OPUS 2

APSSIS

GUIDE CYBER RÉSILIENCE

LES CYBERATTAQUES

SOMMAIRE

CYBER RÉSILIENCE

0.2 LES CYBERATTAQUES

SOMMAIRE

CYBER RÉSILIENCE

0.2 LES CYBERATTAQUES

1. INTRODUCTION

Le contexte mondial n'a jamais été aussi tendu au regard des cyberattaques. Même si le cas existe toujours, l'adolescent qui pirate le Pentagone depuis sa chambre mansardée a laissé depuis longtemps la place aux organisations plus ou moins mafieuses et aux groupes plus ou moins soutenus par des Etats plus ou moins voyous. Pour un certain nombre de cyberattaques qui ont pu être imputées à la Russie, le Président Russe s'est défendu en prétendant qu'il s'agissait de groupes internes incontrôlés. Cela ne veut pas dire que les occidentaux ne mènent pas ce genre d'opérations, simplement qu'ils sont dans la plupart des cas plus discrets - si l'on excepte le cas bien connu de l'attaque des centrifugeuses Iraniennes par le Mossad et la CIA[1].

Les malwares classiques existent depuis aussi longtemps que l'informatique elle-même, mais la préoccupation date des années 1990, avec les fameux virus type « I Love You », qui provoquaient l'écran bleu de la mort sur les systèmes Windows. Pendant des décennies, le domaine de la protection antivirale s'apparentait au jeu du gendarme et des voleurs, des missiles et des anti-missiles : c'était à celui qui stockait le maximum de signatures, à celui qui dépistait le plus vite les zéro-day, à celui qui savait mixer, dans le moteur de son antivirus (AV), à la fois de l'analyse par signature et de l'analyse comportementale.

La dernière grosse attaque virale dans le monde de la santé date des années 2008 et 2009 : il s'agissait d'un malware nommé Conficker (qui a sévi sous sa forme A, puis B puis C, chacune étant une mutation plus sophistiquée de la précédente) et dont l'effet essentiel était de provoquer des tempêtes de broadcast sur le LAN, mettant à genoux les équipements réseau. Pour échelle, la forme B arrivait à bloquer totalement le cœur de réseau d'une entreprise de plus de 5000 personnes avec seulement 100 PC infectés qui saturaient les liens, ce qui donne une idée de la virulence du malware.
Mais le seul effet de ce type de malware classique était de bloquer l'informatique : une fois l'ensemble du parc déverminé, patché et redémarré - ce qui pouvait prendre plusieurs semaines tout de même -, le fonctionnement du SI revenait à son mode nominal. En somme les malwares classiques correspondaient à une attaque en disponibilité (D) sur le triptyque DIC (Disponibilité, Intégrité et Confidentialité).

En 2015, est apparu le premier cryptolocker, forme spécifique de malware dont l'action consiste à chiffrer les données pour les rendre inintelligibles à celui qui ne possède pas la clé de déchiffrement. Les premiers cryptolockers étaient juste capables de chiffrer les données en local du poste de travail, ce qui est certainement plus grave pour un particulier (qui la plupart du temps stocke tout sur son C et fait peu de sauvegardes) que pour une entreprise (où les données sont stockées sur des partages, même si la dérive d'utilisation du C a toujours existé). Mais comme beaucoup l'avaient prévu, les générations suivantes ont été capables de chiffrer les données de tous les partages accessibles - et pas seulement ceux montés sur une lettre sur le poste de travail-, voire les DB accessibles, voire les systèmes plus sophistiqués telles les sauvegardes, les plateformes d'administration, etc.

Expliquer les cryptolockers
J'ai pu constater que certains non spécialistes ne comprennent pas l'impact d'un chiffrement de données, étant persuadés qu'une donnée chiffrée peut être déchiffrée sans problème par n'importe qui. Il est important d'expliquer que le chiffrement nécessite une clé - sans rentrer forcément dans les arcanes des systèmes à clés symétriques ou asymétriques- et que celui qui ne possède pas cette clé a définitivement perdu ses données dans la plupart des cas.

Les attaques les plus sophistiquées sont aujourd'hui capables non seulement de chiffrer les partages de fichiers, mais aussi les plateformes de stockage des VM, des CITRIX ou TSE, les consoles d'administration,

1 Malware Stuxnet, voir https://fr.wikipedia.org/wiki/Stuxnet

etc. En somme de bloquer tout le SI de façon durable, et d'en exfiltrer les données soit pour être capable de démontrer à la cible que l'attaquant dispose des données chiffrées et de la clé de chiffrement afin d'être plus crédible pour « vendre » cette clé de déchiffrement, soit pour faire du chantage à la publication de données sensibles sur Internet. En ce sens, ces attaques impactent non seulement le D, mais aussi le I et le C.

Avec les cryptolockers, on atteint un sommet - même à y réfléchir à deux fois on ne voit clairement pas ce qui pourrait être pire -, et les outils de protections classiques atteignent leur limite.

Pas que dans les livres

En 2016 et 2017, LOCKY avait attaqué pas mal d'hôpitaux. Fin 2019 le CHU de ROUEN a subi une attaque d'ampleur, qui a bloqué une bonne partie de son SI. On ne compte plus les hôpitaux US, anglais, allemand qui ont dû faire face à des attaques avec demande de rançon. Les cryptolockers, ce n'est pas que dans les livres.

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

2. La limite des réponses classiques

2.1 Le zero-day

Pendant des années, ce qui a empêché les RSSI de dormir était le zero-day (ou 0-day) : le malware qui vient à peine de sortir et dont la signature n'est pas dans les bases des AV du marché. Par définition, tout AV dont le seul mode de détection / protection est basé sur l'analyse de signature est inefficace contre ce genre de menaces. Dans les faits, tous les AV du marché embarquent des moteurs d'analyse comportementale ou heuristique.

Techniques marketing d'entrée de gamme
Je suis régulièrement sollicité par des fournisseurs d'AV concurrents à celui dont dispose mon établissement. Les ingénieurs commerciaux de ces éditeurs tentent de m'expliquer en quoi leur AV est « révolutionnaire », « bien au-dessus des autres » et me produisent des courbes et des statistiques tendant à démontrer la plus grande efficacité de leur produit par rapport à la concurrence. Bien évidemment ils se gardent bien de dire quelles versions sont comparées, sur quel périmètre, et les chiffres produits sont totalement invérifiables, donc faux par définition.

La question se pose de savoir si le zero-day est toujours la pire menace. Certes, en fabriquer un n'est pas techniquement compliqué (il existe sur le Dark Web des plateformes spécialisées avec de belles interfaces graphiques qui permettent d'en générer à la volée). Mais si vous êtes un hacker, pourquoi vous ennuyer à fabriquer un zero-day (qui par définition ne va être efficace qu'une journée ou deux) alors qu'il suffit de balancer un mail comportant une pièce jointe qui installe un Trojan sur le PC de l'utilisateur imprudent et vous donne ainsi un accès au SI que vous ciblez ? Les attaques de 2019 ont mis en œuvre ce mécanisme, ce qui prouve son efficacité. C'est aujourd'hui la pire menace qui existe.

2.2 La pêche au filet ou la chasse à courre

Si vous êtes une cible pour la NSA ou le FSB, clairement les éléments du présent guide ne sont pas pour vous. Seules des mesures de confinement quasi total de la partie sensible de votre SI seront efficaces, bien entendu couplées à de la protection périmétrique physique trapue, de la surveillance de vos propres salariés, etc.

Les modes d'attaques de 2019 ne relèvent pas de l'attaque ciblée, mais plutôt de la pêche au filet : un pirate balance un mail à un grand nombre de personnes avec un lien ou une pièce jointe de type Troyan, et regarde qui a mordu à l'hameçon. Dès qu'une personne appartenant à une organisation publique ou privée a cliqué par erreur sur le lien ou la pièce jointe, le pirate a un pied dans la place et l'étape d'observation du réseau interne par le pirate commence : collecte des IP et de la cartographie du LAN, des serveurs sensibles, des DB métiers, etc. Enfin dès que le pirate estime être en possession de suffisamment d'informations techniques, il lance la troisième phase, celle de l'attaque.

Les temps de détection
Les attaques silencieuses telles que celle décrite ci-dessus peuvent durer des jours, voire des mois car elles sont très difficiles à détecter. Quand l'attaquant passe à l'action c'est déjà trop tard. Cas emblématique: la société Deloitte a subi une attaque d'exfiltration de ses données sensibles et a mis des mois à s'en rendre compte. Cela peut arriver à n'importe qui.

2.3 Ne pas être naïf

Pour éviter qu'un utilisateur clique par erreur sur une pièce jointe suspecte, il est de bon ton d'affirmer qu'il faut former les employés : direction générale, cadres, agents, informaticiens, etc. Si la formation ou l'information des gens était efficace avec le nombre de campagnes anti-tabac ou contre la violence routière déroulées par les pouvoirs publics depuis des décennies, il y a belle lurette qu'il n'y aurait plus un seul fumeur ni un seul accident de la route dans les pays occidentaux. La formation, il faut en faire pour ne pas se faire reprocher d'avoir négligé cet aspect de la sécurité, mais clairement face aux attaques modernes, cela ne suffit pas.

Efficacité d'une formation sécurité.
Parler de chiffrement asymétrique à des non-informaticiens est une erreur de programme. Une bonne formation de sécurité doit s'adapter au public concerné, être régulière, s'appuyer sur du vécu et dans l'idéal sur des mises en situation.
N'importe quel agent a déjà reçu des mails provenant d'un héritier africain souhaitant lui faire bénéficier d'une partie de son immense fortune, ou d'une sculpturale beauté russe qui veut absolument l'épouser : c'est un bon point de départ d'une action de sensibilisation.

En effet, il n'est pas possible de parier sur l'efficacité de ce dispositif, du fait que même si 99,99 % des agents vont être prudents, il suffit d'un seul clic malencontreux pour écrouler le LAN d'une grande entreprise - et qui peut décemment affirmer que pas un seul de ses utilisateurs, pas une seule fois, ne commettra le clic de trop ?

Il ne faut pas partir du principe que l'on fera tout pour qu'un pirate ne rentre jamais sur votre LAN. En revanche, il faut partir du principe que cela arrivera et mettre en place des mesures pour augmenter la résilience du SI, c'est-à-dire d'une part sa capacité à résister aux éventuels dégâts que le pirate peut commettre, et d'autre part à redémarrer après un niveau de dégâts tel que le SI s'est arrêté tout ou partie.

3. STRATÉGIE GÉNÉRALE

3.1 Particularités du monde la santé

La santé est particulière dans le sens où, d'un hôpital à l'autre, voire même d'un service à l'autre, les préoccupations au regard des critères habituels de sécurité ne sont pas les mêmes. Dans un service de soins aigus, c'est surtout la disponibilité qui est importante (voler des données et les publier sur le Dark Web n'empêchera pas de soigner, même si cela aura des conséquences), alors que dans un service de psychiatrie, la confidentialité des données est la préoccupation majeure (bloquer le DPI a moins de conséquences, et encore ce n'est que partiellement vrai car la partie circuit du médicament peut être critique au regard du D).

