DIGID ASSESSMENT

Sinds enige jaren zijn alle organisaties met een DigiD-aansluiting verplicht deze jaarlijks te laten controleren door een RE (Register EDP-Auditor) en het auditrapport te delen met Logius. Ook voor nieuwe DigiD-aansluitingen geldt dat deze binnen twee maanden na inproductiename moeten worden gecontroleerd. Deze verplichte DigiD-assessments kennen een aantal fases en onderdelen waaronder kwetsbaarhedenscans en penetratietests.

IN CONTROL WITH SECURA

Secura heeft bijna twee decennia ervaring in informatiebeveiliging en privacy op het gebied van mensen, processen, technologie en organisatie. Wij identificeren IT-beveiligingsrisico's vanuit een onafhankelijk standpunt, terwijl het hoogste niveau van vertrouwelijkheid en integriteit behouden blijft. Dit stelt u in staat om proactief de controle te houden over de eigen digitale veiligheid.

OVERZICHT DIENSTEN

Secura biedt u diverse diensten aan om te voldoen aan de verplicht gestelde beveiligingsrichtlijnen van Logius. Dit zijn:

- De jaarlijkse audit, uit te voeren door een Register EDP-auditor (RE).
- De enkelvoudige webapplicatie test op de DigiD-ontsloten applicaties (kort voor het DigiD-assessment);
- De periodieke kwetsbaarhedenscans op de complete DigiD infrastructuur;
- De periodieke webapplicatie testen op de DigiD-ontsloten applicaties.

Deze diensten kunnen apart, of in combinatie met elkaar worden afgenomen. Juist in de combinatie van deze diensten wordt de impact van het DigiD-audit proces voor u tot een minimum teruggebracht.

OVERZICHT VAN HET DIGID ASSESSMENT PROCES

In de voorbereidingsfase overleggen wij met u over de planning, ontvangt u een overzicht van benodigde stukken en een toelichting daarop. Hierna start de uitvoering van het onderzoek met o.a. interviews, onderzoek van documentatie en systeeminstellingen. Hierbij maken wij tevens gebruik van de uitkomsten

van een webapplicatietest. De bevindingen leggen wij vast. Deze bevindingen nemen wij op in een rapport conform de standaard van Logius. Dit conceptrapport met bevindingen stemmen wij met u af. Na ontvangst van uw bevestigingsbrief over dit conceptrapport, brengen wij het definitieve assessment rapport uit die u kunt delen met Logius. Het DigiD assessment sluiten wij af met een evaluatie.

BESCHRIJVING VAN DE DIENSTEN

Het Logius normenkader (thans in versie 2.0) dat aan de audit ten grondslag ligt is afgeleid van de NCSC normen voor veilige webapplicaties. Daar zijn veel technische beveiligingsrichtlijnen een onderdeel van.

Bij een kwetsbaarhedenscan scannen wij geautomatiseerd een reeks systemen op bekende zwakheden, zoals bijvoorbeeld verkeerd geconfigureerde servers en ontbrekende patches. De Logius norm schrijft voor dat deze scans periodiek dienen plaats te vinden. Wij adviseren dit minimaal maandelijks (te laten) doen. Secura kan deze scans voor u uitvoeren, waarbij wij alle false-positives (onjuist geïdentificeerde zwakheden) zullen verwijderen door deze handmatig te valideren. U krijgt alleen de relevante zwakheden gerapporteerd. Deze scans voeren wij op de productie-omgeving uit. Zo hebben u, en de auditor, een correct beeld van de omgeving en zal de opvolging van eventuele kwetsbaarheden effectiever kunnen zijn.

Daarnaast dient u minimaal jaarlijks, en na elke grote wijziging in de applicatie, een penetratietest uit te voeren op de applicatie (webapplicatietest). Secura voert dit type onderzoek veelvuldig uit op basis van de meest actuele kennis over bedreigingen voor webapplicaties. Deze tests voeren wij uit in de test-/acceptatieomgeving, omdat er geen DigiD test-accounts zijn in de productieomgeving.

De test is een onderzoek naar de beveiliging van de web applicatie(s) zoals maatregelen rond de gebruikersinvoer, het inloggen en uitloggen, de autorisaties en veel andere aspecten. Over deze test ontvangt u een rapport met bevindingen, risico-inschattingen en aanbevelingen. Tevens nemen wij een specifiek DigiD-hoofdstuk op, waarin alle relevante bevindingen voor de auditor duidelijk worden toegelicht. Bij tekortkomingen spreken wij met u, rekening houdend met een herstelperiode, een heronderzoek af.
Dan bent u, voor de relevante Logius normen, klaar voor de volgende stap: de audit. Voor meer informatie over onze kwetsbaarhedenonderzoeken en penetratietests verwijzen wij naar onze brochure inzake deze diensten.

Voor de overige normen adviseren wij u een DigiD Pré-Audit waarin wij samen met u naar de, bij u aanwezige, maatregelen kijken. Het onderzoek is kort en nog niet gericht op het geven van ‘assurance’ (zekerheid) maar geeft u inzicht in eventuele tekortkomingen. Het is daarmee een goede voorbereiding op de uiteindelijke audit voor.

Een Register EDP-Auditor (RE) leidt de uiteindelijke (assurance) audit die volgens de eisen van de Richtlijn 3000 plaatsvindt. Hij maakt daarbij veel gebruik van de uitkomsten van de penetratietests en de kwetsbaarhedenscan rapportages. Het rapport kunt u (zonder de bijlage met de detailbevindingen) verstrekken aan Logius waarmee u aan de auditplicht hebt voldaan.

Omdat Secura alle onderdelen uit dit auditproces in onderlinge samenhang kan uitvoeren, kunnen wij zeer efficiënt werken. De auditor en de penetratietesters staan dagelijks met elkaar in contact en kunnen ervoor zorgen dat bevindingen snel opgelost kunnen worden en dat u niet voor verrassingen komt te staan.

INTERESSE?
Wilt u meer over onze diensten weten?
Neem contact met ons op.

Volg ons op

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)40 23 77 990
E info@secura.com
W www.secura.com