Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Centre national pour la cybersécurité NCSC
GovCERT.ch

TLP:WHITE

Cybersécurité dans le secteur de la santé: recommandations

Date:	le 24 mai 2022
Version:	v1.0
Auteur:	NCSC / GovCERT

Introduction

Le présent document expose les exigences minimales de sécurité informatique qui correspondent aux meilleures pratiques actuelles («Best Current Practice») et que le Centre national pour la cybersécurité (NCSC) recommande à tous les prestataires de services dans le secteur de la santé de mettre en œuvre. Il est important que les mesures définies et déployées recouvrent à la fois les domaines technique et organisationnel.

Aperçu des mesures

Voici un aperçu des mesures décrites en détail dans le présent document:

Mesure	Niveau de mise en œuvre	Nature de la directive
Gestion des correctifs et du cycle de vie aux niveaux technique et organisationnel	Organisationnel	Obligatoire
Suivi étroit des données du journal concernant le périmètre de sécurité	Organisationnel et technique	Obligatoire
Surveillance étroite des terminaux	Technique	Facultative
Gestion des correctifs et du cycle de vie	Organisationnel et technique	Obligatoire
Intégration dans le cercle fermé des clients du NCSC	Organisationnel	Facultative
Copies de sauvegarde («back-ups») hors ligne / rétablissement après un sinistre	Technique	Obligatoire
Segmentation du réseau	Technique	Obligatoire
Protection de l'authentification	Technique	Obligatoire
Blocage des fichiers dangereux joints aux courriels	Technique	Facultative
Contrôle de l'exécution des fichiers	Technique	Facultative

Gestion des correctifs et du cycle de vie (niveau organisationnel)

L'organisation **doit** élaborer et maintenir à niveau un plan de gestion des correctifs et du cycle de vie des logiciels.

Les logiciels ont une certaine durée de vie, au cours de laquelle ils bénéficient de mises à jour fonctionnelles et de sécurité (correctifs). Il est donc essentiel qu'ils reçoivent très rapidement chacune des mises à jour de sécurité. Un plan directeur à ce sujet précise la durée de vie des logiciels (quand ces derniers doivent être remplacés) ainsi que les moments où une mise à jour de sécurité doit être appliquée. Il est par ailleurs utile d'identifier régulièrement les logiciels en fin de vie («End Of Life») qui ne bénéficient plus de mises à jour de sécurité (correctifs) et qui devraient par conséquent être remplacés.

Gestion des correctifs et du cycle de vie (niveau technique)

L'organisation **peut** avoir recours à un système de gestion des logiciels et des mises à jour de sécurité (correctifs) afin de gérer les correctifs et le cycle de vie des logiciels.

Les logiciels ont une certaine durée de vie, au cours de laquelle ils bénéficient de mises à jour fonctionnelles et de sécurité (correctifs). Il est donc essentiel qu'ils reçoivent très rapidement chacune des mises à jour de sécurité. Un programme de distribution automatique des logiciels comme Microsoft SCCM[1] permet à l'organisation d'avoir une vue d'ensemble de ses logiciels (de savoir ainsi quelle version d'un logiciel donné est installée sur quels appareils), de distribuer automatiquement les logiciels et de faciliter la gestion des correctifs. Microsoft SCCM contribue en outre à identifier les logiciels en fin de vie («End Of Life») qui ne bénéficient plus de mises à jour de sécurité (correctifs) et qui devraient par conséquent être remplacés.

Il y a lieu de doter d'une protection supplémentaire les systèmes et logiciels qui ne reçoivent plus de mises à jour de sécurité mais que l'organisation doit continuer à utiliser pour des raisons organisationnelles ou opérationnelles. Elle peut par exemple les transférer vers des zones séparées et isolées du réseau. Les appareils médicaux représentent en l'occurrence un défi particulier dans la mesure où ils doivent souvent exécuter une pile logicielle précise en raison de leur certification.

Suivi des données du journal concernant le périmètre de sécurité (niveaux organisationnel et technique)

Les logiciels et les appareils inclus dans le périmètre de sécurité (antivirus, pare-feu, serveurs proxy ou systèmes de prévention des intrusions IDS/IPS etc.) **doivent** enregistrer toutes les activités. Ces activités **doivent** faire l'objet de contrôles immédiats permettant d'identifier toute situation suspecte, tentative d'intrusion ou attaque. Il faut également veiller à repérer rapidement des fuites de données ou des anomalies au niveau des flux de données, améliorer la visibilité et les possibilités de réaction au niveau des terminaux et des serveurs, et analyser très rapidement aussi les alertes générées par des logiciels ou des appareils au sein du périmètre de sécurité. Ces tâches **doivent** être confiées à des personnes dûment formées.

[1] https://fr.wikipedia.org/wiki/System_Center_Configuration_Manager

Une possibilité consiste à avoir recours à un «Security Operation Center» (SOC), qui est en mesure d'identifier les tentatives d'attaque ainsi que de prendre les mesures nécessaires pour contrecarrer ces dernières, et qui aide l'organisation en cas de crise lorsqu'il faut traiter des incidents de cybersécurité («Incident Response Process»).

Il existe différentes possibilités d'exploitation d'un SOC:

- **SOC interne**: le SOC est exploité au sein de l'organisation avec les ressources et l'expertise de cette dernière.

- **SOC externe**: un SOC externe («SOC-as-a-Service») proposé par un fournisseur de services de sécurité gérés («Managed Security Service Provider»), ou par une ville ou un canton se charge de l'exploitation du SOC.