D et I avant tout
La crise du COVID19 a montré que dans un SI de santé, dans une situation critique, les deux critères les plus importants sont le D et le I : dans ces cas on fait souvent une croix sur le C. Mais c'est aussi une faiblesse vis-à-vis des attaques qui pourraient survenir dans ce contexte.

L'appréciation des risques selon les activités doit donc être déroulée a minima. Mais cela ne remet en rien en cause le fait que le blocage de tout le SI par un cryptolocker peut rapidement devenir problématique : même dans un hôpital psychiatrique, il y a des activités qui relèvent du D en termes de préoccupation majeure.

3.2 Inverser la question

La question n'est pas tant de savoir ce qui est critique dans un établissement de santé : répondre à cette question entraîne le déroulé complet d'une analyse de risques à la sauce EBIOS (dans différentes moutures plus ou moins lourdes), qui produira au final un épais rapport difficile à exploiter car difficile à hiérarchiser. De plus, ce type de démarche aborde le risque en partant du métier, ce qui est normal mais qui ne correspond pas à l'approche d'un pirate qui dans la plupart des cas se fiche éperdument des « actifs métiers» au sens EBIOS : il veut simplement bloquer le SI.

La question est plutôt la suivante : si je suis un pirate, si je dispose d'un accès dans un SI hospitalier et si je veux mettre HS de façon durable tout le SI, comment dois-je m'y prendre ?

Si on veut mettre HS le DPI, certes un pirate peut passer par la couche haute (l'application), mais pourquoi faire compliqué quand il lui suffit de mettre HS les baies de stockage, ce qui lui permet en même temps de mettre HS tous les logiciels ? En d'autres termes, l'approche « par le haut » est une erreur: si je suis un pirate, je vais m'attaquer aux fondations du SI plutôt qu'à ses applicatifs métier ; ce sont donc ces fondations qu'il faut identifier et sécuriser.

Survivalisme et sécurité du SI
La démarche présentée se rapproche de celle des survivalistes : si je dois presque tout perdre, que dois-je sauver en priorité ? C'est aussi une approche de type « Armageddon», à savoir le fait d'envisager un scénario qui dépasse de très loin la petite panne électrique dans un Datacenter.

La bonne nouvelle, c'est que ces éléments de fondation sont peu nombreux. La mauvaise nouvelle, c'est que ces éléments de fondation sont peu nombreux, dans le sens où il n'y a pas à taper sur beaucoup de briques pour écrouler l'édifice.

3.3 Classification des actifs

3.3.1 La classification METAL

Dans toute démarche de PCA-PRA, il est nécessaire de classifier les actifs. Je suggère d'adopter une classification « marketing-friendly » : GOLD, SILVER et BRONZE. Chaque classe doit faire référence à un niveau de service (par exemple les applications GOLD bénéficient d'une GTR de 4h alors que pour le BRONZE c'est 48h), et tout ce qui n'est pas dans ces 3 classes (regroupées sous l'acronyme METAL) ne bénéficie que d'un service en mode best effort.

En d'autres termes, le jour où le SI s'arrête totalement, on commencera à remettre en service les actifs GOLD, puis les SILVER puis les BRONZE, et le reste quand on pourra.

Dans l'idéal, la DSI a listé l'ensemble des actifs METAL et leur a attribué des niveaux de service, comprenant a minima :

- **les GTR en heures ouvrables** ;
- **les GTR en heures non ouvrables** ;
- **le taux de disponibilité cible sur l'année** ; ce point est complexe, car ce n'est pas la même chose d'afficher 99,9 % de taux de disponibilité (soit 8 heures environ d'arrêt) avec 1 panne de 8h ou avec 480 pannes d'1 minute ;
- **les plages d'arrêt pour maintenances**, avec a minima celles qui nécessitent un arrêt / relance du client ou du serveur, celles qui nécessitent un arrêt d'1h et celles qui nécessitent un arrêt de 4h ou plus.

Vers le PCA-PRA
La classification METAL est un point d'entrée vers une démarche globale de PCA-PRA, mais sort du cadre de ce guide.

3.3.2 La classification DIAMOND

La cyber résilience au regard des attaques en cryptolocker impose de définir une quatrième classe d'actifs : les actifs DIAMOND. Les actifs DIAMOND ne sont que des actifs techniques: pas besoin de faire des dizaines de réunions avec les MOA et la DG pour en faire la liste ni définir des cotations.

Lien avec la directive NIS

Définir les actifs DIAMOND est un très bon début pour les établissements qui sont soumis à la directive NIS : certaines personnes pensent que la directive NIS ne fait référence qu'à des actifs sensibles métier, ce qui est totalement faux. Une première itération des SIE (Système d'Information Essentiel) peut parfaitement restreindre la discussion aux actifs DIAMOND.

3.3.3 Les actifs DIAMOND

Ils sont au nombre de 11 :

- **l'Active Directory (AD)** ou tout annuaire centralisé de type LDAP ;
- **l'infrastructure PKI** ;
- **le réseau**, au moins pour ce qui concerne le cœur de réseau, et le niveau site et bâtiment ;
- **les serveurs de fichiers** ;
- **la messagerie** ;
- **les consoles de supervision** (NAGIOS ou équivalent) ;
- **la console d'administration de l'AV** ;
- **la console de déploiement (SCCM)** ;
- **le système de sauvegardes** ;
- **la DMZ** ;
- **les DNS et DHCP.**

Il est à noter qu'en fonction du périmètre de l'étude, on pourra rajouter à cette liste les consoles de supervision GTB / GTC, les systèmes de sécurité / sûreté. Attention, le contexte d'utilisation de ces équipements rend compliqué la mise en œuvre de certains chantiers.

Quoi d'autre ?

Si l'établissement dispose d'un écosystème complet SCADA qui est administré par une console de supervision, il faut bien entendu rajouter cette console aux actifs DIAMOND.

3.4 La démarche globale

Elle consiste à dérouler 7 chantiers, qui impactent chacun les actifs DIAMOND.

Même si la mise en œuvre initiale doit focaliser l'essentiel des ressources, dans un premier temps, il faut garder à l'esprit que ces chantiers doivent s'inscrire dans une démarche globale d'amélioration continue de type PDCA[2].

3.4.1 Phase Plan

Nul besoin de chercher la complexité, la phase Plan comporte :

- **un responsable de ce projet global** : souvent le RSSI, ou un responsable technique, ou un spécialiste sécurité SI ;
- **le présent document** ;

3.4.2 Phase Do

Il s'agit du déroulé des mesures décrites dans le présent document, chapitre Do.

3.4.3 La phase Check

Il s'agit du déroulé des mesures décrites dans le présent document, chapitre Check.

3.4.4 La phase Act

Idéalement, le responsable du projet doit produire un rapport annuel d'état d'avancement. Cela peut aussi être un paragraphe dans le rapport annuel global sur la SSI de l'établissement.

2 PDCA : Plan, Do, Check, Act

4. LA PHASE DO

4.1 Chantier 1 : durcir l'AD

4.1.1 Contexte

L'AD est certainement le composant le plus sensible d'un SI : c'est quasiment le seul actif logique avec lequel il est possible de mettre HS tout un SI en trois clics. Pour autant, l'expérience montre que son état général au regard des bonnes pratiques de sécurité est souvent préoccupant voire inquiétant. Le chantier 1 est une priorité absolue.

Cas d'école
Dans un établissement de moins de 100 lits dont le SI comportait en tout et pour tout 2 applications, 3 serveurs physiques et un informaticien à mi-temps, j'ai pu observer que l'AD comprenait pas moins de 35 comptes admin de domaine : tous les fournisseurs disposaient d'un compte ayant ce niveau de privilège, sans compter les stagiaires et les informaticiens précédents (dont les comptes étaient toujours actifs).

Il existe pas mal d'outils de très bonne facture pour faire un audit technique de l'AD. Un des plus connu est ALSID[3], créé par des anciens de l'ANSSI. Il existe aussi le remarquable PingCastle[4], outil Open Source et qui remonte déjà un bon nombre de non-conformités.

4.1.2 Actions

C01A01 : nettoyer les comptes à privilège
Il convient de nettoyer les comptes admin de domaine et d'en limiter le nombre à un maximum de 5.

PingCastle sur une chaise
Si vous n'avez jamais lancé un PingCastle (ou un outil équivalent) sur votre AD, un bon conseil : quand vous le ferez pour la première fois, restez bien assis !

Les ingénieurs système doivent disposer d'un compte à hauts privilèges (admin de serveur, admin de sauvegardes, etc.), mais pas d'un compte admin de domaine qui, par définition, sert à faire des opérations sensibles sur le domaine.

Résistance au changement
Les adminsys vous expliquent qu'il n'est pas possible de fonctionner sans compte admin de domaine, que cela complexifie leur travail, le ralentit, etc. Tous les arguments avancés sont faux. Sans exception.

Il ne doit y avoir absolument aucun compte de service qui soit admin de domaine :

- si un compte de service réalise des opérations sur un serveur spécifique, il doit être admin du serveur ou d'un groupe de serveur, problématique qui se règle par un groupe global ;
- si un compte de service réalise des opérations transversales telle la sauvegarde, il existe des rôles spécifiques (admin de sauvegardes) ;

En particulier, le compte d'admin du schéma doit faire l'objet d'une protection spécifique.

Lorsqu'un ingénieur système a besoin de

3 https://www.alsid.com/fr
4 https://www.pingcastle.com/

réaliser des opérations qui nécessitent un compte admin de domaine, le compte ou le privilège doivent lui être temporairement attribués et leur usage doit être strictement limité à la durée et à l'opération et retirés immédiatement après.

Aucun fournisseur ne doit disposer d'un compte admin de domaine. La seule exception concerne une opération technique programmée qui nécessite ce niveau de privilège (par exemple une migration de version AD), mais dans ce cas le compte doit être nominatif et actif uniquement le temps de l'opération. Et dans tous les cas, le compte à privilèges dont dispose le fournisseur doit respecter la règle du moindre privilège.

La facilité de l'inflation

Morceaux choisis de discussion entre un RSSI coriace et un fournisseur qui veut un compte admin de domaine :

- *bonjour monsieur le RSSI, j'aurais besoin d'un compte admin de domaine pour mon intervention ;*
- *vous comptez faire une modification sur le domaine ?*
- *ben non ;*
- *alors vous n'avez pas besoin d'un compte admin de domaine ;*
- *en général chez les autres clients on me le donne ;*
- *ici vous n'êtes pas chez les autres clients, vous êtes à l'hôpital XXX ;*
- *alors je fais comment ?*
- *vous me donnez la liste des privilèges techniques strictement nécessaire à votre intervention, et c'est ce que vous aurez ;*
- *on ne m'a jamais posé la question, je ne sais pas ;*
- *il y a toujours une première fois !*

C01A02 : durcir les mots de passe des comptes à privilèges

Tous les comptes à privilèges doivent se conformer à une politique spécifique de mot de passe fort : longueur et complexité adéquate.

Il ne faut pas d'obligation de changement régulier hors reset du mot de passe suite à départ ou opération spécifique : par expérience cela conduit à affaiblir les mots de passe ou à les retrouver sur des carnets à spirales.

Faiblesse des mots de passe

Certains malwares tentent de casser les mots de passe faibles des comptes à privilèges par une attaque en force brute ou par dictionnaire.

