Le 25 avril dernier, en amont de SantExpo, se tenait une agora autour de la thématique : « Etre cyberrésilient, le principal challenge des établissements de santé. Comment y parvenir ? » Les pistes de réponse sont nombreuses mais un élément est largement revenu au centre des débats : la notion de SOC (Security Operations Center) managé.

DES ATTAQUES DE PLUS EN PLUS DIVERSES ET RAPIDES

En 2022, le niveau général de la menace s'est maintenu. Et les établissements de santé représentent désormais 10% des victimes de compromissions par rançongiciel, contre 7% en 2021 (rapport sur la cybermenace de l'ANSSI).

Au fil des ans, le risque ne fait que s'accroître. Les vecteurs d'attaques se multiplient. Il est loin le temps où il fallait faire face à de simples virus, diffusés par des clés USB. Le développement de l'IoT notamment a ouvert des failles dans les systèmes et donc augmenté les risques. « Le standard a été depuis toujours de protéger les postes de travail, détaille Jérôme Lanniaux, directeur commercial chez BECYCURE, spécialiste en cybersécurité. Mais les équipements IoT (type sondes, équipements biomédicaux,...) n'ont pas fait l'objet des mêmes attentions, alors qu'une intrusion sur ces supports peut avoir de graves impacts :

- un robot en chirurgie qui pourrait être dévié de sa trajectoire,
- un dispositif médical qui ne donnerait pas le dosage adapté au soin,
- la vidéosurveillance paralysée

A cela s'ajoute une autre difficulté : le fait que les modes opératoires évoluent eux aussi. Auparavant axés sur la recherche de données monnayables, les intrusions pouvaient durer plusieurs jours (voire jusqu'à plusieurs mois) pour collecter et extraire un maximum de données et chiffrer les sauvegardes. « Désormais, on a affaire à des cybercriminels dont le seul but est de nuire, poursuit Jérôme Lanniaux. Ces attaques sont beaucoup plus rapides, et nous n'avons bien souvent que quelques heures pour réagir. » Avec une telle configuration, un outillage adapté s'avère indispensable. La réglementation pousse en ce sens. « Directive NIS II (Network and Information Security), exigences du Ségur du Numérique, nouveau référentiel pour les hébergeurs de données de santé, projet de Cyber resilience Act... Les textes de toute nature pleuvent, et le niveau de maturité progresse très rapidement», précise Me Marguerite Brac de la Pierrière, avocate spécialiste en cybersécurité, IT et Data de santé.

PRÉVENIR AVANT TOUT

Dans ce contexte, en quoi consiste la cyberrésilience ? La cyberrésilience, c'est la capacité d'un système d'information à résister aux cyberattaques et aux pannes accidentelles, puis à revenir à un état de fonctionnement et de sécurité satisfaisant. « Dans le secteur de la santé, cela se traduit par la capacité de prise en charge du patient en cas de cyberattaques, détaille Paul Milon, directeur adjoint chargé du SI convergent du GHT du Var et DSI des Centres Hospitaliers de Toulon et de Hyères. Augmenter notre cyberrésilience, c'est augmenter la continuité de notre service. » Et Xavier Stoppini, RSSI du Groupement Hospitalier du Territoire des Alpes Maritimes (GHT 06), d'ajouter : « C'est aussi l'aptitude à limiter la perte de données et le maintien en activité opérationnelle de nos services. »

Pour ce faire, le préventif est à la base de la protection. Plusieurs étapes doivent être validées : débloquer des budgets, évaluer le niveau de maturité des systèmes, établir des plans de remédiation, mettre en place un plan d'assurance sécurité dans les établissements, applicable aux prestataires et aux éditeurs, établir un contrat de maintenance et en faire une pièce incontournable au même titre que le contrat RGPD... « Le plan de remédiation et l'attention qui sera donnée à sa mise en oeuvre, c'est ce qui peut empêcher l'attaquant de passer à l'action et lui fera détourner le regard », analyse Xavier Stoppini.

