Web based gebouwbeheer-systeem: vloek of zegen?

Gebouwinstallaties kunnen uitstekend beheerd worden met een gebouwbeheersysteem (GBS). Storingen zijn direct zichtbaar, waarop de beheerder of onderhoudsfirma direct actie kan ondernemen. Voor een externe beheerder is het erg handig als hij op afstand in het systeem kan kijken. Dit is mogelijk met een web based GBS, waarvoor een browser en internetverbinding volstaan. Zowel opdrachtgever, onderhoudsfirma als adviseur kunnen zo eenvoudig in het GBS kijken, hieruit informatie halen en de nodige verstellingen plegen. Maar als de onderhoudsfirma en adviseur dit kunnen, wie dan nog meer?

Ir. H. (Henk) Winters, specialist regeltechniek, Deerns Nederland BV;
E.G. (Gerben) Broenink MSc, IT security specialist, TNO

Om de kwetsbaarheid van een GBS te beoordelen, is het van belang dat het hele netwerk te bekijken. In dit artikel wordt uitgegaan van een gebruikelijke, hedendaagse uitvoering; allereerst van een relatief klein GBS, aangesloten op het kantoor ICT-netwerk van een gebouw (zie figuur 1). Het Direct Digital Control (= DDC)-automatiseringsstation is hierbij voorzien van webpagina's voor bediening en beheer van de installaties. De software in het DDC-automatiseringsstation regelt, bestuurt en beveiligt de gebouwgebonden installaties, zoals de cv-, koel- en luchtbehandelingsinstallatie. Het is ook mogelijk om bijvoorbeeld een luchtbehandelingskast (LBK) met geïntegreerde regeltechniek met een RS-485-koppeling (zoals Modbus RTU, BACnet MS/TP) aan te sluiten op het DDC-automatiseringsstation. Het DDC-automatiseringsstation kan de LBK bedienen en beheren, waarbij verstellingen van setpoints, vrijgave van de LBK en dergelijke, mogelijk zijn. Als alternatief kan de LBK ook via een IP-koppeling (Modbus/IP of BACnet/IP) aangesloten worden op het DDC-automatiseringsstation. Een beheerder die van buiten het gebouw contact wil leggen met het DDC-automatiseringsstation, kan via een firewall toegang verkrijgen.

Bij grotere systemen ziet het netwerk er veelal uit als in figuur 2. Afhankelijk van de opzet van de installaties kan gekozen worden voor alleen web-based DDC-automatiseringsstations met geïntegreerde beeldplaatjes, of worden de web-beeldplaatjes in een separate webserver geplaatst. Op deze webserver zijn nog meer beheermogelijkheden aanwezig (met vier te onderscheiden management topics: installatie-, onderhouds-, risico- en energiebeheer). Er wordt dan vaak een separaat technisch LAN-netwerk aangelegd voor de gebouwgebonden automatisering. Dit kan zowel een fysiek gescheiden netwerk zijn als een apart VLAN op een bestaand netwerk. Bij nieuwbouw is de opbouw van een VLAN complex, aangezien de gebruiker de ICT-infrastructuur (routers, switches, e.d.) doorgaans pas aanlegt na oplevering van het gebouw, terwijl de regeltechniek bij oplevering al moet functioneren. De ICT-infrastructuur die hiervoor nodig is, is dan doorgaans nog niet aangelegd. In dat geval is het beter om voor een eigen fysiek LAN te kiezen, dat door de installateur wordt geleverd en aangelegd. Dit biedt tevens een beveiligingsvoordeel, omdat dit LAN gescheiden is van de overige ICT.

BEVEILIGINGSANALYSE

Wat de beveiliging van deze systemen betreft, zijn er de nodige uitdagingen. In de praktijk zien we regelmatig voorbeelden waarbij de beeldplaatjes via een gewone http-verbinding benaderd kunnen worden. Dit terwijl inbreken op deze open verbinding eenvoudig is voor hackers, die al het verkeer kunnen meelezen (en aanpassen). [Het gebruik van wireshark (www.wireshark.org) kan voldoende zijn om wachtwoorden af te luisteren.] Op deze wijze kunnen gebruiksnamen en wachtwoorden bemachtigd worden.