Il convient de prévoir un système de stockage sécurisé : un bon KeePass[5] fait parfaitement l'affaire.

C01A03 : disposer d'un outil d'attaque des mots de passe

Le plus connu de ces outils est Mimikatz[6] et sert à auditer la robustesse des mots de passe. Il doit être utilisé pour tester la robustesse des mots de passe des comptes à privilèges, mais aussi pour réaliser des campagnes ciblées sur l'encadrement, voire le reste de la DSI.

Afficher le top 10

Après une campagne interne de brutforce, et bien entendu après la remédiation des mots de passe faibles, on peut afficher (envoi massif par mail interne, affichage sur l'Intranet) le top 10 des mots de passe les plus faibles, ou les plus nuls, bien entendu sans nommer les agents à l'origine. Effet garanti.

5 https://keepass.info/
6 https://github.com/gentilkiwi/mimikatz

4.1.3 Conseils

L'AD est un composant ultra-sensible : un bon nombre des attaques récentes et médiatisées (TV5 Monde, Saint-Gobain, etc.) ont subi des attaques dont la chaîne d'actions implique l'AD.

Il est impératif de nommer un propriétaire de cet actif : autant la question du propriétaire de l'actif « Réseau » ou « Sauvegarde » fait peu débat dans les DSI, autant celui de l'AD rencontre le plus souvent un silence gêné : or, tout actif sans propriétaire voit son entropie croitre irrémédiablement et très rapidement.

Les deux dangers des organisations modernes
La patate chaude (aucun responsable), et le recouvrement de missions (se marcher sur les pieds).

Il existe des outils très puissants de l'analyse de l'AD (certains sont fournis par l'ANSSI ou sous forme de prestations par des sociétés spécialisées), mais avant d'aller chercher les failles connues des ultra spécialistes, il convient en premier lieu de sécuriser la base: les comptes et les mots de passe.

De plus, les mesures de base de sécurisation de l'AD qui ne seraient pas prises ni maintenues dans le temps, non seulement exposeraient l'établissement à des attaques potentielles, mais en plus à des sanctions venant des autorités de régulation (CNIL, ANSSI, etc.) qui constateraient, lors d'un audit post-incident, ces manquements.

4.2 Chantier 2 : segmenter le réseau

4.2.1 Contexte

La contribution du réseau à la protection antimalware se résumé à un mot : segmentation. D'une part parce qu'il est nécessaire de segmenter pour compartimenter la propagation d'un malware, d'autre part parce qu'il peut être nécessaire de couper certains sous-réseaux en cas d'infection pour protéger des sous-réseaux plus sensibles que d'autres.

Principe du sous-marin
Les sous-marins sont conçus de telle sorte qu'en cas de fuite d'eau, il est possible d'isoler la partie du sous-marin qui est inondée pour préserver le reste.

4.2.2 Actions

C02A01 : Isoler les VLAN vitaux

Dans un établissement de santé, il y a certains réseaux qui doivent fonctionner absolument, alors que d'autres peuvent être sacrifiés pendant des jours voire des semaines dans les cas les plus extrêmes.

Ces réseaux critiques sont essentiellement :

- le réseau SAMU ;
- le réseau GTB / GTC ;
- le réseau BIOMED ; ce cas est complexe car dans les gros CHU, il n'existe pas un mais de multiples réseaux BIOMED. Une ingénierie de bon niveau est nécessaire sur ce point. De façon générale, il s'agit des systèmes SCADA, mais l'identification et la classification de ces réseaux est un sujet à part entière qui dépasse largement le cadre de cette publication ;

De plus et dans certains cas, le lien avec des réseaux tiers critiques doit pouvoir être isolé car ces communications inter réseaux sont critiques : lien avec le SDIS (les pompiers), avec l'EFS, etc. Attention, ce point induit des complexités importantes en matière d'architecture.

4.2.3 Conseils

Côté réseaux, la difficulté des mesures est essentiellement technique : cela nécessite une ingénierie de très bon niveau, surtout pour les grosses structures.

Il existe des outils logiciels qui permettent une découverte automatisée de l'infrastructure réseau ; le plus souvent, ce sont des outils qui accompagnent les équipements actifs, donc souvent fournis par le constructeur. L'acquisition d'un outil de ce genre est importante, car la structure d'un réseau bouge souvent et tenir à jour un PowerPoint est compliqué dans la durée.

C02A02 : séparer le VLAN d'administration

Une des mesures visant à protéger la partie admin consiste à séparer le VLAN d'administration technique (c'est une des mesures, mais pas la seule). Par VLAN d'administration technique, on entend le VLAN qui permet aux administrateurs systèmes de gérer les serveurs, les routeurs, les baies de disques, les sauvegardes, etc.

Le test du Firewall

Si à partir de n'importe quel PC de l'établissement, vous avez accès à l'interface d'administration (en Web) du Firewall, c'est une très bonne nouvelle pour les hackers.

4.3 Chantier 3 : restreindre les accès aux serveurs DIAMOND

4.3.1 Contexte

Les serveurs ou actifs de classe DIAMOND sont ceux pour lesquels une compromission par un attaquant aurait des conséquences rapidement désastreuses. Par exemple, si un attaquant parvenait à prendre le contrôle du serveur de management des AV du parc (PC, serveurs, etc.), il pourrait désactiver à distance toute la protection AV de l'établissement, voire introduire une mise à jour des signatures comportant des erreurs permettant de mettre HS l'ensemble du parc.

Erreur dans la mise à jour des signatures AV, crash assuré
Plusieurs entreprises en ont fait l'expérience: une erreur dans la base des signatures délivrée périodiquement (toutes les heures pour certains éditeurs) avec, par exemple, un processus système identifié à tort comme un malware, et tout le parc est HS pour une bonne semaine.

En plus de l'isolation du VLAN d'administration, il y a un certain nombre de mesures de base à déployer sur cette classe d'actifs.

4.3.2 Actions

C03A01 : supprimer les accès anonymes
Aussi surprenant que cela puisse paraître, il est courant de trouver des accès anonymes sur certains de ces actifs. Par exemple, la console de supervision (POM, NAGIOS, etc.) dispose souvent d'un compte anonyme. Certes ce compte ne dispose que d'accès en lecture seule, mais c'est une aubaine pour un attaquant potentiel, qui a ainsi accès à toute la cartographie du réseau en un clic.

C03A02 : restreindre les accès par filtrage des IP
Les serveurs DIAMOND doivent être accessibles, pour des actions d'administration, uniquement par les PC des adminsys. Le filtrage peut être effectué à partir d'un groupe d'adresses quand il s'agit de petites équipes pluridisciplinaires, ou par IP pour les grosses équipes.

Cette mesure peut être mise en œuvre si le projet de VLAN d'administration décrit plus haut n'est pas prévu à courte échéance.

C03A03 : délivrer des accès nominatifs avec mots de passe fort
Tout accès à un actif DIAMOND pour des actions d'administration doit être réalisé :

- avec un compte nominatif, distinct du compte agent comme le préconisent les bonnes pratiques ;
- avec un mot de passe fort conforme à la politique interne.

Les comptes génériques doivent être bannis.

Audit des accès SCCM
Le moindre audit sur la console SCCM fait apparaître des comptes d'admin qui ont quittés l'entreprise ou changés de fonction.

En particulier, le processus d'attribution ou de suppression d'un compte admin doit être documenté (cela prend une page maximum) et rigoureusement suivi.

4.3.3 Conseils

La sécurisation des actifs DIAMOND n'a rien de compliqué. Cela relève juste de la discipline régulière : revue régulière des mots de passe, suppression des comptes des agents ayant quitté l'équipe, politique de mot de passe robuste, etc.
Clairement, cela enquiquine tout le monde, les informaticiens voyant souvent cela comme une préoccupation de riche. Mais quand une entreprise se fait corrompre son AD et que l'on se rend compte après audit post-mortem que les mots de passe admin étaient génériques, avec des mots de passe de 4 caractères, alors on comprend mieux le sens de la phrase « la qualité coûte cher, mais la non-qualité encore plus ».

4.4 Chantier 4 : adapter l'infrastructure système

4.4.1 Contexte

Toujours dans l'optique d'améliorer la résilience face à un cryptolocker, il est nécessaire de mettre en œuvre plusieurs mesures. Certaines relèvent du bon sens et se trouvent dans toutes les publications de bonnes pratiques (mettre à jour les patches). D'autres sont en revanche un peu plus rares dans leurs mises en œuvre, telle la supervision des partages de fichiers.

Cette liste a clairement vocation à s'étendre avec le temps. Elle ne doit d'ailleurs être prise que comme guide. Nous invitons le lecteur à l'enrichir !

4.4.2 Actions

C04A01 : superviser l'uptime des serveurs
Un serveur qui n'a pas été redémarré depuis des mois voire des années est par définition non patché (les patches nécessitent souvent un reboot pour être effectifs). Il convient donc de réaliser des audits rapides (réalisables facilement avec PingCastle), et mener des campagnes de nettoyage.

C04A02 : superviser les partages accessibles en contrôle total
PingCastle permet de remonter la liste des partages accessibles en contrôle total sur le LAN, et le premier lancement est proprement stupéfiant : C$, D$, partages oubliés sur des serveurs, serveurs biomédicaux, etc.

Un partage en CT est une aubaine pour un attaquant humain ou un cryptolocker. Il convient de surveiller particulièrement ce paramètre.

C04A03 : pouvoir diffuser par SCCM des modifications du paramétrage des pare-feu internes de PC sur parc
En cas d'attaque en cours, il peut être

nécessaire d'augmenter temporairement le niveau de protection des PC, quitte à rendre inaccessibles certains applicatifs métier : cela nécessite de pouvoir déployer en quelques clics une nouvelle politique (GPO ou autre). Ce n'est pas le fait de savoir que c'est possible qui fait que le « jour j », on pourra dérouler cela rapidement. Cela doit donc être procéduré et testé.

C04A04 : tester le passage des serveurs de fichier (SF) en mode lecture-seule (RO, read-only)
En cas d'attaque en cours par un cryptolocker, pour stopper le processus de chiffrement, un moyen possible est de passer rapidement les partage en RO. Encore une fois, c'est techniquement possible mais cela doit être procéduré et testé.

C04A05 : tester la coupure des SF
Dans les cas extrêmes, il peut être nécessaire de couper totalement les SF. Encore une fois, c'est techniquement possible mais cela doit être procéduré et testé !

C04A06 : identifier les adhérences entre les SF et les progiciels métiers
En cas de coupure des SF, ou même simplement de passage en RO, il est possible qu'il y ait des adhérences entre les progiciels métiers et les SF, qui empêchent le fonctionnement de ces progiciels, par exemple un fichier de configuration sur un partage de fichier.

Il convient donc d'identifier ces adhérences, afin de les résorber dans un premier temps, et les isoler sur un ou plusieurs partages dédiés et managés par la suite.

C04A07 : mettre à jour les patches
Cela va sans dire, les patches doivent être systématiquement passés.