La prévention passe également par la mise en place d'un SOC (Security Operations System). Les firewalls filtrent la plupart des tentatives d'intrusion mais laisse passer certains signaux faibles. Il s'agit d'analyser le « bruit de fond » pour déceler en continu ce qui sort de l'ordinaire. « Avec des attaques qui vont de plus en plus vite, il est indispensable d'avoir une écoute 24h/, 7j/7, constate Paul Milon. Or nous n'avons pas les effectifs pour cela ». D'où la nécessité d'un SOC managé (SOC externalisé auprès d'un partenaire spécialisé en matière de cybersurveillance) qui apporte selon Xavier Stoppini « une connaissance plus fine ». Et c'est là qu'intervient BECYCURE. « Notre rôle est, dans un premier temps, de proposer aux établissements un outillage adapté à la détection des menaces : EDR, SIEM, NDR (sonde réseau), scanner de vulnérabilité, décrit Jérôme Lanniaux. L'outillage SOC alors mis en place vise à superviser et analyser le SI, les objets connectés et les équipements biomédicaux pour alerter en cas de comportements anormaux. Puis, en mode routine, des experts sont à disposition des établissements pour traiter, analyser et investiguer les alertes de

cybersécurité. » « A ce niveau, précise Xavier Stoppini, le challenge est de parvenir à contextualiser les alertes par rapport au périmètre ciblé. Ces experts, de par leur compétences, leur intuition, sont capables de déterminer si l'anomalie est avérée ou pas, en fonction des habitudes et des usages en cours dans chaque structure. » Ce service managé respecte l'outillage existant des clients. « Nous ne faisons pas de vente de service en mode boîte noire, insiste le commercial. Notre client reste propriétaire de ses produits et de ses données et nous venons en complément de ses besoins ». « Avant toute mise en place d'un SOC, un travail préliminaire d'identification de la surface d'attaque et du durcissement de l'existant est indispensable. Le SOC et le SOAR (Security Orchestration, Automation and Response) représentent les dispositifs de prévention et remédiation permanents qui interviennent dans la continuité. C'est la promesse que nous portons au sein des équipes animées par Fabien SWIERGIEL notre directeur SCC Hyperscale », souligne Agnès SAUTEL, directrice du Pôle Santé SCC France.

UNE PROTECTION SUR DIVERS VOLETS

Cette protection, reposant donc sur des capacités humaines, est bien évidemment également alimentée par du machine learning, tout comme les cybercriminels. « L'attaquant va chercher à toujours plus créativité dans ses attaques, déplore le spécialiste de BECYCURE. C'est donc à nous de comprendre quelles voies il pourra emprunter pour être créatifs à notre tour et déjouer ses plans. »

Le volet de la formation ne doit pas être en reste. Des échelons de directions jusqu'aux postes industriels, tout le personnel se doit d'être formé. « Sur lew côté technologique, je ne suis pas inquiet, affirme Frédéric Avalet, directeur des achats du GRADeS PACA, il y a beaucoup de savoir-faire pour protéger les systèmes correctement. En revanche, c'est la formation des opérateurs en bout de ligne qui peut créer des failles. Voilà pourquoi il faut à tout prix une formation en continu, pour rester au fait des nouvelles menaces. »

En résumé, selon Xavier Stoppini, voici les recommandations principales en matière de cyberrésilience. « La première étape est de mettre en place une équipe SSI identifiée qui sera associées aux équipes systèmes et sauvegardes. Il faut ensuite gérer les vulnérabilités par l'audit de sécurité en continu de l'ensemble des serveurs, postes de travail et tout objet connecté sur le réseau. L'instauration d'un sanctuaire de la sauvegarde et le durcissement de l'AD sont également à privilégier. Enfin, les équipes doivent prévoir un site de repli disponible en cas d'attaque au-delà du PRI (Plan de Reprise Informatique) et sensibiliser le personnel à la vigilance cyber. »

C'est à ce prix que l'on améliorera la cyberrésilience en santé et que la dématérialisation pourra se poursuivre, tout en garantissant un niveau de sécurité optimal.

Agnès Sautel
Directrice du Pôle Santé SCC France
Crédit photo : DR

Frédéric Avalet
Directeur des achats du GRADeS PACA
Crédit photo : DR

Xavier Stoppini
RSSI du Groupement Hospitalier du Territoire des Alpes Maritimes
Crédit photo : DR

Marguerite Brac de la Pierrière
Avocate spécialiste en cybersécurité
Crédit photo : DR

Jérôme Lanniaux
Directeur commercial BECYCURE
Crédit photo : DR

Paul Milon
Directeur adjoint chargé du SI convergent du GHT
Crédit photo : DR

Les recommandations de Xavier Stoppini en matière de Cyberrésilience :

- Mise en place d'équipe SSI identifiée qui est souvent associées aux équipes systèmes et sauvegardes
- Gestion des vulnérabilités par l'audit de sécurité en continu de l'ensemble des serveurs, pc et tout objet connecté sur le réseau
- Sanctuaire de la sauvegarde
- Durcissement de l'AD
- Prévoir un site de repli disponible en cas d'attaque au-delà du PRI plan de reprise informatique
- Sensibilisation du personnel à la vigilance cyber