UNIVERSITEIT VAN AMSTERDAM

Centrale Ondernemingsraad

COR-secretariaat

Spui 21
1012 WX Amsterdam
Postbus 19268
1000 GG Amsterdam

T 020 525 6955
E-mail: cor@uva.nl

College van Bestuur van de Universiteit van Amsterdam
Mw. prof. dr. G.T.M. ten Dam
Spui 21
1012 WX Amsterdam

Datum	Telefoon	Uw kenmerk
21 juni 2017	020 525 6955	2017cu0660
Contactpersoon	**Bijlagen**	**Ons kenmerk**
E.B.I. Moors	-	cor17/u031

Onderwerp
Reactie instemmingsverzoek digitalisering P-processen en P-dossiers

Geacht College,

De Centrale Ondernemingsraad heeft uw instemmingsverzoek betreffende het project Digitalisering P-processen en P-dossiers d.d. 2 mei jl. in goede orde ontvangen.

De COR is het uiteraard met u eens dat het project een significante verbetering kan brengen in de efficiency, transparantie en naleving van regelgeving van personeelsprocessen, maar vindt het van uiterst belang dat er bij de vervanging van de papieren werkelijkheid door een digitale werkelijkheid alles aan gedaan wordt om de rechten van de medewerkers te beschermen aangaande privacy, informatiebeveiliging en de arbeidswetgeving.

Het is een complex proces over veel fases dat al sinds eind 2015 loopt in de vorm van voorbereidingswerkzaamheden en verscheidene pilots. Het College heeft met de COR en de decentrale ondernemingsraden op allerlei momenten informatie hierover uitgewisseld. De COR heeft dit als positief ervaren en hoewel de evaluatiecriteria niet altijd even helder zijn opgesteld zijn de pilots naar tevredenheid verlopen.

Verder is de COR verheugd dat er goed oog is voor de personele gevolgen van deze transitie, dat er geen reorganisatie nodig zal zijn en dat er ruimte wordt gecreëerd voor hoogwaardigere werkzaamheden.

Toch blijven er zorgen bij de COR op de gebieden van privacy en beveiliging.

Op het gebied van de technische beveiligingsaspecten is er een aantal gesprekken gevoerd tussen leden van de COR en (toenmalig) directeur ICTS Voorbraak met zijn experts op het gebied van beveiliging. Deze discussies gingen over het document 'Beveiligingsarchitectuur Digitale Personeelsprocessen en Digitale Personeelsdossiers'. Tijdens deze gesprekken is een groot aantal zorgen van de COR weggenomen. Toch blijven er twee over.

Het eerste probleem betreft de verbinding tussen het SAP systeem waarin personeelsgegevens zijn opgeslagen en de SAP GUI ('graphical user interface') op de PC van een medewerker die deze gegevens raadpleegt of verwerkt. Deze verbinding is niet versleuteld met als gevolg dat een kwaadwillende personeelsgegevens zou kunnen onderscheppen. De ernst van deze kwetsbaarheid is gemitigeerd doordat de gegevensstroom alleen binnen het UvA-netwerk wordt uitgewisseld maar met

duizenden gebruikers per dag kan er niet worden gegarandeerd dat de perimeter van het UvA-netwerk ook ondoordringbaar blijft.

De huidige ad interim directeur ICTS Vervaat erkent dit probleem en geeft aan dat de beveiliging op dit punt in 2017 verbeterd wordt. Hij stelt dat het een structurele wijziging in de SAP-infrastructuur aangaat en dat het pas in september 2017 op de wijzigingenkalender staat.

Het tweede beveiligingsprobleem is ernstiger. Medewerkers benaderen de P-Processen en P-dossiers via de Zelfbedieningstool. De Zelfbedieningstool is alleen bereikbaar binnen het UvA-netwerk. Een medewerker die zich buiten het UvA-netwerk bevindt, bijvoorbeeld een medewerker thuis die zich ziek moet melden, moet eerst toegang tot het UvA-netwerk verschaffen via zogenaamde VPN software ('virtual private network'). Alle gegevens tussen de medewerker en het UvA-netwerk worden uitgewisseld over dit VPN.

