Auteurs W.C. (Wim) Slabbekoorn [1], J.F. (Jan) Kerdel [2]

1. Systeemarchitect, Manager service bij Sauter Building Control Nederland.
2. Zelfstandig management consultant bij Kerdel Business Development.

ICT-specialisme als kerncompetentie?

Onze moderne wereld is sterk afhankelijk van informatie- en communicatietechnologie (ICT). Hierin zijn netwerken het vitale onderdeel waarmee mensen, organisaties, belangengroepen, overheden en landen met elkaar verbonden worden. Moderne systemen zijn, in tegenstelling tot de beginjaren van ICT, verbonden via een wereldwijd netwerk. Daarbij komt dat technologieën zoals het Internet of Things (IoT) zorgen voor een exponentiële groei van componenten en systemen. Helaas is daarmee de kwetsbaarheid van het netwerk exponentiëel toegenomen. Het moedwillig 'platleggen' van delen van een netwerk, inbraak of fraude kan daadwerkelijk onze maatschappij deels of geheel ontwrichten.

Technisch specialisme is tegenwoordig ondenkbaar zonder toepassing van ICT en gedegen kennis daarvan. Ook bij gebouwautomatiserings- en beheersystemen (GBS) is dit nadrukkelijk het geval. Daarop ligt dan ook de focus in deze artikelenreeks. Kunnen technische bedrijven in de installatiesector bestaan als hun ICT-expertise onvoldoende is of moet worden ingehuurd? Hoe kunnen klanten en gebruikers erop vertrouwen dat hun eigen ICT niet door ons werk wordt verstoord. Welke bijdrage levert een klant hebben om samen succesvol te zijn met ICT? Een vervolgartikel zal in detail ingaan op veiligheid en beveiligingsmaatregelen.

De situatie na intrede van het coronavirus, heeft veel organisaties moeten doen besluiten om veelvuldig van huis uit te werken. In luttele maanden gebruikte het overgrote deel van Nederland digitale beeldcommunicatie voor vergaderen, iets wat nauwelijks gewoonte was. Verbazingwekkend was ook dat de netwerken over het algemeen bestand bleken tegen de enorme toename van het dataverkeer. Netwerkcapaciteit was er kennelijk genoeg. Inmiddels is het hybride-werken ingebed in elke sector die daarvoor geschikt is. Alweer is in korte tijd een nog grotere afhankelijkheid van netwerken ontstaan boven op het bestaande ICT-gebruik voor processen en communicatie.

Cybercriminaliteit

Grote cyberincidenten kunnen en zullen onze maatschappij in het hart raken en communicatie of processen gedurende korte- of langere tijd verlammen. Terugvalopties zijn meestal niet voorhanden of zelfs niet maakbaar zonder ICT. Niet alle incidenten zijn gelijk. Ze richten zich op verschillende doelgroepen en hebben uiteenlopende doelen. Onderstaand overzicht geeft enkele hoofdgroepen weer:

- **Overheid en algemene voorzieningen:** De digitale dreiging van landen in de vorm van spionage en sabotage is enorm. Zeer onlangs werden nog de overheidswebsites van Oekraïne aangevallen met als doel het land te destabiliseren en desinformatie te verspreiden. Ook zijn voorbeelden bekend van aanvallen op energiecentrales.
- **Bedrijfsleven en overheid:** Daarnaast vormen criminelen door inbraak, diefstal en afpersing een permanente dreiging voor organisaties. In veel gevallen leidt tot uitvallen van de kernactiviteit, m.a.w. de corebusiness wordt geraakt.
- **Persoonlijk en bedrijfsleven:** Het 'hengelen' naar persoonlijke of bedrijfsinformatie (phishing) is een vorm waarbij het slachtoffer onbedoeld zelf toegang verleent tot gevoelige persoonlijke- of financiële informatie.

