

Verklaring 'Gereed voor ICT-Beveiligingsassessment DigiD'

Verklaring met betrekking tot het gereed zijn voor
het ICT-Beveiligingsassessment DigiD 2015

Ondergetekende

Naam :Maarten van der Hoek

Leverancier :Excellence

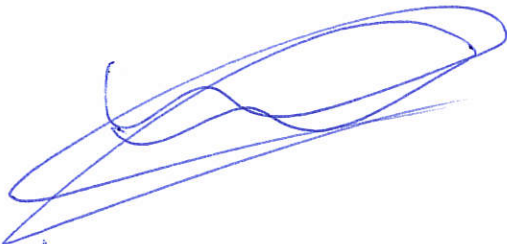
Verklaart hierbij:

- a. gereed te zijn voor het ICT-Beveiligingsassessment DigiD voor het jaar 2015, als het gaat om de normen waarvoor de leverancier verantwoordelijk is. Dit betreft de volgende normen:
- B0-5: Alle wijzigingen worden altijd eerst getest voordat deze in productie worden genomen en worden via wijzigingsbeheer doorgevoerd.
 - B0-6: Maak gebruik van een hardeningsproces, zodat alle ICTcomponenten zijn gehard tegen aanvallen.
 - B0-7: De laatste (beveiligings)patches zijn geïnstalleerd en deze worden volgens een patchmanagement proces doorgevoerd.
 - B0-8: Penetratietests worden periodiek uitgevoerd.
 - B0-9: Vulnerability assessments (security scans) worden periodiek uitgevoerd.
 - B0-12: Ontwerp en richt maatregelen in met betrekking tot toegangsbeveiliging/toegangsbeheer.
 - B0-13: Niet (meer) gebruikte websites en/of informatie moet worden verwijderd.
 - B0-14: Leg afspraken met leveranciers vast in een overeenkomst
 - B1-1: Er moet gebruik worden gemaakt van een Demilitarised Zone (DMZ), waarbij compartimentering wordt toegepast en de verkeersstromen tussen deze compartimenten wordt beperkt tot alleen de hoogst noodzakelijke.
 - B1-2: Beheer- en productieverkeer zijn van elkaar gescheiden.
 - B1-3: Netwerktogang tot de webapplicaties is voor alle gebruikersgroepen op een zelfde wijze ingeregeld.
 - B2-1: Maak gebruik van veilige beheermechanismen.
 - B3-1: De webapplicatie valideert de inhoud van een HTTP-request voor die wordt gebruikt.
 - B3-2: De webapplicatie controleert voor elk HTTP verzoek of de initiator geauthenticeerd is en de juiste autorisaties heeft.
 - B3-3: De webapplicatie normaliseert invoerdata voor validatie.
 - B3-4: De webapplicatie codeert dynamische onderdelen in de uitvoer.
 - B3-5: Voor het raadplegen en/of wijzigen van gegevens in de database gebruikt de webapplicatie alleen geparametriseerde queries.
 - B3-6: De webapplicatie valideert alle invoer, gegevens die aan de webapplicatie worden aangeboden, aan de serverzijde.
 - B3-7: De webapplicatie staat geen dynamische file includes toe of beperkt de keuze mogelijkheid (whitelisting).

- B3-15: Een (geautomatiseerde) blackbox scan wordt periodiek uitgevoerd.
- B3-16: Zet de cookie attributen 'HttpOnly' en 'Secure'.
- B5-1: Voer sleutelbeheer in waarbij minimaal gegarandeerd wordt dat sleutels niet onversleuteld op de servers te vinden zijn.
- B5-2: Maak gebruik van versleutelde (HTTPS) verbindingen.
- B5-3: Sla gevoelige gegevens versleuteld of gehashed op1.
- B5-4: Versleutel cookies.
- B7-1: Maak gebruik van Intrusion Detection Systemen (IDS).
- B7-8: Voer actief controles uit op logging.
- B7-9: Governance, organisatie, rollen en bevoegdheden inzake preventie, detectie en response inzake informatiebeveiliging dienen adequaat te zijn vastgesteld.

b. dat de gemeentelijke klanten per 2015 een Third Party Mededeling (TPM) kunnen afnemen, als betaalde extra dienstverlening.

Hengelo, 25 januari 2016,

A handwritten signature in blue ink, consisting of several overlapping loops and a long horizontal stroke at the bottom.

W. van der Hoeck