4.4.3 Conseils

Il n'y a aucune action complexe dans ce chantier : elles peuvent être étalées dans le temps, mais sont toutes indispensables. Le fait, par exemple, de constater un nombre affolant de partages en CT sur un LAN est révélateur du fait que cette problématique n'a jamais été prise en compte. Il n'y a aucune action complexe dans ce chantier: elles peuvent être étalées dans le temps, mais sont toutes indispensables. Le fait, par exemple, de constater un nombre affolant de partages en CT sur un LAN est révélateur du fait que cette problématique n'a jamais été prise en compte.

4.5 Chantier 5 : utiliser la sauvegarde

4.5.1 Contexte

En dehors des actions relevant du chantier 3 (en particulier maîtriser les comptes d'administration ayant accès à la console de supervision des sauvegardes), le système de sauvegarde doit être utilisé comme contre-mesure vis-à-vis des cryptolockers.

Il est de bon ton d'affirmer que le serveur de sauvegarde - ou les sauvegardes elles-mêmes - doit être mis hors ligne, seule façon de ne pas voir ses sauvegardes chiffrées. Une telle mesure est réalisable dans la sphère privée : il est tout à fait possible de faire ses propres sauvegardes sur une clé USB que l'on garde avec son trousseau de clés, même si, avec l'évolution des technologies mises en œuvre sur les Drive classiques (Dropbox entre autres), ce n'est plus forcément indispensable, car ces Drive mettent à disposition un système de snapshot permettant de remonter dans le

temps sur 30 jours, fichier par fichier.

Dans la sphère professionnelle, dès que l'on parle d'un établissement de plusieurs centaines d'employés, de plusieurs dizaines de serveurs ou plus, c'est totalement illusoire: la masse des données à sauvegarder a connu une telle explosion ces dernières années qu'entre la sauvegarde et la copie de cette sauvegarde, le système tourne en mode 24-7.

4.5.2 Actions

C05A01 : vérifier la capacité à isoler le serveur de sauvegardes

En cas d'attaque, les sauvegardes représentent le dernier filet de sécurité : quand tout aura été chiffré, c'est le seul endroit où récupérer ses données. Il convient de vérifier qu'il est possible rapidement (en quelques clics de souris) d'isoler totalement le serveur de sauvegardes du LAN. Attention, ce n'est pas si simple qu'il n'y paraît : si le serveur est en cours de job, arrêter les jobs peut prendre du temps ; si le système est virtualisé, l'isolation ne peut se résumer à débrancher un câble RJ45, etc.

Cette action nécessite juste d'écrire une procédure, de la tester et de la rendre facilement accessible.

C05A02 : sauvegarder tout ou partie des actifs DIAMOND sur les SF en mode RO

Les informaticiens font en général une confiance aveugle à leur AD et à ses mécanismes intégrés de redondance. En cas de corruption (cf. Saint Gobain), la corruption sera répliquée sur tous les serveurs AD. Il convient de réaliser, assez régulièrement, une sauvegarde de l'AD (export), à envoyer sur un partage de fichier qui est en mode RO. Le même raisonnement peut être tenu pour tous les actifs DIAMOND.

C05A03 : établir un plan de test des restaurations des serveurs DIAMOND

Affirmer qu'il faut tester ses sauvegardes relève à la fois du poncif et de l'aveuglement: quelle entreprise teste régulièrement (tous les mois) toutes ses sauvegardes ? Aucune ou presque.

En revanche, focaliser sur les tests des serveurs DIAMOND semble plus atteignable.

4.5.3 Conseils

Là encore il n'y a rien de complexe dans ce chantier : toutes ces mesures sont techniquement faciles à mettre en œuvre et peuvent être étalées dans le temps.

4.6 Chantier 6 : adapter la DMZ

4.6.1 Contexte

Par DMZ on entend tout le dispositif de protection périmétrique : firewalls bien entendu, mais aussi les proxy, relais de messagerie, passerelles techniques, revers-proxy, serveurs applicatifs, etc. Ce sont autant de point d'entrée dans le LAN.

4.6.2 Actions

C06A01 : scanner périodiquement l'ensemble des assets de la DMZ pour détecter les vulnérabilités
La présence d'une vulnérabilité connue sur un composant (OS, middleware, applicatif) est le premier vecteur d'attaque. Il existe une offre complète de scanners, à noter que l'add-on Wappalyser de Firefox permet de réaliser un premier état des lieux a minima.

C06A02 : durcir la gestion des comptes locaux aux machines de la DMZ
La présence d'un compte à privilège local sur une machine de la DMZ avec un MDP faible est une aubaine pour un attaquant potentiel. La difficulté, c'est que ces comptes sont justement locaux, les machines de la DMZ n'étant en général pas connectées à l'AD du LAN. La plus grande rigueur est de mise pour la gestion de ces comptes locaux : processus d'attribution, force des MDP, processus de suppression, audits.

C06A03 : restreindre l'accès Internet aux comptes internes à privilèges
Lorsqu'un admin surfe sur le Web avec son compte admin, le fait d'attraper par mégarde un malware donne de facto à ce malware des privilèges étendus sur le SI : le cryptolockage des SF n'en sera que plus simple, tout comme la compromission des actifs DIAMOND. Les bonnes pratiques, rappelées régulièrement par l'ANSSI[7], consistent à supprimer l'accès Web à partir des comptes à privilège, et de contraindre la navigation Web à partir de comptes agent « classiques ».

C06A04 : vérifier la capacité à couper rapidement l'accès aux webmails externes
En cas d'attaque ou d'alerte, il peut être nécessaire de couper, pour un temps donné, l'accès aux webmails externes à partir de PC du LAN. Les webmails sont en effet des vecteurs importants d'infection car les communications se font en https et l'inspection de ces flux chiffrés par les équipements de la DMZ (proxy, firewall) n'est pas toujours possible, pour des raisons techniques trop complexes à exposer dans ce guide.

C06A05 : monitorer le trafic SSL sortant
Une des caractéristiques courantes des malwares - surtout ceux qui fonctionnent en mode silencieux pendant une première phase qui précède l'attaque à proprement parler - est qu'ils échangent régulièrement des données en mode SSL avec un site « peu recommandable », donc en mode sortie du LAN. Monitorer les trafics SSI sortants vers des sites Web inhabituels est donc un bon moyen de détecter ce que les AV classiques ne voient pas forcément.

C06A06 : réviser périodiquement les règles du Firewall
Les règles d'un Firewall bougent très souvent : ajout, modification, plus rarement retrait. A l'occasion d'un changement d'équipement, un audit sur les règles en

7 https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

cours fait immanquablement apparaître des règles redondantes, des règles dont la combinaison laisse passer plus de flux qu'on ne le croit, voire des anomalies flagrantes mises en place à l'occasion de tests et jamais supprimées. Une revue périodique s'impose, les constructeurs disposent d'outils pour cela mais on peut le faire à la main, c'est d'ailleurs un excellent sujet de stage.

4.6.3 Conseils

Là encore il n'y a rien de complexe dans ce chantier : toutes ces mesures sont techniquement faciles à mettre en œuvre et peuvent être étalées dans le temps.

4.7 Chantier 7 : durcir le parc PC

4.7.1 Contexte

Un des vecteurs d'attaque est le parc des PC : PC non protégés par des AV, comptes locaux à privilèges non maîtrisés, utilisateurs qui cliquent sur des liens dangereux, etc. Il n'est pas possible de sécuriser un parc de 5000 ou 10000 PC à 100 %, mais il y a des mesures de base à mettre en œuvre.

4.7.2 Actions

C07A01 : définir un pattern OS et AD de chaque PC avant déploiement
Il est courant d'entendre dire qu'il y a des comptes admin locaux sur un parc de PC dont il est très difficile de changer les mots de passe : il s'agit clairement d'une source de risques car les comptes à privilèges, mêmes locaux, doivent pouvoir être supervisés et monitorés de façon centralisée. Cela peut être part des requêtes de type SCCM, par des gestions de groupe AD, etc. Et surtout cela doit cibler aussi bien les PC utilisateurs que les systèmes SCADA.

Il convient de définir des patterns OS (niveau d'OS, mise à jour de patches, etc.) et AD (politique de compte admin, mécanisme de mise à jour des mots de passe y compris des comptes locaux qui ne sont pas dans un groupe AD global.

C07A02 : être en capacité de changer en masse les mots de passe des comptes admin locaux
Rien à rajouter.

C07A03 : distinguer les comptes admin locaux des PC et des serveurs
Il convient que ces deux typologies de comptes soient bien séparés : l'attaque par le biais d'un PC pourra plus difficilement déborder sur l'infrastructure serveurs.

C07A04 : effectuer des revues périodiques des comptes admin locaux
Soit ces comptes sont gérés directement dans l'AD (groupes globaux), auquel cas la collecte des éléments techniques est simple ; soit ces comptes sont strictement locaux, auquel cas il faut développer des scripts SCCM pour collecter les éléments techniques. D'où l'importance de la première action de cette liste.

C07A05 : mettre systématiquement à jour les patches OS
Rien à rajouter.

C07A06 : effectuer des scans de parc
Le problème des AV et des outils de gestion de parc est qu'ils ne protègent ou ne recensent que ceux qu'ils connaissent. Si un équipement est connecté au LAN sans avoir été rentré dans la console AV, il ne sera pas protégé. Idem pour la console SCCM qui ne connaît que ce qui a été rentré dans l'AD.
Il convient de scanner le parc en croisant au moins 4 sources :

- les équipements intégrés au domaine AD ;
- les équipements qui ont une adresse IP ;
- les équipement qui sont connus de la console AV ;
- les équipements qui sont connus de la gestion administrative du parc.

4.7.3 Conseils

La protection du parc PC est un des piliers de la cyber résilience, et en même temps certainement le sujet le plus complexe à traiter tant il y a de trous dans la raquette.

Dans l'idéal, tout asset IP se trouve référencé dans les 4 sources. Si ce n'est pas le cas, il convient d'instruire rapidement le sujet : soit l'asset n'est pas protégé par un AV, soit il n'est pas dans le domaine, soit il n'est pas dans la gestion de parc. Dans tous les cas, il s'agit d'une anomalie à régler sans délais.

4.8 Chantier AV

4.8.1 Contexte

Last but not least, la protection antivirale ! De nos jours, le simple AV local à un PC ne suffit plus pour prétendre disposer d'une protection AV complète. La protection AV doit s'envisager en tant que solution globale composée de plusieurs modules.

Partons du principe que les fondamentaux sont présents, à savoir :

- une protection AV de chaque PC du parc, avec signatures à jour et moteur AV à jour ;
- une protection AV de chaque serveur sous OS Windows, idem ; le cas des serveurs Unix ou Linux fait débat ;
- une protection AV périmétrique entrante pour la messagerie et les flux http/https ; la plupart du temps, les firewalls et proxy embarquent ce type de fonctions.

La question de savoir si les modules AV de protection périmétrique doivent ou non être de la même marque (éditeur) que les AV internes fait débat :

- si non, la différence de moteur fait que certains malwares peuvent être détectés

par l'un alors que l'autre ne les détecte pas ;

• si oui, cela permet de remonter les alertes à une console centrale. ar exemple, certains AV diffusent auprès des autres modules de la solution globale (par exemple l'AV des PC) les malwares détectés par le mode heuristique du module de protection périmétrique.

4.8.2 Actions

C08A01 : déployer en DMZ un module d'analyse heuristique

La détection sur signature ne suffit pas, un module d'analyse comportementale est indispensable.

