SBA_Commission Cyberbuilding
3 septembre 2020

Présents :
Solenne Lefranc - ORANGE
Eric Hazane - ANSII
Patrice Ferrant - MOBOTIX
Jen-Yves Orsel - DOVOP
Philippe Hubert - CYBERHUB
Patrice de Carné - SBA
Jean-Christophe Denis – WALLIX
Alain Kergoat – URBAN PRACTICES / SBA
Emmanuel François - SBA

La commission se déroule à distance à l'aide de l'outil ZOOM.

Rappel de la dernière réunion :
Lors de la dernière réunion il a été convenu de rédiger un Théma Cybersécurité reprenant les thèmes :

- Risques et menaces
- Conséquences
- Cas d'usage

Et en parallèle de compléter la partie Cybersécurité de notre label R2S

Introduction :
Eric Hazane rappelle qu'il faut remonter d'un cran. Toucher la gouvernance et impliquer les décideurs. Le nombre d'attaque par rançongiciels a connu une augmentation sans précédent avec des conséquences de plus en plus dévastatrice comme repris dans le guide de l'ANSSI :
https://www.ssi.gouv.fr/publication/rancongiciels-face-a-lampleur-de-la-menace-lanssi-et-le-ministere-de-la-justice-publient-un-guide-pour-sensibiliser-les-entreprises-et-les-collectivites/

A ce propos Patrice Ferrant nous conseille de nous rapprocher du CNPP et de s'interfacer avec la règle R82 qui concerne les équipements : https://www.preventica.com/actu-enbref-referentiel-apsad-videosurveillance-2016-080316.php
https://www.cnpp.com/Boutique-Formations/Catalogue-Formations/Surete/Technologies-de-surete/Videosurveillance/R82

Nous sommes tous d'accord, il y a un vrai problème dans le domaine de la sécurité et de la sûreté. Il s'avère que les BE sont potentiellement force de proposition mais n'intègrent pas assez la dimension cybersécurité dans leurs CdC quant aux intégrateurs ils déploient ce que les BE recommandent. Il est donc important d'agir et de proposer un cadre de référence sur la base duquel les cahiers des charges puissent s'appuyer.

Patrice Ferrant nous recommande également d'associer le CNPP à notre démarche et nous met en relation avec Ronan Jezequiel (Action en cours : Patrice de Carné). Ils apporteraient des compléments par rapport à R2S ainsi que des supports pour la formation. Leur concours permettrait de renforcer notre approche.

Il convient également de se référer aux normes Européennes en termes de sécurité soit
EN 50132 – 1 : Norme qui définit les produits
EN 50132 -2 : Norme qui définit les services

Ce sont les normes de références utilisées par les installateurs / intégrateurs.

En termes de sécurité il y a sinon pour les produits : NF A2P et pour les services : APSAD.

Avoir un label « Services » comme R2S a cependant du sens puisqu'il couvre la partie numérique de l'ensemble des réseaux et des équipements du bâtiment. Il faudra par contre l'interfacer avec la certification des produits en faisant référence aux normes produits. Tout est écrit à ce sujet. Ce n'est donc pas nécessaire de recréer ce qui existe déjà mais bien d'interfacer R2S avec l'existant.
Il est par contre urgent d'apporter un référentiel aux BE. Aujourd'hui les « sachants » en la matière sont les BE. Ce sont les influenceurs pour la rédaction des normes. A titre d'exemple, aujourd'hui tous les lycées et collèges sont équipés de solution de vidéo qui ne sont pas sécurisées car n'ont pas été prescrites par les BE. C'est affligeant.
Il faut donc apporter un référentiel technique pour responsabiliser le BE.

Il est donc important d'associer le CNPP à nos travaux car il va au-delà du produit et s'intéresse également au service. Le R2S doit pouvoir s'enrichir des travaux déjà réalisés. Interconnecter les équipements de vidéo et de sécurité avec les systèmes de pilotage du bâtiment et du quartier a un vrai sens en termes de sécurité, c'est même une nécessité !

Emmanuel François demande à cet effet s'il n'existe pas déjà un référentiel dans le monde sur ce sujet et il semble en effet qu'il n'y ait rien que ce soit sur le Smart Building ou sur la Smart City comme le confirme Solenne Lefranc.
Emmanuel François propose de fait d'enrichir R2S existant qui est déjà très exigeant en termes de cybersécurité par des références aux normes produits et règles d'installation relatives aux équipements de vidéo protection. Alain Kergoat confirme qu'à ce jour les bâtiments certifiés R2S ne répondent que pour 45% au mieux des critères de cyber sécurité. On a mis des exigences de DSI et le bâtiment est très loin de ces exigences informatiques. Il y a un problème de mise à niveau qui est nécessaire et qui va être quelque part violente pour tous les acteurs traditionnels du bâtiment. Alain Kergoat invite à ce titre tous les experts ici présents à récupérer le descriptif de 111 pages de R2S et y apporte leurs commentaires qui devront faire l'objet de réunions spécifiques avec les équipes en charge de la révision de R2S pilotée par Serge Le Men. Emmanuel François recommande également un échange avec la commission R2S Connect pilotée par Alexandre Fund sur le sujet de la sécurisation des APIs. On parle des équipements de terrain tandis que R2S traite de la partie réseau. R2S Connect ayant pour vocation à relier la partie réseau traitée par R2S aux équipements de terrain en

définissant des exigences d'authentification pour en assurer l'interconnexion de manière simple, résiliente et sécurisée. C'est juste incontournable

Au-delà de la révision de R2S, Emmanuel François propose que la commission CyberBuilding travaille sur une **version S+ de R2S** qui ferait l'objet d'une certification à part pour des bâtiments ou activités sensibles et donnera lieu à des formations spécifiques rémunératrices. Compte tenu de l'enjeu que représente la Cybersécurité pour le bâtiment et la ville, ce travail pourrait faire l'objet d'une coopération internationale notamment avec les autres SBA nationales qui devraient être créées dans les prochains mois. La Cybersécurité pourrait être à ce titre un des sujets majeurs dont s'emparerait la future SBA Internationale.

