Thomas BRETON
et **Damien RIBEIRO**
Membres du CERT

CYBERSÉCURITÉ : **GPLEXPERT** CRÉE SON PROPRE CERT

PAR JOËLLE HAYEK / C'EST UN PAS SUPPLÉMENTAIRE EN MATIÈRE DE CYBERVIGILANCE. APRÈS AVOIR CONSTITUÉ, L'AN DERNIER, UN PÔLE GOUVERNANCE, CONFORMITÉ ET SÉCURITÉ DES SYSTÈMES D'INFORMATION (GCSSI), LE CABINET DE CONSEIL EN E-SANTÉ GPLEXPERT A RÉCEMMENT CRÉÉ UN CERT, OU CENTRE D'ALERTE ET DE RÉACTION AUX ATTAQUES INFORMATIQUES, QUE NOUS DÉCOUVRONS AVEC THOMAS BRETON, GÉRANT DE CETTE ENTREPRISE FRANÇAISE, ET DAMIEN RIBEIRO, RESPONSABLE DU PÔLE GCSSI.

Dans quel contexte ce CERT a-t-il vu le jour ?
Thomas Breton : Face à l'augmentation des cyberattaques ciblant spécifiquement les établissements de santé, nous avons – malheureusement – acquis une réelle expertise dans la gestion des incidents de sécurité pour le compte de nos clients. Menée en lien avec les GRADeS et le CERT Santé, celle-ci impose le respect d'un protocole cadencé, pour faciliter la remédiation et la reconstruction du système d'information une fois la crise résolue. La création de notre CERT entend justement appuyer l'industrialisation des processus afin que la gestion des incidents de sécurité informatique soit la plus efficace possible. Elle facilite en outre nos échanges avec les équipes des autres CERT, car nous partageons ainsi un langage commun.

Pourriez-vous nous détailler le déroulement d'un incident de sécurité ?
Damien Ribeiro : La procédure initiale ne change pas : l'établissement commence par contacter le centre de support GPLExpert, qui va constater la réalité de l'incident, donner de premières recommandations et déclencher le CERT. Celui-ci prend alors le relais pour tenter d'isoler les serveurs et postes atteints, mais aussi confiner les sauvegardes afin d'éviter les impacts secondaires. Il va également recueillir et conserver un maximum de preuves numériques, qui seront par la suite transmises aux autorités concernées. Le CERT coordonne ensuite le traitement de l'incident pour le compte de l'établissement, afin que ce dernier puisse se concentrer sur la poursuite de son activité en mode dégradé.
Thomas Breton : Il faudrait, dans l'idéal, avoir formalisé en amont un Plan de continuité de l'activité (PCA). Mais peu d'établissements de santé en disposent dans les faits. Le CERT peut donc, aussi, aider à structurer un PCA en urgence. Une fois la crise passée, il continue de coordonner les opérations pour que la restauration s'effectue dans les meilleures conditions possibles. L'existence d'un Plan de reprise de l'activité (PRA) est ici utile, mais son absence peut également être palliée par notre CERT. Notre connaissance parfaite du secteur de la santé représente ici un atout de taille, car nous pouvons ainsi prioriser les actions à mener en fonction des contraintes propres à chaque établissement. Pour résumer, l'appui d'une structure experte comme le CERT permet à chacun de garder son sang-froid pour respecter les bonnes procédures.

Auriez-vous des recommandations particulières pour prévenir les incidents de sécurité ou les gérer plus efficacement ?
Damien Ribeiro : Nous incitons fortement les établissements de santé à mener des exercices de gestion de crise. Exactement comme lors d'une alerte incendie, si chacun connaît son rôle, on peut rapidement sortir du feu. Il est également primordial d'effectuer régulièrement des audits de sécurité et des tests de vulnérabilité, ou *Pentests*, pour parer toutes les éventualités. La présence, en interne, de personnel formé à la gestion technique d'un incident de sécurité, est aussi un plus. Ce sont là autant de prestations offertes par GPLExpert, une société par ailleurs labellisée Expert Cyber. Je terminerai par rappeler un point essentiel : la gestion d'un incident informatique est un processus transversal, qui va mobiliser de nombreux acteurs. L'appui de la direction de l'établissement est donc impératif pour que chacun puisse justement jouer son rôle. ●