- **Regroupement**: plusieurs hôpitaux répertoriés se regroupent afin d'exploiter un SOC en commun (association hospitalière par ex.).

Suivi des données du journal concernant le périmètre de sécurité (niveau technique)

Les terminaux d'un réseau (serveurs et clients) doivent bénéficier du meilleur suivi possible. Il est également judicieux de disposer d'une excellente visibilité et de possibilités de réagir très rapidement, un objectif que le recours à un outil EDR/XDR («Endpoint Detection and Response») **peut** aider à atteindre.

Intégration dans le cercle fermé des clients du NCSC (MELANI-Net)

L'intégration dans le cercle fermé des clients du NCSC («MELANI-Net») est **recommandée** car, en échange de la seule obligation pour ses membres de garder le secret, elle offre une multitude d'avantages:

- l'accès à la plateforme d'échange sécurisée «MELANI-Net», qui informe et alerte les membres également en cas d'événement important ou lorsqu'elle reçoit des informations au sujet de cybermenaces.

- l'accès aux prestations du NCSC, qui apportent aux membres une protection technique supplémentaire face aux cybermenaces ainsi que des ressources techniques et personnelles additionnelles pour analyser et contrecarrer l'attaque en cas d'incident informatique.

Protection de l'authentification, notamment par l'authentification multifacteur (MFA) lors des accès à distance

Les ressources internes d'une organisation qui sont accessibles via Internet (par ex. Sharepoint, messagerie web, mais aussi les solutions d'accès à distance – VPN, Citrix ou RPD

notamment) **doivent** impérativement être sécurisées à l'aide d'un second facteur (authentification multifacteur, MFA). Si, pour des raisons techniques ou organisationnelles, le recours à la MFA ne devait pas être possible, l'accès **doit** être sécurisé à l'aide d'autres dispositions techniques comme la limitation de ce dernier à certains domaines d'adresses IP. En outre, la gestion de l'infrastructure informatique **doit** reposer sur une solution d'authentification multifacteur.

Les éléments principaux de l'infrastructure d'authentification comme la gestion des utilisateurs (Windows Active Directory notamment) doivent bénéficier d'une protection et d'une surveillance spécifiques.

Blocage des fichiers dangereux joints aux courriels

Il existe de nombreux types de fichiers dangereux qui sont joints à des courriels et qui servent à diffuser des logiciels malveillants (appelés maliciels, ou «malware» en anglais). Or la plupart de ces types de fichiers ne sont que rarement voire jamais utilisés dans un contexte professionnel. Sur le plan technique, ils **peuvent** donc être bloqués[2] soit dès qu'ils arrivent sur la plateforme de messagerie électronique soit par le filtre antipourriel.

Toutefois, dans la mesure où de nombreuses familles de logiciels malveillants se répandent désormais aussi via des documents Office malveillants (fichiers Word ou Excel), il est en outre **recommandé** de filtrer tous les documents Office qui contiennent du code de programmation de macros ou d'identifier clairement ces courriels à l'attention de l'utilisateur.

Contrôle de l'exécution des fichiers

Une mesure qui permet de renforcer très efficacement la sécurité consiste à contrôler quel utilisateur peut exécuter des fichiers à partir de quels dossiers, au moyen d'outils de contrôle de l'exécution (Windows AppLocker par ex.). De même, l'exécution d'un code de programmation de macros dans les documents Office peut aussi être limitée aux macros fiables (et accompagnées d'une signature numérique). Ces deux mesures offrent un niveau de protection élevé contre les cyberattaques menées à l'aide de documents Office malveillants.

Segmentation du réseau

La segmentation des réseaux reste une mesure de sécurité très importante pour les hôpitaux car,dans la plupart des cas, c'est l'informatique de l'organisation qui sert de vecteur initial de l'attaque. Il faudrait dès lors que les passerelles vers les zones du réseau qui incluent des appareils médicaux soient aussi peu nombreuses que possible, bien définies et surveillées.

La virtualisation des terminaux constitue une autre approche intéressante en l'occurrence: l'on sépare au moyen d'une couche de virtualisation – à l'insu de l'utilisateur – les zones sensibles dans lesquelles on accède aux données sur les patients par exemple des activités non sécurisées comme les recherches sur Internet ou la lecture des courriels.

[2] https://www.govcert.ch/downloads/blocked-filetypes.txt

Copies de sauvegarde hors ligne et rétablissement après un sinistre

Des copies de sauvegardes des données (que l'on appelle «back-ups») **doivent** être placées en sécurité et séparées dès lors du réseau (**hors ligne**), ce qui permet notamment de s'assurer que l'on dispose, lorsqu'une organisation est victime d'une attaque avec un rançongiciel et que ses données ont ainsi été cryptées, d'une copie de sauvegarde fonctionnelle pouvant être restaurée quand les éléments infectés auront été nettoyés.

Les objectifs de rétablissement («Recovery Time Objective» et «Recovery Point Objective») constituent le plus grand défi lors des attaques par rançongiciel à grande échelle: il y a lieu de connaître exactement le temps nécessaire pour restaurer l'infrastructure après une cyberattaque de grande ampleur. Et dans la mesure où cela prend un certain temps, l'hôpital doit disposer de solutions transitoires lui permettant d'assurer au moins son fonctionnement a minima. Enfin, il faudrait que cette solution transitoire soit techniquement opérationnelle tout en étant complètement découplée des activités quotidiennes, qu'elle bénéficie d'une maintenance, et qu'elle soit régulièrement testée.