C08A02 : déployer des modules d'inspection à la volée en protection des VLAN « sales »

Certains VLAN comportent des équipements qui ne peuvent pas être protégés (systèmes SCADA, systèmes embarqués, etc.). Il existe chez certains éditeurs AV (par exemple TREND) des solutions de boitiers appliance qui se positionnent en écoute de port sur un switch ou un routeur et qui analysent les flux (base signature ou heuristique) afin de détecter les trames suspectes, sans bloquer le trafic.

4.8.3 Conseils

L'action C07A06 stipule qu'il faut réaliser des scans réguliers de parc, entre autres pour pister les équipements non connus de la DSI, non protégés, etc. D'expérience, la première fois qu'on lance ce type de scan, on a de grosses surprises : PC connectés au LAN depuis des années sans aucune mise à jour OS ou patch et qui font tourner des équipements critiques, bricoleurs qui s'amusent à modifier les configurations des PC (ce qu'en principe la charte informatique doit interdire), voire qui montent eux-mêmes leurs bouts de LAN à base de courant CPL ou en achetant leurs propres switches (cela coûte quelques dizaines d'euros), etc.

Il faut partir du principe que toute protection AV déployée à un instant T se dégrade mécaniquement au fil du temps : AV en erreur, signatures obsolètes sur un équipement ou deux, etc. Le « Plan » seul n'est donc pas la réponse satisfaisante à cette partie.

5. PHASE CHECK

5.1 Principes

Il faut garder en tête quelques principes de base pour mettre en place une phase Check efficace.

D'abord, l'entropie (ou le désordre) a une tendance naturelle à augmenter : si l'on définit des comptes à privilèges et que l'on ne révise jamais ces comptes, on est certain que dans 6 mois, 1 an ou plus, ce nombre de comptes aura explosé car personne n'aura jamais fait passer « la voiture-balai ».

Ensuite, dans certains cas, il n'est pas possible de procéder à une phase Check sur tout une classe d'actifs. Par exemple, vérifier que sur un parc de 30 000 IP, il n'y a strictement aucun PC « rogue » est quasi impossible. Il est plus efficace de vérifier sur un échantillon, par exemple un VLAN ou un bâtiment ou un site. Les commissaires aux comptes utilisent ce genre de technique d'échantillonnage et considèrent qu'avec un panel de 30 items, on dispose d'une représentation claire du reste de la classe.

Enfin, il est important de mettre en place la traçabilité des contrôles, d'une part car c'est auditable, d'autre part car cela participe à la montée générale en maturité

5.2 Les familles de Check

5.2.1 Audit des accès

Il s'agit de l'audit des comptes à privilège sur l'AD (comptes admin de domaine et comptes admin du schéma a minima), des serveurs DIAMOND, et des serveurs en DMZ.

En général, on préconise que chacune de ces 3 sous-familles fassent l'objet de deux audits annuels (c'est un minimum), voire des contrôles cibles, par exemple un tous les mois sur telle ou telle machine. Il faut mixer l'échantillonnage et l'utilisation d'outils tels SCCM et PingCastle.

5.2.2 Test des procédures

Il convient de tester l'extinction et l'isolation de VLAN : cela peut être réalisé à l'occasion d'une maintenance préventive, d'un test programmé, etc. Notamment, il est important de réaliser un test de coupure de l'accès Internet : cela paraît simple, mais la première fois que j'ai demandé cela à des équipes opérationnelles, l'infrastructure était tellement bien redondée qu'ils n'y sont pas parvenus !

Il convient de tester la coupure des serveurs de fichiers, et le passage en mode Read-Only. Il convient de tester l'isolation du système de sauvegardes, c'est-à-dire à la fois du serveur de sauvegarde (qui contient les catalogues) et les sauvegardes elles-mêmes.

5.2.3 Supervision

A minima, il faut superviser régulièrement :

- l'uptime des serveurs : il n'est pas rare de trouver, dans une infrastructure complexe, des machines qui n'ont pas été redémarrées depuis plusieurs années ;
- les droits sur les partages de fichiers; on a de grosses surprises !
- les niveaux de patches PC et serveurs

5.2.4 Scan DMZ

Il convient d'acquérir un service ou un produit de scan de la surface périmétrique.

5.2.5 Scan du parc

C'est de loin la partie la plus complexe, car les outils fournis en natif avec l'environnement Microsoft ne permettent de scanner que ce qui est connu : si une machine non-intégrée au domaine AD a été connectée en mode «sauvage », SCCM ne la verra pas.

Il existe des outils fournis par les équipementiers réseau, et il est possible d'utiliser des outils open source tels nmap et de développer ses propres scripts. Voici typiquement un domaine où la coopération entre équipes de GHT est forcément bénéfique.

6. CONCLUSION

La cyber résilience est un domaine qui évolue très vite, au gré des menaces. Les premiers cryptolockers sont apparus en 2015 et nul ne prévoyait l'impact que cela aurait sur les entreprises : on ne compte plus les groupes qui ont été attaqués, les entreprises bloquées et rançonnées, etc.

Non seulement personne ne voit, à l'heure où ces lignes sont écrites, le bout du tunnel, mais en sus il y a une seconde catégorie, qui fait peu parler d'elle car beaucoup moins létale, mais qui provoque des effets certains sur les SI : les crypto mineurs.

Un crypto mineur ne bloque pas un SI en chiffrant les données. Il se contente d'utiliser de la puissance machine (CPU) pour « miner» des crypto monnaies et ainsi s'enrichir au dépend de celui dont la puissance de calcul est allègrement siphonnée. Cerise sur le gâteau, la base légale de condamnation est très ténue, pour des raisons qui dépassent le cadre de cette publication.

De façon générale, il faut partir du principe que la question n'est pas de savoir si l'entreprise va subir une attaque par cryptolocker, mais quand : à ce moment, il faudra avoir prévu les procédures et les dispositifs pour :

- démontrer que l'on n'est pas resté les bras ballants devant un risque connu de tous;
- limiter la casse ;
- accélérer le retour à la normale ;
- être en mesure d'éjecter l'attaquant du LAN, ce qui n'est pas si simple qu'il n'y paraît. Dans le cas de l'attaque de TV5 Monde, cela a conduit à la nécessité de reconstruire totalement l'AD (on imagine l'impact quand il y a derrière un parc de milliers de PC et de centaines de serveurs).

7. ANNEXE 1 – SYNTHÈSE DES ACTIONS

7.1 Chantier 1 : durcir l'AD

ACTION	OBJET	COMPLEXITÉ	COÛT
C01A01	Nettoyer les comptes à privilège	+++	+
C01A02	Durcir les mots de passe des comptes à privilèges	+	+
C01A03	Disposer d'un outil d'attaque des mots de passe	++	+

7.2 Chantier 2 : segmenter le réseau

ACTION	OBJET	COMPLEXITÉ	COÛT
C02A01	Isoler les VLAN vitaux	+++	++
C02A02	Séparer le VLAN d'administration	+++	++

7.3 Chantier 3 : restreindre les accès aux serveurs DIAMOND

ACTION	OBJET	COMPLEXITÉ	COÛT
C03A01	Supprimer les accès anonymes	+	+
C03A02	Restreindre les accès par filtrage des IP	++	+
C03A03	Délivrer des accès nominatifs avec mot de passe fort	+	+

7.4 Chantier 4 : adapter l'infrastructure système

ACTION	OBJET	COMPLEXITÉ	COÛT
C04A01	Supprimer l'uptime des serveurs	+	+
C04A02	Superviser les partages accessibles en contrôle total	+	++
C04A03	Pouvoir diffuser par SCCM des modifications du paramétrage des pare-feu internes de PC sur parc	++	+
C04A04	Tester le passage des serveurs de fichier (SF) en mode lecture-seule (RO, read-only)	+	+
C04A05	Tester la coupure des SF	+	+
C04A06	Identifier les adhérences entre les SF et les progiciels métier	++	+
C04A07	Mettre à jour les patches	++	+

7.5 Chantier 5 : utiliser la sauvegarde

ACTION	OBJET	COMPLEXITÉ	COÛT
C05A01	Vérifier la capacité à isoler le serveur de sauvegardes	+	+
C05A02	Sauvegarder tout ou partie des actifs DIAMOND sur les SF en mode RO	++	+
C05A03	Etablir un plan de test des restaurations des serveurs DIAMOND	+	+

7.6 Chantier 6 : adapter la DMZ

ACTION	OBJET	COMPLEXITÉ	COÛT
C06A01	Scanner périodiquement l'ensemble des assets de la DMZ pour détecter les vulnérabilité	+	++
C06A02	Durcir la gestion des comptes locaux aux machines de la DMZ	+	++
C06A03	Restreindre l'accès Internet aux comptes internes à privilèges	++	+
C06A04	Vérifier la capacité à couper rapidement l'accès aux webmails externes	+	+
C06A05	Monitorer le trafic SSL sortant	+	++
C06A06	Réviser périodiquement les règles du Firewall	+	++

7.7 Chantier 7 : durcir le parc PC

ACTION	OBJET	COMPLEXITÉ	COÛT
C07A01	Définir un pattern OS et AD de chaque PC avant déploiement	++	+
C07A02	Être en capacité de changer en masse les mots de passe des comptes admin locaux	++	+
C07A03	Distinguer les comptes admin locaux des PC et des serveurs	+	+
C07A04	Effectuer des revues périodiques des comptes admin locaux	+	++
C07A05	Mettre systématiquement à jour les patches OS	+	+
C07A06	Effectuer des scans de parc	++	++

7.8 Chantier AV

ACTION	OBJET	COMPLEXITÉ	COÛT
C08A01	Déployer en DMZ un module d'analyse heuristique	++	++
C08A02	Déployer des modules d'inspection à la volée en protection des VLAN « sales »	++	++

TREND MICRO : UNE CYBERDÉFENSE INTERCONNECTÉE POUR LUTTER CONTRE LES MALWARES

De plus en plus courantes au cours de ces dernières années, les cyber-attaques ciblant les établissements de santé se sont encore accélérées depuis le début de la crise sanitaire. 50% des interventions menées par les équipes de « Réponses à incident » de Trend Micro en Europe, ont été conduites pour des hôpitaux, laboratoires et autres fournisseurs d'équipements médicaux : un chiffre multiplié par 10 par rapport à une période dite «normale». Et les cas relayés par la presse sont nombreux. On se rappelle par exemple de l'attaque qui avait paralysé le système informatique du CHU de Rouen en novembre 2019, imposant un arrêt général de ses équipements... tout comme de l'attaque par déni de services (DDos) ayant touché l'Assistance Publique-Hôpitaux de Paris (AP-HP) en mars 2020, menaçant fortement son continuum de soins dans une période critique. Les données de santé, comme par exemple les numéros d'assurance maladie, les certificats de naissance, les ordonnances, … possèdent une grande valeur pour les pirates informatiques et se monnaient à prix d'or sur le Dark web.

