BIJLAGE BIJ BRIEF MET KENMERK 2017-0000152821

Vraag 1
U geeft in uw brief aan dat logging wel heeft plaatsgevonden bij D&A, maar actieve monitoring niet. U noemt in uw brief als één van de aanvullende maatregelen om de databeveiliging te verbeteren, het werken aan een structurele (technische) oplossing van continue monitoring.

a. Doelt u met de "actieve monitoring" op actieve monitoring van de logging?
Zo nee, geef aan waar u wel op doelt.

Ja, met de "actieve monitoring" wordt inderdaad actieve monitoring van de logging bedoeld.

b. Doelt u met "het werken aan een structurele (technische) oplossing van continue monitoring" op actieve continue monitoring van de logging?
Zo nee, geef aan waar u wel op doelt.

Zo ja, geef gedetailleerd aan wat de problemen zijn op het gebied van continue monitoring (van de logging).

Met "het werken aan een structurele (technische) oplossing van continue monitoring" wordt inderdaad op actieve continue logging gedoeld.

De uitdaging op het gebied van continue monitoring is met name het zodanig correleren van de verschillende log-meldingen en het daaruit destilleren van mogelijke verdachte handelingen, dat er alleen de echte verdachte handelingen uitrollen. Teveel meldingen maakt dat het systeem als onbetrouwbaar gezien wordt (lage attentiewaarde), terwijl te weinig meldingen de kans vergroten op ongeziene verdachte handelingen.

c. Geef gedetailleerd aan welke maatregelen er vanaf 1 januari 2013 tot aan het moment dat u in uw onderzoek bent gestuit op de gevallen van ongeoorloofde gegevensuitwisseling bij D&A en haar voorgangers, op het gebied van monitoring van de logging bestonden.

Er was geen sprake van actieve monitoring van de logging. Bij het ontwerp van de AWS+ was het beoogde inzetgebied beperkt tot de data waar de betrokken gebruikers toch al toegang toe hadden. In 2012 was de context anders dan vandaag, de wijze waarop D&A de AWS+ heeft ingezet was weliswaar werkbaar, maar niet conform oorspronkelijk technisch ontwerp van deze IT dienst. Daarom is er in 2015 een start gemaakt met de SAS-Grid oplossing.

d. Geef een gedetailleerde omschrijving van de maatregelen die de structurele technische oplossing van continue monitoring moeten bieden.

Een gestructureerd proces voor de continue monitoren van de logging is in voorbereiding. Naar verwachting bestaat hierover begin september 2017 meer duidelijkheid.

Op hoofdlijnen bestaat de maatregel uit het aansluiten van de relevante logging op de centrale logvoorziening van Splunk, met een actieve set aan business rules die specifieke zaken detecteren. Splunk is de centrale logging en monitoring faciliteit waar de Belastingdienst gebruik van maakt voor diverse services. De Autoriteit Persoonsgegevens is al verschillende malen geïnformeerd over de mogelijkheden en inzet van deze service.

De Belastingdienst is uiteraard bereid de Autoriteit Persoonsgegevens te zijner tijd nader te informeren.

e. Geef aan wanneer de maatregelen bedoeld onder d geïmplementeerd zullen zijn.

Voor de bestaande services worden deze maatregelen niet geïmplementeerd, aangezien deze omgeving end of service verklaard is. Voor de nieuwe Analytics voorziening is de logging vanaf 21 juli 2017 aangesloten op Splunk. Let wel: daarmee is actieve set aan business rules (zie 1d) nog niet gerealiseerd. Momenteel wordt aan de functionele migratie naar het nieuwe platform gewerkt, aansluitend worden de business rules gemaakt. Met de huidige kennis is het de verwachting dat de eerste versie gedurende het vierde kwartaal van 2017 operationeel zal worden. Aangezien het onderhouden een continu proces is bestaat er geen “einddatum” waarop het klaar is. De Belastingdienst heeft dan echter wel een gestructureerde toegang tot de logging voorhanden.

Vraag 2
U noemt in uw brief tevens als één van de aanvullende maatregelen het datacompartimentering van de analyseomgeving.

a. Geef gedetailleerd aan op welke punten de datacompartimenering van de analyseomgeving tekort schoot.

Door binnen de AWS+ omgeving gebruik te maken van een beperkte set aan rol-autorisaties (zoals reeds gemeld is aan de Autoriteit Persoonsgegevens) heeft elke gebruiker die opgevoerd is in een specifieke rol de gelegenheid om bij alle data op dat systeem te kunnen, die met deze rol benaderd kan worden. Binnen de desbetreffende AWS+ was er dus geen sprake van data compartimentering.

b. Geef een gedetailleerde omschrijving van de maatregelen die u gaat nemen op het gebied van datacompartimering van de analyseomgeving.

