Beveiliging procescontrole is

Veel vitale en risicovolle processen worden bestuurd met zogenoemde SCADA-systemen. Die maken echter meer en meer plaats voor op Windows en Linux gebaseerde SCADA-toepassingen die internetprotocollen gebruiken. Koppelingen met bedrijfsnetwerken maakt de processen kwetsbaar voor ongewenste beïnvloeding van buitenaf. Vooral omdat de beveiliging onvoldoende aan de nieuwe risicofactoren wordt aangepast.

Supervisory Control and Data Acquisition (SCADA)- en andere procescontrolesystemen besturen, regelen en monitoren fysieke processen. Traditioneel zijn dit systemen bestaande uit speciale apparatuur met ingebedde, leverancierseigen programmatuur. In toenemende mate worden deze systemen vervangen door programmatuur die draait boven op normale besturingssystemen als Linux en Windows en gebruiken zij internetprotocollen. Koppelingen met bedrijfsnetwerken en het internet brengt het risico van ongewenste beïnvloeding van die essentiële bedrijfsprocessen met zich mee. Uit nationale en internationale onderzoeken blijkt dat in veel bedrijven de informatiebeveiliging van deze systemen onvoldoende aandacht krijgt. Ernstige gevolgen voor de veiligheid van personen, geproduceerde producten en de dienstverlening van nutsvoorzieningen voor de samenleving zijn daardoor niet uit te sluiten. Hieronder wordt besproken waarom dit een onderbelicht beveiligingsgebied is, wat het risico is en waar in het bedrijf op moet worden gelet.

Management-summary

SCADA en andere procescontrolesystemen besturen en monitoren fysieke processen. Die processen lopen uiteen van het regelen van eenvoudige gebouwbeheersystemen, automatische vulinstallaties voor dranken tot complexe besturingen van onze vitale infrastructuren als gas, elektriciteit, drinkwater, metro, treinen, tunnels en havensystemen. De informatiebeveiliging van dergelijke systemen is vaak onderbelicht. Dit artikel gaat in op de hoofdoorzaken voor dit gebrek aan aandacht, de zwakheden en het risico voor bedrijven en samenleving.

Procescontrole SCADA-systemen monitoren processen met sensoren, zoals drukopnemers of temperatuurvoelers, besturen de processen met actuatoren, zoals pompen, bediende kleppen en deuropeners en worden bestuurd via menselijke computerinteractie. SCADA kan heel kleinschalig zijn, zoals bij een gebouwbeheerinstallatie of brugbediening. Maar er bestaan ook complexere systemen voor bijvoorbeeld voedingsproductie- en afvullijnen en de bagagebehandeling op Schiphol. Zeer complexe systemen met vele duizenden sensoren en actuatoren en grote regelkamers zijn te vinden in bijvoorbeeld de (petro)chemische industrie.

Tot voor kort bestonden de programmatuur en hardware van de SCADA-systemen uit gesloten systemen en zeer speciale hardware. In toenemende mate worden die systemen vervangen door toepassingsprogrammatuur die draait boven op normale PC's met normale besturingssystemen als Linux of Windows. Tegelijkertijd wordt de seriële communicatie vervangen door TCP/IP over een brede keuze aan verbindingstechnieken van eigen glasfibers tot aan ISDN, GSM/GPRS en zelfs over internet.

De informatiebeveiliging van de oudere SCADA-protocollen laat sterk te wensen over omdat deze ontworpen zijn voor een procescontroleomgeving die volledig fysiek gescheiden is van andere netwerken en de buitenwereld. Doordat er geen dreiging aanwezig is, is er ook geen noodzaak voor enige mate van informatiebeveiliging. Binnen zo'n gesloten netwerkomgeving is er niemand die zich niet aan de protocolafspraken houdt en zal in principe niemand geïnteresseerd zijn in het plegen van een aanval op de SCADA-systemen en de daarmee bestuurde en gecontroleerde processen. Verder is informatie over SCADA-protocollen alleen bij de leveranciers aanwezig, wat een inbreuk nog eens extra moeilijk maakt.

ICT-dreigingen Inmiddels zijn al deze ontwerpcriteria achterhaald. Bedrijven moeten informatie uit de procescontrolesystemen hebben om direct informatie te hebben voor hun bedrijfssystemen. Denk bijvoorbeeld aan de traceerbaarheid van de kwaliteit van de productieprocessen bij het produceren van voedselproducten. Hiertoe worden de SCADA-systemen gekoppeld aan andere bedrijfsnetwerken. Dit maakt de systemen gevoelig voor typische ICT-dreigingen als virussen, wormen en Trojaanse paarden, waarmee internetaansluitingen continu worden bestookt. Die 'malware' maakt het niet uit of het aangevallen besturingssysteem een compleet industrieel proces bestuurt. Uit testen blijkt ook nog eens dat SCADA-toepassingen extra gevoelig zijn voor aanvallen door hackers en virussen. Driekwart van de systemen herstart zichzelf of gaat hangen zodra ze een pakket ontvangen dat zich niet aan de protocolafspraken houdt. Ook zijn de SCADA-protocolontwerpen minder geavanceerd dan de internetprotocollen, wat SCADA extra kwetsbaar maakt voor denial-of-service aanvallen. Bovendien zijn de protocolbeschrijvingen op internet te vinden en zijn er 'slimme' proces-