ICTS heeft gekozen voor een VPN oplossing die propriëtair is. Het heet "VPN Plus" van het bedrijf Juniper Networks. VPN Plus is een "closed source" softwarepakket, dat wil zeggen dat niemand inzicht kan krijgen in de veiligheid en betrouwbaarheid ervan behalve Juniper zelf. Cryptografen beschouwen dergelijke "closed source" software als inherent onbetrouwbaar en onveilig.[1] In het geval van Juniper bleek deze argwaan gegrond toen het bekend werd dat software van Juniper een achterdeurtje had waardoor gevoelige informatie naar derden (in het bijzonder de Amerikaanse National Security Agency) doorgespeeld was.

In de *stand van zaken P-processen* ontvangen via mevrouw Widdershoven op 8 juni jl. wordt vermeld 'De oplossing maakt gebruik van standaard encyptie algorythme en heeft van het National Institute of standards and Technology (NIST) een FIPS-140-2 level 2 certificering gekregen.' Omdat het bekend is dat NIST zijn standaarddocumenten heeft laten verzwakken op bevel van de NSA geeft zo een beroep op NIST standards weinig vertrouwen.[2]

Het gebruik van deze VPN oplossing heeft niet alleen gevolgen voor gegevensuitwisseling van P-processen, maar voor ***alle*** gegevensuitwisselingen van een UvA-medewerker met het UvA-netwerk van buitenaf. In dit licht is het uiterst zorgelijk dat het niet met de grootste urgentie wordt opgepakt.

Ondanks eerdere toezeggingen dat er 'half 2017' een veilige oplossing gereed zou zijn, blijkt uit de recente update dat er pas later dit jaar alternatieven worden verkend. De COR neemt het standpunt in dat deze beveiligingskwetsbaarheden op orde moeten zijn voordat hij in kan stemmen.

Verder ziet de COR graag dat er in het kader van de overgang naar P-processen en P-dossiers de medewerker goed geïnformeerd wordt over zijn rechten voortvloeiend uit de Wet bescherming persoonsgegevens en de arbeidswetgeving. In het bijzonder dat de artikelen 3 t/m 13 worden toegevoegd aan de regeling 'Regeling toegang en beheer digitale personeelsdossiers.'
Het opnemen van een klachtuitspraak in zowel het dossier van klager als in dat van beklaagde dient ook opgenomen te worden in de regeling personeelsdossiers omdat dit voortvloeit uit art.5 lid 1 van het Reglement Klachtencommissie UvA. Het feit dat dit in die regeling reeds is opgenomen volstaat

[1] “In the cryptography world, we consider open source necessary for good security; we have for decades. Public security is always more secure than proprietary security. It's true for cryptographic algorithms, security protocols, and security source code.” -- Bruce Schneier, 1999.
[2] Zie ook:
https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology#Controversial_Backdoored_NIST_Standard

Ons kenmerk
cor17/u031

niet, omdat het in de regeling personeelsdossiers ook betrekking moet hebben op andere klachtuitspraken zoals die van het College voor de Rechten van de Mens.

Derhalve kan de COR niet instemmen met dit voorstel tot:

1. Er een veilige verbinding geregeld is tussen SAP en SAP-GUI (intern UvA);
2. Er een veilig alternatief is voor de VPN verbinding om van buiten de UvA toegang tot het UvA-netwerk te verkrijgen (extern UvA);
3. Er goed gecommuniceerd wordt naar de medewerkers over de privacyaspecten vastgelegd in de Wet bescherming persoonsgegevens en arbeidswetgeving en de 'Regeling toegang en beheer digitale personeelsdossiers' hierop aangepast wordt;
4. Het opnemen van een klachtuitspraak in zowel het dossier van klager als in dat van beklaagde opgenomen wordt in de regeling personeelsdossiers.

Met vriendelijke groet,

Breanndán Ó Nualláin,
Voorzitter

Maarten Terpstra,
DB-lid