Aux laboratoires de biologie clinique
Aux laboratoires d'anatomie pathologie

Service : Qualité des laboratoires médicaux

Date : 15/02/2021
Vos réf. : -
Nos réf. : Sciensano-AC-2021-04
Annexe(s) : -

Contact : Arnaud Capron
Tél. : +32 2 642 53 97
Fax : +32 2 642 33 26
E-mail : arnaud.capron@sciensano.be

Concerne : Cyber attack de laboratoires médicaux et d'institutions hospitalières – Apprentissage continu.

Cher(e)s collègues,

Dans le courant des mois de décembre 2020 et janvier 2021, plusieurs centres hospitaliers et laboratoires ont été victimes d'une cyber-attaque. En conséquence, l'unité de lutte contre la criminalité informatique (Computer Crime Unit) de la police fédérale a ouvert une enquête.

Ces attaques peuvent affecter la sécurité des données gérées par les institutions concernées ainsi que l'organisation des activités des laboratoires (inaccessibilité des serveurs, etc.). Ces attaques peuvent impacter les laboratoires et tous les services associés sur le même réseau pendant plusieurs jours.
Par ailleurs, compte tenu du nombre croissant d'interconnexions entre les acteurs de la santé (laboratoire, médecin généraliste, maison de repos, hôpitaux, etc.), les conséquences d'une cyber-attaque peuvent rapidement s'étendre à plusieurs institutions et mettre en péril le réseau national de santé.

Plusieurs laboratoires (privés et hospitaliers) nous ont activement déclaré avoir été victime de ces attaques. Toutes fois nous suspectons qu'un plus grand nombre pourraient être concernés.

Afin d'évaluer les causes possibles et l'impact que ces attaques ont pu avoir sur l'activité des laboratoires médicaux, si votre laboratoire est concerné, nous vous prions de nous communiquer les informations suivantes (si votre laboratoire est concerné) :

a) la cause probable de l'attaque et la méthode prétendument utilisée par les pirates
b) Les activités/services impactées et une description succincte de la manière dont cet attentat a affecté ces activités,
c) les actions correctives immédiates qui ont été prises pour garantir la sécurité des données et la continuité des activités du laboratoire (application d'un plan dégradé, sous-traitance de certaines analyses…),
d) les mesures préventives prises par le laboratoire, ou par l'institution hospitalière, pour éviter ou limiter l'impact de ce type d'attaque à l'avenir,
e) la, ou les références, du ou des enregistrement(s) de cet évènement dans votre système qualité (sous forme de plainte ou de non-conformité),

Si votre laboratoire devait être victime de telles attaques à l'avenir, veuillez nous en informer et nous fournir au moins les informations énumérées dans cette lettre, y compris une personne de contact.

Des propositions sont en cours d'élaboration au niveau du SPF Santé publique afin de fournir un soutien supplémentaire et approprié dans ces situations particulières. Grâce aux questions ci-dessus et à vos réponses, nous espérons qu'avec les connaissances et la coopération de la CCU, de eHealth et du SPF Santé publique, des propositions spécifiques pourront être élaborées pour les laboratoires et les établissements de santé.

Dans un premier temps, vous serez désormais alerté via eHealth en cas de cyber-attaque / risque potentiel pouvant affecter l'ensemble des acteurs de santé (laboratoires, établissements de santé, hôpitaux, etc.).

Vous recevrez ces messages en tant que directeur de laboratoire. Nous comptons sur vous pour diffuser cette information auprès des membres de votre personnel qui participent à la gestion de vos installations informatiques.

Les informations demandées peuvent être transmises directement au secrétariat du service Qualité des Laboratoires QL_secretariat@sciensano.be avec en objet du mail « Cyber attaque – labo xxxxx ». Cette communication respectera la confidentialité liée à l'incident signalé.

Nous vous remercions pour votre précieuse coopération dans la création d'un environnement plus sûr pour notre système de santé.

Très cordialement,

Arnaud Capron (Signature)
2021.02.15 23:45:35
+01'00'

Dr Arnaud Capron
Chef de service Qualité des Laboratoires