[redacted]

Managementsamenvatting “Cupertino”

Van	Fox-IT
Aan	Ministerie van Justitie en Veiligheid
Datum	7 juni 2023
Referentie	Cupertino
Onderwerp	Managementsamenvatting onderzoek ‘Cupertino’

Op de volgende pagina is de managementsamenvatting uit het onderzoeksrapport van het onderzoek “Cupertino” te vinden. Deze managementsamenvatting geeft een beeld over de aanleiding, aanpak, bevindingen en de door Fox-IT getrokken conclusies uit dit onderzoeksrapport.

Alle naar een persoon herleidbare informatie is middels een zwarte balk geredigeerd. Dit om de privacy van betrokken natuurlijke personen te waarborgen.

Managementsamenvatting

De plaatsvervangend Secretaris-Generaal van het Ministerie van Justitie en Veiligheid heeft Fox-IT benaderd inzake een incident bij Justis betreffende het proces rondom het opleveren van auditrapporten. Het vermoeden bestond dat auditrapporten zijn aangepast. Fox-IT is gevraagd dit te onderzoeken.

Daarbij is Fox-IT gevraagd op basis van (digitale) sporen de volgende onderzoeksvragen centraal te stellen:

1 Welke aanpassingen zijn er gemaakt aan de rapportages en begeleidende documenten betreffende de ICT beveiligingsassessments DigiD op de “Digitaal Aanvragen”-omgeving?
2 Welk pad hebben de rapportages betreffende de ICT beveiligingsassessments DigiD afgelegd vanaf het moment van ontvangen door Justis tot het moment van opleveren aan Logius?
3 Kan worden bepaald wanneer en door welke gebruiker(s) specifieke wijzigingen zijn aangebracht?
4 Kan worden bepaald of anderen dan degene die vermoedelijk de aanpassingen heeft uitgevoerd betrokken zijn geweest bij of op de hoogte zijn geweest van de aanpassingen?

Om deze vragen te beantwoorden heeft Fox-IT verschillende versies van auditrapportages ontvangen van ADR, Justis en Logius. Omdat [redacted] verantwoordelijk was voor het ontvangen (van ADR) en opleveren (aan Logius) van de rapporten heeft Fox-IT behalve naar de auditrapporten ook onderzoek gedaan naar de mailbox en persoonlijke mappen van [redacted]. In het onderzoek van Fox-IT kwam verder naar voren dat op vergelijkbare wijze Suwinet-rapporten zijn aangepast. Deze rapporten zijn daarom ook in de scope van het onderzoek meegenomen.

Om vast te kunnen stellen welke wijzigingen zijn aangebracht heeft Fox-IT de originele en aangepaste versies van de rapporten met elkaar vergeleken. Voor het beantwoorden van de vragen over waar de documenten aanwezig waren, wanneer de wijzigingen hebben plaatsgevonden en welke gebruiker de wijzigingen heeft aangebracht heeft Fox-IT ook de e-mails en documenten in de ontvangen mailbox en persoonlijke mappen onderzocht.

Uit het onderzoek blijkt dat tussen 2018 en 2022 elf rapporten zijn aangepast of nagemaakt. In deze periode zijn voor DigiD, na het eerste volledige rapport in 2018 die niet is aangepast of nagemaakt, alle volgende (vier) volledige rapporten aangepast en alle (vier) verbeterrapporten nagemaakt. Voor Suwinet is in 2020 een rapport aangepast en zijn in 2021 en 2022 twee rapporten nagemaakt. Voor de aanpassingen geldt in essentie dat oordelen van “Voldoet niet” veranderd zijn naar “Voldoet” en bevindingen zijn verzwakt of weggelaten.

Verder heeft Fox-IT vastgesteld dat het gebruikersaccount van [redacted] telkens de originele rapporten per e-mail ontvangt van ADR op [redacted]. Zowel een aantal originele als aangepaste rapporten zijn door dit account doorgestuurd naar [redacted] Uit het onderzoek blijkt dat dit account nooit een aangepaste versie van een rapport heeft ontvangen. De aanpassingen in de documenten vonden telkens plaats nadat Justis de rapporten van ADR ontving en voordat Justis ze aan Logius opleverde. Op basis hiervan acht Fox-IT het aannemelijk dat de wijzigingen in de documenten met het gebruikersaccount van [redacted] zijn uitgevoerd.

Fox-IT heeft geen sporen aangetroffen die aantonen dat andere gebruikers dan het gebruikersaccount van [redacted] op de hoogte zijn geweest van aanpassingen in de rapporten, of betrokken zijn geweest bij het aanpassen of namaken van de rapporten.