DigiD Audit uitvoeren

De DigiD norm is gebaseerd op de normen zoals die door het Nationaal Cybersecurity Center (NCSC) zijn geformuleerd voor web applicaties. De norm voor de DigiD audit bestaat uit de richtlijnen met de hoogste impact op de veiligheid van DigiD. Logius adviseert alle organisaties om buiten de maatregelen uit de norm ook de andere maatregelen uit de ICT-beveiligingsrichtlijnen voor web applicaties te adopteren.

12secure-u hanteert het volgende stappenplan

Stap 1 Zelf toetsen aan de hand van de richtlijnen Door het uitvoeren van een interne beoordeling en vast te stellen in hoeverre de systemen aan de norm voldoen, krijgt u inzicht in maatregelen die in ieder geval moeten worden getroffen. 12secure-u kan u hierbij ondersteunen door het uitvoeren van een pre-audit.

Stap 2 Verbetermaatregelen implementeren Op basis van de zelftoets of de pré-audit heeft u zicht op de zaken die nog moeten worden geïmplementeerd. In deze stap dient u de nood- zakelijke maatregelen in te voeren.

Stap 3 Uitvoeren van een security scan en een penetratietest Uitvoeren van een security scan (gericht op de interne ICT-omgeving) en een penetratietest (ook wel 'ethical hacking test') uitvoeren op uw systemen. 12secure-u kan dit voor u organiseren. Mocht u dit al hebben uitgevoerd dan beoordelen wij het pentestrapport met bevindingen om vast te stellen of wordt voldaan aan de eisen uit het normenkader.

Stap 4 Bevindingen oplossen De uitkomsten van zowel de security scan als de penetratietest kunnen aanleiding zijn om verbeteringen door te voeren. Deze verbeteringen kunnen betrekking hebben op de interne organisatie maar moge- lijk ook bij de externe leverancier (bij gebruik van oplossingen)

Stap 5 Audit uitvoeren Als alle voorgaande activiteiten zijn afgerond wordt het feitelijke ICT-be- veiligingsassessment uitgevoerd. Dit dient te gebeuren door een Register EDP-auditor (RE). 12secure-u beschikt over RE's en kan de audit voor u uitvoeren.

Stap 6 Bevindingen naar Logius sturen De rapportage over het uitgevoerde ICT beveiligingsassessment DigiD dient verstuurd te worden naar Logius. De rapportage bevat een overzicht van de feitelijke bevindingen per maatregel. Per maatregel wordt aangegeven of deze voldoet: Ja, Nee of Niet van Toepassing.

2 dagen voor de zogenaamde governance normen, 2 dagen voor de applicatienormen, 2 dagen voor de hostingsnormen. Hierin zit ook een pentest van de omgeving (applicatie en DMZ) opgenomen. Qua indicatie ben je ongeveer 6,5k-8k kwijt (afhankelijk van hoe groot de applicatie is gezien de pentest).