LA SÉCURITÉ INFORMATIQUE : UN ENJEU MAJEUR DANS UN PAYSAGE DE MENACES TOUJOURS PLUS OFFENSIF

Vol d'identité, phishing, atteinte à la sécurité des flottes mobiles, logiciels espions, déploiement de ransomwares prenant les postes de travail et les fichiers en otage en échange de rançons pouvant se chiffrer en millions d'euros… ces attaques sont multiformes, complexes et abouties. A cela s'ajoute une sophistication croissante des logiciels malveillants, comme on le voit avec les APT (Advanced Persistent Threat), des malwares ciblés et furtifs conçus pour durer dans le temps et exfiltrer des données stratégiques sans être découverts.

Le paysage de menaces offensif invite aujourd'hui les organisations à remettre en cause leurs certitudes : le risque zéro n'existe pas. Elles sont toutes des cibles potentielles et doivent donc mettre en place une infrastructure et une politique de sécurité qui leur permettra de se tenir au même niveau que la menace.

ASSURER LA PROTECTION DE L'ENSEMBLE DU SIH

Le dysfonctionnement ou l'arrêt du SIH peut entrainer des difficultés de prise en charge des patients, l'exposition à de graves risques sanitaires et d'importantes conséquences financières. En témoigne le récent fait divers en Allemagne, où une femme est malheureusement décédée à cause de l'indisponibilité de l'hôpital, ciblé par une attaque massive par ransomware au moment où elle avait besoin de soins urgents.

Le système d'informations hospitalier est le garant de la gestion globale de l'hôpital. Il supporte non seulement les fonctions de gestion comme le DMP et les outils administratifs, mais également les dispositifs biomédicaux (IRM, pompes à perfusion, défibrillateurs cardiaques…), ainsi que le fonctionnement technique du bâtiment (chauffage, alarmes, caméras de surveillance, ascenseurs, ventilation, ….). Le SIH est ainsi composé de trois SI distincts et interconnectés entre eux : si l'une des parties est corrompue, c'est l'ensemble du système décloisonné qui peut potentiellement être touché, entraînant une indisponibilité, la paralysie du système dans sa totalité, voire une fuite d'informations.

Pour se protéger, les établissements de santé s'appuient souvent sur un arsenal de solutions de sécurité multifournisseurs dont la gestion s'avère lourde et coûteuse et induit une implication humaine importante. Par ailleurs, les environnements biomédicaux et les équipements normalisés et critiques restent à ce jour insuffisamment sécurisés, bien souvent par manque de compétences internes et des réseaux rendus complexes par la transformation numérique.

DES ENJEUX RÉELS AUTOUR DU GHT ET DU CADRE RÉGLEMENTAIRE RENFORCÉ

En ouvrant et en mutualisant le système d'informations hospitalier, l'Hôpital numérique ainsi que le regroupement des établissements au sein des territoires de santé (GHT) étendent la surface d'attaque et la vulnérabilité aux malwares. Le tout sur fond d'encadrement réglementaire imposant aux établissements une sécurité renforcée, le développement d'une gouvernance de sécurité des données et l'obligation d'un signalement des incidents graves de sécurité aux ARS.

SECURITE CONNECTEE ET GHT : LE CAS DU CHRU DE TOURS

Le CHRU de Tours, support pour le Groupement Hospitalier du Territoire du département de l'Indre-et-Loire, devait assurer la disponibilité d'un SIH de plus en plus ouvert, garantir la sécurité de ses données sensibles et démontrer son exemplarité en matière de sécurité en tant qu'établissement support. L'hôpital a implémenté la suite de solutions de sécurité Trend Micro et accéléré la détection et la prise en charge des attaques globales. «Cette plateforme de sécurité intégrée et unique a renforcé la simplicité opérationnelle et rationalisé la sécurité, garantissant l'intégrité de l'ensemble de nos données, et surtout de nos données financières dans le cadre de l'audit du SIH pour la certification des comptes. La console d'administration commune pour toutes les solutions a permis de simplifier au maximum la gestion de la sécurité.» Didier Provot, Responsable du Département Technique à la DSI CHRU de Tours

UNE STRATÉGIE DE DÉFENSE INTERCONNECTÉE POUR OPTIMISER LA SÉCURITÉ DU SIH

Spécialiste de la sécurité informatique, Trend Micro a investi depuis plusieurs années le secteur de la santé, en mettant notamment l'accent sur la sécurisation du matériel biomédical. Les principaux risques qui pèsent sur les environnements biomédicaux - considérés à juste titre comme des systèmes industriels – sont, à part les cyber-attaques, les erreurs humaines, les vulnérabilités de leurs SI et les freins organisationnels. Finalement, des risques similaires à ceux de l'informatique de gestion !

Face au contexte des menaces actuel, il est également difficile pour les organisations de santé de gérer la complexité et la quantité de solutions de sécurité disparates, qui ne s'intègrent généralement pas les unes avec les autres.

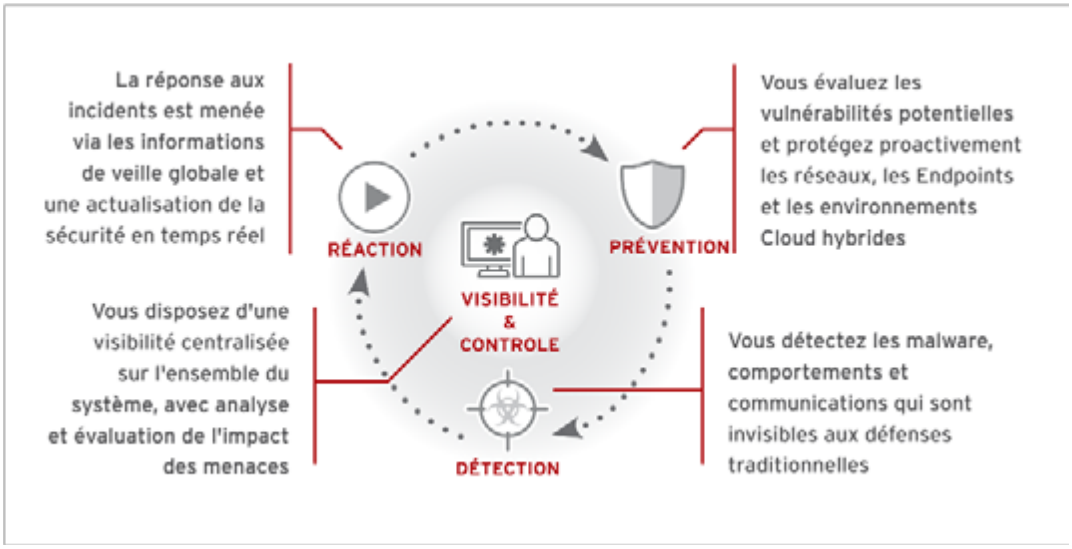
•Trend Micro propose une approche unique, en profondeur de la sécurité : **un panel de plusieurs solutions technologiques qui communiquent et interagissent entre elles en temps réel, partageant l'intelligence de sécurité à tous les niveaux** pour protéger efficacement les utilisateurs, les dispositifs et les applications. Disponibles en mode on premise, SaaS, ou hybride, ces solutions sont compatibles avec l'infrastructure existante de l'hôpital, dont les environnements biomédicaux.

•La plateforme de gestion **APEX Central allège la charge du service IT** en offrant au travers d'un tableau de bord, une visibilité centralisée et complète de l'ensemble de l'infrastructure de sécurité ainsi que des menaces - vecteurs, propagation et impact.

•**Les équipes sont capables de surveiller et de traiter les événements de sécurité avec un minimum de ressources**, évitant ainsi les tâches redondantes et chronophages pour un ROI maximisé.

•Elles disposent en outre d'une **solution complète de détection et de réponse aux incidents** avec des capacités d'analyse prédictive sur la totalité des infrastructures.

Qu'elles soient sur le Cloud, le réseau ou au cœur d'un data center, Trend Micro protège les données patients en détectant les intrusions causées par les attaques ciblées et les APT, mais aussi en neutralisant le spear phishing et les techniques d'ingénierie sociale. Les solutions Trend Micro identifient les malwares avancés, les activités réseau entrantes, sortantes et internes suspectes, ainsi que les comportements de cybercriminels. D'autre part, elles offrent une analyse en sandbox personnalisée pour détecter les malwares avancés. Les activités sont protégées dans le plus grand respect des normes réglementaires HIPAA, HITECH, PCI DSS et de la RGPD.



CYBERSANTÉSÉCURITÉ : SOYONS TOUS CYBERVIGILANTS EN SANTÉ !

Franck Frayer, Senior Vice President Physician Information Systems Europe CompuGroup Medical

Pendant longtemps, le secteur de la santé s'est peu préoccupé des questions de cybersécurité car l'utilisation des technologies connectées était limitée. Elle s'est sans cesse développée et atteint aujourd'hui l'hyperconnectivité. En 2018, **le taux de pénétration du numérique dans le système de santé français était de 88 % en France**[1], et ce chiffre n'a pas fini de grandir. Du côté des patients, les dispositifs médicaux comme les capteurs d'insuline digitaux fleurissent, les dossiers médicaux partagés sont de plus en plus adoptés et la communication patients-professionnels de santé prend de plus en plus une dimension numérique. **3 Français sur 4 se disent déjà prêts à communiquer avec leurs praticiens par des canaux numériques**[2]. Du côté des **professionnels de santé**, les applications et logiciels de gestion informatique les accompagnent de façon croissante dans leur pratique médicale, dans la gestion de leur relation avec le patient mais aussi dans leurs pratiques interprofessionnelles. D'après une étude récente de la DREES, **80 % des médecins généralistes de moins de 50 ans utilisent les principaux outils de la e-santé** : le dossier patient informatisé, le logiciel d'aide à la prescription et la messagerie sécurisée de santé[3].

Cette hyperconnectivité apporte de nombreux bénéfices à notre système de santé, mais comprend également des risques: ce phénomène multiplie les possibilités de failles et les points d'entrée pour les cyberattaquants. Cette infiltration peut se faire par des actions qui peuvent sembler mineures et pourtant informatiquement stratégique. **Toute négligence, qu'elle soit technique ou humaine, peut avoir des conséquences dramatiques pour les patients**. La cyberattaque du CHU de Rouen le 15 novembre 2019, pour n'en citer qu'un, a mis en péril la prise en charge des patients en causant le report de nombreuses interventions et le transfert de patients dans d'autres établissements.

Face à ce constat, que faire ?

Les grands opérateurs travaillent à une meilleure sécurité des systèmes d'informations et des applications par une approche technique. Elle est nécessaire et non suffisante. **Les solutions techniques ne peuvent se suffire à elles-mêmes, les questions liées à la protection des données touchent toute la société, aussi il est nécessaire d'élever la connaissance du plus grand nombre à ce sujet**.

Cela doit passer par **trois axes** : le développement d'une culture de la cybersécurité, l'amélioration de la gouvernance de la protection des systèmes d'information et le partage des bonnes pratiques au-delà de nos frontières.

1, 2 Ministère de la santé, Dossier d'information, campagne nationale d'information sur la cybersécurité en santé, 28 novembre 2019.
3 DREES, URPS Médecins Libéraux, ORS, Panel d'observation des pratiques et des conditions d'exercice, n°1129, janvier 2020.

