Standard minimum des appareils connectés

Standard ministériel approuvé après COPIL SSI du 12 octobre 2016

TABLE DES MATIERES

MENACES

La dépendance aux systèmes informatiques ne fait qu'augmenter. « L'Internet des objets » est une réalité, qui s'étend des jouets à l'industrie lourde.

Pour offrir leurs fonctionnalités avancée, ces appareils sont interconnectés via des réseaux mutualisés, « tout IP ». Leur déploiement doit s'effectuer avec un minimum de maîtrise, à la fois pour assurer leur sécurisation, mais aussi ne pas mettre en danger celle des autres appareils, y compris les postes de travail « classiques ».

ETAT DE L'ART

La première approche mise en œuvre pour limiter les risques et les conséquences est le cloisonnement et les sauvegardes. Il faut bien évidemment dédier des LAN aux appareils utilisés par la gestion du bâtiment, des entrées-sorties, la vidéosurveillance, etc.

Cependant cette approche n'est pas toujours possible :

- périmètre trop petit pour que le cloisonnement soit praticable
- appareils qui ont besoin d'être interconnectés avec les postes de travail pour rendre leur fonction ; dans ce registre, on peut citer les imprimantes multifonctions, les équipements télécoms, etc.

Face à ce constat, un certain nombre d'organisations, notamment dans les milieux universitaires et hospitaliers ont pris le parti de réglementer l'introduction d'appareils sur leur réseaux, en définissant des prérequis minimum. Un exemple est fourni dans les liens par l'université de Berkeley pour son campus.

Ces prérequis peuvent se synthétiser de la façon suivante (NB : les PC classiques remplissent évidemment toutes ces conditions).

Mises à jour et correctifs

Les appareils connectés ne doivent faire fonctionner que des logiciels qui sont suivis, et disposent de correctifs distribués régulièrement. Les correctifs disponibles sont à appliquer selon une urgence en rapport avec le risque qu'elle limite.

Dispositifs contre les programmes malveillants

Les appareils connectés doivent disposer d'un dispositif contre les programmes malveillants. Les principaux sont les anti-virus, les dispositifs anti-intrusion par condensats et les signatures de logiciels.

Limitations des connexions

Les appareils connectés limitent les connexions entrantes qu'ils acceptent à leur niveau, sans se reposer sur des parefeux réseaux. Dans tous les cas, ils documentent leurs usages de connexions réseaux (ports et protocoles utilisés), aussi bien pour les flux entrants que sortants, les connexions utilisateur ou administrateur.

Authentification

En particulier s'ils offrent une fonction de relai, les appareils connectés doivent exiger une authentification via un moyen réputé sûr (sauf si l'appareil est par fonction public : borne d'accueil, etc.)

Les moyens connus comme non sûr inclus Telnet, WEP, HTTP et SMTP sans TLS.

Les mots de passe par défaut doivent tous être changés au moment de l'installation.

Pour lutter contre les attaques par dictionnaire en ligne et hors ligne, l'appareil connecté doit suivre des règles de :

- complexité minimum de mot de passe
- mesures contre le rejeu
- déconnection après une certaine durée d'inactivité

A défaut de moyen d'authentification réseau répondant à ces critères, l'appareil connecté doit restreindre les fonctions correspondantes à des ports locaux (USB, console, boutons sur l'appareil), qui font reposer la sécurisation sur la sécurité physique des locaux.

STANDARD MEF

Chaque mesure exposée dans l'état de l'art relève de la simple « hygiène ». Pour autant, dans la course au développement de produits, leur mise en œuvre n'est pas acquise.

Réalistement, le standard visé par les MEF pour application au 1er janvier 2017 est :

- inclusion systématique de clauses dans les cahiers des charges d'acquisition de matériels ; les fournisseurs s'ils ne remplissent pas les prérequis doivent expliciter leurs déviances.
- explicitation dans les dossiers d'homologation de systèmes d'information des prérequis non remplis et des mesures compensatoires mises en œuvre

LIENS

https://security.berkeley.edu/minimum-security-standards-networked-devices-mssnd

Contact : dssi.shfds@finances.gouv.fr
Diffusion Intranet : http://hfds-bercy.monportail.alize/cms/sites/hfds-bercy/accueil/ssi.html

HFDS Bercy