Patrice Ferrant : Il faut y aller ! Il faut par contre certifier l'ensemble de la chaîne. Bien se référer à la norme EN 62676 (ex EN 50132) qui traite des équipements de vidéo protection et qui est portée par la British Standard.

Jean-Yves Orsel qui est intégrateur de caméras ajoute à ce titre qu'il y a un vrai sujet déjà autour de la gestion des mots de passe qui ne sont pas changés. Il a par ailleurs rejoint le comité de normalisation IEC 62676 qui travaille sur les équipements vidéo où Anitec est très présent. Il se propose d'établir le lien avec la SBA. Il souligne l'enjeu des JO. Il y a un vrai risque. Il a récemment répondu à l'AdO de Solideo dans lequel le sujet cybersécurité n'était pas ou peu mentionné. Il s'est rapproché de Jean Noël de Galzain, CEO de Wallix à ce sujet.

Il est souligné à cet égard que la notion de **security by design** doit être prise en compte pour l'ensemble des équipements raccordés au réseau. Il est fondamental de sensibiliser tous les équipementiers à ce sujet.

Nous confirmons donc l'intérêt de travailler sur un référentiel R2S renforcé traitant de la cyber sécurité dans son ensemble avec un niveau S+ pour les bâtiments sensibles. Cette démarche doit être internationale. L'enjeu est effectivement international et à minimum Européen et c'est une question de souveraineté. Il est important de s'interfacer aussitôt avec Bruxelles d'où l'intérêt d'impliquer la SBA Internationale dès qu'elle sera créée.

Il faut bien définir le périmètre. Il n'y a pas de référentiel qui travaille sur la globalité : Smart Home / Smart Building / Smart City. D'où l'intérêt d'avoir un référentiel commun.

Emmanuel François souligne qu'il y a d'autant plus urgence que le bâtiment évolue et s'ouvre en offrant des services multiples intégrant le partage d'espace et mobilité et donc l'accès aux bâtiments.

Patrice Ferrant confirme et insiste sur la pertinence de proposer un référentiel qui associe infra et équipements. *Le produit devient essentiel sur l'infra. On pense que parce que le produit remplit les fonctionnalités il est de confiance mais ce n'est pas le cas.*
Il faudra traiter de la sécurité numérique sur le réseau mais également des produits ainsi que la mise en œuvre et l'exploitation. Tous les acteurs de la chaîne de valeur doivent être impliqués et concernés. C'est essentiel. Bien s'interfacer notamment avec les normes telles que EN 62676 ou la RGPD pour la confidentialité des données.

Emmanuel François précise que notre place est sur l'intégration / l'assemblage en s'appuyant sur des règles existantes. Il y a une faille évidente et donc une opportunité pour la SBA.

Eric Hazane conclut que sont des échanges que l'on a depuis plusieurs mois.
Si on considère chaque partie séparément c'est bien mais insuffisant. Comme le dit Emmanuel François il faut cette approche Systémique voire globale. Il n'y a rien qui existe à ce jour qui soit aussi poussé et avancé au niveau international. Oui pour un label R2S S+. Ok pour y adjoindre l'ANSSI. Il existe beaucoup de littérature par contre important de remplir les cases.

Emmanuel François ajoute qu'il y a également un vide juridique. Il va sensibiliser la commission juridique qui travaille sur ces sujets afin que la cyber sécurité fasse également partie de leur feuille de route avec des exigences contractuelles impliquant tous les acteurs de la chaîne valeur.

Solenne Lefranc confirme qu'apporter un cadre de référence traitant de la sécurité et de la sûreté permettra d'accompagner le cadre juridique et permettra tous acteurs de se poser les bonnes questions. La question de gouvernance et de responsabilité est effectivement fondamentale.

Patrice Ferrant confirme que cette partie juridique est essentielle à commencer également par la RGPD. Il n'y a pas un document qui représente l'ensemble de la chaîne avec la responsabilité.

Nous validons à ce titre l'importance de définir un document illustrant la chaîne des utilisateurs en pointant leurs responsabilités. Cela ne plaira peut-être pas à tout le monde mais c'est essentiel pour commencer à sensibiliser tous les acteurs. Cela fera l'objet d'une sous-commission en mode éclair.

Feuille de route de notre commission

- **Établir un document de synthèse illustrant l'ensemble des acteurs sur la chaîne de valeur et pointant leur responsabilité. Chacun réfléchit dans son coin.**
- **Contribution des experts présents à la partie Cybersécurité de la V2 de R2S : Octobre avec une prise en compte des normes actuels produits et normes Européennes. Se rapprocher du CNPP. En parallèle chacun observe le document. R2S V1 et apporte ses annotations à Alain Kergoat. Alain Kergoat leur envoie à cet effet le document.**
- **Travailler ensuite sur une version S+ de R2S pour des bâtiments sensibles.**

Important d'associer la commission Safe Building et convier à minimum Dominique Legrand et Ariane Truffert à nos travaux.

Nous décidons également d'organiser un Webinair sur ce sujet d'ici la fin de l'année pour sensibiliser tous les acteurs et contribuer à élargir le cercle des contributeurs. A ce titre, inviter Wallix et Gatewatcher à la prochaine réunion.