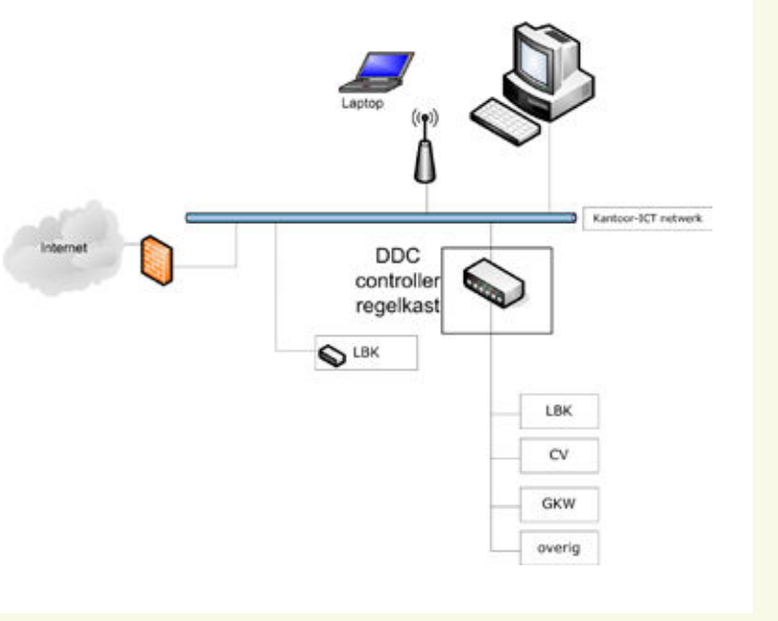
Het wordt al moeilijker om mee te lezen wanneer een beveiligde verbinding wordt toegepast, via https. Maar ook dan kan een aanvaller gebruik maken van 'tooling' om deze beveiliging te omzeilen. [Hier zou een hacker

gebruik kunnen maken van tooling als SSLStrip (http://www.thoughtcrime.org/software/sslstrip/) en WebMITM (http://whiskeycola.wordpress.com/2008/05/10/ssldump-web-mitm-and-arpspoof-the-trio-ssl-sniffing/)]
Om de beveiliging goed te analyseren, kan een systeem altijd op drie punten bekeken worden (de zogenaamde CIA-eigenschappen):

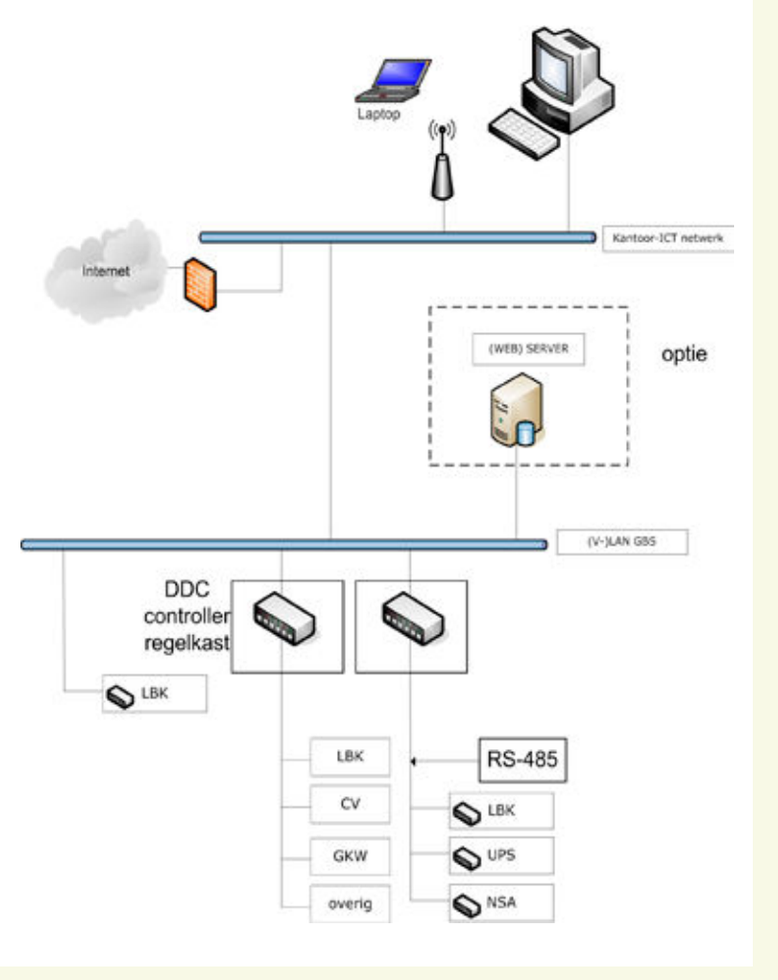
- vertrouwelijkheid (confidentiality) dwingt af dat alleen geautoriseerde personen het systeem mogen bedienen (of de data mogen inzien);
- integriteit (integrity) dwingt af dat een systeem correct functioneert en alle data correct is;
- beschikbaarheid (availability) geeft aan of het systeem en de data gebruikt kunnen worden door de gebruiker.

