Beveiliging gebouwsystemen vaak onvoldoende

Help! Onze gebouwinst

Het onderhoud, de monitoring en de bediening van technische gebouwinstallaties gebeurt steeds vaker op afstand, vanaf een andere locatie, door een extern bedrijf, via internet. De redenen zijn helder: het is handig en bespaart kosten. Maar is het ook veilig? Grote kans dat dat niet zo is. De hoogste tijd voor een stuk bewustwording van het risico en actie.

Eric Luiijf *

Hackers die systemen van overheden en grote instellingen zoals banken en credit card-maatschappijen aanvallen en met succes platleggen of op zijn minst verstoren. We lezen en horen er geregeld over in de media.
Managers van wat kleinere organisaties, zoals bedrijven en instellingen, zullen er met verbazing naar kijken maar tegelijk ook denken dat het een 'ver van hun bed'-show is. Maar is dat echt wel zo?
Gebouwbeheersystemen en technische gebouwinstallaties kunnen vandaag de dag ook gemakkelijk slachtoffer worden van een hack. Immers, deze systemen zijn voor de bediening, monitoring en het onderhoud steeds vaker aangesloten op een publiek netwerk zoals het internet of het mobiele telefonienetwerk. Een slimme hacker kan, waar hij zich ook bevindt, op die manier heel makkelijk toegang krijgen tot een niet goed beveiligd systeem. Met alle consequenties van dien.
Dus wat een ministerie of een grote organisatie kan overkomen, kan ook op gebouwniveau bij uw organisatie gebeuren. Bent u zich daar wel van bewust? En als uw organisatie wordt getroffen door een hack, wat zijn dan de gevolgen en hoe gaat u daarmee om?

Een Vandaag

Laten we eens teruggaan naar het begin van dit jaar. Op 14 februari bracht het tv-programma Een Vandaag in beeld hoe simpel het is de verwarming in een pand van het Leger des Heils via het internet op een andere temperatuur in te stellen. De toegang tot het systeem was gemakkelijk: er was geen wachtwoord nodig.
Ook de technische systemen van gemeenten zijn in toenemende mate gekoppeld aan het internet. Het programma liet zien dat de systemen van de gemeente Veere waren voorzien van een heel 'verrassend' wachtwoord namelijk: Veere.
Dat kwam prominent in beeld omdat het twee weken en een aantal telefoontjes duurde voordat de installateur/externe onderhoudspartij aangaf actie te gaan ondernemen. De burgemeester vertelde dat de gemeente uiteindelijk 'de stekker uit het systeem getrokken had'.
Niet direct in beeld waren de bedieningssystemen bij een aantal andere gemeenten die met eenzelfde 'gemeentewachtwoord' werkten. Ook de pompen van een zwemparadijs waren via het internet te manipuleren.

Nederlandse aanpak

Is dit dan nieuw? Nee. Deskundigen waarschuwen al tien jaar voor het risico van niet goed beveiligde procescontrolesystemen.
Begin 2006 schreven TNO en KEMA een rapport voor de overheid over de organisatorische en technische aspecten van de onveiligheid van SCADA-systemen (SCADA staat voor Supervisory Control and Data Acquisition. Het is software die wordt gebruikt om machines en systemen aan te sturen in industriële complexen als waterleidingsystemen, kerncentrales, olieplatformen en gasinstallaties). Sindsdien wordt hard gewerkt aan het nog strakker op orde brengen van de beveiliging van deze systemen in de vitale sectoren. Dit binnen het thematische kader van het Informatieknooppunt Cybercrime van het Nederlandse Centre for Protection of the National Infrastructure (CPNI.NL). Naast benchmarks in de drinkwater- en energiesectoren zijn SCADA Good Practices en een bewustwordingsboekje ontwikkeld. Drie groepen medewerkers van Nederlandse vitale infrastructuur- en andere bedrijven ondergingen een teamtraining in de VS waar ze kennis opdeden over het inbreken en verdedigen van procescontrolesystemen. Ze keerden steeds terug met overtuiging

Facility managers en hoofden TD hebben vaak andere zaken aan hun hoofd dan na te denken over de informatiebeveiliging

allaties zijn gehackt!

over de kwetsbaarheid van deze 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.

In de wereld loopt Nederland hiermee voorop. Waarom gaat het dan toch fout bij de niet als vitaal aangemerkte bedrijven en lagere overheden? Het probleem wordt veroorzaakt op een aantal niveaus.

