OPUS 5

APSSIS

GUIDE CYBER RÉSILIENCE

CONTRÔLES, INDICATEURS & TABLEAUX DE BORD

Par Cédric CARTAU

SOMMAIRE

CYBER RÉSILIENCE

0.5 CONTRÔLES, INDICATEURS & TABLEAUX DE BORD

L'AUTEUR

Cédric CARTAU est RSSI et DPO du CHU de NANTES et du GHT44. Il est vice-président de l'APSSIS et enseigne à l'EHESP, à l'ESIEA et au CNEH. Il est également auteur de plusieurs ouvrages chez Eyrolles ou aux Presses de l'EHESP, sa dernière publication étant « La sécurité du système d'information des établissements de santé », en 2018.

cedric@cartau.net

L'auteur et l'APSSIS remercient ces contributeurs d'avoir accepté le difficile exercice de présenter une approche métier sur une question aussi complexe que les contrôles, les indicateurs & les tableaux de bord.

relyens sham | sofaxis

EGERIE
INTEGRATED CYBERRISK MANAGEMENT

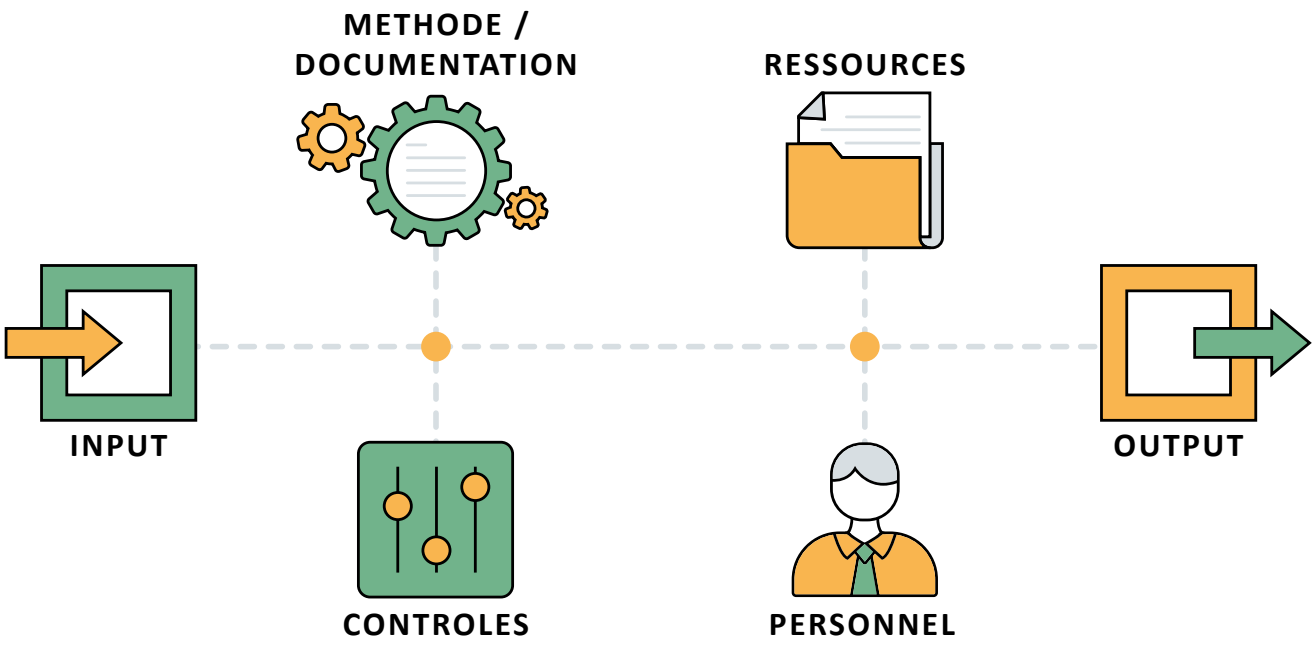
APSSIS

1. INTRODUCTION

S'il est un domaine pour lequel, souvent, les DSI sont perfectibles, c'est bien la production d'indicateurs.

Personne n'imaginerait en effet conduire une voiture sans tableau de bord (pas de compteur de vitesse, pas de jauge carburant) : dans certains cas, on risque simplement la panne sèche mais dans d'autres de se retrouver carrément dans un fossé. Le fait de confier à une machine un processus physique (déplacement, chaîne de montage automobile, etc.) implique d'avoir une vision de ce qui est réalisé, que ce soit en temps réel ou sur le moyen terme.

Le même principe se décline dans les organisations humaines : pas de délégation sans contrôle, pas d'action sans mesures. Le modèle classique du processus est celui de la Tortue de Crosby, qui mentionne explicitement la mesure dudit processus, et donc indirectement l'indicateur : la tortue prend en entrée des éléments (INPUT) pour les transformer (OUTPUT), et le fait en disposant de moyens financiers (MOYENS) et humains (PERSONNEL), le tout en s'appuyant sur des procédures (METHODE) et des indicateurs (CONTROLES).



Dans le domaine de la Sécurité des Systèmes d'Information (SSI), on retrouve une dichotomie classique issue de la théorie du risque et qui fait la distinction claire entre une activité risquée et une activité dangereuse :

• une activité dangereuse est celle pour laquelle il existe peu d'appréciation des risques, peu de contre-mesures, peu de retour d'expériences sur les risques encourus et les sinistres ; il s'agit par exemple de l'exploration spatiale habitée à ses débuts dans les années 1950[1] ;
• a contrario, une activité risquée est celle pour laquelle les risques sont connus, les contre-mesures identifiées et sous contrôle avec des valeurs contenues dans des plages maîtrisables ; la voltige aérienne fait partie de cette catégorie, tout comme le fait de jouer en bourse et bien évidemment la SSI ;

Pas de SSI sans contrôle ni indicateurs, c'est

1 Voir à ce sujet l'excellent film « L'étoffe des héros »

le thème de ce cinquième opus.

L'objectif de ce guide n'est pas de trancher sur une liste définitive d'indicateurs SSI, mais de servir de guide au chef de projet, au DSI voire à une direction générale pour contrôler et piloter le risque SSI au sein de l'organisation.

Cette publication s'inscrit dans la suite des précédents guides de cyber résilience (Tome 1 : les mots de passe ; Tome 2 : les cyberattaques ; Tome 3 : les habilitations d'accès aux données métier, Tome 4 : la protection du Cloud), publiés avec le précieux concours de l'APSSIS[2] avec l'ambition de constituer un corpus de référence sur les questions relatives à la sécurité du SI, tout secteur confondu.

Comme pour chaque guide, les contributions en annexe constituent un complément très riche, des points de vue de professionnels du secteur chacun dans leur spécialité.

Et comme toujours, les remarques, suggestions d'amélioration sont à envoyer directement à l'auteur pour être prises en compte dans les prochaines versions.

Bonne lecture.

2 https://www.apssis.com/nos-actions/publication.html

2. DE L'ORIGINE DES PROCESSUS

Si processus il y a, c'est qu'il existe un incitateur ou vecteur. Ces vecteurs sont, par ordre chronologique :

• les habitudes, trucs et astuces des professionnels du secteur : un informaticien sait qu'il ne faut jamais effectuer une mise en production un vendredi ni attribuer des comptes admin à haut privilège sans un processus encadré ;
• les référentiels de bonnes pratiques : c'est le cas d'ITIL, catalogue de bonnes pratiques issues d'une grande étude menée dans le Royaume Uni des années 80, le gouvernement de l'époque voulant savoir pourquoi certaines entreprises s'en tiraient mieux que d'autres avec l'outil informatique et voulant en dégager des bonnes pratiques éprouvées ; la hot line avec un numéro d'appel unique est un exemple ; dans cette catégorie on trouve notamment COBIT ;
• les normes officielles ; ITIL a fini par donner lieu à l'ISO 20000, et de nombreuses normes ISO sont apparues : on trouve l'ISO 27001 et la famille des ISO 27 ;
• les normes ou référentiels sectoriels ; l'archétype est la certification HAS qui, sans être une loi, est suffisamment contraignante pour que les établissements de santé s'y plient ; on y trouve également HOPEN, la Certification HDS, la Certification Hôpital Numérique, le référentiel MATURIN-H en construction ;
• et, enfin, le corpus juridique : les lois, les décrets ; RGPD, directive NIS, Certification des Comptes, etc.