Een vertrouwelijkheidsissue is dus een hacker die er door een aanval op het systeem in slaagt om dit te bedienen, terwijl uitval door een stroomstoring een beschikbaarheidsissue is. Het spreekt dan ook voor zich dat voor al deze aspecten andere beveiligingsmaatregelen genomen moeten worden. Zo zal het dubbel uitvoeren van een systeem een zeer effectieve maatregel zijn tegen een mechanische storing, maar geen enkel nut hebben tegen een hacker of stroomstoring.
Vanuit beveiligingsoogpunt is het van belang dat ze alle drie geanalyseerd worden. De keten is zo sterk als de zwakste schakel. Het feit dat de beveiliging op één aspect goed voor elkaar is, betekent nog niet dat het systeem veilig is.

In het verleden zijn veel gebouwbeheersystemen als zelfstandige autonome systemen ontwikkeld. Dit houdt in dat een GBS op een locatie zelfstandig opereert en niet van buitenaf bereikbaar is. Onderhoud of het uitlezen van het systeem moet fysiek op locatie gebeuren. Hierdoor is de beveiliging tegen kwaadwillenden uitstekend. Een aanvaller moet namelijk eerst fysiek toegang hebben, voordat hij bij het systeem kan. In de beveiligingsanalyse is vertrouwelijkheid dus geen issue. Iedereen die fysiek bij het systeem kan, is namelijk fysiek toegelaten en dus geautoriseerd voor het systeem. De genomen beveiligingsmaatregelen hadden in het verleden dan ook een sterke nadruk op beschikbaarheid, minder op integriteit en niet op vertrouwelijkheid. Zowel het gebruik van een UPS als het inbouwen van redundantie is een goede maatregel voor de beschikbaarheid, maar voegt niets toe aan de vertrouwelijkheid. Later zijn de systemen via inbelmodems en speciale software op afstand benaderbaar geworden. Met specifieke software kan een beheerder nu inloggen op het systeem en



