DIGID ASSESSMENT

Met bijna 14 miljoen "Digitale Identiteiten" is DigiD relevant en veel gebruikt voor de identificatie en authenticatie van gebruikers van webapplicaties van de overheid, de zorg maar ook steeds meer andere organisaties. Voor het garanderen van de veiligheid van DigiD neemt de overheid veel maatregelen maar stelt zij ook eisen waaronder de jaarlijkse controle door een RE (Register EDP-Auditor). Secura heeft audit teams met inhoudelijke kennis en ervaring die onder leiding van RE's uw DigiD Assessments kunnen uitvoeren. Met de brede dienstverlening van Secura op digital security zijn alle benodigde auditwerkzaamheden en de technische testen op de webapplicaties die gebruik maken van DigiD in één hand.

IN CONTROLE MET 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 (in de assessment verplichte) technische testen op de webapplicaties die gebruik maken van DigiD;
- De periodieke kwetsbaarhedenscans op de DigiD infrastructuur;
- De periodieke testen op de, met DigiD ontsloten, webapplicaties;
- Een TPM DigiD assessment voor derden partijen die zijn betrokken in de dienstverlening rond de webapplicatie die gebruik maakt van DigiD;
- Pré-Audit DigiD om u optimaal voor te bereiden op de formele DigiD Assessment.

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 en beperkt u het risico op tekortkomingen die naar voren kunnen komen bij de formele DigiD assessment. Uw RE is daarbij het ideale klankbord voor vragen over de uitleg van de DigiD normen.

OVERZICHT VAN HET DIGID ASSESSMENT PROCES

Na de officiële opdrachtbevestiging overleggen wij met u in de voorbereidingsfase over de planning en ontvangt u een overzicht van benodigde stukken. In een kick-off geven wij verder toelichting op de normen, het audit proces en de specifieke aandachtspunten.

Hierna start de uitvoering van het onderzoek met o.a. interviews, analyse van documenten, waarneming ter plaatse, webapplicatietesten en onderzoek van systeeminstellingen. De bevindingen leggen wij vast in een conceptrapport dat al conform de standaard van Logius is. Dit conceptrapport met bevindingen stemmen wij met u af. Na ontvangst van uw bevestigingsbrief over de juistheid en compleetheid van dit conceptrapport, brengen wij het definitieve assessment rapport uit. Een meegeleverde verkorte versie (exclusief bijlagen A en B) kunt u, conform de regels van Logius, met Logius delen. Het DigiD assessment sluiten wij af met een evaluatie waarin wij ook met u vooruitkijken naar de volgende assessment en daarvoor verwachte of al bekende veranderingen in de eisen.

BESCHRIJVING VAN DE DIENSTEN

DigiD Assessment

Het Logius normenkader (huidige 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. De Handreiking voor DigiD assessments van de NOREA bevat veel uitleg en bevat aanvullende eisen en aandachtspunten die de RE als uitgangspunt moet hanteren bij het DigiD assessment. Het DigiD Assessment verrichten wij conform de gestelde eisen en de verplicht te hanteren Richtlijn 3000 van de NOREA voor het uitvoeren van Assurance onderzoeken.

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.

Kwetsbaarhedenscan

Hierbij 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.

DigiD Pentest

Het DigiD normenkader vereist dat de aansluithouder minimaal jaarlijks, en na elke grote wijziging in de applicatie, een penetratietest uitvoert op de applicatie (webapplicatietest). Secura voert dit type onderzoek veelvuldig uit op basis van de meest actuele kennis over bedreigingen voor webapplicaties. Naast de diepgaande penetratietest is het ook mogelijk een beperkte penetratietest te laten uitvoeren die enkel ingaat op de gestelde eisen in het Logius normenkader. De test van maatregelen in de webapplicatie rond de gebruikersinvoer, het inloggen en uitloggen, de autorisaties en veel andere aspecten voeren wij uit in een test-acceptatie omgeving waarin demo DigiD accounts beschikbaar zijn. De andere testen voeren wij conform de handreiking van de NOREA uit op de productie omgeving. Over deze testen 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. Voor meer informatie over onze kwetsbaarhedenonderzoeken en penetratietests verwijzen wij naar onze brochure inzake deze diensten.

DigiD Pré-Audit

In een DigiD Pré-Audit kijken wij samen met u naar de, bij u aanwezige, maatregelen. 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.

TPM DigiD Assessment

Dit is een DigiD Assessment op de normen die van toepassing zijn bij de door de betrokken ICT dienstenleverancier. Zo’n TPM kan de ICT dienstenleverancier, die bij meer DigiD Assessments is betrokken, aanzienlijke kostenbesparingen opleveren en de auditinspanningen beperken. Voor de aansluithouders zal de auditinspanning ook afnemen en daardoor minder budget vergen.

Het is de focus van Secura de aansluithouder zo optimaal mogelijk voor te bereiden en het DigiD assessment soepel te laten verlopen. Naast het fungeren als klankbord volgen wij de ontwikkelingen nauwgezet en organiseren minimaal één keer per jaar een goed bezocht webinar waarin wij iedereen informeren over waarin wij iedereen informeren ter voorbereiding op het verplichte DigiD-assessment. Voor ons laatste DigiD webinar zie: https://www.secura.com/nl/webinars.

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

Volg ons op

Vestdijk 59
5611 CA Eindhoven

Karspeldreef 8
1101 CJ Amsterdam

T 088 888 31 00
E info@secura.com
W secura.com