Un petit inventaire s'impose

Les RSSI et DPO seraient bien avisés de réaliser une cartographie de chaque item de ces catégories. Si vous pensez que la liste finale est relativement courte, vous vous trompez : elle comporte des dizaines et des dizaines d'item...

Si « Cela » est réalisé, c'est qu'un vecteur l'a impulsé et qu'il va falloir en contrôler le bon déroulement : c'est la patte « CONTROLE » de la tortue de Crosby. A ce stade, il convient de bien faire la distinction entre le contrôle et l'indicateur : le premier est indispensable et n'implique pas forcément le second.

3. VERS L'IDENTIFICATION D'UN PROCESSUS DE CONFORMITÉ

3.1 Le paradigme de la certification des comptes

Pour avoir vu le démarrage d'une certification des comptes au sein du monde hospitalier (2015), le processus fonctionne à peu près comme suit.

La première année, les commissaires aux comptes (CAC) débarquent et réalisent des contrôles sur des flux financiers (peu importe le thème ou l'objectif) : dans cette première phase, les CAC réalisent eux-mêmes ces contrôles.

La deuxième année, les CAC demandent que l'Organisation ait mis en place elle-même ces contrôles internes, et accompagnent l'Organisation dans cette mise en œuvre.

Les années suivantes, les CAC se « contentent » de vérifier que le processus de contrôle interne fonctionne dans l'Organisation : les CAC ne se positionnent donc pas en contrôle opérationnel des flux financiers, mais en contrôle d'un processus de contrôle interne.

Dans le langage des CAC, ils vérifient que l'Organisation a mis en place un processus interne de contrôle et vérifient l'efficacité de ce processus : c'est ce que l'on appelle la conformité.

3.2 Traduction dans le modèle de Crosby

La traduction dans le modèle de la tortue de Crosby est :

- chaque processus (la tortue) embarque sa fonction de contrôle ;
- les n tortues produisent donc un ensemble de contrôles ;
- on crée une n+1ème tortue qui supervise les contrôles précédents, c'est le principe de la conformité ;
- cette n+1ème tortue embarque elle-même sa fonction de contrôle - la conformité se pilote - et en général on ne va pas plus loin (on ne crée pas une conformité de la conformité) ;

Ambiguïté mesure / contrôle

La version anglaise de la norme ISO utilise le terme de « measurement », qui est à entendre au sens de « mesurer un élément telle une longueur ». Le mot français « mesure » est ambigu car il signifie aussi bien « prendre des mesures » au sens de « réaliser une série d'actions dans le but de... » que « mesurer la longueur d'une table ».

Dans la suite de cet opus, on s'en tiendra aux strictes définitions suivantes :

- *« mesure » est à entendre au sens de « réaliser une série d'actions », au sens de l'ISO 27002 ;*
- *« contrôle » au sens de contrôler l'efficacité d'une mesure.*

Le modèle de la tortue possède entre autres avantages d'être très visuel, et donc très utile pour expliquer à la fois aux opérationnels et aux décideurs la notion de conformité, en partant du bas.

3.3 Notion de maturité du processus de contrôle

Il est donc possible de dégager une échelle de maturité d'un processus de contrôle, qu'il s'agisse de la patte avant gauche d'une tortue ou de la tortue « Conformité » elle-même :

• niveau 0 : l'Organisation[3] n'a rien mis en œuvre pour contrôler le processus ;
• niveau 1 : un contrôle du processus est effectué, de façon irrégulière, à la faveur d'une demande ponctuelle ou à la suite d'un incident ;
• niveau 2 : le contrôle du processus est effectué de façon régulière et périodique par un agent externe à l'Organisation : DPO, RSSI, Qualiticien, etc. ;
• niveau 3 : l'Organisation contrôle elle-même le processus, un agent externe à l'Organisation vient vérifier l'efficacité de ce contrôle ;
• niveau 4 : l'ensemble des contrôles est centralisé dans un processus de Conformité interne à l'entreprise et transversal ; les responsables internes de cette conformité (DPO, RSSI) piochent dans ce référentiel central pour diligenter en interne des audits visant à mesurer l'efficacité des contrôles selon un calendrier spécifique.

Exemples :

• la gestion de l'AD ne comporte aucun contrôle du nombre de comptes admin de domaine : niveau 0 ;
• la gestion de l'AD comporte des contrôles périodiques réalisés par le RSSI ; niveau 3 ;
• la gestion de l'AD embarque un contrôle périodique des comptes admins de domaines, le RSSI vérifiant le bon déroulement de ces contrôles : niveau 4 ;
Autre classification
On peut aussi imaginer un découpage des niveaux de maturité calqué sur l'échelle COBIT à 5 niveaux, c'est selon.

3 Organisation est à entendre comme « service » : la DSI est une Organisation selon cet acronyme

3.4 Structure générale de la conformité

La structure générale de la conformité est donc :

• des vecteurs / incitateurs déclenchent la mise en place de processus métier ;
• ces processus doivent être surveillés (contrôlés), ce qui implique la création d'un registre des contrôles ;
• chaque item de la cartographie des processus pointe sur ou plusieurs éléments du registre des contrôles, chaque élément du registre des contrôles couvre un ou plusieurs processus (liaison n-n) ;
• l'objectif est de factoriser les items du registre des contrôles ; un même contrôle peut couvrir plusieurs processus, typiquement la revue des comptes d'accès au Datacenter qui sert à la fois pour la certification des comptes, l'ISO 27001, la certification HDS, etc.

3.5 Déclinaison opérationnelle

3.5.1 Le registre des contrôles

Avec un objectif de niveau 4 sur l'échelle de maturité ci-dessus, il convient de centraliser l'ensemble des contrôles effectués dans un registre central - un simple tableau. Par exemple :

ID	Détail	Statut	Propriétaire	Référentiel	Chapitre	Procédure	Rapport
CTRL001	Scan surface périmétrique Internet	Actif	cSSI	ISO 27001		W:/ISO27001/CTRL001/Procedure	W:/ISO27001/CTRL001/Rapport
CTRL002	Contrôle du nombre de compte admin de domaine	Actif	cSSI	ISO 27001		W:/ISO27001/CTRL002/Procedure	etc.
CTRL003	Revue des habilitations GEF	Actif	DSI	Certif C		W:/CAC/CTRL003/Procedure	etc.
CTRL004	Revue des accès Datacenter	Actif	DSI	ISO 27001, Certif C		W:/ISO27001/CTRL004/Procedure	etc.
CTRL005	Revue de la PSSI	Actif	RSSI	HAS, HOPEN, ISO 27002, Certif C		W:/HAS/CTRL005/Procedure	etc.
CTRL006	Contrôle des accès DPI	Actif	DPO	RGPD		W:/RGPD/CTRL006/Procedure	etc.
CTRL007	Révision du registre des traitements RGPD	Actif	DPO	RGPD		W:/RGPD/CTRL007/Procedure	etc.

