ceis

JANVIER 2018

LE SECTEUR DE LA SANTE FACE AU RISQUE CYBER

ENJEUX, RISQUES, REMEDIATIONS

Michel Benedittini
Cyril Nalpas

Les notes stratégiques

L'INTELLIGENCE DE LA DÉCISION

LES NOTES STRATÉGIQUES

Notes d'étude et d'analyse

TABLE DES MATIÈRES

1. INTRODUCTION

1.1. LE NUMÉRIQUE AU CŒUR DES ÉVOLUTIONS DE LA MÉDECINE, FACTEUR DE GRANDS PROGRÈS …

Compte tenu de leur foisonnement et de leur diversité, la présente note ne peut pas présenter en détail les applications de la transformation numérique dans le secteur de la santé. Les acteurs de ce secteur les connaissent, et la presse spécialisée ou grand public s'en font l'écho quasi quotidiennement. Tous les processus médicaux-sociaux ont bénéficié du développement de l'hyperconnectivité, de la miniaturisation des capteurs, des performances grandissantes des objets connectés, de l'avènement du Cloud, de l'intelligence artificielle, du Big Data et du Machine Learning, de l'impression 3D, ou de bien d'autres technologies et usages numériques en plein essor.

Le numérique est, tout d'abord, au cœur des évolutions de la médecine. Les appareils biomédicaux sont de plus en plus nombreux et performants, connectés à distance et dotés d'une certaine forme d'intelligence apportant une aide précieuse au diagnostic ou aux soins. La télémédecine se développe dans chacun des cinq types d'actes qui la compose : la téléconsultation, qui facilite l'accès aux soins notamment dans les déserts médicaux, la télésurveillance médicale, qui autorise les malades à vivre normalement tout en étant suivis médicalement sans encombrer les hôpitaux, la téléexpertise, qui permet aux acteurs de santé d'échanger sur les cas les plus complexes, la téléassistance médicale, qui prolonge la téléexpertise par une assistance dans la réalisation d'actes médicaux, et la régulation médicale assurée dans le cadre de la mission de service public de permanence des soins. Le ministère des Solidarités et de la Santé a lancé

deux ambitieux programmes «Hôpital numérique» et «Territoire de soins numérique». Dans le même temps, la numérisation des dossiers médicaux et leur regroupement dans le Dossier Médical Partagé (DMP) rendent possibles l'accès des acteurs de santé aux données personnelles des patients, enjeu majeur pour garantir la pertinence des soins en tout lieu, ainsi que des recoupements à grande échelle favorables à l'efficacité de la veille sanitaire et à la définition des politiques de santé. Enfin, le numérique porte une évolution majeure en matière de santé, qui verra le passage d'une médecine encore très majoritairement curative vers une médecine prédictive, en anticipant le développement des pathologies afin d'agir en amont pour retarder voire empêcher leur apparition ou tout du moins en réduire les effets.

Citons aussi, bien qu'il ne soit pas strictement un outil numérique du secteur de la santé, le *quantified-self*[1], de plus en plus couramment pratiqué à titre personnel mais qui pourrait peu à peu rejoindre la sphère médicale, de la même façon que les outils numériques personnels ont envahi l'espace professionnel.

Au-delà de la médecine, la numérisation concerne aussi tout le back office des centres de santé, de la même manière que toutes les organisations : messagerie, bureautique, gestion administrative, financière et fiscale, gestion des ressources humaines, gestion technique des bâtiments …

---

[1] *Le quantified-self (ou automesure connectée, dénomination adoptée par la Commission de noéologie), correspond à la pratique visant à mieux connaître son état de santé et sa forme physique en mesurant des données relatives à son corps et à ses activités.*

1.2. … ET DE GRANDS RISQUES

Dans le domaine de la cybersécurité, le secteur de la santé fait donc face aux mêmes menaces et risques que toute organisation fortement numérisée, mais également à des risques spécifiques à ses divers domaines d'action. Par ailleurs, ses caractéristiques le rendent particulièrement vulnérable, et donc une cible de choix : il est par nature très ouvert sur le monde pour relier les acteurs publics et privés de la santé, aussi nombreux que variés, et les patients ; les systèmes numériques et les architectures qui les relient, de natures et d'âges très variés, ont rarement été sécurisés « by design », et sont bien souvent difficiles à protéger ; les budgets considérables que brasse le secteur médico-social sont très attractifs pour les cybercriminels ; et enfin, l'impact psychologique d'une attaque sur un établissement de santé en font une cible idéale pour des attaques terroristes.

