

**Ter attentie van de laboratoria voor Klinische Biologie**  
**Ter attentie van de laboratoria voor Pathologische Anatomie**

**Dienst: Kwaliteit van Laboratoria**

Datum: 15/02/2021

Uw ref: -

Onze ref: Sciensano-AC-2021-04

Bijlage(n): -

Contact: Arnaud Capron

Tel.: +32 2 642 53 97

Fax: +32 2 642 33 26

E-mail: [arnaud.capron@sciensano.be](mailto:arnaud.capron@sciensano.be)

**Betreft: Cyberaanval op medische laboratoria en ziekenhuisinstellingen - Levenslang leren.**

Geachte collega's,

In de maanden december 2020 en januari 2021 zijn verschillende ziekenhuizen en laboratoria het slachtoffer geworden van een cyberaanval. Naar aanleiding hiervan, heeft de eenheid computercriminaliteit ([Computer Crime Unit \(CCU\)](#)) van de federale politie een onderzoek ingezet.

Dergelijke aanvallen hebben mogelijks gevolgen voor de veiligheid van de door de betrokken instellingen beheerde gegevens, alsook de organisatie van de laboratoriumactiviteiten (ontoegankelijkheid van de servers, enz.). Deze aanvallen kunnen zorgen voor dagenlange stilstand van het laboratorium en eventueel verbonden diensten in hetzelfde netwerk. Daarenboven kunnen gezien het toenemende aantal onderlinge verbindingen tussen spelers in de gezondheidszorg (laboratorium, huisarts, verpleeghuis, ziekenhuizen,...) de gevolgen van een cyberaanval zich snel over meerdere instellingen verspreiden en het nationale gezondheidsnetwerk in gevaar brengen.

Verscheidene laboratoria (privaat en ziekenhuis) hebben ons actief gemeld dat zij het slachtoffer zijn geworden van deze aanvallen. Wij vermoeden echter dat het totaal aantal getroffen laboratoria hoger ligt.

Om na te gaan wat de mogelijke oorzaken waren en welk effect deze aanvallen op de activiteiten van de medische laboratoria hebben gehad, wordt u verzocht (indien betrokken) ons de volgende informatie te verstrekken:

- a) De vermoedelijke oorzaak van de aanval en de methode die de hackers gebruikt zouden hebben
- b) De activiteiten/diensten waarop de aanval een impact heeft en een korte beschrijving van de consequenties van deze aanval voor deze activiteiten,
- c) De onmiddellijke, corrigerende maatregelen die werden ondernomen om de veiligheid van de gegevens en de continuïteit van de laboratoriumactiviteiten te waarborgen (toepassing van een noodplan, onderaanneming van bepaalde analyses...),
- d) De preventieve maatregelen die door het laboratorium of door de ziekenhuisinstelling zijn genomen om dit soort aanvallen in de toekomst te vermijden of de invloed ervan te beperken,
- e) De referentie(s) van de registratie(s) van dit incident in uw kwaliteitssysteem (in de vorm van een klacht of non-conformiteit).

**Mocht uw laboratorium in de toekomst het slachtoffer worden van dergelijke aanvallen, dan verzoeken wij u ons op de hoogte te brengen en ons ten minste de in deze brief genoemde gegevens te bezorgen, met inbegrip van een contactpersoon.**

Op het niveau van het FOD Volksgezondheid worden voorstellen uitgewerkt om in deze bijzondere situaties aanvullende en aangepaste steun te verlenen. Via bovenstaande vragen en dankzij uw antwoorden hopen wij dat met de kennis en de medewerking van de CCU, eHealth en het FOD Volksgezondheid specifieke voorstellen kunnen worden uitgewerkt voor de laboratoria en zorginstellingen.

In eerste instantie wordt u vanaf nu via eHealth gewaarschuwd in geval van een cyberaanval/potentieel risico dat gevolgen kan hebben voor alle actoren in de gezondheidszorg (laboratoria, zorginstellingen, ziekenhuizen, ...).

U, als laboratoriumdirecteur, zal deze berichten ontvangen. Wij rekenen erop dat u deze informatie verspreidt onder uw medewerkers en andere partijen die betrokken zijn bij het beheer van uw IT-faciliteiten.

In eerste instantie wordt u vanaf nu via eHealth gewaarschuwd in geval van een cyberaanval/potentieel risico dat gevolgen kan hebben voor alle actoren in de gezondheidszorg (laboratoria, zorginstellingen, ziekenhuizen, ...).

De gevraagde informatie kan rechtstreeks worden toegezonden aan het secretariaat van de dienst Kwaliteit van Laboratoria ([QL\\_secretariat@sciensano.be](mailto:QL_secretariat@sciensano.be)) met als onderwerp "Cyberaanval – labo xxxxx". Uw privacy van het gemelde incident zal bij deze communicatie gerespecteerd worden.

We danken u voor uw waardevolle medewerking aan de totstandbrenging van een veiliger omgeving voor ons gezondheidszorgsysteem.

Met de meeste hoogachting,

Dr Arnaud Capron  
Diensthooft Kwaliteit van Laboratoria, Sciensano