3.5.2 Le calendrier des contrôles

Le registre correspond à du « Plan », l'exécution des contrôles (le « Do ») est tenue à jour dans un tableau de ce genre :

ID	Détail	Trimestre 1	Trimestre 2	Trimestre 3	Trimestre 4
CTRL001	Scan surface périmétrique Internet	29/01/AA			
CTRL002	Contrôle du nombre de compte admin de domaine	15/01/AA			
CTRL003	Revue des habilitations GEF		14/04/AA		
CTRL004	Revue des accès Datacenter	OK			
CTRL005	Revue de la PSSI			15/09/AA	
CTRL006	Contrôle des accès DPI	13/02/AA			
CTRL007	Révision du registre des traitements RGPD				30/12/AA

OK	KO

3.5.3 Remarques

Il faut noter que le processus de conformité lui-même se mesure, il n'est donc pas anormal de trouver dans le registre des contrôles un contrôle portant justement sur le processus de conformité.

De la même manière, la norme ISO27001 rend obligatoire un audit interne ainsi qu'une revue des objectifs du SMSI (la revue de direction) : ce sont deux contrôles que l'on doit retrouver dans le registre.

4. INDICATEURS : LA MESURE COMME OUTIL DE PILOTAGE

4.1 La restriction de l'ISO 27001

Stricto sensu, la norme ISO27001 n'impose pas de tenir à jour des indicateurs (le mot « indicateur n'apparaît absolument nulle part dans les normes ISO27001 et ISO 27002 de 2017). La seule obligation est de définir des objectifs de sécurité du SI (chapitre 6.2) qui doivent être mesurables (si possible). Cela fait référence à l'un des deux documents chapeau d'un SMSI, à savoir la Politique de Sécurité de l'Information (PSI), à ne surtout pas confondre avec la PSSI.

En substance, la PSI est la lettre que la Direction Générale pourrait afficher dans le hall de l'entreprise et qui stipule les grands objectifs stratégiques voulus par le grand patron. Par exemple, la société Darty pourrait afficher un objectif clair d'avoir un maximum de clients satisfaits de ses services, la chaîne d'hôtel Accord pourrait avoir pour objectif de n'avoir que peu de réclamations client, etc.

Pour un SMSI, il pourrait s'agir par exemple :

- d'avoir une DSI formée aux enjeux de sécurité du SI ;
- d'avoir un taux de disponibilité de la plateforme technique élevé ;
- d'avoir un fort taux de confiance des « clients », internes ou externes.

La PSI n'est pas supposée mentionner un chiffre précis, il revient aux opérationnels de collecter ce chiffre lors de contrôles dédiés. Par exemple, un contrôle peut porter sur le taux de personnels de la DSI qui ont reçu une formation à la SSI depuis moins de 2 ans, et produire cet indicateur, qui sera ensuite présenté en revue de direction du SMSI. Dans l'exemple ci-dessus, il n'y a donc que trois indicateurs obligatoires, pas un de plus.

4.2 Les autres indicateurs produits par l'ISO 27001

Il y a bien entendu d'autres cas d'usage qui engendrent la production d'indicateurs. Lorsqu'un contrôle produit un rapport KO qui relève pas mal d'anomalies, il est souhaitable de produire un indicateur le temps que les anomalies susnommées aient été résolues. Par exemple, si au dernier scan de la DMZ, vous relevez que 30 % des serveurs exposés sont vulnérables à la faille Log4j, il est conseillé de produire un indicateur de suivi, mais cet indicateur est éphémère, il n'a pas vocation à perdurer.

4.3 Les catégories d'indicateurs

Au-delà de ce qu'impose ou pas l'ISO 27001, il est tout de même possible de produire des indicateurs, pour différents objectifs. Ces indicateurs se classent en 2 macro-catégories : les indicateurs de système et les indicateurs d'état.

Les indicateurs de système ont pour objectif de mesurer le fonctionnement d'un processus, quel que soit ce qui est produit par le processus.

Exemple : le processus d'homologation

Différentes normes ou règlements imposent de mettre en place un processus d'homologation des projets. Fondamentalement, il s'agit d'analyser la conformité d'un projet selon tel ou tel critère (SSI, RGPD, etc.), mais cette homologation n'est jamais suspensive : la MOA peut parfaitement décider de suivre ou pas l'avis de l'entité qui homologue au nom du principe selon lequel la MOA est propriétaire de ses risques, ici de conformité.

Le fait que 100 % des projets soient passés par le processus d'homologation est un indicateur qui concerne le bon fonctionnement du processus d'homologation, mais pas que 100 % des projets aient reçu le quitus GO de l'entité qui homologue. L'entité qui homologue a très bien pu émettre un avis négatif pour 100 % des projets, il n'en reste pas moins que le processus d'homologation fonctionne.

Les indicateurs d'état ont pour objectif de mesurer une grandeur précise hors de tout contexte de processus : % de projets qui ont reçu une homologation positive, % de projets en retard, % de personnels formés à la SSI, % de PC sans AV conforme, etc.

Monitorer et mesurer

La norme ISO 27004 dans sa version anglaise utilise deux termes distincts : monitorer un processus (système) et mesurer (état).

Ces indicateurs d'état peuvent souvent être classés selon le triptyque habituel : stratégique, tactique, opérationnel.

Contrôle des tableaux d'indicateurs

Rien n'empêche de positionner un contrôle dans le registre des contrôles, qui vérifie la production régulière des tableaux d'indicateurs officiels, ainsi que la révision du périmètre de ces tableaux. Cela peut donner lieu à un indicateur de système (monitoring) et à un ou plusieurs indicateurs d'état (mesure).

On peut bien entendu imaginer d'autres classifications des indicateurs : indicateurs d'efficacité, de conformité, de communication, d'avancement, qualitatifs, quantitatifs, etc.

5. La construction opérationnelle des tableaux de bord

5.1 Les erreurs courantes

En général, lorsqu'une organisation (DSI, établissement, etc.) se met à la production d'indicateurs, elle commet quelques erreurs classiques, sans grandes conséquences si le tir est corrigé mais pour lesquelles on constate quelquefois un entêtement inutile. Et notamment :

• trop d'indicateurs : maintenir une liste importante d'indicateurs, cela suppose de collecter régulièrement des informations du terrain (pas toujours automatisables), de les travailler, de les filtrer, etc. ; pour le tableau de bord à destination de la Direction Générale, il est fortement conseillé de ne pas dépasser une page A4 recto et pas plus de 30 indicateurs simples ;
• indicateurs impossibles / coûteux à collecter : par exemple mesurer l'efficacité du système de sauvegarde suppose de collecter, jour par jour, les sauvegardes en échec (et les causes), tâche qui devient rapidement chronophage voire impossible ;
• indicateurs non pertinents : c'est un grand classique, le nombre de spam bloqués en entrée de DMZ est un indicateur qui ne sert absolument à rien, tout comme le nombre de bugs corrigés dans le code d'un logiciel : dans ces deux exemples, le chiffre pertinent est justement ce qui n'est pas bloqué ni corrigé, chiffres évidemment très difficiles à obtenir ;
• ambiguïté dans la définition des indicateurs : c'est aussi une erreur classique au début ; par exemple « taux de personnels de la DSI formés à la SSI » est imprécis et se transforme rapidement en « taux de personnels de la DSI formés à la SSI sur 12 mois glissants » ;
• confusion entre indicateur de système et indicateur d'état : voir plus haut pour la différence ;
• modification de la définition des indicateurs à posteriori pour « rentrer dans les clous » : les auditeurs ISO adorent tomber sur ce genre de tour de passe-passe, qui est très difficile à masquer ;

Trop, toujours trop
L'erreur la plus courante reste tout de même la profusion d'indicateurs. Il semble que les organisations pêchent systématiquement par le « toujours plus », sans se demander si « toujours mieux » ni signifierait pas « toujours moins ».

5.2 La méthode - PDCA

Il est fortement conseiller de procéder pour les indicateurs selon le principe de l'amélioration continue : commencer petit et modeste pour ensuite étendre la liste des indicateurs selon un processus entièrement maîtrisé. Appliquer l'amélioration continue,

ici aussi : Plan Do Check Act ou PDCA.