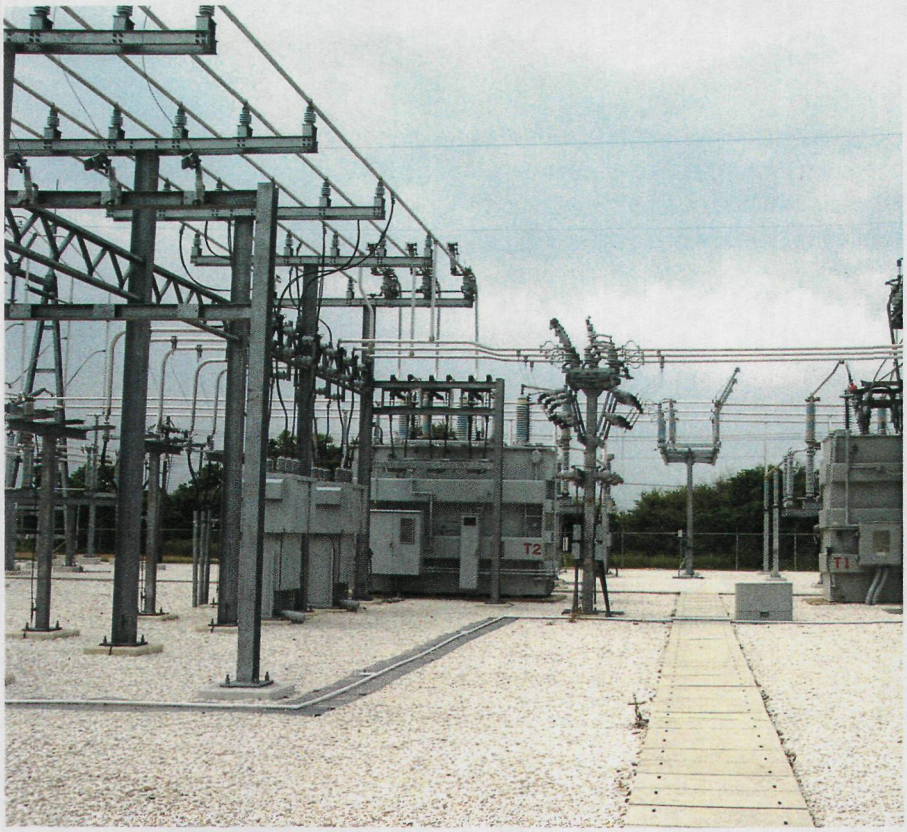
onderbelicht onderwerp

controleborden (PLC) die standaard een niet-beveiligde webserver aan boord hebben die het eenvoudig maakt om allerlei parameters op de PLC te wijzigen.

Organisatorisch falen Al deze technische veranderingen vinden plaats in het automatiseringsdomein in de bedrijven. De verantwoordelijken hiervoor hebben in het algemeen niet of nauwelijks zicht op informatiebeveiliging. Hun verantwoordelijkheid is een ongestoorde en veilige productie, liefst meer productie met minder personeel en middelen. De ICT-afdelingen van dergelijke bedrijven zijn druk bezig met de bedrijfssystemen, -netwerken en PC's. De automatiserings- en productieafdelingen zijn voor hen veelal 'kleppen, pijpen en pompen'. Als ze dezelfde ICT-middelen ontdekken binnen de SCADA-omgeving, willen ze veelal hun eigen standaarden opleggen die soms haaks staan op de 24 uur/7 dagen per week SCADA-omgeving. Men kan een inkoopsysteem rustig twee keer per dag herstarten, maar het voor een programmatuur-update stilleggen en herstarten van systemen die de stroomvoorziening regelen vergt een lange planningscyclus. Twee verschillende culturen dus, die veelal slecht met elkaar kunnen communiceren.

Externe omstandigheden Een ander risicoaspect is de vermenging van het SCADA-netwerk met bedrijfs- en kantoorautomatiseringsnetwerken. Naast het risico van malware en directe verbinding met internet is er het risico dat een storing in een van de kantoorautomatiserings PC's het volledige netwerk blokkeert met als gevolg het verlies aan besturing van de productieprocessen. Ook externe omstandigheden kunnen netwerken beïnvloeden, denk aan het gebruik van ADSL of mobiele telefonie voor het op afstand aansturen van bruggen, pompen en waterbeheersystemen in polders. Verder is het technisch heel moeilijk om een firewall tussen de SCADA-omgeving en de bedrijfsautomatiseringomgeving te configureren. Er zijn weinig goede handleidingen en het vereist kennis van beide omgevingen, een brugfunctie die in bedrijven niet op natuurlijke wijze ontstaat.

