Externe Security scan – Juni 2021

A&O Fonds gemeenten heeft Tesorion gevraagd om door middel van social engineering de robuustheid van de genomen veiligheidsmaatregelen binnen (de helpdesk) van Carthago ICT tegen kwaadaardige verleiding/misleiding via sociale, menselijke interactie te onderzoeken.

Tesorion heeft op verschillende momenten met verschillende scenario's geprobeerd informatie, gevoelige informatie en credentials te verkrijgen.

De helpdesk heeft Tesorion voorzien van informatie over de helpdesk procedure's. Ook hebben ze Tesorion voorzien van de namen en emailadressen van de GIR-admin's van de gemeente. Dit is conform de huidige afspraken. De helpdesk heeft geen gevoelige informatie losgelaten. De helpdesk heeft ook geen credentials verstrekt.

Algemene conclusie van Tesorion is dat de Helpdesk erg hulpvaardig is. Wellicht iets te hulpvaardig. Advies van Tesorion is dat we het verstrekken van de namen en emailadressen van de GIR-admin's pas doen na validatie van de identiteit van de beller. Bv door de beller een email te laten sturen. Carthago ICT gaat deze aanbeveling per direct overnemen.