D'autre part, lorsque la DSI est soumise à plusieurs obligations réglementaires (HAS pour tout le monde, Instruction 309 / MATURIN-H, voire NIS) il y a un réel travail d'ingénierie à réaliser pour ne pas avoir à maintenir autant de tableaux d'indicateurs que de textes.

ISO 27001 à la base de tout

Selon le périmètre retenu, l'ISO 27001 couvre environ 90 % des 23 indicateurs de NIS. D'où l'intérêt de factoriser. Et d'où l'intérêt d'une certification ISO si tant est que cela devait être prouvé.

5.3 Exemples de tableaux de bord

Une simple recherche par mots-clés ramène pas mal d'exemple de tableaux de bord. On trouve par exemple :

- l'annexe B de l'ISO 27004 qui liste 35 indicateurs relatifs à la sécurité opérationnelle du SI ;
- un exemple de tableau de bord de la DSI produit par la DGOS et accessible sur le site de l'ANAP (voir Annexe 1) ;
- les indicateurs de l'instruction 309 (repris en partie dans MATURIN-H) ; (voir Annexe 2) ;
- les indicateurs HOPEN, qui ont connus plusieurs évolutions et également repris en partie dans MATURIN-H (voir Annexe 3) ;
- les 23 mesures de la directive NIS pour les OSE (Opérateurs de Service Essentiels) ;
- un exemple de tableau d'indicateurs permettant de mesurer la protection face au risque cyber (voir Annexe 4) ;

On ne produit pas les mêmes indicateurs selon le public cible. Il est conseillé pour une DSI de produire a minima les tableaux de bord suivants :

- un tableau de bord d'indicateurs stratégiques pour une Direction Générale ;
- un tableau de bord des indicateurs tactiques communiqué en interne de la DSI pour du pilotage d'activité ;
- un tableau de bord des indicateurs SSI, par exemple celui de l'Annexe 4 ;

Bien entendu, si la DSI dispose de certifications (ISO 27001, ISO 9001, ITIL, etc.), ces certifications imposent de produire certains tableaux de bord, nonobstant les précautions d'usage mentionnées plus haut.

6. Les bénéfices collatéraux

Avoir mis en place un dispositif formel de production d'indicateurs (qui rentre lui-même dans la roue PDCA) consomme certes du temps (et encore il faudrait faire la balance entre ce que cela consomme et ce que cela fait économiser rien qu'en interne, mais c'est un autre débat), mais a aussi l'immense avantage de produire des « bénéfices collatéraux » avec certains acteurs externes.

Par exemple si l'établissement souhaite souscrire une assurance cyber (le périmètre de couverture des assurances n'est pas l'objet de cette publication), alors l'assureur potentiel pourra prendre comme point d'entrée le tableau des indicateurs déjà existant en interne, tableau qui pourra d'ailleurs évoluer selon ce que l'assureur demandera de rajouter (pour autant que cela soit faisable).

Autre acteur, les commissaires aux comptes qui, d'expérience, adorent littéralement tomber sur un établissement qui a déjà mis en place un processus de conformité car ils le voient comme un cap dans la maturité des processus de contrôle.

Enfin, la maturité d'un processus de conformité est de nature à augmenter la confiance des parties intéressées au sens ISO 27001 : les fournisseurs, les utilisateurs internes, les usagers, la direction générales, les organismes de tutelle, etc.

7. CONCLUSION

Demander à des MOA de mettre en place des dispositifs (documents, organisation, etc.) dans le cadre par exemple d'un PCA-PRA ou d'un plan blanc est une nécessité que personne ne conteste. Mais personne ne conteste non plus que, sans vérification régulière, ces dispositifs suivent la loi de la thermodynamique qui stipule que l'entropie (le désordre) tend inexorablement à se répandre, et il est certain que 6 mois plus tard, le document est obsolète, les moyens matériels ne fonctionnent plus ou ont été « temporairement » empruntés sans retour, etc.

La seule réponse à cela est la mise en place d'un processus de conformité : le propriétaire de l'actif (le document ou le dispositif) est aussi chargé des vérifications, et un processus central est chargé de vérifier que cette vérification a bien été réalisée. Un dispositif à deux étages, en somme.

Pour un RSSI comme pour un DPO, et en particulier dans le cas d'une arrivée sur un poste ou dans une nouvelle entreprise, évaluer la maturité générale de ce dispositif de conformité est un exercice redoutable - d'ailleurs à ce stade, dans le monde de la santé, seules les DSI qui ont franchi l'étape d'une certification ISO peuvent prétendre à une organisation de ce type.

Cela pose d'ailleurs la question de savoir si les équipes qui travaillent avec le RSSI doivent être des techniciens, ou des qualiticiens. Si le RSSI est hors de la DSI, la mise en place de ce processus de conformité a pour conséquence évidente que ce sont des qualiticiens qu'il faut recruter pour assister le RSSI, les personnels de culture technique doivent rester dans la DSI.

INDICATEURS DE CYBERSECURITE DES DISPOSITIFS MEDICAUX

Par Christophe MILLET, Cyber Risk Manager, Sham - groupe Relyens

Approche métier : Point de vue du Groupe Relyens

1. Introduction

A l'occasion d'échanges avec les équipes en charge de la sécurité du système d'information des établissements de soins, il est assez fréquent d'observer une certaine crispation lorsqu'il s'agit d'évoquer le périmètre des dispositifs médicaux. En effet, nombre d'établissements font preuve d'un certain fatalisme face aux différents fournisseurs, auxquels il est reproché de se montrer distants, voire hermétiques, face aux enjeux de cybersécurité qui peuvent impacter leurs équipements.

Pourtant, l'obligation qui leur est faite de maintenir le risque technologique sous contrôle les amène bien à intégrer, de fait, des enjeux de cybersécurité. Pourquoi les établissements ne perçoivent-ils pas cet apport de valeur ? Comment évaluer la prise en compte de la sécurité par les fabricants ?

2. Quels sont les motifs de divergence de point de vue entre établissements et fabricants ?

2.1 Motif réglementaire

En détaillant le règlement UE 2017/745 relatif aux dispositifs médicaux [1], nous remarquons que le mot cybersécurité, ainsi que d'autres caractéristiques connexes (ex : extorsion), ne sont pas explicitement mentionnés. D'autres risques sont bien identifiés en tant que tels et fortement priorisés, comme, par exemple, le risque de blessure, la présence de champs magnétiques, les effets électriques, les gaz, la maintenance, l'incendie, l'explosion, l'ergonomie (etc…). Toutefois, nous trouvons une « timide » indication indirecte de l'attention aux enjeux de cybersécurité au paragraphe 14.5 où il est stipulé que « Les dispositifs qui sont destinés à être mis en œuvre avec d'autres dispositifs ou produits sont conçus et fabriqués de manière à ce que leur interopérabilité et leur compatibilité soient fiables et sûres. ». Lorsque l'on

regarde les normes embarquées dans le processus de marquage CE, nous retrouvons les mêmes priorisations des risques à traiter, la cybersécurité étant encore considérée comme un « nice-to-have » plutôt qu'un « must-have ».

Point très positif, notons que l'article 103 du nouveau règlement EU a prévu l'instauration d'un groupe de coordination en matière de dispositifs médicaux (GCDM). Celui-ci a publié un document spécifiquement dédié à la cybersécurité à destination des fabricants sous la référence « MDCG 2019-16 Guidance on Cybersecurity for medical devices » [2]. Il y a bien une volonté d'inscrire durablement la cybersécurité au sein de la démarche de pilotage des risques technologiques.

