Tekst: Danny Hermans - Coördinator technologie & regelgeving
Versie: 03/2019 – Bijgewerkt: 02/2024

NTN 178-C Alarm systems - Remote services - Requirements on the organization of the services

Situering van de NTN 178-C
Europese bekommernis om cybersecurity

Met het oog op een dynamisch veranderend dreigingslandschap en voortbouwend op de herziening van de cybersecurity-strategie van 2013 in de EU, was de aanpak van de cybersecurity-gevaren een van de drie uitdagingen die werden geïdentificeerd in de tussentijdse evaluatie van de digitale eengemaakte markt.
Op 13 september 2017 heeft de Europese Commissie een cyberbeveiligingspakket goedgekeurd. Het pakket bouwt voort op bestaande instrumenten en presenteert nieuwe initiatieven om de cyberveiligheid en reactie van de EU verder te verbeteren.

Hierin heeft het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (ENISA) een belangrijke rol te spelen. Dat Agentschap wordt echter beperkt door zijn huidige mandaat. De Commissie presenteert een ambitieus hervormingsvoorstel, met inbegrip van een permanent mandaat voor het agentschap om ervoor te zorgen dat ENISA-steun kan verlenen aan lidstaten, EU-instellingen en bedrijven op sleutelgebieden, waaronder de tenuitvoerlegging van de NIB-richtlijn. Het zal ook bijdragen aan een intensievere operationele samenwerking en crisisbeheersing in de hele EU.

De NIB-richtlijn (richtlijn over de beveiliging van netwerk- en informatiesystemen) die in juli 2016 is aangenomen, moet snel worden geïmplementeerd. Dit zal worden vergemakkelijkt dankzij richtsnoeren van de Commissie over de manier waarop de richtlijn in de praktijk moet werken en aanvullende interpretatie van specifieke bepalingen in de September 2017-pakket.

De groei van de cyberbeveiligingsmarkt in de EU - op het gebied van producten, diensten en processen - wordt op een aantal manieren tegengehouden, ook vanwege het ontbreken van een cyberbeveiligingscertificeringssysteem dat in de hele EU wordt erkend. De Commissie komt daarom met een voorstel om een EU-certificeringskader op te zetten waarin ENISA centraal staat. Er zal ook een gezamenlijk initiatief van de Commissie en de industrie worden geïnitieerd om een "zorgplicht" -beginsel te definiëren om de kwetsbaarheid van producten en software te verminderen en een "security by design" -benadering voor alle aangesloten apparaten te bevorderen.

Ook in de brand- en diefstalbeveiligingssystemen alsook in CCTV

Het internet der dingen en de nieuwe communicatiemiddelen (bekabeld of draadloos) zijn doorgedrongen tot de wereld van de brand- en diefstalbeveiligingssystemen. Daar waar vroeger de diensten op afstand zich beperkten tot de bediening en het beheer van foutberichten maakt de huidige technologie de toegang op afstand tot de essentiële functies van het alarmsysteem zoals het activeren, programmeren, definiëren van parameters, oplossen van problemen, uitvoeren van bepaalde onderhoudsactiviteiten. Afstandsbedieningen vullen alzo het bezoek ter plaatse van bevoegde personen aan en bieden nieuwe opportuniteiten aan de gebruikers. Door de kortere reactietijd zijn een grotere betrouwbaarheid en beschikbaarheid van het systeem een logisch gevolg.
Ook de installateur-dienstverlener die deze diensten op afstand aanbiedt, krijgt een grotere beschikbaarheid van zijn personeel omdat zij minder tijd verliezen tijdens verplaatsingen.

Normen en eisen met betrekking tot het toepassen en veilig gebruik van afstandsbedieningen van deze systemen door eindgebruikers en installateurs-dienstverleners ontbreken helaas nog in de meeste landen. Eisen voor het ontwerp en de werkprocedures zijn nochtans heel belangrijk om te voorkomen dat ongewenste en ontoelaatbare handelingen vanop afstand gebeuren zoals het deactiveren van deze systemen of het ongewenst meekijken via het camerabewakingssysteem.

