RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

COLLECTION
GESTION DES RISQUES CYBER

GUIDE DE L'HOMOLOGATION DE SECURITE DES SYSTEMES D'INFORMATION

FICHE METHODE

SYSTEME D'INFORMATION ISOLE ET SIMPLE

Les fiches méthodes permettent aux responsables de la démarche d'homologation ou au comité d'homologation d'identifier les points essentiels d'attention en fonction de la typologie du système d'information ou des concepts utilisés.
Elles n'ont pas vocation à remplacer les guides techniques de l'ANSSI ou les politiques de sécurité et les réglementations en vigueur qui doivent être appliquées.

LE SYSTEME D'INFORMATION ISOLE ET SIMPLE : DE QUOI S'AGIT-IL ?

Un système d'information dit « isolé et simple » est le regroupement d'un ou de plusieurs ordinateurs fixes ou portables, éventuellement équipés de périphériques (d'affichage, de transfert de données ou de sauvegarde sur support de masse, de numérisation ou d'impression), isolé de tout réseau externe.

Ce type de système intègre des équipements d'interconnexion (commutateurs) permettant la communication entre les ordinateurs.

A noter qu'un système d'information hébergeant des annuaires d'administration (LDAP, Active Directory) ne rentre pas dans cette catégorie.

Si une connexion réseau est possible entre plusieurs ordinateurs du même système d'information, celle-ci doit se faire exclusivement par le biais de réseaux filaires. Les réseaux sans fil ne doivent pas être utilisés dans ce type de système d'information.

NOTE :
Les systèmes d'information simples et déconnectés sont souvent utilisés dans le cadre du traitement de données sensibles ou classifiées.

Les usages courants de ces systèmes d'information sont :

- des activités bureautiques (consultation de documentation, élaboration de rapports d'audits, etc.) ;
- des activités de conception et d'évaluation de produits logiciels et/ou matériels (modélisation, programmation de composants ou de matériels, tests, etc.).

Bien que déconnectés de tout réseau, ces systèmes reçoivent ou génèrent des informations. Afin de sécuriser ces systèmes et de pouvoir les homologuer, les points suivants doivent être adressés. Ils peuvent être retrouvés dans les différents guides de l'ANSSI.

DURCISSEMENT DES ORDINATEURS

Les ordinateurs composant le système d'information doivent être durcis suivant les bonnes pratiques de cybersécurité :

- Les ordinateurs doivent être mis à jour avec les dernières versions des logiciels et de systèmes d'exploitation installés ;
- Les services et protocoles non-utilisés doivent être désinstallés ou désactivés ;
- Un antivirus et un pare-feu personnel doivent être installés et tenus à jour ;
- Les disques durs doivent être chiffrés ;
- Un contrôle d'accès strict doit être mis en place. Il s'agit à minima des accès au BIOS et au système d'exploitation.

SUPPORTS AMOVIBLES

Dans les systèmes d'information déconnectés, des supports amovibles[1] permettent l'échange de données avec d'autres systèmes d'information et l'application du plan en maintien en condition opérationnel et de sécurité.

Les bonnes pratiques d'utilisation des supports amovibles au sein d'un système d'information doivent être appliquées.

1 par exemple clés USB ou CD ROM

MAINTIEN EN CONDITION DE SECURITE

Le système d'information isolé doit être mis à jour de façon régulière afin de limiter les risques liés à l'introduction de logiciel malveillant. Le maintien en condition de sécurité doit se faire à l'aide de mécanismes manuels, par des administrateurs de confiance.

Lorsque pour des raisons organisationnelles ou techniques, le système d'information ne peut être maintenu à jour, une solution alternative permettant qu'une menace ne soit pas propagée doit être mise en place.

ADMINISTRATION

Les utilisateurs doivent être gérés en respectant les bonnes pratiques[2].

Les identifiants et mots de passe permettant d'accéder à des ressources à privilèges ne doivent être connus que par les administrateurs du système d'information.

DECONNEXION DES RESEAUX

Pour s'assurer que les postes restent déconnectés, une attention particulière doit être portée sur les équipements réseau de chaque ordinateur :

- Les services réseau sans-fil (wifi et bluetooth) doivent être désactivés au niveau le plus proche de la machine (BIOS).

Il est à noter que d'autres protocoles permettent le transfert d'information (par exemple 3/4/5G, Zigbee, réseau à basse consommation…). Ils doivent être désactivés.

Les services réseau filaires ne doivent être activés que dans la nécessité de connexion entre les ordinateurs du même système d'information.

[2] https://cyber.gouv.fr/publications/guide-dhygiene-informatique

NOTE :
Même si les services réseau sont désactivés, il reste toujours possible de brancher des équipements USB permettant de se connecter sur des réseaux sans fil. Ces connexions doivent être surveillées.

LOCALISATION

Lorsqu'ils gèrent de l'information classifiées, les ordinateurs composants un même système d'information simple et déconnecté doivent se situer dans un même local.

Les équipement et câbles du réseau permettant de connecter les ordinateurs doivent être spécifiques au système d'information.

Lorsque les ordinateurs ne sont pas utilisés, ils doivent être protégés de tout accès malveillant.

Un poste isolé, déconnecté, contenant des informations sensibles, nécessitant une homologation ne doit pas être déplacé.

LES RESSOURCES DISPONIBLES POUR ALLER PLUS LOIN

L'homologation de sécurité	https://cyber.gouv.fr/lhomologation-de-securite
La méthode EBIOS Risk Manager	https://cyber.gouv.fr/la-methode-ebios-risk-manager
Le guide d'hygiène informatique	https://cyber.gouv.fr/publications/guide-dhygiene-informatique
Mon Service Sécurisé	https://monservicesecurise.cyber.gouv.fr
Se protéger des fuites de données	https://cyber.gouv.fr/publications/se-proteger-des-fuites-de-donnees