DigiD beveiligingsassessment

Wat is een DigiD beveiligingsassessment?

Een DigiD ICT-beveiligingsassessment is een controle van de betrouwbaarheid van een webapplicatie. Deze controle is gericht op het volledige stelsel van maatregelen en procedures. Zowel de geautomatiseerde als niet geautomatiseerde.
Via DigiD kunnen burgers via een beveiligde verbinding toegang tot uw digitale loket krijgen. Deze beveiligde toegang moet veilig en betrouwbaar zijn. Het assessment toetst of uw webapplicatie, webinfrastructuur en uw procedures en governance aan de eisen voldoen. Alle DigiD-gebruikende organisaties moeten voor 1 mei een ICT-beveiligingsassessment laten uitvoeren en daarna jaarlijks herhalen. Logius is de organisatie die bepaalt wat verplicht gesteld wordt.

U heeft de vrijheid om het assessment te laten uitvoeren op alle maatregelen en procedures van de norm of alleen op de verplicht gestelde beveiligingsrichtlijnen. Onderzoek toont aan dat onze klanten eigenlijk altijd voor de laatste optie kiezen.

Wat kunnen wij u bieden?

Wij testen uw digitale loket op veiligheid en voeren de risicoanalyses volgens het protocol voor u uit. Zo weet u zich verzekerd dat u aan de norm van Logius voldoet.
Wij zijn gespecialiseerd in het afnemen van assessments. BKBO werkt exclusief samen met Nováccent. Afhankelijk van uw vraag, zetten wij zogenaamde pentesters van Nováccent in. Dit zijn gecertificeerde medewerkers die de penetratie testen uitvoeren. Ze proberen net als een hacker in uw webomgeving binnen te dringen. Zij herkennen snel de kwetsbaarheden in webapplicaties, systeemkoppelingen en de infrastructuur en leggen deze bloot. Door onze bewezen ervaring werken wij bij meer dan 80 organisaties.

Uit de automatische scans blijkt meestal dat verdergaand handmatig onderzoek nodig is. Wij doet dat eveneens voor u. Zonder meerprijs. We kunnen u nóg meer zekerheid geven wanneer wij het assessment jaarlijks herhalen. Voor uw gemak bieden wij daarvoor een abonnement aan. Wij garanderen dat u probleemloos en effectief aan alle eisen voldoet.

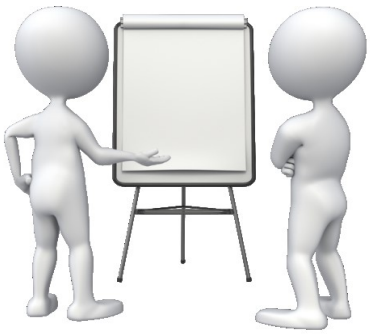
Wat is uw voordeel?

Wij ontzorgen u. Het voorbereiden en uitvoeren van het beveiligingsassessment vraagt de nodige expertise en capaciteit. Wij zijn daarvoor uw betrouwbare partner.

Wij ondersteunen u met een aanpak die zowel tijd als kosten bespaart. Wij zijn zeker van onze zaak en bieden u een vaste prijs. Dat is voordelig en compleet want het is inclusief eventuele hertests dan wel heraudits. Wij bieden leveranciers de mogelijkheid om een TPM-verklaring te verkrijgen. Met een Third Party Memo bespaart u op de auditkosten omdat een penetratietest dan niet bij elke klant die dezelfde webapplicatie of webomgeving gebruikt, hoeft te gebeuren.

DigiD beveiligingsassessment

Hoe pakken wij dat aan?



Wij hebben een gestandaardiseerde en beproefde uitvoeringswijze ontwikkeld. U bepaalt met een zelfonderzoek moeiteloos wat uw situatie is. Dit begint met een vragenlijst. Hierdoor brengt u eenvoudig uw situatie overzichtelijk in kaart. Afhankelijk van uw opdracht zal onze auditor bij u ter plaatse een complete quick scan uitvoeren. Daarna bespreken wij de auditplanning met u. Hierbij geven wij aan welke TPM- verklaringen geldig zijn, welke testen gedaan moeten worden en op welke termijn dat mogelijk is. Wanneer alles duidelijk is voor u, worden afhankelijk van een eventuele TPM, de penetratietesten uitgevoerd. Als eerste testen wij of het mogelijk is om ongeautoriseerd toegang via het digitale loket te krijgen. Vervolgens probeert de pentester ongeautoriseerd toegang te krijgen tot de achterliggende systemen. Afhankelijk van een eventuele TPM, beoordelen wij zowel de interne als externe infrastructuur. Gelijktijdig vindt door de Register EDP-auditor een audit plaats op uw contracten, procedures en de beveiligingsorganisatie. Ingeval van een SAAS oplossing voorzien van een geldige TPM beperkt het onderzoek zich daartoe. Wij zorgen dat voor u alles compleet, geordend en begrijpelijk is.

We leggen onze bevindingen vast in een overzichtelijke conceptrapportage. We doen concrete aanbevelingen om de tekortkomingen efficiënt op te heffen. Het assessment wordt afgesloten met een persoonlijk gesprek waarin we de bevindingen en onze aanbevelingen helder toelichten. Dat gesprek kan ook telefonisch. Daarna wordt de rapportage definitief gemaakt. Wanneer de opdracht ook een penetratie- en of vulnerabilitytest omvat, vragen wij u vooraf om een vrijwaringsverklaring.

Wat is uw investering?

Afhankelijk van wat u wilt dat onderzocht wordt, variëren de kosten tussen de € 2.250,- en € 9.500,-. Dit betreft één DigiD aansluiting. De genoemde prijzen zijn exclusief BTW en inclusief reis- en verblijfskosten.

Dit assessment is ook voordelig te combineren met andere audits. Ook is een twee of drie jarig abonnement met korting mogelijk. Zo bent u verzekerd dat u aan alle eisen blijft voldoen: probleemloos, efficiënt en effectief!

Geen gekibbel garantie

Onze garantie is uniek in de branche! Wij garanderen u een vaste prijs. De prijs is dus inclusief een eventuele hertest, heraudit nadat u verbetermaatregelen heeft kunnen doorvoeren. Door onze bewezen aanpak durven wij hiervoor in te staan. Wij noemen dat onze "geen gekibbel garantie".

Wilt u meer weten?

Wij staan voor u klaar en gaan graag met u in gesprek. U kunt direct bellen met BKBO op telefoonnummer: 073 – 211 03 37. Is het voor u meteen helemaal duidelijk? Dan kunt u ook meteen een offerte aanvragen via info@bkbo.nl

Van deze tekst staat een uitgebreidere versie op https://bkbo.nl/producten/digid-assessment