Andere werelden

Het bewustzijn van de ICT-kwetsbaarheid en cybercriminaliteit is inmiddels goed doorgedrongen tot de IT-afdelingen van bedrijven, organisaties en overheden. De ICT-dienstverlening en de interne informatiesystemen worden om die reden stevig beveiligd en op aangeven van de leveranciers worden systemen, netwerkcomponenten en firewalls gepatcht. Anders gezegd: de 'gewone' kantoorsystemen krijgen vaak voldoende aandacht van de IT-afdeling als het gaat om de beveiliging.

Maar de meeste *IT-afdelingen* hebben geen enkele affiniteit met kleppen, motoren, pompen en 24/7 operaties. Dergelijke technische systemen vallen onder de facilitaire dienst of de technische dienst. IT heeft er dan ook geen zicht op welke technische systemen met ingebouwde ICT zijn geïnstalleerd. IT is ook niet betrokken bij het opstellen van informatiebeveiligingseisen, de verwerving, de installatie, het gebruik en het onderhoud.

Facility managers en hoofden technische afdelingen hebben vaak andere zaken aan hun hoofd dan na te denken over de informatiebeveiliging. Zij zijn verantwoordelijk voor de aanschaf, installatie, werking en het onderhoud van technische gebouwsystemen bedoeld voor de beheersing van luchtvochtigheid, het regelen van overdruk en temperatuur in ziekenhuizen en bedrijven, de aansturing van de liften, de beveiliging, het toegangsbeheer en camerabewaking.

Het belangrijkste voor hen is dat deze systemen ongestoord werken. De besturing van deze systemen draait tegenwoordig 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 de airconditioning, verwarming, enzovoort.
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 tv-reclame van Essent, waarbij iemand vanaf een zonnig strand de verwarming op afstand hoger zet, creëert het beeld dat bediening op afstand niet alleen doodgewoon maar ook veilig is. De begrippen 'veilig' en 'beveiligd' worden hierdoor niet versterkt bij systeemeigenaren.

Ook bij de *meeste fabrikanten, leveranciers en systeemintegrators* staat het onderwerp informatiebeveiliging 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-rom met uitgebreide documentatie.
Die korte handleiding vertelt niets over het aanbrengen van een wachtwoord en hoe sterk dat moet zijn, wel hoe je het systeem koppelt met een lokaal netwerk en de 220V. Ergens op bladzijde 50 van de uitgebreide handleiding worden het instellen en het verwijderen (!) van een wachtwoord in drie regels beschreven. Enkele pagina's later is aangegeven waar het wachtwoord ingetypt moet worden als een slotje op het scherm verschijnt. Niet vreemd dat systeemintegrators en installatiebedrijven geen of slechts een simpel wacht- »

woord aanbrengen dat iedere onverlaat kan raden.

Het onderwerp informatiebeveiliging wordt daarnaast ook niet naar voren gebracht door *inkoopafdelingen* en bij openbare aanbestedingen. Bij aanbestedingen richt de technische afdeling haar focus vooral op de pompen, motoren, sensoren, kleppen en schuiven, maar niet op informatiebeveiliging. En als er al eisen ten aanzien van de beveiliging worden gesteld, worden ze vaak als eerste geschrapt als blijkt dat dat voor extra kosten zorgt. Bij de aanschaf van de systemen geldt namelijk zo min mogelijk franje en zo efficiënt mogelijk, iets wat zich vaak vertaalt in 'de goedkoopste aanbieder'. Met het aanbieden van (extra) informatiebeveiliging ben je als aanbieder duurder en is de kans groot dat je afvalt.

Ten slotte de *bedrijven die onderhoud op afstand uitvoeren*, iets wat steeds vaker gebeurt omdat de eigen technische afdelingen tot een minimum zijn teruggebracht. De kosten voor een extra internetaansluiting of gsm-abonnement zijn nihil op de kosten van het totale onderhoud. De extra aansluiting gaat om de beveiligingsmaatregelen van de IT-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.

In principe bent u als systeemeigenaar verantwoordelijk voor de informatiebeveiliging. Anderzijds zijn de incidenten nauwelijks te verwijten aan u als systeemeigenaar. Niemand heeft u eerder over het risico verteld; u leeft in een andere wereld dan die van IT en informatiebeveiliging! U als proceseigenaar opereert daardoor onbewust onveilig.