Une attaque ciblant le secteur de la santé, ou l'atteignant même s'il n'en est pas la cible, une défaillance ou un dysfonctionnement pourraient perturber, outre son fonctionnement et son modèle économique, la prise en charge des patients, les diagnostics, l'organisation des soins, voire les soins eux-mêmes, mettant ainsi directement en danger la vie des patients. Déjà insupportables à l'échelle d'un centre de santé, ces risques pourraient engendrer une catastrophe majeure au niveau national du fait de l'interconnexion des systèmes.

Le secteur de la santé n'a heureusement pas encore souffert d'attaques de grande ampleur, mais les incidents qu'il a connus doivent nous alerter sur l'acuité de la menace, depuis le ver informatique Conficker qui avait bloqué quelques centres hospitaliers français fin 2008 jusqu'à récemment, le rançongiciel Wannacry, qui a paralysé les services de santé britanniques pendant plusieurs jours de mai 2017.

1.3. … AUXQUELS IL FAUT FAIRE FACE

Face à ces enjeux majeurs, et sans attendre les futures attaques qui ne manqueront pas de concerner le secteur de la santé de près ou de loin et dans un avenir plus ou moins proche, il est essentiel d'améliorer la résilience et la résistance des systèmes numériques qu'il utilise.

Comme la sécurité dans tous les autres secteurs d'activité et face à tous ces risques, la cybersécurité est l'affaire de tous.

L'ACTION DES AUTORITÉS PUBLIQUES

Elle est d'abord l'affaire des autorités publiques. De nombreuses dispositions ont été ainsi prises ces dernières années pour assurer la meilleure cybersécurité possible des systèmes, des soins, des patients et de leurs données personnelles :

- Certains acteurs du secteur de la santé sont soumis aux exigences de cybersécurité s'imposant aux opérateurs d'importance vitale (OIV)[2] ;

- Des dispositions de même nature s'imposeront prochainement sur le périmètre plus vaste des opérateurs «essentiels» du secteur, en application de la Directive européenne sur la sécurité des réseaux et des systèmes d'information[3] ;

- Le ministère des Solidarités et de la Santé a mis en place de nombreux outils pour sécuriser la e-santé en même temps qu'elle se développe sous son impulsion volontariste, avec l'assistance pour l'essentiel de l'ASIP Santé, l'Agence française de santé numérique. On citera notamment : la Politique générale de sécurité des

---

[2] *https://www.ssi.gouv.fr/administration/protection-des-oiv/protection-des-oiv-en-france/*

[3] *https://www.ssi.gouv.fr/actualite/adoption-de-la-directive-network-and-information-security-nis-lanssi-pilote-de-la-transposition-en-france/*

systèmes d'information de santé (PGSSI-S)[4], imposant recueil de règles applicables par l'ensemble des acteurs publics ou privés des domaines de la santé et du médico-social et qui structure également l'offre des industriels du secteur ; des outils permettant l'authentification forte des mêmes acteurs sur les systèmes numériques, comme la Carte de professionnel de santé (CPS) ; un portail dédié à la sensibilisation et à la diffusion de bonnes pratiques en matière de sécurité des systèmes d'information dans le secteur de la santé[5] ; un portail permettant aux acteurs de santé de remplir leur obligation légale, depuis octobre 2017, de signaler toute action ou suspicion d'action malveillante causant une indisponibilité partielle ou totale de leur système d'information[6] ; une cellule « Accompagnement Cybersécurité des Structures de Santé », ouverte en octobre 2017 pour faire vivre les portails cités et assister les organismes en cas d'incident de sécurité ; ou encore un memento de cybersécurité à l'usage des directeurs d'établissement de santé[7].

- La mise en application du Règlement général européen sur la protection des données (RGPD)[8], le 25 mai 2018, imposera à tous les organisations d'exigeantes règles de sécurité pour les données personnelles qu'elles détiennent ou traitent, sous peine de sanctions pécuniaires très élevées. Compte tenu du caractère éminemment personnel des données de santé, le secteur de la santé sera particulièrement impacté. Ces exigences imposeront à l'ensemble des acteurs de la santé de renforcer significativement la cybersécurité de leurs systèmes.

