De Jonge: kwetsbaarheden IT-systemen GGD onder controle

2 april 2021

‘Er zijn mitigerende maatregelen genomen waarmee eerder geconstateerde kwetsbaarheden tot het minimum zijn gereduceerd’, schrijft De Jonge. ‘Om alle kwetsbaarheden op te lossen zullen enkele applicaties – waaronder HP Zone – moeten worden vervangen. Hierover worden nu concrete afspraken gemaakt en acties in gang gezet tussen GGD, RIVM en VWS. Daarnaast vindt er actieve monitoring plaats op de IT-systemen. Bij afwijkingen wordt 7 dagen per week direct actie ondernomen.’

Kwetsbaarheden misbruikt

Aanleiding van de risicoanalyse en het vervangen van het IT-systeem waren de ontwikkelingen rondom de diefstal van persoonsgegevens uit informatiesystemen van de GGD. Uit onderzoek van RTL Nieuws bleek in januari dat een kwetsbaarheid is misbruikt door medewerkers die persoonsgegevens hebben verkocht. Het downloaden ervan was al sinds april 2020 mogelijk. Privacy-toezichthouder AP heeft de GGD sinds januari onder verscherpt toezicht gesteld.

De Jonge geeft verder aan dat er structureel cyberaanvallen testen ingezet worden, waarvan de resultaten worden gebruikt om kwetsbaarheden proactief te traceren en op te lossen. Als er bij de continue en grotendeels automatisch monitoring op misbruik van de GGD-systemen afwijkingen worden geconstateerd, vindt direct een ‘afgewogen actie’ plaats. Persoons- en andere gegevens worden nog altijd gecombineerd opgeslagen, maar ‘de functionaliteiten zijn dermate sterk gereduceerd dat de kans op frauduleuze handelingen zo veel mogelijk is

verkleind’.

Draaiboek bij volgende incidenten

Er ligt nu ook een draaiboek klaar voor volgende Incidenten. Het recent ingerichte en nu volledig operationele SOC (Security Operations Center) van GGD GHOR Nederland staat in nauw contact met alle GGD’en en onderneemt direct actie als er incidenten optreden, belooft de bewindsman. De te nemen maatregelen zijn afhankelijk van het incident.

Vorig jaar is onder verantwoordelijkheid van de Landelijke Coördinatiestructuur Testcapaciteit (LCT) de Regiegroep Digitale Ondersteuning Test- en Traceerketen (DOTT) opgericht. De Regiegroep DOTT heeft afgelopen december in opdracht van VWS, GGD GHOR Nederland en RIVM een risicoanalyse opgeleverd. Op basis hiervan heeft de Regiegroep met alle ketenpartners een verbeterplan opgesteld. Hierin staan maatregelen om eerder gesignaleerde risico’s en kwetsbaarheden in de ketenbrede digitale ondersteuning en infrastructuur binnen de test en traceerketen aan te pakken.

Risicoanalyse niet openbaar

Minister Hugo de Jonge schreef in een Kamerbrief van half februari dat hij deze risicoanalyse van kwetsbaarheden in IT-systemen voor testen en traceren niet openbaar wilde maken. Dit ondanks verzoeken hiertoe vanuit de Tweede Kamer. Het NCSC (Nationaal Cyber Security Centrum) en een door de minister ingesteld Red Team vonden de gevaren te groot, aldus De Jonge. Dat geldt nog altijd, geeft de bewindsman nu aan. In dezelfde Kamerbrief meldde De Jonge dat GGD GHOR Nederland overging tot versnelde vervanging van HPZone (Lite).

De NCSC stelde in februari dat de informatie in de risicoanalyse dieper inzicht geeft in de beveiligingsarchitectuur van de testketen en dat dit kwaadwillenden kan helpen om aanknopingspunten voor aanvallen te vinden. Het centrum benadrukte dat er risico’s zijn verbonden aan het openbaar maken van deze informatie en dat vertrouwelijk houden van de analyse vanuit technisch oogpunt het meest wenselijk was.