Actie gevraagd

Moet dit anders? Ja. Kan het anders? Ja. Maar daar is wel een krachtdadige samenwerking voor nodig van alle betrokkenen. Dit werkt alleen als er een breed bewustzijn van de problematiek is en een sterk gevoel van urgentie ontstaat. Dit betekent een aantal zaken:

1. De *systeemeigenaren* moeten zich verantwoordelijk tonen en hun 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 er heel hard over nadenken of het echt noodzakelijk is dat bediensystemen aan openbare telecommunicatienetwerken gekoppeld worden. Leveranciers, systeemintegrators en installateurs hebben hier een 'zendelingsfunctie'. Het boekje (zie de noten), CPNI.NL activiteiten en de NCSC factsheet vormen een eerste hulp. Voorbeelden van maatregelen zijn het trainen en opleiden van het personeel dat de kritieke systemen beheert, en het voeren van een verantwoord wachtwoordbeleid.

2. *Programma's van Eisen* bij de aanschaf en aanbesteding van technische systemen en onderhoudscontracten waar enige vorm van ICT, zoals procescontrole, deel van uitmaakt, moeten altijd een onderdeel 'informatiebeveiliging' bevatten. Inkoopafdelingen moeten ingrijpen als bij een aanbesteding blijkt dat informatiebeveiliging onvoldoende aandacht krijgt. Een handleiding daarvoor zou in publiek-private samenwerking ontwikkeld kunnen worden. De basis hiervoor is al gelegd in het eerdergenoemde document dat door de WIB 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 zoals Shell dit doen, de leveranciers van systemen die kritieke functies in de samenleving aansturen, verplicht gecertificeerd worden tegen deze IEC 62443-2-4 standaard.

3. *Fabrikanten* van procescontrolesystemen moeten – liefst Europees – gedwongen worden om het onderwerp informatiebeveiliging prominent en uitgebreid in hun handleidingen te behandelen.

4. *Installatiebedrijven, systeemintegrators, installatie- en onderhoudsbedrijven* moeten aansprakelijk zijn voor onveilig opgeleverde (toegang tot) procescontrolesystemen. Bij oplevering en onderhoud moeten zij de systeemeigenaren 'onderwijzen' in veilig gebruik voordat zij ontslagen zijn van de aansprakelijkheid.

5. *Opleidingen* facilitair management en opleidingen gerelateerd aan procescontrole bediende systemen moeten aandacht besteden aan informatiebeveiliging van technische gebouwsystemen.

Het is niet vreemd dat systeemintegrators en installatiebedrijven geen of slechts een simpel wachtwoord aanbrengen

Overigens zijn het niet alleen uw procescontrolesystemen waar dit probleem zich voordoet. Vergeet ook niet de beveiliging van de telefooncentrale, de ICT-systemen in de bedrijfsauto's en allerlei nieuwe toepassingen die uw facilitair management gemakkelijker maken. «

Dit artikel is een bewerking van een artikel dat eerder dit jaar in het blad Beveiliging is verschenen.

Referenties

» EenVandaag 14-02-2012. Sluizen, gemalen en bruggen slecht beveiligd. www.eenvandaag.nl/binnenland/39770/sluizen_gemalen_en_bruggen_slecht_beveiligd

» ir. H.A.M. Luiijf en ir. R. Lassche, SCADA (on)veiligheid: een rol voor de overheid?, TNO-KEMA rapport, april 2006

» H.A.M. Luiijf, 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
» Luiijf, H.A.M., Process Control Security in het Informatieknooppunt Cybercrime, NICC, december 2009, online: www.cpni.nl/publications/PCS_brochure-NL.pdf
» WIB Process Control Domain-Security Requirements for Vendors: www.wib.nl
» Activiteiten en publicaties rondom de beveiliging van procescontrolesystemen: volg www.cpni.nl
» Factsheet SCADA-systemen, NCSC, online: https://www.ncsc.nl/binaries/nl/dienstverlening/expertise-advies/kennisdeling/factsheets/beveiligingsrisicos/1/Beveiligingsrisicos%2Bvan%2Bonline%2BSCADA%2Bsystemen.pdf
» 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
» http://webwereld.nl/nieuws/109573/attracties-van-zwembad-door-hackers-te-beheren.html

* ir. Eric Luiijf is principal consultant bescherming vitale infrastructuur bij TNO. Hij is als expert beveiliging procescontrolesystemen en Smart Grids verbonden aan CPNI.NL (eric.luiijf@tno.nl)

SAMENVATTING

» De monitoring, de besturing en het onderhoud van technische gebouwinstallaties bij veel bedrijven, organisaties en ook lagere overheden lopen vaak via publieke communicatievoorzieningen zoals internet.
» Dit kan onveilig zijn en tot grote gevolgen leiden als een hacker zijn slag slaat.
» Systeemeigenaren zijn zich onvoldoende bewust van deze onveiligheid. Daarom zijn bewustwording en actie nodig.