L'ACTION DES ACTEURS DE LA SANTÉ

Aucune des mesures prises par les autorités publiques ne feront réellement progresser la cybersécurité du secteur de la santé si elles ne sont pas mises en œuvre et complétées par les acteurs de ce secteur. La cybersécurité est donc bien évidemment, aussi et surtout, l'affaire des acteurs de santé.

Par ailleurs, on notera que l'importance du corpus juridique mis en place par les autorités au niveau national et européen conduira les acteurs de santé à courir, en plus des risques sur leur fonctionnement, d'importants risques juridiques s'ils n'assurent pas une cybersécurité suffisante de leurs systèmes numériques.

---

[4] *http://esante.gouv.fr/services/politique-generale-de-securite-des-systemes-d-information-de-sante-pgssi-s/en-savoir-plus-0*

[5] *Le Portail d'Accompagnement Cybersécurité des Structures de Santé, https://www.cyberveille-sante.gouv.fr/*

[6] *https://signalement.social-sante.gouv.fr/*

[7] *http://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/e-sante/sih/article/memento-de-cybersecurite*

[8] *Règlement (UE) 2016/679 du 27 avril 2016, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679 et https://www.cnil.fr/fr/comprendre-le-reglement-europeen*

Chacun, à son niveau et dans son domaine de compétence, doit y apporter toute l'attention nécessaire :

- Les donneurs d'ordres, en spécifiant au juste niveau les exigences de cybersécurité des systèmes qu'ils commandent ;

- Les industriels, en assurant la cybersécurisation «à l'état de l'art» de leurs produits matériels et logiciels, dans la conception (le by design), dans les instructions d'installation et de mise en œuvre, puis dans la durée nécessaire pour corriger les failles de sécurité non décelées à la fabrication et prendre en compte l'évolution des techniques d'attaque ;

- Les intégrateurs et installateurs, en respectant les instructions des donneurs d'ordres et des industriels, et en mettant en place les moyens qui sont de leur ressort pour protéger les systèmes, prévenir et détecter les attaques, et réagir si nécessaire ;

- Les autorités d'emploi, en faisant vérifier le niveau de cybersécurité avant la mise en service, dans l'esprit de la démarche d'homologation recommandée par l'ANSSI[9], en instaurant les mesures techniques et non techniques nécessaires pour un emploi aussi sûr qu'efficace des systèmes, et en donnant à chacun des acteurs les moyens de mettre en œuvre ces mesures ainsi que la formation nécessaire ;

- Les administrateurs, en respectant et en veillant au respect des règles élémentaires d'hygiène informatique[10] et des bonnes pratiques de sécurité[11],

- Les utilisateurs, en appliquant les consignes d'emploi et les bonnes pratiques à leur niveau[12].

UNE RÉORGANISATION QUI FACILITERA LA CYBERSÉCURITÉ DU MILIEU HOSPITALIER

La loi de modernisation de notre système de santé de janvier 2016 a créé les groupements hospitaliers de territoire (GHT) en remplacement des communautés hospitalières de territoire. Dispositif obligatoire pour les établissements publics de santé, le GHT vise notamment à développer les synergies entre les établissements réunis autour d'un « projet médical partagé ». Un établissement support assure ainsi diverses fonctions au profit des autres établissements du groupement, parmi lesquelles notamment la fonction achat et la mise en œuvre du système d'information hospitalier (SIH). Cette mutualisation des moyens, des ressources et des outils numériques permettra à terme de disposer d'une infrastructure commune et de briques applicatives identiques au sein de chaque GHT, facilitant ainsi la cybersécurisation des établissements, notamment des plus petits qui ne disposaient pas d'une expertise SI et SSI suffisante.