Elke criminele handeling die wordt uitgevoerd via ICT-voorzieningen en met ICT als doelwit wordt cybercriminaliteit genoemd. Cybercriminaliteit is de laatste jaren enorm toegenomen. In de eerste vier maanden van 2021 zijn in Nederland ruim 5000 gevallen gemeld bij de politie, bijna verdubbeld t.o.v. 2020 en bijna verviervoudigd t.o.v. 2019.[1] De (momenteel) meest voorkomende vormen van cybercriminaliteit:

- Denk hierbij aan inbraakpogingen via telefoons, tablets, pc's en laptops. Cybercriminelen gebruiken deze middelen om bij organisaties en individuen binnen te komen met vervalste websites, QR-codes, e-mail, WhatsApp- en sms-berichten. Meestal is het klikken op een link die in het bericht staat funest. Soms ook, wordt een gerichte aanval uitgevoerd op het toegangsmanagement-systeem van de ICT-voorzieningen om zo de bedrijfsvoering van een organisatie te verstoren.

Foto 1: *Cybercriminaliteit is de laatste jaren enorm toegenomen. In de eerste vier maanden van 2021 zijn in Nederland ruim 5000 gevallen gemeld bij de politie, bijna verdubbeld t.o.v. 2020 en bijna verviervoudigd t.o.v. 2019.[1]*

- Een veel voorkomende en effectieve vorm van cybercriminaliteit is ransomware (losgeld principe). Hackers krijgen toegang door gebruikmaking van 'phishing'. Hierbij verstrekt de gebruiker onbedoeld zelf de benodigde gegevens of installeert hij onwetend software om een aanval op zichzelf te starten. Een recent voorbeeld is de ransomware-aanval op MediaMarkt in november 2021 waarbij 43 miljoen euro losgeld werd geëist. Na de onbedoelde toelating wordt op de systemen encryptiesoftware geïnstalleerd die bestanden versleutelt en onbruikbaar maakt. Na betaling ontvangt het slachtoffer een 'sleutel' of decryptiesoftware om weer toegang tot de bestanden te krijgen. Wonderlijk genoeg wordt die toegang in de meeste gevallen daadwerkelijk gegeven, iets wat in de beginjaren van ransomware ontbrak. Kennelijk verwachten criminelen door hun 'goodwill' meer betalingen (in crypto-currency en anoniem) te ontvangen. Ze hopen daarmee dat geld overmaken niet bij voorbaat door het slachtoffers als 'zinloos' wordt opgevat.

Foto 2: *Een veel voorkomende en effectieve vorm van cybercriminaliteit is ransomware (losgeld principe).*

Bedrijfsschade door cyberaanvallen

Digitale aanvallen focussen zich, nog los van het motief, op zwakke punten in de ICT-beveiliging van een organisatie. De schade die wordt veroorzaakt raakt meestal de plaatsen die elementair zijn voor een organisatie:

- **Financieel:** Als een aanvaller de dagelijkse bedrijfsvoering van een organisatie weet te verstoren, zoals het verlies van een orderbestand, administratie of boekhouding, zal dat enorme financiële schade veroorzaken.
- **Reputatie:** De negatieve publiciteit als gevolg van ICT-incidenten levert imagoschade op die voorkomen had kunnen worden. Reputatie is niet snel hersteld zoals we weten.
- **Vertrouwen:** Een gevolg van reputatieschade is het verlies van vertrouwen in de organisatie. Veel organisaties bouwen jarenlang aan hun relaties met partners en klanten. Wanneer afnemers niet tevreden zijn met het niveau van de maatregelen die een organisatie neemt om gegevens en systemen te beschermen, gaat het vertrouwen verloren en zoekt men naar andere toeleveranciers.

Weerbaarheid

Het treffen van voldoende basismaatregelen is een eerste stap naar digitale weerbaarheid. De Engelse term 'resilience' wordt hier vaak gebruikt. Het zijn de eerste barrières waarmee schade beperkt en systemen sneller hersteld kunnen worden. Essentieel is dat de basismaatregelen consequent in alle systemen toegepast worden. Door onderlinge verbindingen tussen de verschillende systemen wordt, zoals bekend, de sterkte van de keten door de zwakste schakel bepaald. Ook zien we dat gebruikers zich vaak (onbewust) onveilig gedragen binnen de digitale omgevingen waardoor juist mogelijkheden gecreëerd worden voor kwaadwillenden. Cyberaanvallen worden vaak mogelijk door 'gaten' in de basismaatregelen! De stelling is dan ook dat goede samenwerking tussen de betrokken partijen en het gebruik van kwaliteitsproducten zullen leiden tot een succesvol project.