-Figuur 1- Netwerktopologie voor een relatief klein GBS



-Figuur 2- Netwerktopologie voor een relatief groot GBS

het GBS volledig beheren. Hoewel specifieke software vereist is, zou een aanvaller nog steeds kunnen proberen om de communicatie af te luisteren en manipuleren. Na de opkomst van het internet zijn veel van deze systemen hiermee gekoppeld. Hierdoor kan een web-interface beschikbaar gesteld worden en is het ineens mogelijk om een GBS beheerbaar te maken van over de hele wereld, met als enige vereiste dat de beheerder een browser geïnstalleerd heeft.
Dit heeft echter impact op de beveiligingsanalyse. Waar eerst de noodzaak van fysieke aanwezigheid een impliciete beveiligingsmaatregel was, valt deze maatregel nu weg. Hierdoor moet er in de beveiligingsanalyse rekening gehouden worden met de mogelijkheid van een externe aanvaller. Gevolg is dat gebouwbeheersystemen goed beschermd kunnen zijn tegen beschikbaarheid en integriteitsissues, maar niet tegen vertrouwelijkheidsissues die de veranderde omgeving met zich meebrengt. Als een GBS gecompromitteerd wordt, kan een aanvaller informatie opvragen, maar ook parameters wijzigen, waardoor installaties zoals datacenters en operatiekamer(OK-)complexen ontregeld raken. De gevolgen variëren van ongemak vanwege een uitgeschakelde cv-installatie tot uitval van een datacenter, met grote kosten tot gevolg of mogelijk zelfs doden indien OK-systemen uitgeschakeld worden. Niet alleen gebouwbeheersystemen worden hier kwetsbaarder voor, ook industriële Scada-systemen zijn steeds meer zijn gebaseerd op web-technologie en daardoor 'hackbaar' zijn. Afhankelijk van het proces dat bestuurd wordt, kunnen de gevolgen van inbreken enorm zijn. Dat dit in de praktijk voor problemen zorgt is al een aantal keer (o.a. via de media) naar buiten gekomen. We noemen enkele voorbeelden van gehackte Scada-systemen:

Sluizen en gemalen
Een bekend voorbeeld van beveiligingsrisico's door het op afstand bereikbaar maken van PLC en Scada-apparatuur zijn de Nederlandse sluizen en gemalen, die in 2012 bleken te zijn beveiligd met de plaatsnaam van het gemaal als wachtwoord. [http://20jaareenvandaag.eenvandaag.nl/hoogtepunten/39770/sluizen_gemalen_en_bruggen_slecht_beveiligd.]
Een aanvaller die dit wachtwoord zou weten te raden, had bijvoorbeeld alle sluizen open kunnen zetten met overstromingen als gevolg.

Google warf 7
In 2013 bleek het mogelijk om in te breken op het Tridium platform bij het Google Warf 7 [http://blog.cylance.com/blog/bid/297050/Google-s-Buildings-Hackable]. Het gat in de beveiliging is inmiddels gedicht.

Aurora project
Jan Wiersma in een artikel op zijn website van 20 oktober 2011: *'Dat de verhoogde kans op cybercrime een reële bedreiging vormt, toonden DOE engineers van het Idaho National Engineering Lab (USA) in het Aurora Project (2007) aan. Samen met hackers van het Department of Homeland Security (DHS) startten ze een cyberaanval met als doel een grote dieselgenerator te vernielen. Enkele minuten nadat de hackers toegang kregen tot het Scada-systeem, wist men de generator in handen te krijgen. Op een video die in 2009 getoond werd in het Amerikaanse CBS'60 Minutes, was te zien dat de 27 ton wegende generator gestart werd, flink begon te schudden en na enige seconden volledig gehuld was in rook. De generator overleefde de cyberaanval niet. Het Aurora Project toonde aan dat het mogelijk was voor hackers om via een netwerktoegang fysieke schade toe te brengen aan een generator. De hackers hadden kwetsbaarheden gebruikt die in de meeste industriële besturingssystemen vandaag de dag nog aanwezig zijn.'* [http://jwiersma.wordpress.com/2011/10/20/een-virus-in-je-noodstroom-generator/]

Energiebedrijven
Op Tweakers was 1 juli 2014 te lezen dat recentelijk de Scada-systemen van diverse energiebedrijven zijn gehackt. Grote schade is gelukkig uitgebleven, omdat spionage het doel was en niet sabotage. [http://tweakers.net/nieuws/97013/hackers-hadden-toegang-tot-scada-systemen-energiebedrijven.html]