2.2 Motif budgétaire

Toutes les populations appellent de leurs vœux des équipements à risque zéro, surtout en matière de santé publique. Peu, cependant, plébisciteraient une hausse de la fiscalité pour financer un tel objectif. Si la crise sanitaire a bien permis aux établissements de bénéficier de dotations exceptionnelles, il s'agit de mesures temporaires [3], et il est à craindre que l'insuffisance chronique des budgets santé perdure à l'avenir. Cette politique de cadrage des dépenses publiques ne permet pas aux états de s'offrir le luxe d'accentuer le qualitatif étant donné que la demande porte d'abord sur le quantitatif, c'est-à-dire la mise à disposition d'équipements à grande échelle.

Cette logique d'austérité économique se traduit également dans les processus d'achats d'équipements médicaux. En effet, privilégier l'acquisition des « équipements les moins chers » revient, à moyen terme, à favoriser les fabricants qui ont la lecture la plus épurée (la moins contraignante) de la réglementation, ce qui leur permet de diminuer leurs coûts de conception et de production.

Ainsi, nous sommes questionnés ponctuellement par des praticiens tentés d'utiliser des matériels inappropriés, voire sans marquage réglementaire, spéculant sur le fait qu'à fonctionnalité égale, ceux-ci sont bien moins onéreux, ce qui est effectivement le cas. En agissant ainsi, nous rejoindrions la politique santé de certains pays émergeants qui, faute de moyens, ont abandonné toute politique de contrôle du risque technologique, se concentrant exclusivement sur le bénéfice pour l'exercice de la médecine. Dans une telle approche, le dispositif se résume à un assemblage de technologies utilisables aux seuls risques et périls de l'établissement : il n'y a pas de garantie de contrôle du risque technologique, ce qui permet d'atteindre des prix bien inférieurs, mais désengage le fournisseur de toute responsabilité relative aux défauts technologiques. Dans une telle approche, l'absence du rôle de fabricant, au sens juridique du terme, produit cependant des situations inextricables lorsque la question du partage de responsabilité survient en cas d'accident médical. L'absence de porteur de risque ne peut que se manifester au détriment des victimes, c'est-à-dire les patients qui subissent ces aléas lors de leurs parcours de soins.

2.3 Motif technologique

Depuis de nombreuses années, j'ai eu l'opportunité d'évoquer la prise en compte de la cybersécurité dans l'industrie en général, et auprès de fabricants de dispositifs médicaux en particulier. Il y avait un consensus général pour dire que l'attention à la sûreté d'un système était un sujet plus complexe et qui englobait nécessairement les enjeux de cybersécurité. Il n'y avait donc pas de motif d'inquiétude, puisque qu'il est établi que « qui peut le plus peut le moins ». Cette posture, somme toute radicale de prime abord, est-elle fondée, ou bien s'agit-il d'un déni de réalité ?

Du point de vue technologique, c'est-à-dire considérant la manière dont sont conçus ces systèmes, la réponse serait « oui » et « non ».

D'abord, « oui » du fait que toutes les normes et standards techniques communs aux systèmes à haute fiabilité pour adresser les problématiques de dangerosité (Safety) et de confidentialité (Privacy) reposent sur la même base que les points d'attention qui incombent à la cybersécurité, à savoir :

- Le risque de comportement instable (non conforme au cahier des charges) est principalement causé par des défauts de spécification ou d'implémentation d'éléments logiciels
- L'efficacité de ces systèmes repose sur leur capacité à traiter des données de toutes natures
- La fiabilité des systèmes repose sur une attention forte à maintenir la disponibilité, l'intégrité et la confidentialité des données, ainsi que la constitution d'éléments de traçabilité concernant le cycle de vie des données

Ensuite, « non » car si la vision du risque est bien identique, la prise en compte des impacts diffère de la manière suivante :

- Le design des dispositifs médicaux répond à une logique de comportement en « fail safe ». Cette logique prévoit, en principe, une capacité du système à vérifier en permanence si tous les sous-systèmes (notamment ceux qui font partie des fonctions dangereuses) sont opérationnels. Lorsqu'un défaut survient, une position de repli non dangereuse est adoptée (qui est déterminée du point de vue médical) et un système d'alerte est activé pour solliciter le personnel médical. Dans cette approche, le maintien sous contrôle du risque technologique est confié à l'intelligence humaine, ce qui nécessite la présence permanente de personnels qualifiés au chevet des patients. A contrario, en cybersécurité, on attend des équipements qu'ils soient capables d'agir directement par eux-mêmes sur le supposé défaut, qui a créé une situation de faux positif (ou de faux négatif), ce qui n'est pas acceptable en présence de situation dangereuse.
- Chaque fabricant doit pouvoir garantir le comportement de son système isolément des autres, l'attention aux risques liés à l'interopérabilité (vision « System Of Systems ») demeurant un objectif inatteignable car un fabricant ne peut pas concevoir un système fiable dans de multiples environnements qu'il ne connaît pas (considérant qu'il y a autant de cas d'usage que d'établissements).

C'est d'ailleurs probablement cette multiplicité des cas d'usage qui a conduit les autorités à établir un principe de co-responsabilité entre les fabricants de

dispositifs médicaux et les établissements qui les utilisent.

3. Quels indicateurs peut-on utiliser ?

3.1 Concernant le parc d'équipements déjà en place

Une première indication du niveau de cybersécurité des dispositifs médicaux est inscrite à l'intérieur des contrats qui vous lient avec vos fournisseurs. La cybersécurité y est-elle mentionnée ? Quels sont les engagements de service (SLA) qui y sont associés, notamment à quelle fréquence les maintenances de sécurité sont-elles prévues ? Le contrat prévoit-il une clause de renonciation à recours, ou bien une forte limitation (financière) de la responsabilité du fournisseur ?

Une seconde indication réside dans l'adhésion volontaire des fabricants aux normes ISO80001. Il s'agit d'un écosystème normatif entièrement consacré à la « Sécurité, efficacité et sureté dans la mise en œuvre et l'utilisation des dispositifs médicaux connectés ou des logiciels de santé connectés ». Les bonnes pratiques présentes sont exclusivement à destination du secteur médical et les fabricants qui s'y conforment démontrent une véritable maturité sur le sujet. Pour information, le document MDCG 2019-16 Guidance on Cybersecurity for medical devices [2] s'est largement inspiré de l'ISO80001, ce qui atteste de la pertinence de ce standard.

Une troisième indication réside dans la réactivité dont font preuve vos fournisseurs lorsque vous les sollicitez. En effet, le CERT-SANTE [4] publie régulièrement des bulletins d'alertes de cybersécurité. Vos fournisseurs communiquent-ils sur ces éléments de manière proactive ? Comment réagissent-ils lorsque vous évoquez les alertes en cours ?

3.2 Concernant le processus d'achat des (futurs) équipements

D'autres pays ont fait le choix de questionner les fabricants de dispositifs médicaux dès l'acquisition. En effet, à service métier égal, il est préférable de s'équiper d'une technologie plus vertueuse en matière de contrôle du risque. La difficulté consistait à établir un référentiel qui soit en phase avec les enjeux et les technologies couramment embarquées dans les dispositifs médicaux. Ainsi, aux USA, la NEMA (National Electrical Manufacturers Association) [5] a regroupé depuis 1926 des fabricants de dispositifs médicaux désireux d'établir ensemble des critères de bonnes pratiques. En particulier, le document Manufacturer Disclosure Statement for Medical Device Security [6] ou MDS², aborde la question de l'évaluation du risque technologique

d'un dispositif médical. Il se présente sous la forme d'un questionnaire qui permet au fabricant d'expliciter ses choix, et ce tout au long du cycle de vie de son dispositif médical, ce qui permet aux établissements de mesurer l'effort à fournir pour maintenir ces équipements en condition de sécurité optimale. Ainsi, le risque numérique est exposé et qualifié avant acquisition, de sorte que les décisions sont prises en connaissance de cause. On notera que le document MDS² n'est pas un document à valeur légale, mais sa pertinence et sa notoriété sont telles qu'aucun fabricant américain ne se risquerait à ne pas le remplir ou à refuser de le mettre à disposition lors de ses réponses à appels d'offre. Nous gagnerions à nous inspirer de telles démarches en Europe.