Succesfactoren voor weerbare digitale systemen bij de eindgebruiker

De praktijk is dat organisaties hun weerbaarheid vaak onvoldoende op orde hebben. De oorzaken kunnen liggen in onvoldoende bewustzijn, onvoldoende supervisie op het gebruik, ontbrekende deskundigheid, toeleveranties van onvoldoende kwaliteit, onvoldoende of falend onderhoud (onder andere door kostenbeperking). Hierdoor worden deze organisaties extra kwetsbaar. TNO onderzocht welke organisatorische succesfactoren voor het digitaal weerbaarder maken van systemen bestaan. Het onderzoek richtte zich specifiek op Industriële Controle Systemen en is daarmee ook toepasbaar op gebouwautomatiseringssystemen. De navolgende succesfactoren zijn *bedoeld voor een eindgebruiker* en ze tonen aan hoe belangrijk de eigen inbreng is voor een succesvol ICT. Het volledige rapport met alle succesfactoren is beschikbaar via de site van het Nationaal Cyber Security Center en TNO.[2]

Foto 3: *Een van de succesfactoren: houd regelmatig een interne audit.*

Bewustzijnsvergroting GBS kwetsbaarheden

- Vertaal securitydreiging naar procesrisico; wat kan het primaire proces verstoren? Kwantificeer de potentiële impact.
- ICT-security is een belangrijk onderdeel van de primaire bedrijfsprocessen. Benoem digitale weerbaarheid als jaarlijkse bedrijfsdoelstelling.
- Betrek operationele managers bij het bepalen van risico's en benodigde investering.
- Betrek het management bij operationele audit processen en breng de uitkomsten bij het senior management onder de aandacht.

Basisbeveiligingsmaatregelen op orde

- Maak een keuze voor een overkoepelende standaard of framework om kantoorautomatisering en technische automatisering (onder andere gebouwbeheersystemen) veilig in te richten. IT- en TD-medewerkers moeten de gekozen standaard gezamenlijk ondersteunen.
- Vertaalde standaarden op basis van wensen en eisen naar de eigen organisatie. Dit vraagt capaciteit, maar betaalt zich terug.
- Houd contact met branchegenoten over standaarden en praktijk.

Passende Beheer en Onderhoudsactiviteiten

- Maak een vervangingsplan en stem de investeringen hierop af (ICT kent vaak een cyclus van 3 jaar).
- Denk na over leveranciers. Weeg de voor- en nadelen van één enkele leverancier af tegen het hebben van meerdere.
- Beschik als leidinggevende over kennis op het gebied van ICT om met externe leveranciers te kunnen werken.
- Sluit aan bij bestaande risicomanagementprocessen in de eigen organisatie.
- Zorg voor bewustwording over het belang en de toegevoegde waarde van een weerbaar digitaal systeem. Dit zijn onder andere de punten uit dit overzicht.
- Houd regelmatig een interne audit (bijvoorbeeld phishingmail aan collega's).
- Laat een gecertificeerd bureau regelmatig een 'Pentest' (penetratie-test) doen. Hierbij wordt het begrip 'weerbaarheid' aan de praktijk getoetst.

Verklein de kloof tussen IT en TD

- Het starten van gezamenlijk overleg tussen IT en een Technische Dienst of gebruikersgroep.
- Verschillen in functiewaarderingen bij IT- en TD-medewerkers die gelijkwaardig werk doen beïnvloeden de samenwerking negatief.
- Laat IT- en TD-afdelingen samen oefeningen uitvoeren en scenario's opstellen.

Verhoog ICT-kennis en -kunde

- Deel de actuele security status met het management.
- Zorg dat het management het delen van ervaring en kennis met andere bedrijven en organisaties faciliteert.
- Maak kennisdeling onderdeel van de functioneringsgesprekken.