Eigen ervaring
In gesprekken met GBS-leveranciers blijkt dat bij datacenters de 'voordeur' goed beveiligd is, terwijl de 'achterdeur' het GBS, wagenwijd open staat. Dit zorgt ervoor dat een aanvaller via deze achterdeur alsnog het datacenter uit kan schakelen door via het GBS de koelinstallaties plat te leggen. En zelfs als een GBS beveiligd is door bijvoorbeeld een wachtwoord, zijn er voor een aanvaller nog legio mogelijkheden om binnen te komen op een systeem. Zo kan een aanvaller de inloggegevens op een aantal manieren achterhalen:
- *social engineering*: de aanvaller kan een beheerder bellen en zich voordoen als een medewerker van de IT-afdeling, met als boodschap: "Er lijkt een probleem te zijn met uw account. Mag ik uw accountgegevens even?";
- *afluisteren communicatie*: als er een onbeveiligde netwerkverbinding is (geen https, of onbeveiligd wifi), kan een aanvaller die afluisteren en zelfs manipuleren;
- *brute force*: een aanvaller kan het wachtwoord raden door alle mogelijke wachtwoorden te proberen;
- *malware*: het systeem van de beheerder kan geïnfecteerd zijn met malware. Een aanvaller kan gericht proberen het systeem van de beheerder te infecteren, om zo inloggegevens te achterhalen. Het is dus aan te raden om op de beheersystemen beschermingsmaatregelen te nemen, zoals een virusscanner en voor de browser ad-block extensies
- *aanvallen op server*: ook de server kan geïnfecteerd zijn met malware. Als de software-patches niet goed bijgehouden worden, kan een server bijzonder kwetsbaar zijn voor malware. Dit kan zijn op de GBS-software, maar ook op het besturingssysteem. Zo is op 8 april 2014 de ondersteuning van Windows XP gestopt, wat betekent dat elk GBS dat op een Windows XP platform draait per definitie kwetsbaar is voor verschillende soorten malware.

MOGELIJKE MAATREGELEN

Zoals eerder genoemd, wordt het GBS geleverd door een installateur en de infrastructuur door de gebouwbeheerder om via het internet te kunnen benaderen. Omdat deze partijen samen verantwoordelijk zijn voor het gehele systeem, moeten ook beide partijen maatregelen nemen. Opgemerkt wordt dat het per situatie verschilt welke maatregelen geïmplementeerd moeten worden. Dit is namelijk

Instortende generatorh(ttp://www.youtube.com/watch?v=fJyWngDco3g)

afhankelijk van de mogelijke impact. Zo is het vervelend wanneer het GBS in een kantoorpand uitvalt, maar is het levensgevaarlijk wanneer het GBS uitvalt in een operatiekamer. Als voorbeeld onderstaande maatregelen:

Authenticatie

Authenticatie betekent, dat een gebruiker geïdentificeerd moet worden voordat hij gebruik mag maken van het systeem. Authenticatie kan vergeleken worden met het inzien van een paspoort. Een paspoort bevat een aantal echtheidskenmerken, waarmee de identiteit van de houder vastgesteld kan worden. Authenticatie is van belang voor een GBS, omdat daarmee afgedwongen kan worden dat alleen bevoegde gebruikers toegang krijgen. De meest gebruikte vorm van authenticatie is het gebruik van een *inlognaam* en *password*. Dit is een eenvoudige basistechniek, die in ieder systeem toegepast moet worden. Hoewel dit voor zichzelf lijkt te spreken, gaat dit in de praktijk nog erg vaak mis. Vaak werken veel gebruikers met hetzelfde wachtwoord of wordt een te eenvoudig wachtwoord gekozen. Verder is met name het beheren en updaten van gebruikers een moeilijkheid. Toch is er een aantal eenvoudige richtlijnen:

- iedere gebruiker heeft een eigen inlognaam en wachtwoord;
- er zijn minimumeisen voor de wachtwoordsterkte (bijvoorbeeld 'password123' is te zwak). Deze minimumeisen kunnen echter per systeem verschillen (voor een ziekenhuis zijn deze anders dan voor een kantoorgebouw).

