

Naast benchmarks in de drinkwater- en energiesectoren zijn SCADA Good Practices [3] en een bewustwordingsboekje [4] ontwikkeld. Drie groepen van ieder zo'n veertig medewerkers van Nederlandse vitale infrastructuur- en andere bedrijven ondergingen een red-blue team training in de VS. Ze leerden daar over het inbreken en verdedigen van processystemen. Ze keerden steeds vol overtuigd terug over de kwetsbaarheid van de systemen en de noodzaak om de beveiliging goed in de greep te houden. Verder werken multinationals en leveranciers voor high-end procescontrolesystemen samen aan de ontwikkeling van standaarden voor inkoop, certificatie en installatie van veiliger procescontrolesystemen [5]. Voor andere activiteiten op dit gebied, zie [6]. In de wereld loopt Nederland hiermee voorop. Waarom gaat het dan toch fout bij de niet als vitaal aangemerkte bedrijven en lagere overheden?

Andere werelden

Het bewustzijn over de ICT-kwetsbaarheid en cybercriminaliteit is inmiddels stevig doorgedrongen tot de ICT-afdelingen van bedrijven, organisaties en overheden. De ICT-dienstverlening en de interne informatiesystemen worden om die reden beveiligd en op aangeven van de leveranciers worden systemen, netwerkcomponenten en firewalls gepatcht. De ICT-afdeling is daar dagelijks mee bezig, al gaat het daar ook wel eens mis.

Vitale infrastructuurbedrijven en overheidsorganisaties worden door het Nationale Cyber Security Centrum (NCSC) op de hoogte gehouden van nieuwe kwetsbaarheden en oplossingen. Dat werkt prima voor de 'kantoor-ICT' en internetuitingen. Probleem is dat de meeste ICT-afdelingen geen enkele affiniteit hebben met kleppen, motoren, pompen en 24/7 operaties. Dergelijke technische systemen vallen onder de facilitaire dienst of de vaak diep in de kelder weggestopte technische dienst. ICT heeft dan ook geen zicht op welke technische systemen met ingebouwde ICT geïnstalleerd zijn. Ze zijn ook niet betrokken bij het opstellen van informatiebeveiligingseisen, de verwerving, de installatie, het gebruik en het onderhoud.

De wereld van hoofden gemeentewerken, facilitair managers en hoofden technische afdelingen heeft andere zaken dan informatiebeveiliging aan het hoofd. Zij zijn verantwoordelijk voor de aanschaf, installatie, werking en het

onderhoud van technische systemen. Denk bijvoorbeeld aan systemen voor beheersing van luchtvochtigheid, overdruk en temperatuur in ziekenhuizen en bedrijven (gebouwbeheersing), sturing van liften, beveiligingssystemen als slagbomen, deurtoegangen en camerabesturingen, in- en uitschakelen van de openbare verlichting, riolerings- en afvalwatersystemen, brug- en sluisbediening op afstand, polderpompen en -schuiven. Het belangrijkste voor hen is dat deze systemen ongestoord werken. Nog niet zo lang geleden waren deze systemen en de processen die ze bedienen zeer specifiek ontworpen en maakten gebruik van specialistische techniek. Een ware revolutie is gaande. De procesbesturing draait steeds vaker op 'gewone' ICT. Met een gebruiksvriendelijke bedieninterface in de vorm van een webtoepassing (of zelfs al een app) monitort en bedient men op afstand de werking van brug, riolering, airconditioning, enz.. Weinig tijd is meer nodig voor opleiding en dagelijks beheer. Dat hierbij essentiële fysieke processen gekoppeld zijn aan GSM, telefoonnetwerk of het internet zonder na te denken over enige vorm van informatiebeveiliging komt niet in de gedachten op. De reclame van Essent, waarbij de verwarming op afstand hoger gezet wordt, zorgt voor de perceptie dat bediening op afstand doodgewoon en inherent veilig is. De begrippen veilig en beveiligd worden hierdoor niet versterkt bij systeemeigenaren.

Het onderwerp informatiebeveiliging staat bij de meeste fabrikanten, leveranciers en systeemintegrators niet op de voorgrond. Procescontroleapparatuur zoals getoond in de uitzending van Een Vandaag wordt geleverd met een korte installatiehandleiding van enkele pagina's en een CD met uitgebreide documentatie. De korte installatiehandleiding vertelt niets over het aanbrengen van een wachtwoord en hoe sterk dat moet zijn, wel hoe je het systeem koppelt met een LAN en de 220V. Bladzijde 52 van de uitgebreide handleiding beschrijft in drie regels hoe je een wachtwoord instelt en dat kunt verwijderen (!). Een aantal pagina's later staat waar je het wachtwoord moet intypen als je een slotje ziet. Niet vreemd dat systeemintegrators en installatiebedrijven geen of slechts een simpel wachtwoord aanbrengen dat iedere onverlaat kan raden.