DÉVELOPPER LA CULTURE DU RISQUE CYBER EN SANTÉ AUPRÈS DE TOUS

Comment expliquer que des badges d'accès à l'hôpital d'anciens internes ne soient pas désactivés ? Que les ports USB des ordinateurs d'établissements de santé ne soient pas protégés ? Les exemples sont légions. De nombreux acteurs de santé **ne mesurent pas les risques d'une mauvaise cybersécurité**. A cause de cette absence de réflexes de cybersécurité, les établissements victimes d'attaques mettent en place des actions curatives, souvent désordonnées et court-termistes.

Du côté des **professionnels de santé**, une récente étude a montré qu'ils sont **70 % à se sentir concernés par les questions de cybersécurité et de protection de la vie privée**[4]. Malheureusement, **80 % des sondés déclarent ne pas disposer d'une solution permettant de protéger l'ensemble des outils connectés qu'ils utilisent dans le cadre professionnel**[5], ce qui est assez inquiétant. Cette absence de protection interroge : sont-ils suffisamment sensibilisés à ce qui est appelé « l'hygiène informatique » dans leur parcours universitaire et professionnel ? Cela doit changer.

Enfin, la **sensibilisation et la formation à la cybersécurité** semble également encore nécessaire au niveau des administrations de santé qui stockent et manipulent des données de santé, et du grand public, usager d'objets de santé connecté. Une culture nationale du cyber-risque en santé doit émerger.

Les responsables de structures gérant des données de santé, dont les établissements de santé en particulier, pourraient être davantage impliqués dans la gestion de la protection des systèmes d'information en santé.

AMÉLIORER LA GOUVERNANCE DE LA PROTECTION DES SYSTÈMES D'INFORMATION EN SANTÉ

Les nombreuses cyberattaques récentes dans les hôpitaux interrogent également sur l'efficacité de la gouvernance de la protection des systèmes d'informations hospitaliers. Il a par exemple été suggéré, notamment par la précédente Ministre des solidarités et de la santé, de revoir cette organisation. Agnès Buzyn a ainsi souligné qu'« il faut que la responsabilité de la cybersécurité n'incombe pas à la DSI de l'hôpital, mais bien au directeur et au président de la commission médicale d'établissement, parce qu'en réalité c'est la gouvernance qui donne à la fois le ton et l'importance qui convient à ce sujet»[6]. D'autant plus que le Règlement Général sur la Protection des Données Personnelles (RGPD) impose la mise en place de moyens techniques et organisationnels pour sécuriser les données personnelles et sensibles dont font parties les données de santé.

Une meilleure gouvernance de la protection des systèmes d'information en santé au sein des structures de santé apparait donc essentielle à une meilleure gestion des risques cyber. En tant que membre de l'UE, nous avons par ailleurs la chance de pouvoir optimiser nos actions en nous inspirant des pratiques de nos voisins…

4, 5 Etude Yougov pour Kaspersky, Protection des données de santé- du curatif au préventif, 2019.
6 « La responsabilité de la cybersécurité ne doit pas incomber à la DSI de l'hôpital mais au directeur »

PARTAGER LES BONNES PRATIQUES AU-DELÀ DE NOS FRONTIÈRES

Le numérique en santé ne connait pas de frontières territoriales, le partage d'expériences avec les autres pays européens est essentiel à une meilleure cybersécurité en santé en France.

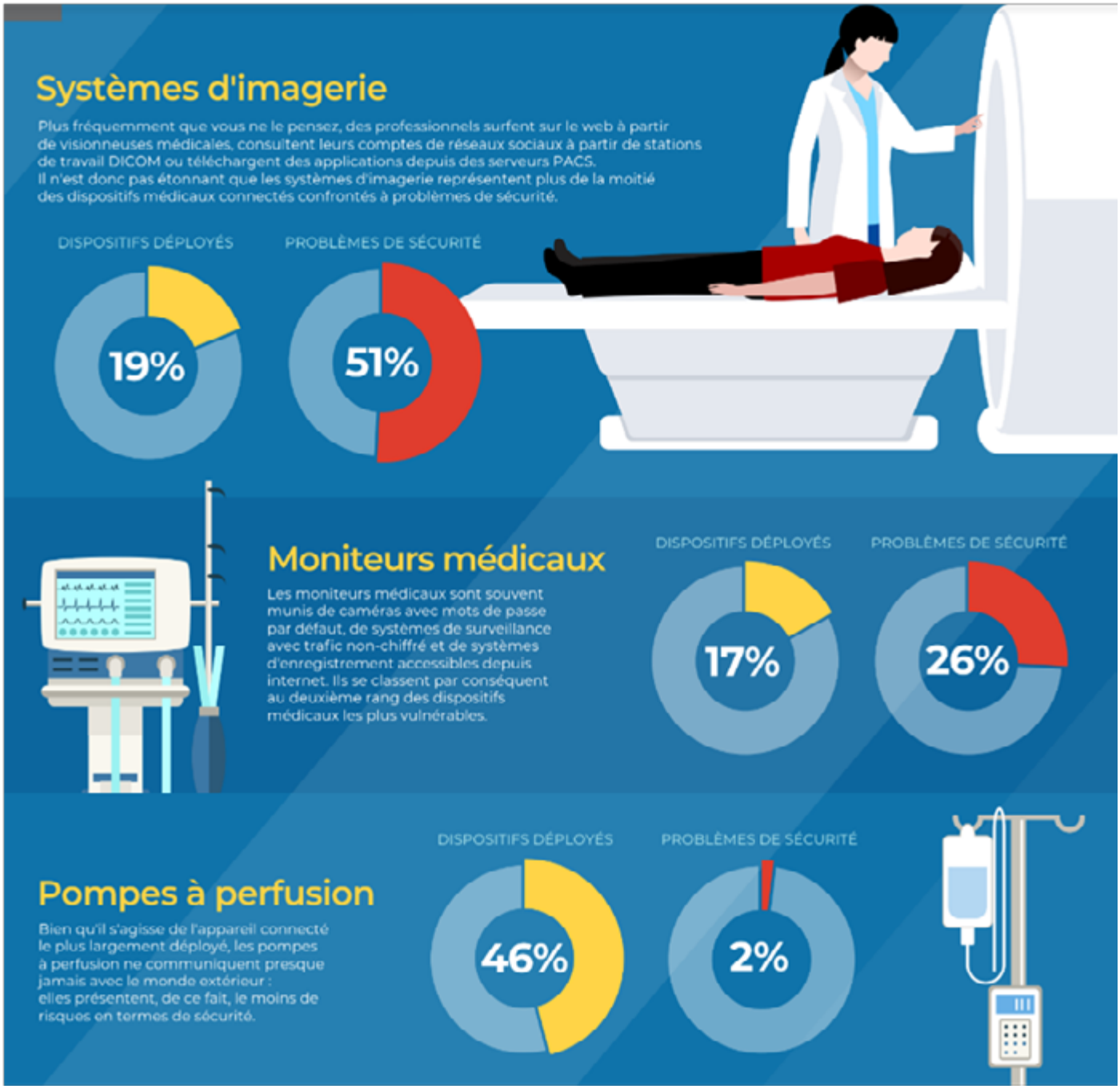
La cybersécurité est un enjeu majeur pour l'Union Européenne comme le démontre l'adoption du 'Cybersecurity Act' en mars 2019 par le Parlement Européen qui définit un cadre européen de certification de cybersécurité, et renforce les compétences de l'Agence Européenne de Cybersécurité (ENISA), entre autres.

L'ENISA a ainsi commencé à favoriser le partage de bonnes pratiques en matière de cybersécurité en santé au niveau européen, en coorganisant les 'Conférences annuelles sur la sécurité en e-santé'. La dernière session à Barcelone le 30 octobre 2019 traitait justement des stratégies à développer dans les hôpitaux pour former et sensibiliser les acteurs de santé à ces enjeux.

Ce cadre européen représente une opportunité qu'il nous faut saisir pour apprendre de nos voisins et diffuser la culture cyber en santé dans notre pays, pas seulement en octobre, le mois européen de la cybersécurité.

Comme le mentionnait Agnès Buzyn en novembre 2019, la cybersécurité dans le domaine de la santé est l'affaire de tous. **Partageons donc les bonnes pratiques au-delà de nos frontières et prenons une résolution pour 2020 : apprenons le langage de la CyberSantécurité pour qu'il soit partie intégrante de notre culture européenne avec l'objectif de toujours mieux protéger nos données.**

BIOMÉDICAL & GTC/GTB, PALO ALTO NETWORKS OUVRE LA BOÎTE NOIRE



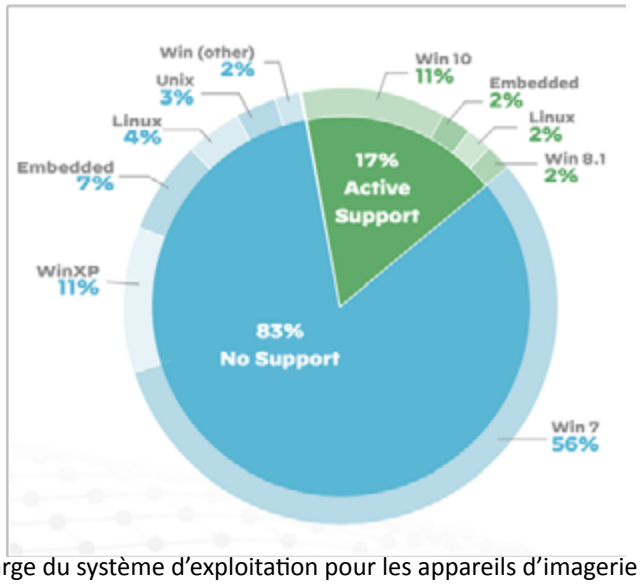
Les chiffres ci-dessus l'illustrent : Le service informatique d'un centre hospitalier peine à maîtriser le risque pesant autour des équipements biomédicaux ou du bâtiment connecté (GTC, GTB).

Au-delà du constat chiffré, cela met aussi en évidence un manque de visibilité des équipes sécurité IT sur la plupart des équipements connectés au réseau des établissements. En effet, ce sont des équipes dédiées biomédicales ou les moyens généraux qui ont la charge de ces équipements et qui viennent les connecter sur le réseau informatique sans pour autant prévenir la DSI. Or ces équipements ont des composants avec des systèmes embarqués trop souvent vulnérables. Les fameuses boîtes noires où l'installation d'un composant additionnel de sécurité n'est pas autorisée !

COMMENT ALORS DÉTECTER, IDENTIFIER ET ANALYSER SES BOÎTES NOIRES ?

Certes, des circulaires tentent de mettre en place des bonnes pratiques notamment en positionnant ces équipements dans des zones à part mais pour autant sont-elles mieux sécurisées ou moins exposées ? La réponse est non.

Certains Centres Hospitaliers tentent d'exiger qu'un minimum de sécurité soit appliqué sur les équipements biomédicaux ou même de mieux connaître les caractéristiques de l'équipement… en vain.