On note également l'alignement entre le document MDS² et le standard ISO 80001-2-2.

4. Conclusion

L'implication des fournisseurs de dispositifs médicaux sur la thématique de la cybersécurité dépend de la capacité des établissements à les interpeler à bon escient. Dans les phases d'acquisition, l'utilisation du formulaire MDS² a fait ses preuves car elle exige des fabricants de rendre publique leur politique de cybersécurité concernant leurs matériels : les moins vertueux doivent donc afficher (et assumer) leur positionnement, ce qui produit un impact notable sur l'image de marque. A cet égard dans l'idéal, le dépouillement d'appels d'offre gagnerait à introduire la cybersécurité en tant que critère de notation.

Une fois les matériels en service, les fournisseurs auront tendance à mieux servir les établissements qui sont bien renseignés sur l'état de leur parc ainsi que les risques en cours. Il est donc préférable de se tenir informé sur l'existence de mises à jour concernant le parc technologique auprès des institutions étatiques, professionnels du domaine ou directement auprès des fabricants. Ainsi, munis de ces éléments d'information, vous sollicitez à bon escient vos fournisseurs qui se sentent « en devoir » de vous répondre, et surtout d'intervenir. En l'absence d'informations concrètes, un établissement n'arriverait pas à capter l'attention de ses fournisseurs avec la même efficacité.

La collecte et la qualification de ces informations étant complexes à gérer à la main, il est préconisé de s'équiper d'un outillage spécialisé en dispositifs médicaux, qui reste le meilleur appui sur le long terme pour mener à bien cette mission de vigilance et de suivi pour conserver les risques numériques sous contrôle.

Références

[1] Règlement EU 2017/745 relatif aux dispositifs médicaux
https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32017R0745

[2] Document MDCG 2019-16 Guidance on Cybersecurity for medical devices
https://ec.europa.eu/docsroom/documents/41863/attachments/1/translations/en/renditions/native

[3] Le gouvernement Castex a-t-il doublé le budget de l'hôpital ?
https://www.francetvinfo.fr/sante/maladie/coronavirus/le-gouvernement-castex-a-t-il-double-le-budget-de-l-hopital_4928455.html

[4] Site du CERT-SANTE
https://www.cyberveille-sante.gouv.fr/

[5] National Electrical Manufacturers Association
https://www.nema.org

[6] Manufacturer Disclosure Statement for Medical Device Security
https://www.nema.org/standards/view/manufacturer-disclosure-statement-for-medical-device-security

relyens sham | sofaxis

04 72 75 20 00
Service client Sham - groupe Relyens
relationclient@sham.fr

www.relyens.eu

ANTICIPATION DU RISQUE ET PARTAGE D'INFORMATIONS : VERS UNE RESILIENCE CYBER DE LA SANTE

Par Pierre OGER, Directeur Général et Fondateur d'EGERIE

Approche métier : Point de vue d'EGERIE

Depuis 2019, des cyberattaques se multiplient contre les hôpitaux français. Ce phénomène témoigne d'un marché criminel en plein essor. Conscients de cette menace, les pouvoirs publics ont dégagé des moyens importants pour renforcer la sécurité informatique des établissements de santé et mieux les préparer face aux risques numériques.
A cela doit s'ajouter la sensibilisation des équipes, la consolidation de l'organisation et de la gouvernance autour de la cybersécurité. De la volonté de partager et de coopérer naîtra une résilience cyber de la santé en France.

1. Une menace cyber grandissante pour les établissements de santé

La fragilité des systèmes informatiques et l'essor du marché des données de santé encouragent les cyber attaques. On recense aujourd'hui une tentative d'attaque par semaine contre des infrastructures de la chaîne hospitalière, alors que ces dernières ne survenaient que mensuellement avant 2019.

2. Des obligations déjà fortes

Les hôpitaux font partie des opérateurs d'importance vitale, et doivent donc, comme l'exige la Loi de Programmation Militaire (LPM) renforcer la sécurité de leurs systèmes d'information. Celle-ci prévoit une mise à niveau de la sécurité des systèmes d'information des OIV afin d'éviter, par exemple, qu'une cyberattaque ne pirate la continuité de service des blocs opératoires, ne prenne le contrôle de tout un hôpital, de son réseau électrique, altère les fonctions d'un objet connecté de santé ou falsifie les données vitales liées à un patient impliquant des conséquences quant au bon fonction

de la Nation mais aussi sur la vie même des patients.
L'entrée en application de la LPM implique un investissement conséquent de la part des OIV, et l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) estime à 3 ans la durée nécessaire à ces derniers pour assurer un déploiement global des mesures de cybersécurité édictée.

Les établissements de soins de santé, y compris les hôpitaux et cliniques privées, sont désormais intégrés à la liste des «opérateurs de service essentiels » (OSE). En effet, l'interruption de leur service a un impact significatif sur le fonctionnement de la société. Ils doivent ainsi appliquer strictement les règles de sécurité propres aux SI considérés comme essentiels (SIE), signaler à l'ANSSI chaque incident et faire réaliser régulièrement des audits de cybersécurité. Fin 2020, une soixantaine de structures seulement avait fait l'objet d'un audit externe de l'ANS. Ceux-ci avaient uniquement pour objectif de valider les prérequis du programme Hôpital Numérique (Hop'EN). Les structures de santé doivent ainsi consacrer systématiquement 5 à 10 % de leur budget à la sécurité des systèmes d'information. Ainsi, aucun projet ne pourra désormais faire l'objet d'un soutien de la part de l'État si cet engagement n'est pas constaté.

Le gouvernement impose également dans tous les cursus de formation des professionnels de santé l'intégration d'une sensibilisation à la cybersécurité.

3. 30% des professionnels de santé ne se sentent pas concernés par les questions de cybersécurité

L'hébergement des données de santé recueillies à l'occasion d'activités de prévention, diagnostic, soin ou suivi social est lui aussi soumis au respect de conditions, dont le respect se matérialise par l'obtention d'un agrément en vertu de l'article L. 1111-8 du Code de la santé publique.

Ainsi, seuls les acteurs certifiés « HDS » peuvent stocker des données. Cette certification nécessite le respect de certains normes et exigences et la prestation d'hébergement doit faire l'objet d'un contrat comportant un certain nombre de mentions obligatoires.

Dans le cadre de leur transition digitale, les acteurs de la santé et du secteur médico-social doivent impérativement tenir compte du risque cyber. Cette prise en compte, pour être efficace, suppose à la fois une gestion technique (mobilisation de la DSI et du RSSI) mais également un pilotage juridique (Direction Juridique et du DPO). Plusieurs objectifs devront être fixé :

- Prévenir efficacement les menaces (contractualisation des relations avec les sous-traitants, rédaction de procédures et chartes, etc.) ;
- Démontrer le respect de la réglementation applicable (RGPD, législation spécifique au secteur de la santé et/ou aux OSE/OIV) ; et
- Réagir aux attaques lorsque celles-ci ont

lieu tant d'un point de vue technique (ex. PCA/PRA) que d'un point de vue juridique (activation de l'assurance, notifications, information des personnes, communication de crise, gestion des responsabilités des prestataires etc.)

4. De nouveaux moyens alloués

Le programme Hôpital Numérique 2012-2017 a permis de développer, de moderniser et de renforcer la sécurité des systèmes d'information hospitaliers (SIH).