De beveiligingswaarde van een gebruikersnaam en wachtwoord is echter beperkt. Zo kan een gebruikersnaam en wachtwoord eenvoudig af te luisteren zijn (of af te kijken) en door verschillende mensen gebruikt worden. Maar er zijn nog andere vormen van authenticatie. Hierbij kunnen we denken aan:

- *security tokens* Een security token is een fysiek 'apparaat' waarmee je kunt inloggen op het GBS. Het meest bekende voorbeeld van een security token is de bankpas. Deze fysieke pas heb je nodig als je wilt telebankieren of pinnen. [Pinnen is ook een vorm van 'two-factor-authentication'. Namelijk authenticatie op basis van iets dat je weet (de pincode) en iets dat je hebt (de pas).];
- *IP-adres filtering* Iedere computer aan het internet heeft een uniek IP-adres. Omdat dit adres (bijna) uniek is, kan dit ook voor authenticatie gebruikt worden. Zo kan bijvoorbeeld op basis van het IP-adres alleen de kantooromgeving toegang gegeven worden tot het GBS en eventueel ook de GBS-leverancier. Hierbij moet wel worden vermeld dat een IP-adres nooit alleen ingezet kan worden, om twee redenen:
- IP-adres filtering identificeert een computer en geen gebruiker;
- een IP-adres is niet volledig uniek. Denk aan meerdere systemen die achter één router (met Network Address Translation) werken en dus hetzelfde IP-adres hebben.

Autorisatie

Autorisatie betekent dat iedere gebruiker een eigen verzameling autorisaties of rechten heeft, die aangeven wat hij wel en niet mag doen. Autorisatie is altijd erg verbonden moet authenticatie: met authenticatie stellen we vast wie de gebruiker is en met autorisatie verbinden we hier conclusies aan door deze gebruiker een aantal rechten te geven. Vergelijk dit met het rijbewijs: een rijbewijs heeft een aantal authenticerende factoren (zoals een foto en handtekening) om vast te stellen wie de eigenaar van dit rijbewijs is. Maar een rijbewijs heeft ook een aantal autoriserende factoren, zoals een 'rijbewijs E bij B' de houder van dit rijbewijs autoriseert om een personenauto met grote aanhanger te besturen. Autorisatie voor een GBS kan als volgt ingevuld worden:

- (MAC) Mandatory Access Control – op basis van het vertrouwelijkheidsniveau van de data (bijvoorbeeld Top Secret) wordt besloten of een gebruiker toegang heeft;
- (DAC) Discretionary Access Control – per gebruiker wordt een aantal rechten toegewezen, zoals gebruiker Jansen mag de klokprogramma's instellen;
- (RBAC) Role Based Access Control –per mogelijke 'rol' in het systeem wordt een aantal rechten verleend. Bijvoorbeeld: een GBS-monteur heeft toegang tot alle installaties.

Voor veel gebouwbeheer systemen zal een DAC een afdoende oplossing zijn. Zodra een GBS echter groter wordt, en de lijst met gebruikers en rechten groeit, is het raadzaam om RBAC toe te passen. Hoewel deze technieken veel mogelijkheden bieden, zijn ze allemaal afhankelijk van een up-to-date whitelist van gebruikers en rechten. Ongeacht welke techniek toegepast wordt, is het van belang dat de lijst met gebruikers bijgehouden wordt en iedere gebruiker voldoende rechten heeft om zijn werk te doen, maar niet meer.

Encryptie

Encryptie heeft als doel te voorkomen dat de communicatie onderschept kan worden door derden. Dit kan zijn door de netwerkleverancier, maar ook door aanvallers op het thuisnetwerk van de gebruiker. Wanneer er geen gebruik gemaakt wordt van encryptie, kan een aanvaller volledig 'meekijken' met de gebruiker en mogelijk ook inlognaam en wachtwoord aflezen. Er zijn in het algemeen twee gebruikelijke technieken om encryptie toe te passen:

- *Https*: dit is een 'veilige' webpagina op het internet. Deze technologie wordt ook toegepast bij telebankieren en e-mail. Het is een gebruikersvriendelijke methode, omdat de gebruiker niets hoeft te doen, behalve het controleren van het 'slotje' in de adresbalk van de browser (zoals bij telebankieren);
- *VPN*: Dit is een techniek om één computer 'virtueel' onderdeel te laten zijn van een ander netwerk. Technisch betekent dit, dat al het netwerkverkeer van dit systeem versleuteld wordt verstuurd naar het GBS en daar verder verstuurd wordt. De meeste VPN-oplossingen hebben ook authenticatie geïmplementeerd, zodat niet iedereen kan inloggen op het GBS-netwerk.