---

[9] *https://www.ssi.gouv.fr/guide/lhomologation-de-securite-en-neuf-etapes-simples*

[10] *https://www.ssi.gouv.fr/administration/guide/guide-dhygiene-informatique/*

[11] *https://www.ssi.gouv.fr/administration/bonnes-pratiques/ et https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/*

[12] *https://www.ssi.gouv.fr/particulier/guide/guide-des-bonnes-pratiques-de-linformatique/*

2. PANORAMA DES RISQUES CYBER

2.1. LES FACTEURS DE RISQUE

LA COMPLEXITÉ DES SYSTÈMES NUMÉRIQUES DU SECTEUR DE LA SANTÉ

La typologie de systèmes que l'on retrouve dans le monde de la santé est très large. Outre l'informatique d'entreprise classique utilisée aussi bien pour les fonctions support que par les praticiens (postes utilisateur, messagerie, partage de fichiers, etc.), il existe un très grand nombre de systèmes « métiers » (dossier médical numérique, systèmes d'imagerie, informatique biomédicale, etc.). S'y ajoute l'informatique de gestion technique des bâtiments, qui assure le contrôle de la température, des fluides médicaux, ou encore du confinement et du filtrage de l'air, essentiels pour les salles d'opération et la conservation des échantillons. Les hôpitaux constituent le cas le plus complexe, regroupant tous les éléments énoncés.

Le développement actuel de la télésanté ajoute une couche de complexité à cet ensemble. Il implique une ouverture toujours plus grande des systèmes d'information de santé vers les organisations externes, qu'il s'agisse d'établissements de santé ou d'organismes tiers. Il existe une chaîne quasi-continue, qui va des systèmes biomédicaux jusqu'aux organismes sociaux en passant par les médecins et l'administration de l'établissement qui facture, impossible à ne pas relier puisque le mode de financement de notre système de santé implique que chaque acte doit aboutir à un remboursement.

LA PROBLÉMATIQUE DES MISES À JOUR DE SÉCURITÉ

Les établissements de santé regorgent de dispositifs numériques très spécialisés dont le maintien en condition de sécurité (MCS) est actuellement encore rarement assuré par les fabricants (absence d'application des correctifs de sécurité des briques grand public utilisées, impossibilité de changer de système d'exploitation lorsque l'ancien n'est plus maintenu par son éditeur, etc.).

Cette question ne peut être efficacement traitée qu'à un niveau global, au moins national sinon européen, voire même par des normes internationales, les structures individuelles ne pouvant peser suffisamment dans la négociation pour imposer aux constructeurs les conditions de sécurité nécessaires.

Aux Etats-Unis, la *Food and Drugs Administration* publiait en décembre 2016 un guide d'orientation recommandant aux industriels de systématiser le déploiement de mises à jour, en acceptant d'alléger les obligations de re-certification médicale dans la plupart des cas. Il s'agit d'un premier pas, mais dénué de mesures contraignantes qui semblent pourtant nécessaires pour obtenir des avancées sérieuses dans ce domaine. Pour cette raison, une action législative nationale ou communautaire est nécessaire.

LA VALEUR MARCHANDE DES INFORMATIONS DE SANTÉ

Les données de santé, sensibles par excellence, sont de plus en plus convoitées, d'autant qu'elles se monnayent au prix fort sur le marché noir. Différents objectifs motivent ces vols :

- L'espionnage industriel ;
- La revente aux compagnies d'assurance ;
- L'usurpation d'identité ;
- Les cas de chantage.

2.2. LES PRINCIPAUX RISQUES

On parle beaucoup des risques en matière de confidentialité, sans doute en raison du cadre juridique très contraignant autour des données personnelles de santé. Pourtant, les enjeux les plus importants pour la santé des patients se situent du côté de la disponibilité et de l'intégrité des données et des systèmes.

Les principaux risques affectant le secteur de la santé sont les suivants :

- Le blocage de tout ou partie du système d'information (SI) par un rançongiciel ;
- Les attaques en déni de service (DDoS) pouvant affecter un service critique ;
- Une perte d'intégrité des données ;
- Les confusions d'identité de patients ;
- Le risque juridique.

2.3. LA PROLIFÉRATION DES ATTAQUES PAR RANÇONGICIEL

La multiplication des attaques par rançongiciel contre des hôpitaux depuis le début de l'année 2016 montre que les cybercriminels n'hésitent désormais plus à s'attaquer aux services vitaux.

Des infrastructures sensibles telles que les hôpitaux ne sont pas ciblées par hasard. Elles constituent une cible très attractive en raison d'une part d'un niveau de maturité de la sécurité informatique en retrait au regard de la complexité de leur système d'information, et d'autre part de la criticité de ces systèmes : comme le blocage de ceux-ci peut en effet avoir des conséquences directes sur des vies humaines, les victimes sont plus facilement susceptibles de céder à des demandes de rançon.