ISO 27001

Certificering ISO27001

Informatiebeveiliging is niet meer weg te denken uit een organisatie. Omtrent de persoonsgegevens zijn de zaken wettelijk geregeld in de AVG (Algemene Verordening Gegevensbescherming, mei 2018), maar daarnaast is er veel meer informatie die ook beveiligd dient te worden. Het ISO 27001 certificaat is bedoeld om zekerheid te geven over de zorgvuldige omgang met alle privacygegevens en te borgen dat informatiebeveiliging serieus wordt genomen. Door middel van procedures en processen wordt de omgang met gegevens vastgelegd en via jaarlijkse audits geborgd. Het ISO 27001 certificaat kent een geldigheid van 3 jaar, waarna her-certificering plaats vindt.

Ook binnen de gebouwautomatisering (waarover hierna meer) wordt dagelijks gewerkt met informatie van en over klanten en hebben toeleveranciers toegang tot (delen van) de systemen van een organisatie. Daarom zal een ISO27001-certificering steeds vaker het uitgangspunt zijn bij het aangaan van overeenkomsten voor leveringen, service en onderhoud.

Praktische Cyber security voor gebouwautomatisering

Cyber security in gebouwautomatisering is zeer belangrijk geworden. Intelligentie wordt op een steeds lager niveau geïmplementeerd zelfs tot op het laagste niveau in sensoren en actuatoren en steeds vaker aangesloten op het bedrijfsnetwerk. Ook is de integratie van het gebouwbeheersysteem in de IT-omgeving van de klant aan de orde en zijn systemen van 'buitenaf' benaderbaar. De beveiliging van gebouwautomatisering is daardoor cruciaal, want zelfs door een 'exploit' in een in een IoT-device kan ongeoorloofde toegang tot systemen of componenten worden verkregen. Een exploit is een klein stukje programmacode waarmee (bekende) zwakten in de software van een systeem of component worden misbruikt. De makers zijn dus zeer goed op de hoogte van het systeem dat ze gaan aanvallen.

Wanneer op de gebouwautomatisering 'alleen' verwarmings-, koelings- en ventilatie installaties aangesloten zijn, is het risico meestal klein tot middelgroot. Echter wanneer deze installaties worden ingezet voor belangrijke primaire processen (denk aan OK's, laboratoria, meet- en testopstellingen) dan kan dit tot grote schade en gevaar voor mensen leiden). Het risico bij licht, toegangscontrole, deurvergrendeling e.d. heeft te maken veiligheid en beveiliging en is daarom altijd hoog. Ook is duidelijk dat het risico bij kleinere, niet-openbare gebouwen anders is dan bij centrale, drukbezochte of beveiligingsgevoelige gebouwen. Bij deze laatste zou een bedreiging in extreme gevallen tot digitaal ondersteunde gewelddadigheid of aanslagen kunnen leiden. De beveiligingsmaatregelen moeten daarom op het risico afgestemd zijn. In ICT-termen is de beveiliging op te splitsen in twee belangrijke vlakken:

- **Network security:** Netwerkbeveiliging concentreert zich op gebruikers en devices die toegang moeten hebben tot data en applicaties. Maar ook, welke data moet voor wie afgeschermd zijn. Een goed toegangsbeleid (autorisatiebeleid) waarin toegang en rechten aan gebruikers en devices worden toegekend is hierbij essentieel. Ook wordt de rechtmatigheid getoetst, met andere woorden: is een gebruiker werkelijk dat wat hij beweert te zijn (authenticatie)? Vervolgens wordt door zogeheten 'firewalls' het verkeer in het netwerk geregeld waarbij zowel gebruikers als diensten worden gescreend. Ook kan een firewall inhoud scannen op potentieel gevaarlijke inhoud (virussen, data, exploits).
- **Endpoint security:** Laptops, pc's, servers en mobiele devices zijn de meest kwetsbare componenten binnen de infrastructuur en het meest voorkomende doelwit van malware, data diefstal en ransomware. Om de snel ontwikkelende bedreigingen voor te blijven wordt kunstmatige intelligentie (AI) toegepast waarmee voortdurend veranderende aanvalstechnieken worden weerstaan.