Le gouvernement alloue désormais un budget total de plus de 375 millions d'euros aux établissements de santé pour lutter contre les cyber menaces. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) et l'Agence du numérique en santé (ANS) leur proposent également un accompagnement humain pour renforcer la sécurité de leurs SI. Elle collabore étroitement avec la cellule Accompagnement Cybersécurité des Structures de Santé (ACSS) de l'Agence du Numérique en Santé (ANS). L'objectif : renforcer la sécurité des SIH. Le gouvernement entend ainsi allouer un budget spécifique au profit de la cybersécurité des établissements de santé : 2 milliards d'euros sacralisés par le Ségur de la Santé afin d'optimiser les SIH, 350 millions d'euros spécifiquement dédiés à la sécurisation des SIH et 25 millions d'euros alloués par l'ANSSI à la réalisation d'audits pour les accompagner dans leur démarche de cyber sécurisation. Ce financement permettra d'accélérer le déploiement du « service national de cyber surveillance en santé » en partenariat avec l'Agence du Numérique en Santé (ANS) et à développer les moyens du dispositif « cyber veille en santé » pour augmenter les capacités de réaction et d'appui aux structures de l'ANS en cas d'incidents ou de cyber attaques.

Le chef de l'État a annoncé la création d'un observatoire permanent du niveau de sécurité des établissements de santé. Il sera chargé de coordonner les pratiques, surveiller les vulnérabilités et mutualiser les expériences.

5. Manager et anticiper le risque cyber

Nous avons l'une des meilleures protections en santé dans le monde. Faisons en sorte qu'il en soit de même pour celle de nos systèmes de santé de demain.
Le management du risque cyber dans la santé est un enjeu clé pour notre avenir. Cette cybersécurité exige une analyse et une cartographie des risques dynamiques. Celle-ci doit être la pierre angulaire de tout plan d'action.

Elle vise à définir toutes les actions nécessaires pour parvenir à un niveau de risque qui puisse être accepté en toute connaissance de cause, au bon niveau de décision. L'outillage permet ainsi de modéliser une cartographie des risques et de rendre la situation plus concrète. Le côté visuel, intuitif, permet de partager plus facilement les informations entre les différentes entités de l'organisation.

6. Partage d'informations & coopération active

« Nous nous efforçons de réaliser un travail d'accompagnement des structures et de concrétiser notre mot d'ordre : le partage. Beaucoup de décideurs pensent se fragiliser en partageant l'information. C'est pourtant tout à fait l'inverse. Les défenseurs ont tout à gagner à échanger l'information, et c'est ce que nous proposons : étudier les modes d'attaque, les profils des attaquants, les failles éventuelles et les compiler dans une bibliothèque pour en faire profiter tous les acteurs de la filière. » explique Pierre Oger, Directeur Général et Fondateur d'EGERIE.

Une situation à risque s'appréhende rarement sans information extérieure et ne peut se résoudre seul. Pour se protéger, il faut partager et diffuser cette appréciation du risque pour que toute la communauté en bénéficie par,effet rebond. *« Le parallèle avec les combattants est frappant : un soldat ne part jamais seul au front. Il a besoin des autres pour avancer, s'adapter à la situation et prendre des décisions. Il est donc tout à la fois émetteur d'une information utile et récepteur d'informations émanant de la communauté. »* souligne Pierre Oger.

Si nous voulons anticiper la prochaine crise qui ne tardera pas à sévir, faire figurer la cybersécurité au coeur de la gouvernance constitue un préalable. S'intéresser aux scénarios prospectifs des schémas d'attaques pouvant toucher le SI demain permettra, non pas d'éviter les cyberattaques, mais de réagir vite et mieux, et d'assurer la résilience de nos systèmes vitaux.

« Le futur de l'analyse de risques sera de plus en plus industrialisé. Le seul moyen d'assurer une prise de décision rapide est de se faire assister par un outil d'intelligence artificielle, qui améliore le processus complet de l'analyse, de la gouvernance et donc de la maîtrise de risques. Aujourd'hui l'enjeu de l'analyse de risques se situe autour de sa modélisation. Il faut l'automatiser davantage pour parvenir à construire des arbres d'attaques encore plus sophistiqués et plus précis, répondants aux besoins évolutifs des utilisateurs finaux » ajoute Pierre Oger.

La gestion de la cybersécurité implique donc autant une sécurisation technique des SI qu'une prise de conscience de l'ensemble des parties prenantes des établissements face aux risques encourus. Les directions générales doivent porter un message et une ambition clairs sur la gestion des risques de cybersécurité. Toutefois, c'est uniquement en impliquant les communautés médicales et soignantes que les établissements de santé pourront faire face aux risques de cyberattaques.

Aujourd'hui, plus que jamais, redonnons une nouvelle dimension collective et collaborative à la cyber-vigilance !

EGERIE
INTEGRATED CYBERRISK MANAGEMENT
Tél. : +33 (0)4 94 63 81 09
contact@egerie.eu
www.egerie.eu

8. ANNEXE 1 : RÉFÉRENCES ET BIBLIOGRAPHIE

Production de la DGOS sur les tableaux de bord d'activité de la DSI :

https://ressources.anap.fr/medias/MAJ_productions/Production_DGOS/Fiche_6_tableaudebord_GHT.pdf

« Management de la sécurité de l'information », Alexandre Fernandez-Toro, Eyrolles, 2018 : la référence sur l'ISO 27001. Date un peu mais le volet gestion de projet reste d'actualité

9. ANNEXE 2 : INSTRUCTION 309

Priorité	Délai	Date limite	Item
1	6 mois	14/04/2017	prise en charge de la fonction sécurité des systèmes d'information par la direction (éventuellement mutualisée dans un GHT)
			mise en oeuvre d'une charte utilisateur
			réalisation d'une cartographie des ressources informatiques (postes de travail, serveurs, équipements actifs, équipements biomédicaux)
			établissement d'une procédure de signalement et de traitement des incidents de sécurité SI
			équipement de tous les postes de travail par un antivirus
			sécurisation des comptes par mots de passe robustes et renouvelés périodiquement
			mise en oeuvre de sauvegardes régulièrement testées
2	12 mois	14/10/2017	établissement d'une procédure formelle d'appréciation du risque avant toute mise en production d'un SI (homologation)
			mise à jour régulière des systèmes d'exploitation
			organisation du maintien en conditions de sécurité de l'ensemble des systèmes numériques (mises à jour des éditeurs et constructeurs)
			identification et protection de tous les accès à internet et de télémaintenance
			sécurisation du wifi, séparation des réseaux professionnels et des réseaux invités
			mise en oeuvre d'une gestion des comptes utilisateurs avec profils et droits différenciés (utilisateur, prestataire, administrateur)
			identification des actions de formation SSI et actions de sensibilisation dans le plan de formation annuel des personnels
3	18 mois	14/04/2018	cloisonnement du réseau de la structure par grandes familles d'usage (administration, paie, plateau technique…) et par niveaux de sécurité homogènes
			définition des modalités d'enregistrement et d'analyse des traces d'accès
			encadrement contractuel de tous les accès par des prestataires au réseau de la structure et vérification des clauses de réversibilité
			réalisation et tenue à jour d'une analyse de risque SI de la structure, avec définition et mise en oeuvre du plan d'action associé
			engagement de la direction sur la réduction d'un nombre limité de risques chaque année