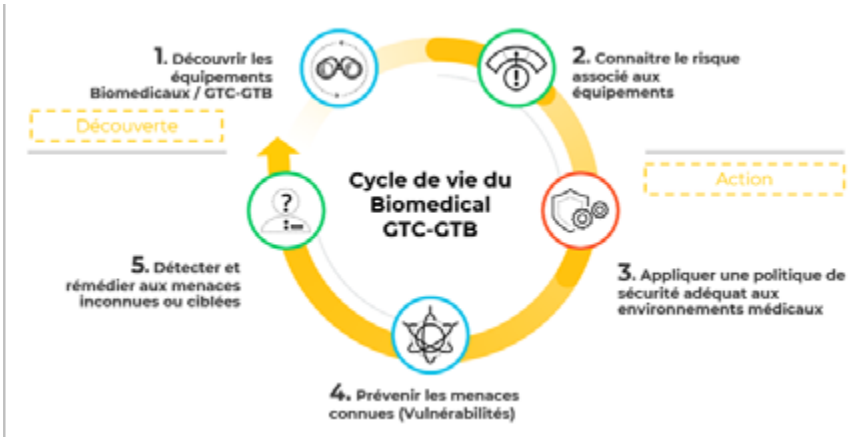


Répartition de la prise en charge du système d'exploitation pour les appareils d'imagerie médicale (Source : UNIT 42)

Si le service informatique n'est pas en mesure de connaître le contenu de ses boîtes noires, comment alors mettre en face les contre-mesures nécessaires ?

Avec le rachat de ZingBox en 2019, Palo Alto Networks est en mesure d'allumer la lumière pour que le service informatique puisse enfin s'approprier les caractéristiques du biomédical & GTC/GTB et ainsi moduler sa politique de sécurité afin de réduire sa surface d'attaque ou d'exposition. D'ailleurs, en 2020, le Forrester place Palo Alto Networks dans les leaders de la protection des équipements biomédicaux.

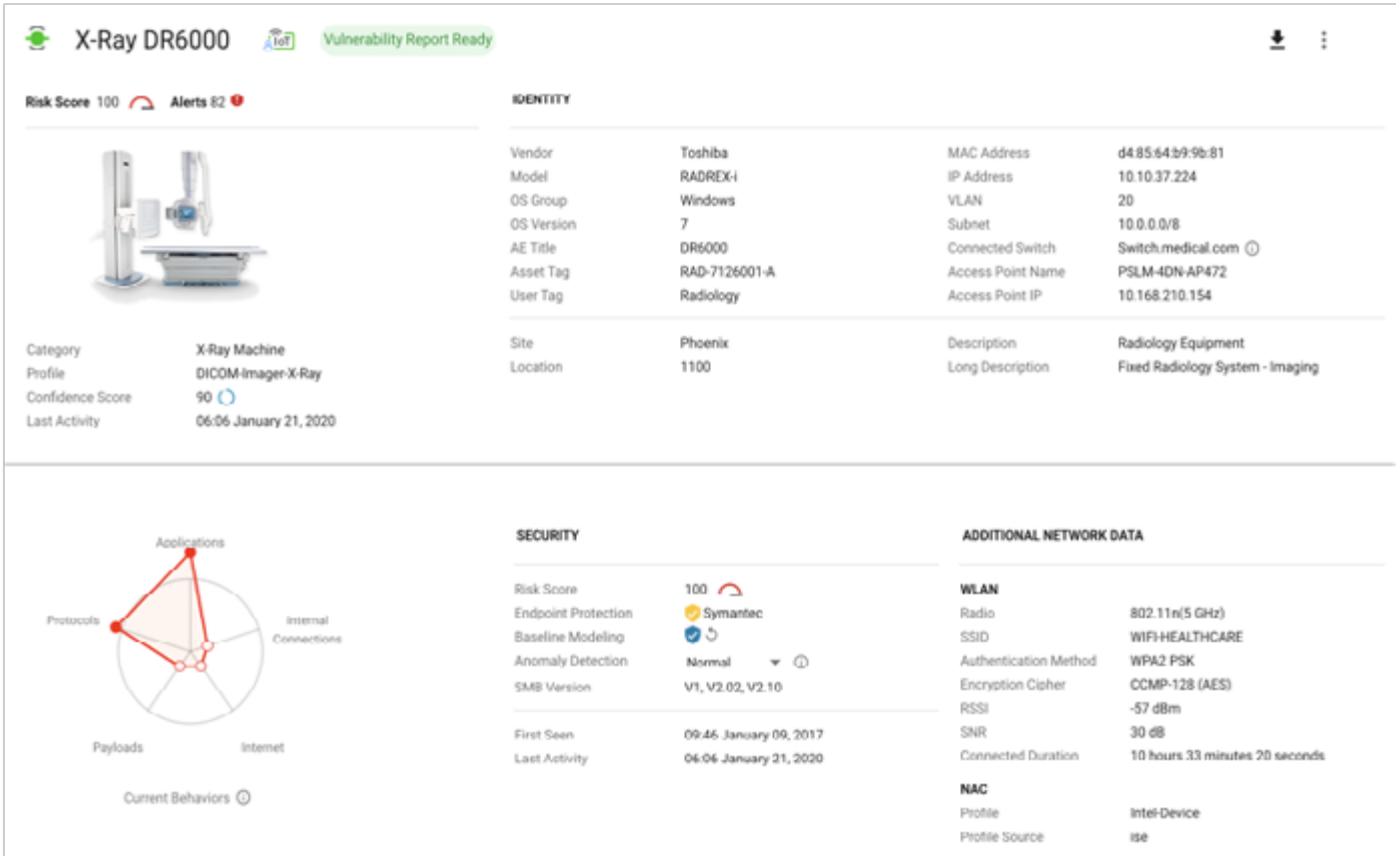
Pour se faire, Palo Alto Networks s'appuie sur sa plateforme de pare-feu Nouvelle Génération qui embarque du Machine Learning et peut ainsi détecter les équipements connectés sur le réseau. Pour les nombreux clients Palo Alto Networks dans le domaine de la santé, ceci est une aubaine car sans rien déployer, la sonde est capable d'identifier les équipements connectés sur leur réseau et de mesurer leur posture de sécurité (Type, OS, Vulnérabilité, Communications réseaux, Applications, …).



paloalto NETWORKS

RAPIDE ET EFFICACE : TRANSFORMER SON PARE-FEU EN SONDE BIOMÉDICAL / GTC-GTB

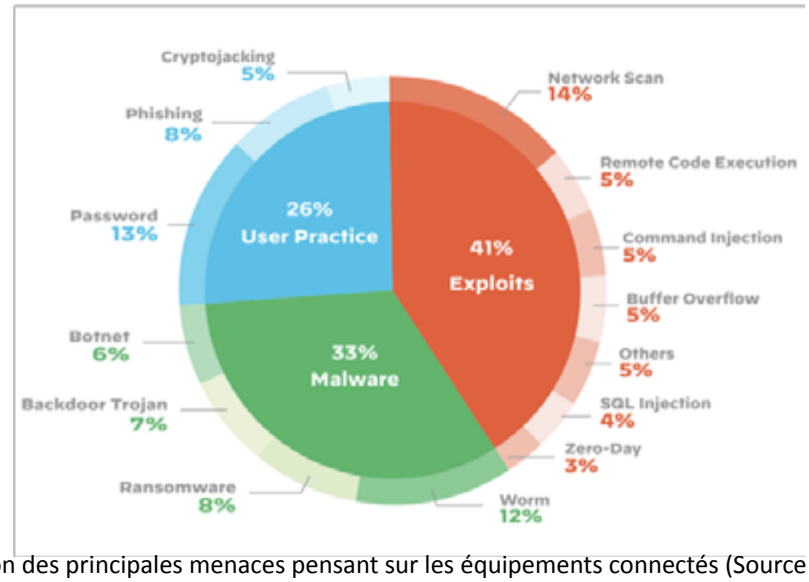
De ce fait, il n'y a plus de difficultés techniques pour maîtriser les composants du SI Santé ou du Bâtiment sans déployer une nouvelle sonde. Grâce à la souscription IOT, le pare-feu se transforme en sonde d'analyse et permet donc d'obtenir la visibilité complète des équipements, d'analyser les risques liés aux équipements et enfin, d'interagir avec le pare-feu si une vulnérabilité ou un comportement non désiré n'est pas souhaité (ou comment ajouter la notion d'équipement dans une règle de Sécurité).



Exemple d'un équipement biomédical détecté par la sonde Palo Alto Networks ML Next Generation Firewall avec toutes ses caractéristiques

INTÉGRER LE BIOMÉDICAL / GTC-GTB DANS LA CONSTRUCTION D'UN CENTRE DE SÉCURITÉ SANTÉ

Pour de nombreux RSSI, la création d'un centre de Sécurité spécifique Santé est un objectif à plus ou moins moyen terme car les RSSI cherchent à détecter de manière proactive les menaces ciblant leur système d'information. Mais avec une méthode traditionnelle, il faut empiler les couches technologiques et utiliser un agrégateur de log pour arriver à pouvoir déterminer des scénarii de compromission. A cela s'ajoutent des ressources humaines insuffisantes pour arriver à détecter rapidement les signaux faibles. Autrement dit, un casse-tête financier, technique, organisationnel et humain presque insoluble.



Répartition des principales menaces pensant sur les équipements connectés (Source : UNIT 42)

Et pourtant Il est indispensable aujourd'hui d'améliorer les capacités de défenses d'un hôpital et d'avoir ce centre de service pour faire tourner un hôpital 24/24 et 7/7. Mais pour cela, il faut éviter de siloter tous les composants et s'appuyer sur une plateforme capable de mettre en place des politiques de prévention (bloquer les menaces connues), mais aussi des politiques avancées de détection (recherche de signaux faibles et investigation rapide en cas de suspicion). Grâce à sa plateforme Cortex, Palo Alto Networks casse ce modèle empirique et casse les silos d'un point de vue Sécurité opérationnelle et un hôpital sera capable de protéger tous les composants d'un SI :

1. **Equipements** (PC, Biomedical, GTC-GTB, Serveurs, Capteur, …),
2. **Utilisateurs** (Population médicale, Population administrative, Personnel Technique,…),
3. **Lieux géographiques** (hôpital, GHT, Teletravail,..)
4. **Applications** (HTL, DICOM, Bureautique, Métier,…)
5. **Données**

Cette vision 360° (SI Santé, SI Traditionnel, SI Industriel) unifiée permet de maîtriser les budgets et d'améliorer la posture de Sécurité. Plus la visibilité est grande, plus il est facile d'anticiper, de rechercher et de comprendre un incident de Sécurité.

L'objectif à long terme pour un centre hospitalier, après avoir mis en place un système de prévention performant (bloquer les signaux forts) et un système de détection proactif (pour bloquer les signaux faibles), sera alors d'orchestrer & d'automatiser la réponse d'incidents pour limiter le temps de réaction mais aussi sa propagation lorsqu'une menace vient frapper un hôpital.

8. ANNEXE 2 – RÉFÉRENCES

8.1 Les ouvrages

« La sécurité du système d'information des établissements de santé », Cédric CARTAU, Presses de l'EHESP, 2ème édition

8.2 Sites Internet

ANSSI : www.ssi.gouv.fr

APSSIS : www.apssis.com

DSIH : www.dsih.fr

Guide d'hygiène de l'ANSSI : https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

Le site de Virus total : www.virustotal.com

9. REMERCIEMENTS

Nous remercions Trend Micro, CompuGroup Medical et Palo Alto Networks pour leur contribution à ce guide.

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

Création graphique : Corvy-Graphisme