Het onderwerp informatiebeveiliging wordt ook niet naar voren gebracht door inkoopafdelingen en bij openbare aanbestedingen. De technische afdeling richt haar focus op de pompen, motoren, sensoren, kleppen en schuiven: de functie, niet op informatiebeveiliging. Er worden zelden informatiebeveiligingseisen gesteld. Informatiebeveiliging hoort bij Internetbankieren, niet bij de bediening van de riolering vanuit thuis uit. "Iedereen vindt rioolwater vies, dus is er geen enkele hacker geïnteresseerd." En als er eisen gesteld worden, worden ze vaak als eerste geschrapt als dat extra kosten met zich meebrengt. Bij de aanschaf van de systemen geldt namelijk zo min mogelijk franje en zo efficiënt mogelijk, iets dat zich vaak vertaalt in 'de goedkoopste aanbieder'. Met het aanbieden van (extra) informatiebeveiliging ben je als aanbieder duurder en val je af.

> De meeste ICT-afdelingen hebben geen enkele affiniteit met kleppen, motoren, pompen en 24/7 operaties

Tenslotte de bedrijven die onderhoud op afstand uitvoeren, iets dat steeds vaker gebeurt omdat de eigen technische afdelingen steeds vaker tot een minimum teruggebracht zijn. De kosten voor een extra internetaansluiting of GSM-abonnement zijn nihil op de kosten van het totale onderhoud.

Afbreukrisico

Recent sprak ik een directeur van een installatiebureau. Die had geen informatiebeveiligingsprobleem meer: de gehele administratie was in handen van een extern bedrijf. Toen ik vernam dat zijn personeel onderhoud op afstand pleegt aan airconditioning-, luchtbehandeling-, en andere technische systemen bij ziekenhuizen en grote bedrijven, vroeg ik hem hoe hij de beveiliging van informatie over deze achterdeuren bij derden borgde en hoe veilig de wachtwoorden waren. Hij werd bleek toen hij zich het afbreukrisico realiseerde.

De aansluiting gaat om de beveiligingsmaatregelen van de ICT-afdeling heen. En om snel ondersteuning te bieden worden simpele onderhoudswachtwoorden ingesteld met daarin de klantnaam, eventueel voorafgegaan met NL_ als het een internationaal opererend onderhoudsbedrijf betreft.

Verantwoordelijkheid?

Minister Opstelten legde in de Kamercommissie Veiligheid en Justitie de verantwoordelijkheid voor de incidenten neer bij de systeemeigenaren. In principe heeft hij gelijk. Anderzijds zijn de incidenten nauwelijks te verwijten aan de systeemeigenaren. Niemand heeft ze over het risico verteld; ze leven in een andere wereld! De proceseigenaren zijn daardoor onbewust onveilig.

> Om snel ondersteuning te bieden worden simpele onderhoudswachtwoorden ingesteld met daarin de klantnaam

Actie gevraagd

Aanpak van deze problematiek vergt een krachtdadige samenwerking van alle betrokkenen. Dit werkt alleen als er een breed bewustzijn van de problematiek is en een sterk gevoel van urgentie ontstaat. Dit betekent dat

Een waterschap, 2003
'Als hele volksstammen hun financiën via internet regelen, dan moet je op die manier een waterzuivering kunnen aansturen'