Les nombreux cas, dont certains très médiatisés, d'établissements médicaux victimes d'attaque par ransomware ont démontré les conséquences potentiellement dramatiques de ce risque.

2.4. LES ATTAQUES EN DÉNI DE SERVICE SUR UN SERVICE CRITIQUE

Depuis la violente attaque en déni de service subie par l'Estonie pendant plusieurs semaines en 2007, ce type d'agression est devenu courant dans le cyberespace, même s'il est actuellement moins fréquent et médiatisé que les rançongiciels apparus plus récemment et plus lucratifs pour leurs auteurs. Faciles à réaliser sur une cible précise, notamment en les sous-traitant à des cybermafias qui en font le commerce, et relativement difficile à parer, les attaques en déni de service peuvent faire tomber des serveurs ou interdire tout échange de flux légitime pendant une durée limitée. Ce risque pèse donc principalement sur certains services très critiques ne supportant aucune interruption, comme les actes de télé-chirurgie par exemple.

2.5. LES ATTEINTES À L'INTÉGRITÉ DES DONNÉES

Le maintien de l'intégrité des données de santé est un élément capital de la sécurité du secteur car sa perte peut avoir des conséquences directes sur les vies humaines. Toute modification de données stockées, toute altération des flux reliant les équipements numériques peut avoir un impact sur les processus qui les utilisent : diagnostics, surveillance médicale des patients, soins, processus administratifs ou techniques.

Si dans bien des cas, l'impact pourra rester limité, dans d'autres, il pourra mettre en danger la vie de patients : l'ajout, la suppression ou la modification d'éléments au sein d'un dossier médical numérique peut conduire un praticien à ordonner un traitement dangereux ; la modification des flux informatiques reliant des appareils biomédicaux connectés (par exemple la pompe à insuline d'un patient à domicile, pilotée depuis l'hôpital via Internet et un réseau Wifi) peut entraîner des dosages inappropriés ; une modification des flux techniques ou du paramétrage du système de gestion d'une salle d'opération fait courir le risque de rendre l'environnement dangereux pour les patients.

2.6. LE RISQUE DE CONFUSION D'IDENTITÉ DES PATIENTS

Les erreurs d'identité dans les dossiers médicaux peuvent avoir de lourdes conséquences pour les patients. L'identito-vigilance consiste en l'organisation et la mise en œuvre d'un système de surveillance, de correction, et de prévention des erreurs et des risques liés à l'identification du patient.

2.7. LES RISQUES JURIDIQUES

La non prise en compte des risques cyber précédemment décrits peut aboutir à des risques juridiques au titre de :

- La non-conformité aux normes, notamment vis-à-vis des mesures visant à préserver la confidentialité des données ;

- La responsabilité civile. Il peut s'agir des conséquences d'un vol de données, mais aussi de cas bien plus graves liés à des pertes d'intégrité ou de disponibilité des données de santé ou de services médicaux ayant provoqué des dommages voire des séquelles aux patients concernés.

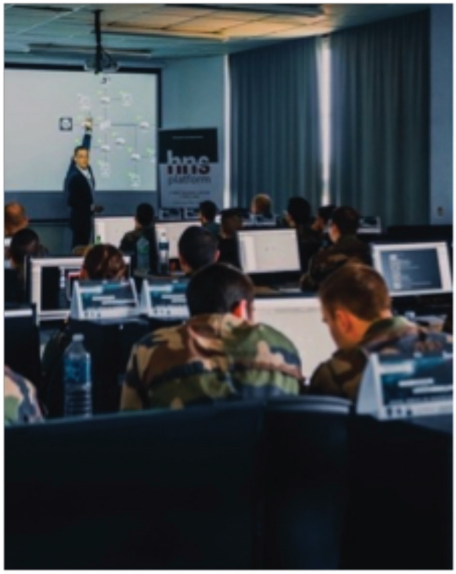
3. DES RÉPONSES AUX RISQUES

Les réponses décrites ici s'adressent aux organisations et s'inscrivent en complément des nécessaires actions visant à respecter les normes juridiques mises en place au niveau national ou communautaire.

3.1. LES FACTEURS DE RISQUE

La sensibilisation du personnel constitue l'une des clés de la sécurité de l'organisation. Il s'agit de traiter le facteur humain, impliqué dans la majorité des attaques, en développant au contraire un « firewall humain ».

