Texte : Danny Hermans - Coordinateur technologie et réglementation
Version : 03/2019 – Mise à jour : 02/2024

NTN 178-C Systèmes d'alarme - Services à distance - Exigences pour l'organisation des services

Situation de la norme NTN 178-C
La préoccupation européenne à propos de la cybersécurité

Dans le contexte de l'évolution dynamique des menaces et suite à la révision de la stratégie de cybersécurité de 2013 dans l'UE, l'approche des risques liés à la cybersécurité constituait un des trois défis identifiés dans l'évaluation intermédiaire du marché unique numérique.

Le 13 septembre 2017, la Commission Européenne a approuvé un train de mesures relatives à la cybersécurité. Cet ensemble de mesures vient compléter les instruments existants et présente de nouvelles initiatives pour améliorer encore la cybersécurité et la réaction de l'UE.

Dans ce cadre, l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) a un rôle important à jouer. Mais cette agence se trouve entravée par les limites de son mandat actuel. La Commission présente une proposition ambitieuse de réforme incluant l'octroi d'un mandat permanent à l'ENISA afin de lui permettre d'offrir son soutien aux états membres, institutions de l'UE et entreprises dans des domaines clés, notamment la mise en œuvre de la directive NIS.
Cela contribuera également à une collaboration opérationnelle et une gestion de crise plus efficaces dans l'ensemble de l'UE.

Adoptée en juillet 2016, la Directive NIS (directive concernant la sécurité des réseaux et systèmes d'information) doit être rapidement déployée. Ce déploiement va être facilité par des lignes directrices de la Commission relatives à la manière dont la directive doit fonctionner dans la pratique, et par une interprétation complémentaire de dispositions spécifiques du train de mesures de septembre 2017.

La croissance du marché de la cybersécurité dans l'UE - dans le domaine des produits, services et processus, se heurte à un certain nombre d'entraves, notamment en raison de l'absence d'un système de certification de la cybersécurité reconnu dans toute l'UE. C'est pour cela que la Commission formule une proposition visant à mettre en place un cadre de certification UE dans lequel l'ENISA jouerait un rôle central.
Une initiative conjointe de la Commission et de l'industrie sera également initiée pour définir un principe « d'obligation de soins » afin de réduire la vulnérabilité des produits et logiciels et de favoriser une approche dite « security by design » pour tous les appareils connectés.

Ce sera également le cas dans le domaine des systèmes de protection contre l'incendie et le vol, ainsi que de la vidéosurveillance (CCTV).

L'Internet des objets et les nouveaux moyens de communication (filaires ou sans fil) se sont désormais imposés jusque dans le secteur des systèmes de protection contre l'incendie et le vol. Alors que les services à distance se limitaient jadis à la commande et la gestion de messages d'erreur, la technologie actuelle permet d'accéder à distance aux fonctions essentielles du système d'alarme : activation, programmation ou définition de paramètres, résolution de problèmes, exécution de certaines activités d'entretien. En d'autres termes, les télécommandes complètent la visite sur place de techniciens compétents et offrent de nouvelles opportunités aux utilisateurs. Le délai de réaction raccourci entraîne logiquement une amélioration de la fiabilité et de la disponibilité du système. Quant à l'installateur/prestataire de services offrant ces services à distance, il bénéficie d'une plus grande disponibilité de son personnel, qui perd moins de temps en déplacements.

Dans la plupart des pays, il n'existe malheureusement pas de normes et d'exigences concernant l'application et l'utilisation sûre des télécommandes de ces systèmes par les utilisateurs finaux et installateurs/prestataires de services. Les exigences de conception et les procédures de travail sont cependant très importantes pour éviter les manipulations indésirables et inadmissibles à distance, comme la désactivation de ces systèmes ou une surveillance indésirable via le système de vidéosurveillance.

Une note a été rédigée sur ce thème par Euralarm, l'association de l'industrie de la sécurité et de la protection incendie. ALIA est membre d'Euralarm. Cette note servira de base à une norme européenne qui sera développée au sein de CEN/CENELEC JTC 4 : Services de sécurité incendie et de sécurité. Une première note de service a déjà été publiée dans cette commission technique. Il s'agit de la NBN EN 16763 : 2016 Prestations de services pour les systèmes de sécurité incendie et les systèmes de sûreté. Elle fixe les exigences auxquelles un installateur/prestataire de services de systèmes de protection contre l'incendie

et le vol doit répondre. C'est ainsi que les profils personnels et les équipements matériels exigés sont énumérés dans cette norme. Cette norme n'est pas harmonisée pour la Directive de services européenne (Directive 2006/123/CE), également appelée directive Bolkestein.

En 2018, JTC 4 a proposé la création d'un groupe de travail pour rédiger une norme sur le thème « Services à distance pour sécurité incendie et systèmes de sécurité » sous l'impulsion d'Euralarm, qui avait déjà établi sur ce thème un manuel intitulé « Guidelines-Alarm Systems-Remote Services » en 2016. Ce manuel servira de point de départ à la future norme européenne. Face à la nécessité croissante de disposer de prescriptions claires en matière de cybersécurité - il suffit de penser à la multiplication des communiqués faisant état du piratage de systèmes (de caméras) - ANPI a rédigé une note technique, la NTN 178-C Systèmes d'alarme - Services à distance. Exigences pour l'organisation des services. Ce document est basé sur le manuel d'Euralarm.

NTN 178-C
À propos de la norme NTN 178-C

Comme un grand nombre de technologies spécifiquement anglaises sont utilisées dans le monde de la transmission de données et de leur protection, la note technique a été rédigée à l'origine en langue anglaise.