Het gebruik van https is een minimale oplossing en zeker geschikt voor een gemiddeld GBS. Afhankelijk van de mogelijke impact bij misbruik kan er gekozen worden voor een VPN-oplossing.

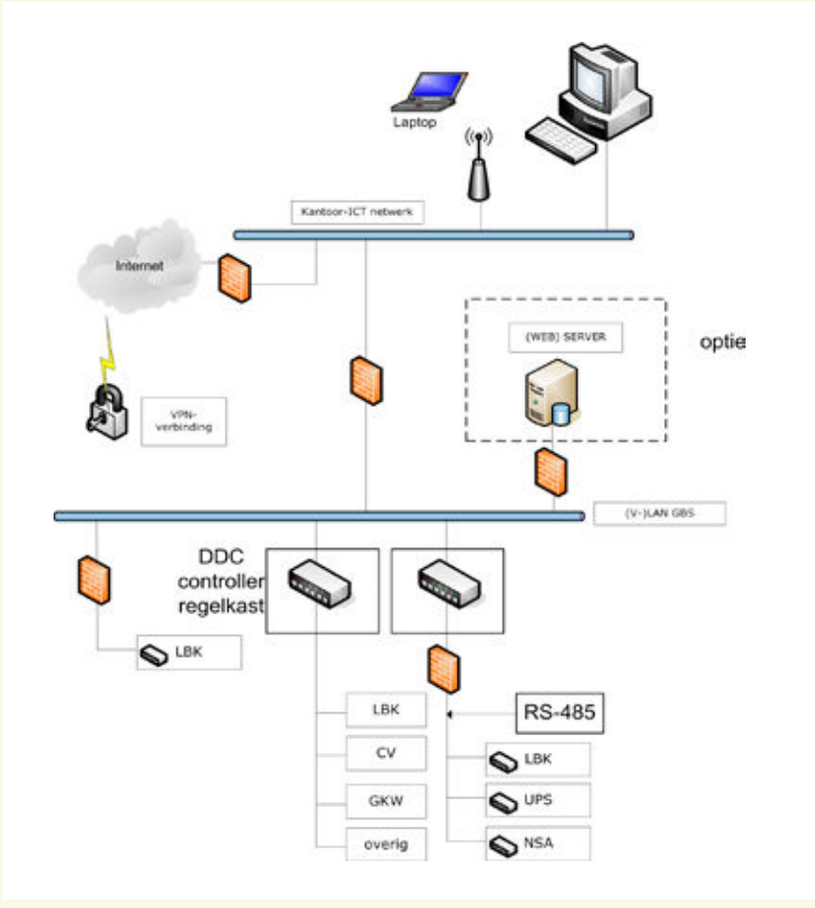
Netwerkscheiding en firewalls

Netwerkscheiding is een techniek om ervoor te zorgen dat niet ieder systeem ieder ander systeem kan bereiken (ze figuur 3). Zo kan er een scheiding tussen de kantoorautomatisering en het GBS gemaakt worden met tussenplaatsing van een firewall. Hierdoor kan niet ieder systeem vanuit de kantoorautomatisering 'zomaar' bij het GBS-netwerk. Voor zeer kritische gebouwbeheersystemen kan er zelfs gekozen worden om deze volledig los te koppelen, zodat ze alleen ter plekke geconfigureerd kunnen worden. Hoewel dit een methode met een grote impact op de gebruikersvriendelijkheid heeft, is het ook zeer doeltreffend voor de beveiliging. De volgende opties bieden variërende niveaus van beveiliging:

- *gescheiden netwerk voor het GBS*, niet van buiten bereikbaar. Dit is de meest ingrijpende vorm, die een grote impact heeft op de gebruikersvriendelijkheid. Hiermee wordt echter de mogelijkheid van een externe (cyber)aanval volledig tegengegaan. Dit is dus met name een goede oplossing voor systemen waarbij de impact van een aanval erg hoog is;
- *gescheiden netwerk voor het GBS*, alleen via firewall bereikbaar. Een minder ingrijpende maatregel is het GBS op een volledig gescheiden netwerk in te richten, maar deze (via een firewall) benaderbaar maken vanuit het kantoorautomatiseringsnetwerk. Op

deze firewall kan vervolgens afgedwongen worden dat alleen specifieke systemen toegang krijgen tot het GBS. En bovendien kan er afgedwongen worden dat alleen de GBS-webinterface bereikbaar is en niet alle andere systemen (zoals LBK's, koelmachines, ed);