Op deze twee basisgebieden dienen op verschillende niveaus technische- en organisatorische maatregelen te worden genomen om veiligheidsvoorzieningen aan te brengen, in te richten en/of te onderhouden. Onder regie van de aannemende partij wordt een projectplan opgezet. Zowel toeleverende partijen als de eindklant hebben zelf hebben een belangrijke rol in de ICT-security als geheel. Onderstaande paragrafen geven compact weer wat op dit vlak moet worden afgesproken en bewaakt. Hieruit volgt ook dat een aannemende partij regisseur is van het proces en zelf beschikt over diepgaande kennis van ICT en ICT-security.

Maatregelen op het niveau van de fabrikant

Dit betreft geleverde producten met een (geïntegreerd) besturingssysteem zoals automatiseringsstations, netwerkapparatuur, eventuele intelligente sensoren, maar ook software voor het managementniveau zoals GBS-software, energieanalyse- en energiemanagementsoftware. Alle apparatuur en software, waartoe gebruikers toegang hebben (webservers, configuratietoegangen enz.), moeten beveiligd worden met een wachtwoordbeveiliging.De complexiteit van het wachtwoord, automatische logout, time out na diverse foutieve inlogpogingen en een periodieke wijziging van het wachtwoord. Een ingesteld standaard admin-account inclusief wachtwoord dient na inbedrijfsstelling te worden gewijzigd. Hackeraanvallen gebaseerd op standaardwachtwoorden zijn veel voorkomend doordat deze op het internet zijn terug te vinden. Als een technicus van de GBS-fabrikant het bedrijf verlaat moet ook het admin-account worden gewijzigd.

Voor veilige communicatie met webservers en interfaces moeten de producten in staat zijn om telkens de laatste protocolversies (SSL/TLS en HTTPS en SSH) te gebruiken. Systemen moeten een 'audit trail' (registratie van gebruikershandelingen) ondersteunen, waarbij de registratie beveiligd kan worden met een handtekening. Dit helpt bij het zoeken wie de aanvaller/veroorzaker was, maar ook waar schade is ontstaan en wat de gevolgen zijn. Security updates en upgrades moeten door de fabrikant beschikbaar worden gesteld.

Maatregelen op het niveau van project engineering

Tijdens de engineering van een gebouwautomatiseringssysteem wordt de IT-infrastructuur en de beveiliging vastgelegd. Ook worden de maatregelen gepland voor het geval een probleem (als gevolg van een aanval) optreedt. Risico's zijn niet voor ieder gebouwtype en GBS gelijk. Een projectspecifieke risicoanalyse is noodzakelijk. Factoren die daarbij een rol spelen zijn o.a. de functie van het gebouw en de omvang van het GBS (klimaat, licht, (brand-) deuren, toegangssystemen). De bestaande IP-netwerkinfrastructuur van een gebouw kan worden gebruikt mits een logische scheiding wordt toegepast, waardoor een subnet ontstaat (een zogeheten eigen VLAN-segment). De netwerktoegangen en subnetten dienen door eigen firewalls te worden beschermd. Door apparatuur en gebruikers op afstand via een zogeheten VPN (Virtual Private Network) met het gebouwautomatiseringssysteem te verbinden, wordt de veiligheid substantieel verhoogd. Een VPN bouwt een gecodeerde verbinding, een zogeheten tunnel, op tussen externe apparaten en het interne netwerk.

'Switches' zorgen voor de fysieke verbinding met elk netwerk-apparaat met het netwerk. Wanneer het GBS gebruik maakt van het netwerk van de klant, kies dan exact dezelfde switches. Switches met geïntegreerde beveiligingsfunctie worden aanbevolen omdat ze dataverkeer naar iedere deelnemer kunnen filteren. De switch zorgt dat iedere deelnemer uitsluitend de datapakketten ontvangt die ook echt voor hem bestemd zijn. Tijdens de engineeringsfase wordt vastgelegd welke bescherming tegen malware op servers en PC's moet worden geïnstalleerd. Om permanent effectief te blijven dient de malwarebescherming up to date gehouden te worden.

