Compte Rendu de la réunion du vendredi 11 novembre2021

Participants:

	Présents
jcdenis@wallix.com	
ai.parodi@stid.com	
ronan.macfarlane@sia-partners.com	
nathalie.labeys@cnpp.com	
m.favre-mercuret@patriarche.fr	
Brice.gilbert@afnor.org	
philippe.raynaud@groupe-arcom.com	
jeremy.esquirol@occitaline.com	
ikosem@aestria.fr	
cconvert@urbanpractices.com	
alain.kergoat@smartbuldingsalliance.org	
emmanuel.francois@smartbuildingsalliance.org	
lidia.zerrouki@smartbuildingsalliance.org	

Objectif de la réunion

Poursuite du travail de structuration du livre blanc sur le Cyberbuilding et collecte des contributions

Evolution du chapitrage :

1. Préface
2. Introduction
3. Objet du document
4. Enjeux, défis et champ d'action
5. Risques : Identification des cibles à protéger
6. Concepts fondateurs et bonnes pratiques de la cybersécurité
7. OT et IT
8. Les référentiels existants
9. Scenarios d'attaque et cas d'usage
10. Méthode
11. Solutions appliquées au bâtiment
12. Conclusion
13. Remerciements
14. Références documentaires, sources
15. Tableau des abréviations

Enjeux => le groupe de travail propose de revoir les enjeux et liste les sujets suivants (à hiérarchiser) :

- ⇨ Cadre juridique et responsabilité des parties prenantes
- ⇨ Formation des utilisateurs (occupants, exploitants, gestionnaires …)
- ⇨ Pertes financières (arrêt d'activité / dégradation des équipements …)
- ⇨ Continuité de service
- ⇨ Impact social (désordre dans l'organisation des activités, perte ou vol des données …)
- ⇨ Impact d'image
- ⇨ Impact environnemental (dérèglement des systèmes de régulation …)

Définition et découpage du SI Bâtimentaire => il est proposé les 3 catégories suivantes :

- ⇨ Systèmes techniques du bâtiment
- ⇨ Applications occupants
- ⇨ Systèmes de gestion des exploitants et propriétaires (FM/PM/AM)

Le tout constituant le SI du bâtiment (ou du parc de bâtiments)

Financement de la cybersécurité bâtimentaire => il es proposé de faire référence aux couts moyens constatés pour les budget cybersécurité des SI d'entreprise pour mémoire entre 5 à 10% du cout total des systèmes.

Risques => il est proposé de rajouter 2 thèmes :

- ⇨ Risques assurantiels (non couverture des risques de cybersécurité)
- ⇨ Risques systémique (exemple risques liés au blackout énergétique)

Par ailleurs le paragraphe sur l'analyse des risques (voir contribution de Ronan Mac Farlane - SIA Partners) est insérée en début de chapitre

OT – IT => ce chapitre reste à écrire :

- ⇨ Action relance GIMELEC …

Référentiels => il est proposé de compléter le chapitre sur les référentiels en :

- ⇨ Développant l'encart consacré au CNPP
- ⇨ Rajoutant les 3 normes suivantes : IEC 62 443 / ISO 27 001 / ETSI 303 645
- ⇨ Faire une synthèse des thèmes liés à la cybersécurité dans R2S (action AK)

Cas d'usages => il est proposé de regrouper tous les cas d'usages dans ce chapitre dédié et d'utiliser un cadre homogène pour développer les cas, comprenant les items suivants :

- ⇨ Titre du cas d'usage
- ⇨ Contributeur

- ⇨ Risque
- ⇨ Cible
- ⇨ Contexte
- ⇨ Description du scénario
- ⇨ Impact
- ⇨ Contre mesures

Prochaine réunion le vendredi 10 décembre de 10h à 12H par visio conférence

OdJ

Partage des nouvelles contributions – et finalisation de la structure du livre blanc