Binnen Euralarm, zijnde de Europese vereniging van fabrikanten van brand- en diefstalbeveiligingssystemen, is een nota opgesteld over deze materie. ALIA is lid van Euralarm. Deze nota zal als basis gebruikt worden voor een Europese norm die zal ontwikkeld worden binnen CEN/CENELEC JTC 4: Services for fire safety and security. Binnen dit technisch committee is reeds een eerste dienstennorm, de NBN EN 16763: 2016 Services for fire safety and security, gepubliceerd waarin de eisen vastgelegd zijn, waaraan een installateur-dienstverlener van brand- en diefstalbeveiligingssystemen moet voldoen. Zo worden in deze norm onder andere de vereiste mensprofielen en materiële middelen opgesomd. Deze norm is niet geharmoniseerd voor de Europese Dienstenrichtlijn (Richtlijn 2006/123/EG), ook wel de Bolkesteinrichtlijn genoemd.

In 2018 is vanuit JTC 4 de vraag gekomen om een WG op te richten om een norm voor “Remote Services for fire safety and securitysystems”, dit onder impuls van Euralarm, dat reeds in 2016 een handleiding, ”Guidelines-Alarm Systems-Remote Services”, hierover had opgesteld. Deze handleiding zal als uitgangsdocument dienen voor de toekomstige Europese norm. Omdat er een steeds grotere nood is aan duidelijke voorschriften met betrekking tot cybersecurity, denken we maar aan de regelmatig weerkerende berichten over gehackte (camera)systemen, heeft ANPI een technische nota opgesteld, de NTN 178-C Alarm systems-Remote services. Requirements on the organization of the services. Dit document is gebaseerd op de handleiding van Euralarm.

NTN 178-C
Over NTN 178-C

Omdat in de wereld van de dataoverdracht en de beveiliging ervan veel specifieke Engelse technologie gebruikt wordt, is de technische nota in de originele Engelse tekst opgesteld.

Inhoudelijk is het een technisch document opgesteld volgens de structuur van een norm met de gekende hoofdstukken zoals Inleiding, de scope, normatieve referenties, definities en afkortingen, gemeenschappelijke eisen, toepassing (brandalarm, spraakalarm, inbraakalarm, videobewaking, toegangscontrole, sociaal alarm, …) specifieke eisen.

De scope

In de scope geeft aan dat het document de minimumeisen bepaalt voor een veilige toegang op afstand voor de volgende systemen:

- Brandbeveiligingssystemen in de brede zin
- Inbraakbeveiligingssystemen in de brede zin
- Sociale alarmsystemen
- Een combinatie van de hierboven vermelde systemen

Het document houdt zich niet bezig met:

- De alarmtransmissie infrastructuur
- Andere middelen voor toegang op afstand
- Het gebruik van toegang op afstand door de eindgebruikers
- Het toezicht op het gebruik van het systeem door de eindgebruikers

Gemeenschappelijke eisen

In de gemeenschappelijke eisen wordt om te beginnen opgelegd om het risiconiveau te bepalen op basis van minstens de volgende gegevens:

- Toegelaten handelingen en beveiligingsmaatregelen
- Locatie/klant specifieke eisen
- Toepasbare handleidingen en reglementeringen voor de apparatuur in de toepassing
- Toepasbare wetten en verordeningen voor de persoonlijke levenssfeer en gegevensbescherming
- Cybersecurity handleidingen

Wat overeengekomen wordt en hoe de verantwoordelijkheden komen te liggen moet duidelijk vastgelegd worden tussen de betrokken partijen, zijnde de dienstverlener op afstand en de eindgebruiker/klant. Zaken die hierin zeker aan bod moeten komen zijn over welke installatie het gaat, de handelingen en tests die op afstand moeten/mogen worden uitgevoerd onder welke omstandigheden, ook automatische handelingen, het proces van de klantautorisaties nodig voor iedere handeling, de middelen om een controletraject van alle externe acties bij te behouden en de bewaarperiode, gegevens afhandeling en opslag, eventueel andere eisen vanwege de verzekering, overheden, tijdslimieten, grenzen van de verantwoordelijkheid van de dienstverlener op afstand.