Een goede back-up functie voor elk gebouwautomatiseringssysteem spreekt voor zich. Vooral ook omdat het GBS na een aanval niet meer functioneert. Een duidelijke herstelprocedure moet op papier staan. Backups moeten ook weer veilig kunnen worden bewaard. Servers, schakelkasten, aansluitpunten en de communicatieapparatuur dienen fysiek beschermd te zijn tegen ongeoorloofde toegang. Ongeautoriseerde toegang tot ethernet-, USB- en configuratie-aansluitingen van computers, automatiseringsstations, routers ed. mag in geen geval mogelijk zijn.

Maatregelen op het niveau van inbedrijfstelling

Tijdens de inbedrijfstelling moeten de specificaties van het ontwerp met betrekking tot IT-beveiliging gerealiseerd en aangevuld worden. Alle veiligheidsrelevante parameters (toegangsrechten, wachtwoorden, poorten enz.) moeten worden ingesteld en waar mogelijk moeten de maatregelen getest worden op hun werking. Voor de exploitatiefase moeten op het gebied van onderhoud service level agreements (SLA) worden ingericht en toekomstige gebruikers worden geschoold.

Bij de inbedrijfstelling worden voor alle relevante apparaten, computers en systemen gebruikers/gebruikersgroepen aangemaakt en hun rechten ingesteld. Hoe beter en nauwkeuriger de rechten aan de taken van de gebruikers/gebruikersgroepen worden aangepast (dat

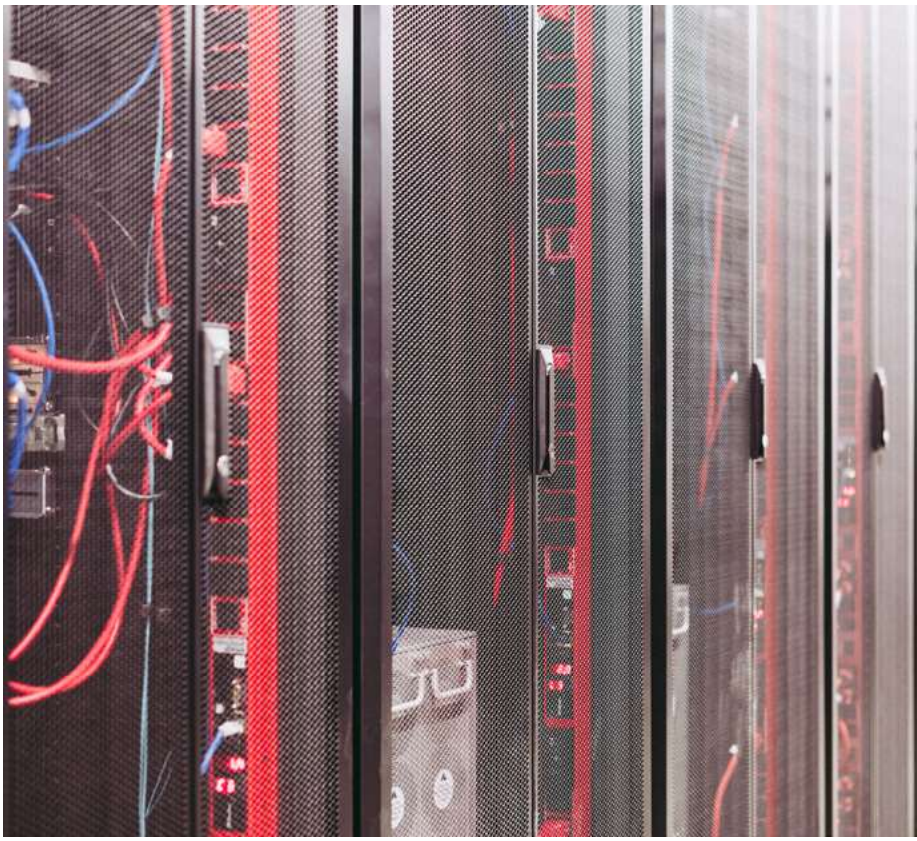

Foto 4: *Servers, schakelkasten, aansluitpunten en de communicatieapparatuur dienen fysiek beschermd te zijn tegen ongeoorloofde toegang.*