Pour être efficace, la sensibilisation doit passer **par l'action** : à travers des démonstrations d'attaques d'une part, et des tests et exercices d'autre part. L'idéal étant pour chaque participant de pouvoir tester et pratiquer lui-même les scénarios d'attaques auxquels il doit être sensibilisé. Il est conseillé de planifier des tests à intervalles réguliers, par exemple via des campagnes de phishing simulées. Comme pour tout apprentissage, la régularité est synonyme de succès. A minima, l'apprentissage doit comprendre :



- La sensibilisation au phishing, premier vecteur des attaques par rançongiciel, attaques elles-mêmes les plus courantes et les plus impactantes pour les établissements de santé ;

- Les recommandations d'hygiène informatique contribuant à diminuer les risques pour le système d'information de l'établissement : séparation des identités personnelles et professionnelles, utilisation de gestionnaires de mots de passe (dont l'utilisation est bien trop marginale aujourd'hui) ;

La sensibilisation du personnel devrait cibler en priorité le top management et les fonctions bénéficiant de droits informatiques étendus, mais idéalement c'est bien l'ensemble du personnel qui doit être formé.

3.2. L'ENTRAÎNEMENT CYBER DES ÉQUIPES IT

Toujours dans l'idée de traiter le facteur humain, l'entraînement des équipes IT à la lutte informatique défensive (LID) est la clé de l'efficacité en cybersécurité. La grande majorité des organisations n'étant pas en mesure de dédier des ressources à la cyberdéfense, il s'avère nécessaire de familiariser les équipes techniques et leur permettre ainsi de développer les compétences correspondantes.

L'entraînement cyber doit permettre aux équipes de :

- S'assurer de la maîtrise d'une chaîne d'outils cohérents ;

- Développer des réflexes opérationnels ;

- Pratiquer les processus de gestion de crise ;

Pour être efficace, l'infrastructure sur laquelle l'équipe s'entraîne doit être la plus similaire possible au système d'information qu'elle doit protéger au quotidien. L'entraînement des équipes peut alors être l'occasion de constater d'éventuels manques avérés dans les processus de gestion de crise ou les moyens de cybersécurité mis en place, et ainsi permettre à l'organisation d'investir en toute connaissance de cause.

3.3. L'ANTICIPATION DES ATTAQUES

S'il faut savoir parer les attaques d'hier, il faut également savoir se défendre face à celles d'aujourd'hui et de demain. Pour cela, l'organisation doit s'intéresser à ce qu'elles pourraient être, et donc à des scénarios prospectifs et/ou anticipatifs des schémas d'attaques pouvant toucher le système d'information. Ce sont ces scénarios, qui doivent être personnalisés c'est-à-dire correspondre à la réalité de l'organisation, qui doivent être utilisés pour l'entraînement des équipes.

La confection de ces scénarios repose sur des capacités de Cyber Threat Intelligence, a priori externes à l'organisation, qui permettent l'analyse de l'ensemble des risques externes par des recherches sur les clear, deep et dark web : fuites de données, vulnérabilités apparentes, revendications d'attaques sur les médiaux sociaux, fraudes, etc.

L'anticipation des attaques peut notamment passer par une surveillance de l'empreinte numérique de l'organisation.

3.4. LA GESTION DE L'EMPREINTE NUMÉRIQUE

Afin de limiter les risques de piratage du système d'information, il est important d'agir sur les éléments pouvant les faciliter. Ceci inclut notamment l'excès d'informations concernant le SI accessibles depuis Internet. En effet, toute démarche offensive passe par une première phase de reconnaissance. Souvent, le choix de la cible découle des informations recueillies au cours d'une opération de reconnaissance automatisée.

Cet excès d'informations concerne d'une part les informations techniques sur les systèmes informatiques de l'établissement, conséquence d'une trop grande verbosité de ceux-ci, et d'autre part des informations concernant les utilisateurs bénéficiant de droits étendus sur les systèmes : chefs de service, administrateurs, techniciens biomédicaux, etc. Il s'agit encore une fois de traiter la protection du système d'information dans ses dimensions non seulement techniques, mais également humaines.