10. ANNEXE 3 : INDICATEURS HOPEN

Pré-requis	Indicateur	Description	Fréquence	Seuil
Identités, mouvements	P1.1	Taux d'applications au cœur de la gestion du processus de soins, de la GAP et du PMSI connectées à un référentiel unique d'identités de patients	Semestrielle	70% des applications connectées
Identités, mouvements	P1.2	Cellule d'IV opérationnelle	Semestrielle	Fonctionnement régulier (1/trim), existence d'un rapport d'activité
Identités, mouvements	P1.3	Taux d'applications au cœur de la gestion du processus de soins, de la GAP et du PMSI connectées à un référentiel unique de séjours et de mouvements de patients	Semestrielle	70% des applications connectées
Identités, mouvements	P1.4	Existence d'un référentiel unique de structure de l'établissement (juridique, géographique et fonctionnel) piloté et mis à jour dans les applicatifs en temps utile	Semestrielle	Existence du référentiel unique de structure interne et des procédures de mise à jour
Fiabilité, disponibilité	P2.1	Existence d'un PRA du SI	Semestrielle	Existence
Fiabilité, disponibilité	P2.2	Définition d'un taux de disponibilité cible des applicatifs et mise en œuvre d'une évaluation de ce taux	Semestrielle	Existence d'une observation du taux de disponibilité avec la fourniture du taux de disponibilité cible des applicatifs, de la méthode d'évaluation et de l'évaluation du taux de disponibilité en utilisant cette méthode
Fiabilité, disponibilité	P2.3	Existence de procédures assurant un fonctionnement dégradé du processus de soins en cas de panne du SI, et un retour à la normale	Semestrielle	Existence
Confidentialité	P3.1	Existence d'une PSSI pour les applications de soins fondée sur une analyse de risque – existence d'un référent sécurité	Semestrielle	Existence
Confidentialité	P3.2	Existence d'une charte utilisateur, en particulier pour le cœur de métier, diffusée aux personnels, nouveaux arrivants et fournisseurs	Semestrielle	Existence et processus d'acceptation
Confidentialité	P3.3	Information des patients sur les conditions d'utilisation des informations de santé à caractère personnel	Semestrielle	Existence et procédure de diffusion
Confidentialité	P3.4	Taux d'applications gérant des données de santé et intégrant un dispositif d'authentification personnelle	Semestrielle	90% des applications concernées, intégrant un système de déconnexion sur inactivité et renouvellement de mot de passe
Confidentialité	P3.5	Taux d'applications permettant une traçabilité des connexions au SIH	Semestrielle	100% des applications incluant l'horodatage de l'accès utilisateur

11. ANNEXE 4 : EXEMPLE DE TABLEAU D'INDICATEUR D'EXPOSITION CYBER

CHAPITRE	SECTION	ITEM	EXIGENCE	PREUVE
A5	A.5.1	Charte utilisateur	Rédiger une charte utilisateur	Charte de moins de 3 ans avec PV de passage aux instances
			Mettre en place un processus de rencontre bi-annuelle RSSI / DG et cSSI / DG	Rapport de la dernière rencontre de moins de 1 an
A6	A.6.1	Homologation projets SI	Mettre en place un processus d'homologation formel avant lancement de projet SI	Modèle d'homologation révisé depuis moins de 1 an + 3 enregistrements de moins de 1 an
A7	A.7.2	Compétences (besoins de formations)	Mettre en place un plan de sensibilisation	Plan de sensibilisation + feuilles de présence de la dernière session
			Dérouler des tests de phishing	Rapport des 3 derniers tests
A9	A.9.2	Politique d'habilitation DPI	Rédiger une politique formalisée et signée de la MOA	Document Politique de moins de 3 ans
			Auditer la Politique	Rapport d'audit de moins de 1 an
		Sécurisation AD	Identifier les comptes à privilèges	Rapport PingCastle de moins de 1 an
			Appliquer la politique de mots de passe des comptes à privilège	Politique de mot de passe de moins de an
			Disposer d'un rapport d'attaque des comptes à privilège	Rapport d'attaque de moins de 1 an
			Disposer d'un rapport de l'état de l'AD avec les outils ANSSI	Rapport AD de l'ANSSI de moins de 1 an
			Etre en capacité de changer les mdp des admin locaux des PC	Procédure de moins de 1 an
			Distinguer les comptes admin locaux PC / serveurs	
			Réviser les comptes admin locaux des PC	Rapport PingCastle de moins de 1 an
			Serveurs DIAMOND : supprimer les accès anonymes	Liste des accès à jour
			Serveurs DIAMOND : délivrer des accès nominatifs avec mot de passe complexe	Liste des accès nominatifs à jour, politique de mot de passe de moins de 1 an
			Durcir les comptes AD locaux aux machines de la DMZ	Rapport de moins de 1 an
			Restreindre l'accès Internet des comptes à privilège (admin)	
			Auditer les comptes d'accès fournisseur VPN	
			Auditer les comptes d'accès distants admin et utilisateurs	
A12	A.12.3	Sauvegarde	Disposer d'une solution de protection des sauvegardes contre un cryptolocker	Schéma d'architecture de moins d'1 an
			Sauvegarder les serveurs DIAMOND en OFF LINE ou en mode Read Only	
			Disposer d'un plan de test de restauration, y compris des serveurs DIAMOND	Document technique de moins de 1 an, rapport des 3 derniers tests de restauration
	A.12.6	Sécurisation des serveurs DIAMOND	Restreindre les accès par filtrage des IP	Liste des filtres à jour
		Adaptation de l'infrastructure système	Maintenir uptime de serveur < 6 mois	Rapport PingCastle de moins de 1 an
			Superviser les partages accessibles en CT	
			Tester le passage des serveurs de fichiers en RO	Rapport de test de moins de 1 an
			Tester la coupure des serveurs de fichiers	
			Identifier les adhérences des SF	
			Mettre à jour les patches OS serveur et PC	Etat de moins de 3 mois
			Tester la coupure Internet	Rapport de test de moins de 1 an
		Sécurisation DMZ	Vérifier la capacité de couper rapidement l'accès aux webmails externes	Rapport de moins de 1 an
			Monitorer le trafic SSL sortant	
			Réviser les règles du FW	
			Contrôler la conformité des serveurs exposées (OS, patchs, etc.)	
		Sécurisation du parc de terminaux	Vérifier l'état des OS et des patchs	Rapport de moins de 1 an
			Etre en capacité d'activer le Firewall des PC	Procédure de moins de 1 an
		Protection AV	Scanner le parc PC et serveurs pour trouver les équipements non-protégés par un AV	Rapport de moins de 1 an
		SIEM/SOC	Déployer un SIEM	Schéma d'architecture de moins d'1 an
			Déployer un SOC	
A13	A.13.1	Segmentation réseau	Segmenter le LAN interne	Schéma d'architecture VLAN de moins d'1 an, existence d'un Firewall interne en coupure
			Séparer le VLAN d'administration, isoler les VLAN vitaux (biomed, REA, Urgences, etc.)	
A16	A.16.1	Gestion des incidents	Rédiger une procédure de déclaration des incidents au portail cyberveille et au RSSI-T	Procédure de moins de 1 an
A17	A.17.1	Applications METAL	Lister des applications METAL	Liste de moins de 1 an, validée par le RSSI-T ou cSSI
		Procédures dégradées	Rédiger les Procédures dégradées	100% des METAL couverts, documents validés par la MOA et révisés depuis moins de 1 an
		Test des Proc Degr et du PCA-PRA	Effectuer un test annuel	Dernier rapport de test
		Gestion de crise SI	Mettre en place un protocole de gestion de crise	Document de moins d'1 an
			Mettre en place un protocole face à une attaque malware	
			Tenir à jour un protocole de redémarrage du SI	
			Intégrer dans le plan de Situation Sanitaire Exceptionnelle un volet cyber	
A18	A.18.1	Assurance cyber	Souscrire un contrat d'assurance du risque cyber	

APSSIS

Association Pour la Sécurité des SI de Santé

84 rue du Luart
72160 Duneau

06 29 36 59 95

secretaire@apssis.com

www.apssis.com

Licence du document
Auteur : Cédric CARTAU
Ce document est sous licence Creative Commons BY-NC-ND-SA :
- BY : attribution de l'auteur initial
- NC : interdiction de tirer un profit commercial
- ND : impossible d'intégrer le document dans une œuvre composite
- SA : partage de l'œuvre, avec obligation de rediffuser selon la même licence ou une licence similaire (version ultérieure ou localisée)

Création graphique : Corvy-Graphisme