wil zeggen beperkt/geminimaliseerd), hoe kleiner de kans op doelgerichte aanvallen, maar ook op onbedoelde bedieningsfouten.
De audit-trail moet bij de inbedrijfstelling geactiveerd en geconfigureerd worden. Minimaal alle gebruikersactiviteiten, wijzigingen in gegevens en alle schakel- en instelacties dienen geregistreerd te worden.

Afsluitende en geteste werkvoorschriften en gedragsrichtlijnen (Standard Operating Procedures, SOP) met betrekking tot de IT-beveiliging moeten vanaf het begin van het gebruik van een systeem op twee niveaus beschikbaar zijn: enerzijds voorschriften voor het normale bedrijf, die er mede voor zorgen dat alle beveiligingselementen permanent functioneren en op de actueelste stand worden gehouden. Voorschriften voor het geval van een aanval/storing met de procedures/informatie voor de opheldering/snelle analyse, de beperking van schade en het verhelpen van schade.

Maatregelen op onderhoudsniveau

Het doel van onderhoud (m.b.t. IT-beveiliging) is alle geïnstalleerde beveiligings- en beveiligde apparaten periodiek te onderhouden, bij te werken en het systeem aan te passen aan de laatste beveiligingsontwikkelingen. Apparatuur en programma's, met name pc's, moeten verplicht worden bijgewerkt met updates van de fabrikant (zowel drivers als Microsoft). Technische ontwikkelingen vragen soms om upgrades en nieuwere en uitgebreidere versies.De hardware en software die in gebouwautomatiseringssystemen is geïnstalleerd, heeft over het algemeen een veel langere levensduur dan commerciële IT-producten. Ontwikkelingen kunnen het nodig maken om grotere, systeemaanpassingen of vervangingen door te voeren. Om dit blijvend te garanderen is een structurele controle nodig. De procedures bij een aanval of verstoring dienen regelmatig te worden geoefend. Laat als eigenaar van het GBS een onafhankelijk en gecertificeerd bureau regelmatig een 'Pentest' (penetratie-test) uitvoeren.

Maatregelen op gebruikersniveau

De mate van complexiteit van wachtwoorden wordt op basis van de risico vastgelegd. Echter wordt ook van gebruikers gevraagd hun wachtwoord zo te kiezen, dat dit moeilijk te achterhalen is. Over het algemeen is voor de veiligheid van wachtwoorden niet alleen de complexiteit, maar vooral ook de lengte bepalend. Zeer goed

Foto 5: *Whitepaper IT Security in Building Automation.*

geschikt zijn bijvoorbeeld zinnen. Geautomatiseerde back-ups moeten op correcte en volledige werking worden gecontroleerd. Omdat back-upbestanden vaak kopieën van vertrouwelijke gegevens bevatten, moeten ze goed beveiligd worden bewaard. Engineeringsdocumenten zoals systeemtopologieën, beveiligingsconcepten enz. zijn voor een aanvaller met kwade bedoelingen zeer informatief en moeten eveneens veilig worden bewaard.

Bedieners van het GBS moeten zich bewust zijn van mogelijke gevaren, rondom het onderwerp IT-beveiliging en worden geïnformeerd in separate trainingen. Het is van groot belang ze te motiveren om waakzaam te zijn. Afwijkingen en ongebruikelijke zaken moeten worden herkend en serieus worden genomen.

Bewerkt vanuit: Whitepaper IT Security in Building Automation: https://www.sauterautomation.co.uk/wp-content/uploads/sites/13/2021/03/1103158-371.pdf

Referenties

1. Bron: www.vpngids.nl
2. Bewerkt op basis van informatie Nationaal Cyber Security Centrum (ncsc.nl): www.ncsc.nl/onderzoek/onderzoeksresultaten/succesfactoren-voor-weerbare-industriele-controlesystemen