Pour être efficace, toute démarche proactive de réduction de son empreinte numérique nécessite un travail de cartographie préalable. Sur cette base pourra être mise en place une veille permettant la réduction du risque. Cela comprendra notamment l'élaboration de la liste du personnel possédant les droits d'administration les plus élevés, en d'autres termes les personnes pour lesquelles la compromission des comptes s'avérerait être la plus critique pour l'établissement. Il s'agit le plus généralement bien entendu de la quasi-totalité du personnel du service informatique, mais également des référents fonctionnels qui dans certains cas peuvent avoir des droits beaucoup plus étendus, notamment sur les applications métier.

Une veille de l'empreinte numérique doit permettre d'identifier au plus vite les fuites de données (identifiants compromis, données personnelles) afin d'agir au plus tôt, mais également de réduire l'empreinte numérique de l'organisation à son strict nécessaire.

3.5. L'APPORT DES ASSURANCES CYBER

La souscription à un contrat d'assurance cyber s'accompagne généralement d'une évaluation plus ou moins poussée du niveau de cybersécurité, faite par l'assureur ou par une entreprise spécialisée. L'assuré peut ainsi bénéficier d'une cartographie des risques voire d'un audit de maturité technique et organisationnelle de sa structure.

L'intérêt des assureurs étant évidemment de réduire le risque, ils chercheront souvent à rehausser le niveau de sécurité des organismes souscripteurs en intégrant dans le contrat des prestations de formation et de sensibilisation. Par ailleurs, la majorité des assurances prévoient des prestations de soutien en cas d'incident. Elles peuvent ainsi apporter une expertise technique, une assistance juridique et une aide à la gestion de crise. Elles pourront également remplir pour l'assuré la future obligation de notification des violations de données personnelles aux utilisateurs concernés. Ces prestations peuvent être précieuses pour les organismes ne disposant pas de l'expertise ou des ressources humaines nécessaires, à un coût global a priori raisonnable comparé à d'autres formules d'assistance.

Au-delà même de la question de son efficacité financière, la souscription d'une police d'assurance cyber a le mérite d'enclencher au sein des établissements assurés une véritable démarche qualité et sécuritaire vis-à-vis de ces nouvelles menaces.

LES AUTEURS

Le Vice-Amiral (2S) ***Michel Benedittini*** a achevé une longue carrière dans la marine française avec le grade de vice-amiral. Détaché en 2006 auprès du Secrétaire général de la défense et de la sécurité nationale, il a notamment contribué à la création de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), dont il était le directeur général adjoint, et à la définition de la stratégie française de cybersécurité. Il a ensuite assuré, en 2012 et 2013, la fonction de Secrétaire général de la Commission du Livre blanc sur la défense et la sécurité nationale. Il poursuit depuis des travaux de recherche sur la cybersécurité et la cyberdéfense, notamment avec CEIS.

Consultant en cybersécurité, ***Cyril Nalpas*** a rejoint CEIS en 2014 après une première expérience dans le développement logiciel. Doté d'un profil pluridisciplinaire (licence en droit, titre professionnel niveau III d'analyste-programmeur, MBA de Management du Risque), il travaille notamment sur les veilles et études prospectives et stratégiques, ainsi que sur les exercices de crise cyber.

PUBLICATIONS RÉCENTES

Le Plan d'action de la Commission européenne pour la Défense – une initiative encourageante mais à l'avenir encore incertain (Septembre 2017)

La survivabilité des hélicoptères : une préoccupation au coeur des engagements modernes, un enjeu majeur pour demain (Septembre 2017)

Le Système d'information des Armées (SIA) – Le programme SIA : changement de paradigme pour l'armée du futur (Août 2017)

Internet des Objets (IoT)- Une nouvelle donne pour la Défense ? (Août 2017)

Impression 3D – Des technologies de rupture au service des Armées (Août 2017)

Emploi du Cloud dans les armées – Première approche des concepts et contraintes (Août 2017)

Enjeux stratégiques du Big Data pour la Défense (Août 2017)

Cybersécurité dans le milieu maritime (Février 2017)

Android Malware in 2016: the emergence of a professional ecosystem (Janvier 2017)

A télécharger sur **www.sia-lab.fr** et **www.ceis.eu**

Compagnie Européenne d'Intelligence Stratégique (CEIS)

Société Anonyme au capital de 150 510 € - SIRET : 414 881 821 00022 – APE : 741 G

Tour Montparnasse – 33, avenue du Maine

BP 36 – 75 755 - Paris Cedex 15

Tél. : 01 45 55 00 20 - Fax : 01 45 55 00 60