



Aide-mémoire concernant les systèmes de Cyber Security

Disclaimer de la SES concernant la Cyber Security des installations de sécurité

Introduction

La sécurité physique est une partie d'un concept de sécurité globale et constitue la première mesure de protection d'un environnement sensible. Il s'agit souvent de systèmes intégrés pour le contrôle d'accès, la surveillance vidéo, la détection d'incendie, la détection d'effractions, l'automatisation du bâtiment, etc. (énumération non exhaustive).

Vu l'évolution constante de la technique et la transformation numérique, l'utilisation et l'exploitation des systèmes de sécurité physique changent. Les systèmes intégrés ont des liens toujours plus étroits avec la technologie IT et ils sont interconnectés dans un réseau hétérogène. Aujourd'hui, même un système isolé n'est plus considéré comme étant sûr et des mesures de Cyber Security doivent être prises en fonction des exigences de protection.

Les changements nécessitent des connaissances techniques approfondies de la part des concepteurs et des constructeurs de systèmes et des bureaux d'étude. Le présent document est conçu comme aide à l'attention du futur utilisateur. Le Disclaimer soutient les constructeurs, les bureaux d'étude spécialisés et les clients finaux dans les phases d'offre, de réalisation, d'exploitation et de maintenance.

La Cyber Security est la protection des systèmes informatiques contre le vol ou la détérioration des matériels, des logiciels ou des données électroniques et contre l'interruption ou le mauvais acheminement des services qu'ils fournissent. Cela s'applique à tous les types de systèmes de sécurité électronique qui utilisent des logiciels, des Firmware ou des composants programmables.

Selon les métiers, la Cyber Security est plus prononcée en termes de précautions organisationnelles et techniques, au regard des objectifs de protection que sont la disponibilité, la confidentialité et l'intégrité.

Les installations de sécurité ne peuvent, par nature, pas être protégées à 100% contre les cyberattaques. Selon le besoin de protection, l'intégration des mesures de Cyber Security pertinentes diffère. Cet aspect doit pouvoir être pris en compte et présenté avec transparence dès la phase d'offre.

Le présent aide-mémoire de l'association SES s'applique à tous les domaines dans lesquels des installations de sécurité sont exploitées.

Responsabilités et devoirs

Le client final est responsable de l'élaboration d'un dispositif de sécurité pour la mise en œuvre des mesures de précautions concernant la Cyber Security. Selon l'objet livré, l'implémentation des mesures de Cyber Security peut être l'affaire du client, du constructeur ou d'un tiers.

Le constructeur émet des recommandations de mesures de Cyber Security dans le champ d'activités de son corps de métier, en fonction de la pondération des objectifs de protection concernant la disponibilité, la confidentialité et l'intégrité.

La SES recommande de toujours conclure un contrat pour la maintenance. Ce dernier porte sur des mesures techniques et organisationnelles concernant la Cyber Security, le but étant de garantir l'exploitation la plus sûre possible des installations de sécurité.

Moyens auxiliaires recommandés

La SES recommande de choisir un constructeur qui connaisse les problématiques de la Cyber Security dans le corps de métier concerné et qui soit en mesure de prendre les mesures de Cyber Security.

La Confédération, ICT Switzerland et d'autres sources fiables mettent à disposition des moyens auxiliaires et des check-lists pour élaborer un dispositif de sécurité adéquat pour la Cyber Security.

Lien: <https://ictswitzerland.ch/themen/cyber-security/check/>

Lien: https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html

Produits et solutions du maître de l'ouvrage

La SES rend attentif au fait qu'aucune garantie ne peut être accordée sur les produits et les solutions livrés. L'installateur peut fournir des recommandations dont la mise en œuvre et la révision doivent être effectuées par le fournisseur de la solution existante.

Informations relatives à la Cyber Security

La SES recommande une convention réglant l'échange, entre les parties, des informations ayant des incidences sur la Cyber Security.

La plate-forme «Centrale d'enregistrement et d'analyse pour la sûreté de l'information» (MELANI) de la Confédération peut fournir un appui en fournissant la vue d'ensemble des menaces relevant de la Cyber Security.

Protection des données

Si le système de sécurité est utilisé dans l'environnement d'une entreprise, SES recommande la création de réglementations spécifiques à l'entreprise pour le fonctionnement et l'utilisation du système de sécurité. Les dispositions relatives à la protection des données conformément au RGPD et au PFPDT doivent - le cas échéant - être respectées.