Santé : le nombre d’incidents de sécurité informatique a doublé en l'espace d'un an

733 incidents de sécurité informatique ont été signalés par les établissements de santé en 2021, soit près du double de l’année précédente. Les cyberattaques, qu’elles aient visé ces derniers ou un prestataire, sont à l’origine de la plupart d’entre eux. L’Agence du numérique en santé réitère ses conseils à l’égard de toutes les organisations.

Temps de lecture : minute

29 avril 2022

C’est un signal d’alerte. L’Agence du numérique en santé indique, dans la dernière édition de son Observatoire des signalements d’incidents de sécurité des systèmes d’information pour le secteur santé, avoir enregistré 733 déclarations d’incidents en 2021. C’est près du double de ce qui avait été relevé l’année précédente (369 signalements). Cette explosion, à laquelle a dû faire face le CERT Santé – l’organisme public regroupant les experts qui aident les établissements à répondre aux incidents en matière de cybersécurité –, serait en grande partie imputable à la hausse des actes malveillants. Ces derniers concernent, à en croire l’institution, 52 % des cas relevés. Les autres signalements relèvent plutôt de la panne de serveurs. Toujours est-il que, quelle que soit l’origine du désagrément, cette situation est de nature à désorganiser des établissements dont le fonctionnement a déjà été mis à rude épreuve par la crise sanitaire liée au Covid-19.

Un fonctionnement en mode dégradé

Dax, Villefranche-sur-Saône, Assistance publique-Hôpitaux de Paris (AP-HP)... Nombreux sont les établissements à avoir été victimes de rançongiciels, au cours des derniers mois. S'il relève qu'il n'y a, "*à ce jour, pas eu d'attaque coordonnée visant à désorganiser fortement le système de soins français*" dans son ensemble, le CERT Santé estime que "*plus que jamais, la mobilisation de l'ensemble des acteurs* [directions, experts techniques et professionnels de santé] *est nécessaire afin de parer aux menaces de cybercriminalité qui s'intensifient dans un contexte général instable*". En effet, les établissements victimes de cyberattaques ont vu leur accès aux données de santé de leurs patients suspendu de manière temporaire. Le rapport note ainsi une forte activité relative au vol d'identifiants de comptes de messageries et d'accès à distance. Les pirates informatiques récupèrent ces informations par trois biais : l'hameçonnage (phishing), l'exploitation de vulnérabilités sur des équipements non mis à jour et en essayant un très grand nombre de mots de passe.

* * ici sont présentées les données de 2021 en rose et les données de 2020 en bleu
1 : appui pouvant mobiliser un ou plusieurs experts durant plusieurs jours

À noter que le rapport souligne que la hausse des incidents en 2021 s'explique aussi par les incidents survenus chez les prestataires de services – à l'image des divers hébergeurs d'applications métiers, eux-mêmes touchés par des attaques et pannes – ayant une part de marché significative. Arrive ensuite la perte du "lien télécom" , qui perturbe fortement le fonctionnement des activités des structures de santé. 60 % de ces dernières jugent ainsi que l'incident qu'elles ont connu dans l'année a "*eu un impact sur des données, qu'elles soient à caractère personnel ou technique*". 52 % ont même dû mettre en œuvre un mode "dégradé" de la prise en charge des patients, soit 7 % de plus qu'en 2020. Il faut aussi relever que 26 % des établissements ont demandé un accompagnement au CERT Santé, notamment pour gérer la compromission de leur système informatique.

À lire aussi
Covid-19 : Comment CybelAngel a neutralisé une escroquerie visant un fabricant de vaccins

"*Les structures auditées exposent souvent trop de ressources sur l'Internet et ne portent pas suffisamment d'attention à la sécurisation de*

leurs services (portail en ligne, accès à distance, etc.)*. L’exploitation de certaines vulnérabilités peuvent permettre à un attaquant d’accéder par rebond à leur système d’information avec, parfois, des privilèges élevés*" , alerte l’Agence du numérique en santé. Et de formuler des recommandations : réduire les surfaces d’attaque en désactivant les comptes, protocoles et services non indispensables ; appliquer une politique de mot de passe assez robuste ; améliorer le suivi des correctifs ; analyser régulièrement les journaux de ses équipements périmétriques ; renforcer les configurations et la sécurisation des accès ; vérifier la suppression des failles Web classiques ; mais aussi inclure un engagement du prestataire sur le maintien des conditions de sécurité de l’infrastructure. Des conseils valables pour toute organisation.

Article écrit par Arthur Le Denn