De eisen voor het alarmsysteem worden eveneens aangehaald. Een belangrijke melding in deze is dat een dienst op afstand niet kan beschouwd worden als een vervanging van het onderhoud op het terrein. Sommige vitale controles kunnen immers alleen op het terrein uitgevoerd worden en bij gevolg blijven reguliere bezoeken ter plaatse essentieel. Er moet een indicatie ter plaatse aanwezig zijn indien een verbinding op afstand actief is. Elke connectie moet in een logboek bijgehouden worden. Een inactieve connectie moet beperkt zijn in de tijd, bij voorbeeld 30 minuten. Activatie van alarmsystemen op afstand moet tot een minimum beperkt worden. Bij overdracht, al dan niet gewild van beeld en geluid, moet de nodige aandacht gegeven worden aan de voorschriften voor de persoonlijke levenssfeer. Bij geïntegreerde of gecombineerde systemen moeten alle eisen voor de systemen gerespecteerd worden en is het mogelijk dat enkel tot een deel toegang op afstand kan.

Eisen voor het veiligheidsplatform

Van dit platform bevindt zich een blokdiagram in het document. Het bevat het Informatie Overdracht Systeem met zijn verbindingen en het Veiligheidsplatform. Dat laatste is afhankelijk van het type toegang op afstand en de types van diensten. Voor de beveiligingsmaatregelen per installatietype (hold-up en inbraak, brand, videobewaking, toegangscontrole, …) wordt verwezen naar de normenreeks ISO/IEC/JTC1/27000. Alleen personen die vallen onder de controle van de dienstverlener op afstand, zijnde geautoriseerde personen, mogen toegang hebben tot het Veiligheidsplatform en de applicatie op afstand. Dit personeel moet adequaat opgeleid worden voor het gebruik van de applicatie om de nodige competenties te verwerven.

Eisen voor het Informatie Overdracht Systeem (ITS)

De veiligheid van het ITS wordt ondersteund door de gekende beveiligingsmaatregelen zoals verificatie, encryptie, substitutiebeveiliging en traceerbaarheid. Een alarm heeft voorrang op een handeling op afstand, eventueel gebruik makend van meersignalen overdrachtskanalen.

Eisen voor de uitvoering van diensten op afstand

De klant moet op de hoogte zijn als dergelijke testen gebeuren. Zij mogen niet uitgevoerd worden tijdens een alarmtoestand. Hierin worden eveneens de voorwaarden beschreven voor het uitvoeren van configuratie/parameter wijzigingen, systeemcontroles op afstand al dan niet geautomatiseerd.

Toepassing specifieke eisen

In dit deel van de norm worden per toepassing (brandalarm, spraakalarm, inbraakalarm, toegangscontrole, …) nog specifieke eisen opgesomd zoals welke controles en acties mogen er op afstand op een bepaalde toepassing uitgevoerd worden, hoe moet een verbinding tot stand worden gebracht, met welke frequentie mag er gecontroleerd worden, welke ondersteuning op afstand kan.

Besluit

Cybersecurity verdient zeker de nodige aandacht in een wereld waar digitalisatie en interconnectie met rasse schreden verder evolueert. Dit is ook zo in de beveiligingssystemen. Diensten op afstand maken steeds meer deel van het dienstenaanbod. Het is dan ook belangrijk dat het gehele systeem van dienstverlener tot klant ontworpen en gebouwd wordt volgens de regels van goed vakmanschap. Goede afspraken over verantwoordelijkheden en over de toegelaten handelingen op afstand maken daar deel van uit. Regels van goed vakmanschap, zinde de normen, over deze materie zijn schaars. NTN 178-C die gebaseerd is op een handleiding van Euralarm over deze materie, is een goede aanzet om deze leegte op te vullen. Een groot nadeel in dit document is echter dat de te nemen maatregelen afhangen van het risiconiveau dat bepaald wordt op basis van een risicobeoordeling. Hoe deze laatste moet uitgevoerd worden en welke niveaus er zijn, daarover blijft het document te vaag. Eenduidigheid ontbreekt dus en bijgevolg moet het document verder aangevuld of uitgewerkt worden met betrekking tot deze risicobeoordeling en risiconiveaus, en dit per toepassing (brandalarm, spraakalarm, inbraakalarm, toegangscontrole, …).

*****