Door in de SAS-Grid omgeving op de datafundamenten middels een fijnmaziger autorisatie model te werken, zal de data gecompartimenteerd zijn en alleen bruikbaar zijn voor de rol en toepassing die geautoriseerd is.
Daarnaast zullen er een Point of Delivery (PoD) worden gebouwd waarbij de volledige data analyse omgeving zal worden geïsoleerd.

c. Geef aan wanneer de maatregelen bedoeld onder a geïmplementeerd zullen zijn.

Ervan uitgaand dat de Autoriteit Persoonsgegevens de maatregelen bedoelt die onder 2b geïmplementeerd worden:
- fijnmaziger autorisatie model is reeds geïmplementeerd;
- de PoD zal in het eerste kwartaal van 2018 gerealiseerd zijn.

Vraag 3

a. Geef aan welke maatregelen u gaat treffen of heeft getroffen om ervoor te zorgen dat datatransfer vanuit de dataomgeving van D&A naar buiten de Belastingdienst middels e-mailverkeer in de toekomst niet meer mogelijk is of tot een minimum wordt beperkt. Ga daarbij zowel in op de beleidsmatige keuzes als de praktische maatregelen die daartoe genomen worden.

Het gaat om de volgende technische implementatie van praktische maatregelen:
- Het blokkeren van externe e-mail buiten de Belastingdienst van medewerkers op de desbetreffende analyse omgeving;
- Het blokkeren van internettoegang en alleen whitelisting toepassen; whitelisting betekent dat internet toegang enkel mogelijk is voor websites die op een speciaal daartoe opgezette

lijst staan, deze lijst heet whitelist. Dit in tegenstelling tot het fenomeen blacklisting waarbij toegang open staat voor alle sites behalve degene die op een lijst staan waarmee deze sites geblokkeerd worden;
- Het blokkeren van de File Transfer Dienst (Aspera).

Vraag 4

Op 29 juni 2017 heeft uw Adviseur informatiebeveiliging, L.B. Kobes, een datalek gemeld bij de AP. In de melding heeft u aangegeven dat bij een unit van de Belastingdienst een aantal bestanden met persoonsgegevens onbevoegd naar externe e-mailadressen zijn gestuurd.

U heeft in de melding op de vraag hoeveel betrokkenen u heeft geïnformeerd of gaat u informeren, geantwoord dat dat er 100.000 zijn?

a. Kunt u aangegeven of u de betrokkenen al heeft geïnformeerd?

De Belastingdienst heeft nog niet alle betrokkenen geïnformeerd. De Belastingdienst doet namelijk nog onderzoek naar de feiten. Pas wanneer de feiten vaststaan, kan worden beoordeeld of er een kennisgeving aan betrokkenen moet worden gedaan. Daarbij zullen eveneens redenen van behoorlijkheid en zorgvuldigheid worden meegewogen.

Ten aanzien van de onder A genoemde casus uit de brief aan de Kamer kan ik u berichten dat de betrokkenen zijn geïnformeerd. De Belastingdienst heeft daarbij gebruik gemaakt van informatie die is verkregen van de werkgever waar het desbetreffende bestand om lijkt te draaien. De reden van de kennisgeving is dat eind juni 2017 bij de Belastingdienst op basis van de toen bekende feiten en omstandigheden het sterke vermoeden bestond dat er ook sprake was van misbruik van gegevens, van kwade opzet. Betrokkenen zijn daarop onverwijld geïnformeerd. Zodra het onderzoek naar de feiten is afgerond, wordt bezien of deze betrokkenen nader moeten worden geïnformeerd. De Belastingdienst doet nog onderzoek naar de feiten met betrekking tot de andere personen in dit bestand. Dit feitenonderzoek is vrijwel afgerond, zodat kan worden beoordeeld of er een kennisgeving aan betrokkenen moet worden gedaan.

b. Indien het antwoord ontkennend is, geef aan binnen welke termijn u de betrokken gaat informeren.

Mochten de feiten die uit het onderzoek naar voren komen daartoe aanleiding geven, dan zal de Belastingdienst betrokkenen onverwijld informeren. Ik merk hierbij op dat wanneer het om een groot aantal betrokkenen mocht gaan, er enige tijd gemoeid kan zijn met het inregelen van het massale proces voor de verzending van brieven en het instrueren van het centraal informatiepunt, de Belastingtelefoon, voor het behandelen van vragen naar aanleiding van de verzonden brieven.