Nationale aandacht In 2006, is in opdracht van het ministerie van Economische Zaken een TNO/KEMA rapport opgesteld met daarin een analyse van de hiervoor genoemde ontwikkelingen in techniek en kwetsbaarheden (*1). Daarnaast gaat het rapport in op internationale standaardisatie-ontwikkelingen. De onderzoekers inventariseerden ook een aantal SCADA-ongelukken en 'near-miss'-situaties in verschillende sectoren. Uit krantenberichten lijken dergelijke incidenten zich alleen in de VS en Australië voor te doen. Uit nader onderzoek blijken wel degelijk SCADA-incidenten in Europa en Nederland plaats te vinden, ze komen echter bijna nooit naar buiten. Het rapport noemt een aantal incidenten, waarvan sommige als ernstig gekwalificeerd kunnen worden. Inmiddels is die lijst gegroeid.
Enkele incidenten die het risico voor bedrijven en samenleving aangeven: het alarmpaneel van een nucleaire centrale is vijf uur lang onbruikbaar omdat deze met een worm is geïnfecteerd (VS, 2003), delen van het elektriciteitsnetwerk in de VS zijn niet te ▸



bedienen door een virus in het SCADA-netwerk, een hacker heeft in principe de volledige controle over het masterconsole in de regelkamer van een chemische plant, een worm legt 23 fabrieken van Daimler-Chrysler plat waaronder een Ford fabriek in België. In het elektriciteitstransmissienetwerk van een groot land in Europa was gedurende tien dagen een hacker actief en een worm in een controlesysteem van een olieplatform heeft geleid tot een kleine explosie. Door middel van een inbraak in het (SCADA) gebouwbeheersysteem van het computercentrum van een bank wist men de airconditioning af te zetten, waarna de financiële systemen zichzelf na enige tijd uitschakelden. Recent nog wist een jeugdige hacker in Łodz, Polen, twee trams tegen elkaar te laten botsen door manipulatie van het wissel- en signaleringssysteem.

Vitale infrastructuur Ook in Nederland zijn SCADA-systemen besmet geraakt met virussen en wormen, zijn hackers ingedrongen in SCADA-systemen en hebben softwarefouten geleid tot uitval van gas- en elektriciteitsvoorzieningen. Naar aanleiding van het eerder genoemde TNO-KEMA rapport heeft een aantal bedrijven die deel uitmaken van de Nederlandse vitale infrastructuur, de SCADA beveiligingsproblematiek actief opgepakt. Sommige vitale sectoren, zoals de drinkwater- en de energiesectoren, doen dat samen binnen de Nationale Infrastructuur (tegen) Cybercrime (NICC). Het NICC wisselt in het European SCADA and Control Systems Information Exchange (EuroSCSIE) overleg informatie over SCADA-beveiliging uit met overheidsorganisaties en SCADA grootgebruikers uit andere Europese landen. Nederland is daarin tezamen met het Verenigd Koninkrijk (CPNI) en Zweden (SEMA) een van de voortrekkers.

Actieplan overheid Daarnaast pakt de Nederlandse overheid de SCADA-beveiligingsproblematiek breder op. Tijdens de vakbeurs 'Het Instrument' zal in een symposium met workshops op verschillende managementniveaus van board room tot aan de automatiseringsmanager aandacht besteed worden aan de SCADA-problematiek. In een aanpalend artikel in deze editie van BEVEILIGING (zie pagina 88) is hierover meer te lezen. Toch is er nog een lange weg te gaan, vooral bij kleine en middelgrote organisaties waar informatiebeveiliging minder nadrukkelijk op de agenda staat en zeker niet waar het gaat om de SCADA-omgeving. Wilt u zelf aan de gang? In de referenties treft u enkele startpunten aan.

■ Eric Luiijf
Eric.Luiijf@beveiliging.nl

Referenties

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

2) NERC, Top 10 Vulnerabilities of Control Systems, version 2007. Online: www.us-cert.gov/control_systems/pdf/2007_Top_10_Formatted_12-07-06.pdf

3) Department of Energy, 21 Steps to Improve Cyber Security of SCADA Networks, Office of Energy Assurance, Office of Independent Oversight And Performance Assurance, U.S. Department of Energy, USA, 2005. On-line: www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

4) K. Stoffler, J. Falco, K. Kent, Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security, NIST Special Publication SP800-82 (draft), USA, september 2006.

5) Gary Finco et al., Cyber Procurement Language for Control Systems, version 1.6, INL Critical Infrastructure Protection/Resilience Center, Idaho Falls, USA, June 2006.

6) NISCC, Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks, NISCC, 2004 te vinden bij www.cpni.gov.uk.

7) Andere SCADA Good Practice Guides, zie www.cpni.gov.uk

WATERZUIVERING

Wilt u ook eens de waterzuivering van 600.000 Nederlandse huishoudens regelen? 'Als hele volksstammen hun financiën via internet regelen, dan moet je op die manier een zuivering kunnen aansturen. Is er echt een alarmsituatie, dan wordt de hele automatische bediening geblokkeerd en komt er ouderwets handwerk aan te pas', vertelt de projectleider van een Waterschap in een interview met www.neerslag-magazine.nl in 2003.