- *firewall tussen het GBS-netwerk en de zelfstandig opererende installaties, zoals LBK's*. Met name in grotere netwerken kan het raadzaam zijn om individuele LBK's af te schermen met een firewall of een data-diode. Het voordeel hiervan is dat als een aanvaller het GBS-netwerk bereikt heeft, hij nog steeds niet de vrije hand heeft en gelimiteerd is in zijn aanvallen. Omdat deze firewall zo dicht bij de specifieke apparatuur staat, kan deze ook zeer specifiek filteren;
- *read only Modbus*. Bij toepassing van Modbus voor zelfstandige installaties is er de mogelijkheid om deze bij de inbedrijfstelling in te stellen als 'read only'. Bij BACnet bestaat deze mogelijkheid niet. Via een browse-actie in het GBS kunnen bij BACnet alle datapunten, ook die niet gebruikt worden door het DDC-automatiseringsstation, boven water gehaald worden (dus ook de schrijfpunten) waarna deze installatie alsnog over te nemen is. Daarom is voor BACnet een extra firewall noodzakelijk, zoals die van Tofino of Chipkin. Hiermee kan voorkomen worden dat schrijfpunten benaderd worden dan wel dat er in geschreven kan worden (een setpoint is dan nog wel uitleesbaar maar niet meer te veranderen).
- *firewall voor de GBS-server*. Net als de firewall tussen het GBS-netwerk en de zelfstandig opererende installaties, kan er ook een firewall geplaatst worden voor de GBS-server. Ook hiervoor geldt dat dit met name nuttig is bij grotere en complexere GBS-netwerken, waarbij deze firewall extra bescherming geeft als een aanvaller al is binnengedrongen op het GBS-netwerk.



-Figuur 3- Architecturele beveiligingsmaatregelen voor het GBS

Logging

Hoewel logging de beveiliging niet in eerste instantie verhoogt, is logging wel van meerwaarde bij het herstellen en beperken van de schade en het achterhalen van de dader. Wanneer er geen logging beschikbaar is, is het in het geval van een hack niet mogelijk om te zien wat de aanvaller precies gedaan heeft en bestaat er nooit zekerheid over de vraag of de aanvaller niet meer heeft gedaan dan zichtbaar is geworden.

Enkele gegevens die zeker bijgehouden moeten worden in de logs zijn:

- inlogpogingen (zowel intern als extern, en geslaagd of niet geslaagd);
- connectiedetails van de inlogpogingen (IP-adres, datum, tijd);
- opgevraagde informatie;
- gedane aanpassingen.

Afhankelijk van de toepassing van de beheerde installaties moet in de beveiliging meer of minder ver gegaan worden. Bij het ontwerp van de installaties moeten hierover goede afspraken gemaakt worden met de toekomstige eigenaar van de installaties.

CONCLUSIE

De hedendaagse webbased GBS- en Scada-systemen maken het eenvoudiger voor installateurs, adviseurs en gebouwbeheerders om een open en toegankelijk systeem te hebben, waarmee zij hun legitieme werkzaamheden kunnen uitvoeren om de installaties optimaal te beheren, te onderhouden en te voorzien van de benodigde managementinformatie. Maar deze open systemen zijn ook kwetsbaarder voor mensen met kwade bedoelingen, zoals professionele hackers, kwaadwillende ex-medewerkers en dergelijke. De gevolgen kunnen variëren van ongemak tot financiële en personele rampen. Afhankelijk van de ernst van deze gevolgen, zullen dus ook maatregelen genomen moeten worden. Hierover zullen de betrokken partijen goed overleg moeten voeren. Het is goed als alle betrokken partijen zich hiervan bewust zijn en adequate maatregelen treffen, zodat de zegen van een webbased systeem een zegen blijft en geen vloek wordt.