26 mai 2020 -09:00

Les cyberexperts prêts à assurer la cybersécurité des hôpitaux

We help our hospitals

Si le pic du nombre d'infections au coronavirus est heureusement derrière nous, les temps demeurent difficiles pour les hôpitaux. Pour que les soins apportés aux patients se déroulent sans encombre, les services d'appui tournent à plein régime. Les services informatiques en sont un bel exemple : ils ont la responsabilité de fournir une infrastructure informatique sûre à des départements infirmiers qui, actuellement, ne cessent de changer de spécialisation et de lieu.

« Au début de la crise, il y a eu une nette augmentation des cyberincidents liés à la Corona, dans divers domaines. Jamais assez, nous ne pourrons exprimer notre reconnaissance envers l'ensemble des collaborateurs au sein des hôpitaux. C'est pourquoi plusieurs entreprises et experts indépendants spécialisés dans la cybersécurité ont décidé de mettre leur expertise à titre bénévole à la disposition des hôpitaux. », explique Ulrich Seldeslachts, LSEC, porte-parole de *We help our hospitals*.

Dès le début de la crise, ces experts ont uni leurs forces et l'initiative *We help our hospitals* a rapidement vu le jour. Ce sont ainsi plus de 30 experts volontaires et un nombre croissant d'entreprises qui se tiennent prêts depuis quelques semaines à intervenir si nécessaire. Le Centre pour la Cybersécurité Belgique (CCB) soutient cette initiative.

Quel type de soutien peuvent-ils proposer ?

Les experts peuvent avant tout dispenser des conseils et de l'aide en cas de cyberincident tels que le 'ransomware', les fuites de données ou les accès non autorisés. En outre, ils sont disposés à donner des conseils moins urgents en matière de mesures de cybersécurité préventives. Comment interviennent-ils ?

Les hôpitaux qui sont victimes d'une cyberattaque peuvent toujours s'adresser à CERT.be, le service opérationnel du Centre pour la Cybersécurité Belgique (CCB). CERT.be est accessible 24/24h. Grâce à l'initiative *We help our hospitals*, CERT.be peut désormais également faire appel à ce groupe d'experts individuels en cybersécurité pour obtenir un soutien supplémentaire si nécessaire.

Les questions non urgentes en matière de sécurisation préventive du réseau informatique peuvent directement être adressées à www.wehelpourhospitals.be. Les volontaires participants dispensent des conseils et une assistance adéquats dans leur domaine d'expertise.

> « Rien n’indique que les cybercriminels visent aujourd’hui plus qu’hier les organismes de soins. Chaque organisation est une cible potentielle des cybercriminels. Il est vrai que si un cyberincident devait se produit dans le contexte actuel, il risquerait de fortement perturber le bon fonctionnement des hôpitaux, ce que nous voulons tous éviter bien entendu. Mieux vaut prévenir que guérir. »

Miguel De Bruycker
Directeur du Centre pour la Cybersécurité Belgique

Europol* signale toutefois une augmentation des cyberattaques en Europe qui sont en lien avec le COVID-19 : davantage d’attaques de type ransomware sur le COVID-19, aussi dans les hôpitaux, et davantage de messages de phishing et de faux sites Internet.

Cette initiative a-t-elle déjà pu offrir ses services ?

Quelques hôpitaux ont déjà fait appel à cette initiative et ont demandé des conseils préventifs, tels qu’une analyse des risques, un inventaire des différents systèmes et des points critiques ou un soutien dans l'organisation d'éventuels incidents. Pour l’heure, heureusement, aucun incident n’a nécessité d’intervention en urgence.

« Un hôpital général proposant une large gamme de soins et bénéficiant d’un rayonnement régional vaste témoigne : En ces temps exceptionnels, plusieurs initiatives citoyennes ont proposé leur aide à l’hôpital. Grâce à l’initiative Wehelpourhospitals, l’hôpital a pu faire appel à différents experts qui s’engagent sur une base volontaire pour la sécurisation des infrastructures IT critiques des hôpitaux. Des spécialistes en sécurité ont ainsi analysé l’intégralité du réseau de données de l’hôpital et soumis plusieurs de ses systèmes IT critiques aux contrôles de sécurité les plus sévères. »

Plus d'information

- CERT.be: https://cert.be/fr/nous-aidons-les-hopitaux-en-cas-de-cyberincident
- We help our hospitals: https://wehelpourhospitals.be/
- *Europol: https://www.europol.europa.eu/staying-safe-during-covid-19-what-you-need-to-know

Contact presse organisations participantes: We help our hospitals

- Ulrich Seldeslachts - T: +32 475 71 3602 - ulrich@leadersinsecurity.org - www.wehelpourhospitals.be

Contact presse Centre pour la cybersécurité Belgique

- Katrien Eggers - T: +32 485 76 53 36 - Katrien.eggers@cert.be

Centre pour la Cybersécurité Belgique
Rue de la Loi 16
1000 Bruxelles
Belgique
http://www.ccb.belgium.be

Katrien Eggers
Responsable communication
+32 485 76 53 36
katrien.eggers@cert.be

Andries Bomans
Responsable communication
+32 471 66 00 06
andries.bomans@ccb.belgium.be