Sur le fond, il s'agit d'un document technique adoptant la structure d'une norme avec des chapitres connus tels qu'introduction, portée, références normatives, définitions et abréviations, exigences communes, application (alarme incendie, alarme vocale, alarme effraction, vidéosurveillance, contrôle des accès, alarme sociale, etc.).

Portée
La portée indique que le document définit les exigences minimums d'un accès à distance sûr pour les systèmes suivants :
- Systèmes de protection contre l'incendie au sens large
- Systèmes de protection contre l'effraction au sens large
- Systèmes d'alarme sociaux
- Une combinaison des systèmes précités

Ce document ne porte pas sur :
- Les infrastructures de transmission des alarmes
- D'autres moyens d'accès à distance
- L'utilisation de l'accès à distance par les utilisateurs finaux
- Le contrôle de l'utilisation du système par les utilisateurs finauxDe alarmtransmissie infrastructuur

Exigences communes
Les exigences communes commencent par imposer la définition du niveau de risque sur la base au moins des données suivantes :
- Manipulations et mesures de protection autorisées
- Situation/client exigences spécifiques
- Opérations et réglementations en vigueur pour les appareils utilisés dans l'application
- Lois et ordonnances en vigueur pour le respect de la vie privée et la protection des données
- Manuels de cybersécurité

Ce qui a été convenu et la façon dont les responsabilités sont partagées doit être clairement défini entre les parties concernées, à savoir le prestataire de services à distance et l'utilisateur final/client. Les éléments dont il faut tenir compte ici sont : l'installation dont il s'agit, les manipulations et tests qui peuvent/doivent être effectués à distance et dans quelles circonstances, y compris les opérations automatiques, le processus d'autorisation du client nécessaire pour chaque opération, les moyens pour consigner un trajet de contrôle de toutes les actions externes et la période de conservation, les données de traitement et de stockage, les autres données éventuelles relatives à l'assurance, aux autorités, limites de temps, limites de responsabilité du prestataire de services à distance.

Les exigences imposées au système d'alarme sont également abordées. Il est important de mentionner qu'un service à distance ne peut pas être considéré comme substitut d'un entretien sur site. Certains contrôles vitaux ne peuvent en effet être exécutés que sur le terrain, ce qui signifie que des visites régulières sur place restent essentielles. Une indication doit être présente sur place si une connexion à distance est active. Chaque connexion doit être consignée dans un journal. Une connexion inactive doit être limitée dans le temps, par exemple à 30 minutes. L'activation des systèmes d'alarme à distance doit être limitée au minimum. En cas de transmission, volontaire ou non, d'images et de sons, l'attention nécessaire doit être accordée aux règles de protection de la vie privée. Dans le cas de systèmes intégrés ou combinés, toutes les exigences imposées aux systèmes doivent être respectées et il est possible que seule une partie soit accessible à distance.

Exigences relatives à la plateforme de sécurité

Un organigramme de cette plateforme est fourni dans le document. Il inclut le système de transmission de l'information et ses connexions ainsi que la plateforme de sécurité. Ce dernier dépend du type d'accès à distance et des types de services. Pour les mesures de protection pour chaque type d'installation (hold-up et effraction, incendie, vidéosurveillance, contrôle des accès, etc.), nous renvoyons le lecteur à la série de normes ISO/IEC/JTC1/27000. Seules les personnes concernées par le contrôle du prestataire de services à distance, c'est-à-dire les personnes autorisées, peuvent accéder à la plateforme de sécurité et à l'application à distance. Ce personnel doit avoir suivi une formation adéquate à l'utilisation de l'application pour acquérir les compétences nécessaires.

Exigences relatives au système de transmission de l'information (ITS)

La sécurité de l'ITS est soutenue par les mesures de protection connues telles que vérification, encodage, sécurité de substitution et traçabilité. Une alarme a priorité sur une manipulation à distance, utilisant éventuellement des canaux de transmission à signaux multiples.

Exigences pour l'exécution de services à distance

Le client doit être au courant si des tests de ce type sont effectués. Ces derniers ne peuvent pas être réalisés pendant une situation d'alarme. Ce document décrit également les conditions d'exécution de modifications de configuration/paramètres, contrôles des systèmes à distance, automatisés ou non.

Applications des exigences spécifiques

Cette partie de la norme énumère des exigences spécifiques pour chaque application (alarme incendie, alarme vocale, alarme effraction, contrôle des accès, etc.), comme les contrôles et manipulations pouvant être effectués à distance sur une application donnée, la façon dont une connexion doit être établie, la fréquence de contrôle autorisée, l'assistance à distance autorisée.

Conclusion

La cybersécurité mérite assurément toute l'attention nécessaire dans un monde où la numérisation et l'interconnexion avancent à grands pas. Il en va de même pour les systèmes de sécurité. Les services à distance font de plus en plus souvent partie de l'offre de services. Il est dès lors important que l'ensemble du système, du prestataire de services au client, soit conçu et construit selon les règles de bonne pratique. Des engagements clairs concernant les responsabilités et manipulations à distance autorisées en font partie. Les règles de bonne pratique, c'est-à-dire les normes, à ce sujet sont rares. Basée sur un manuel d'Euralarm, NTN 178-C constitue une bonne base pour combler cette lacune. Le gros désavantage de ce document est cependant que les mesures à prendre dépendent du niveau de risque défini sur la base d'une évaluation des risques. Le document reste vague sur la manière dont cette dernière doit être exécutée et sur les niveaux existants. Un certain flou subsiste donc et le document doit par conséquent être complété et révisé en ce qui concerne l'évaluation des risques et les niveaux de risques, et ce pour chaque application (alarme incendie, alarme vocale, alarme effraction, contrôle des accès, etc.).

*****