systeemeigenaren verantwoordelijk zijn en eigenaarschap tonen. Ze moeten op basis van een gedegen risicoanalyse gepaste maatregelen treffen om hun kritieke processen te beschermen. Daarvoor moeten ze wel beschikken over kennis over het beveiligingsprobleem en over handelingsinformatie. Ze moeten heel hard nadenken over of het echt noodzakelijk is dat bediensystemen aan openbare telecommunicatienetwerken gekoppeld worden. Leveranciers, systeemintegratoren en installateurs hebben hier een 'zendelingsfunctie'. Het boekje [4] (een nieuwe editie is gepland), CPNI.NL activiteiten [6] en de NCSC factsheet [7] vormen een eerste hulp. Voorbeelden van maatregelen zijn het trainen en opleiden van het personeel dat de kritieke systemen beheert als ook het voeren van een verantwoord wachtwoordbeleid. Eisenpakketten bij de verwerving/openbare aanbesteding van technische systemen en onderhoudscontracten waar enige vorm van ICT, zoals procescontrole, deel van uit maakt, dienen altijd een hoofdstuk informatiebeveiliging te bevatten. Inkoopafdelingen dienen in te grijpen in het verwervingsproces als blijkt dat informatiebeveiliging onvoldoende aandacht krijgt. Een good practice handleiding daarvoor zou in publiek-private samenwerking ontwikkeld kunnen worden. De basis hiervoor is al gelegd in het eerder genoemde document dat door de WIB [6] is opgesteld en dat op dit moment tot een officiële IEC standaard wordt ontwikkeld. Certificering van de leverancier is onderdeel van dit proces. De overheid kan afdwingen dat, net als grote bedrijven als Shell dit doen, de leveranciers van systemen die kritieke functies in de samenleving aansturen verplicht gecertificeerd worden tegen deze IEC 62443-2-4 standaard [8]. Fabrikanten van procescontrolesystemen moeten – liefst Europees – gedwongen worden om het onderwerp informatiebeveiliging prominent en uitgebreid in hun handleidingen te behandelen.
Installatiebedrijven, systeemintegrators, installatie- en onderhoudsbedrijven moeten aansprakelijk zijn voor onveilig opgeleverde (toegang tot) procescontrolesystemen. Bij oplevering en onderhoud moeten zij daarom de systeemeigenaren onderwijzen in veilig gebruik voordat zij ontslagen zijn van de aansprakelijk.
Opleidingen facilitair management en opleidingen gerelateerd aan procescontrole bediende systemen moeten aandacht besteden aan informatiebeveiliging van technische systemen.

> De samenleving zal nog een reeks aan informatiebeveiligingsincidenten met procesbesturingen beleven

Als u als ICT-er al met de beveiliging van deze systemen bezig bent, vergeet dan ook niet de beveiliging van de telefooncentrale, de ICT-systemen in de bedrijfsauto's, draadloze medische apparatuur, enzovoorts.

Conclusie
Vooralsnog moeten we echter bang zijn dat de samenleving nog een reeks aan informatiebeveiligingsincidenten met procesbesturingen, mogelijk zelfs met ernstig gevolg voor gezondheid en goederen, zal beleven. Procesbesturingen bij lagere overheden en veel bedrijven zijn nu onveilig gekoppeld met publieke communicatievoorzieningen. Eigenaren zijn zich onvoldoende bewust van de onveiligheid. Actie is nodig. Laten we snel van onbewust onveilig gaan naar de status van bewust veilig of misschien nog beter naar onbewust veilig.

Referenties

[1] *EenVandaag 14-02-2012, Sluizen, gemalen en bruggen slecht beveiligd: kinderlijk eenvoudig van thuis uit te bedienen, on-line: http://www.eenvandaag.nl/binnenland/39770/sluizen_gemalen_en_bruggen_slecht_beveiligd*

[2] *Ir. H.A.M. Luijif en Ir. R. Lassche, SCADA (on)veiligheid: een rol voor de overheid?, TNO-KEMA rapport, april 2006.*

[3] *H.A.M. Luijif, SCADA Good Practices for the Dutch Drinking Water sector, TNO DV 2008 C096, maart 2008, on-line: https://www.cpni.nl/publicaties/scada-security-good-practices-for-the-drinking-water-sector.*

[4] *Luijif, H.A.M., "Process Control Security in het Informatieknooppunt Cybercrime", NICC, december 2009, on-line: http://www.cpni.nl/publications/PCS_brochure-NL.pdf*

[5] *WIB "Process Control Domain-Security Requirements for Vendors": www.wib.nl*

[6] *Activiteiten en publicaties rondom de beveiliging van procescontrolesystemen: volg www.cpni.nl*

[7] *Factsheet SCADA-systemen, NCSC, on-line: https://www.ncsc.nl/binaries/nl/dienstverlening/expertise-advies/kennisdeling/factsheets/beveiligingsrisicos/1/Beveiligingsrisicos%2Bvan%2Bonline%2BSCADA%2Bsystemen.pdf*

[8] *IEC 62443-2-4: Security for industrial process measurement and control - Network and system security - Part 2-4: Certification of IACS supplier security policies and Practices.*

[9] *http://webwereld.nl/nieuws/109573/attracties-van-zwembad-door-hackers-te-beheren.html*