

Bijlage 3 Verbeterplannen op hoofdlijnen

VERTROUWELIJK

Suwinet:

De acht openstaande bevindingen op het gebied van Suwi normen zijn:

1. Onvolledige beschrijving van de taken, verantwoordelijkheden en functiescheiding
Oplossingsrichting: De beschrijving van de taken, verantwoordelijkheden en functiescheiding wordt conform de richtlijnen van de norm opgesteld en gecommuniceerd.
2. Te weinig control op de rechtmatigheid van activiteiten door medewerkers in Suwi.
Oplossingsrichting: Een proces inrichten dat leidinggevenden in staat stelt actie te ondernemen op onregelmatigheden bij gebruik van Suwi.
3. Te weinig controle op anonieme accounts en de vertrouwelijkheid van gebruikte wachtwoorden.
Oplossingsrichting: Uitfaseren onnodige anonieme accounts en aanpassen van wachtwoorden.
4. De instellingen van [REDACTED].
Oplossingsrichting: [REDACTED] onderzoeken van de mogelijkheid tot uitfaseren of het accepteren van het risico.
5. Te weinig controle over wie geautoriseerd is.
Oplossingsrichting: Het proces verbeteren dat leidinggevenden middels periodieke overzichten van geautoriseerden in staat stelt oog te houden op wie er toegang heeft.
6. Er is [REDACTED] aanwezig.
Oplossingsrichting: Instellen van de juiste logging en opmaken van de bijbehorende rapportages, zodat evaluatie mogelijk is.
7. Te weinig evaluatie van rapportages en de daarbij behorende verbeteracties.
Oplossingsrichting: Er worden rapportages opgemaakt en waar afhankelijkheid is van leveranciers worden afspraken gemaakt om de juiste rapportages aan te leveren, zodat de controle binnen het cluster kan worden ingericht.
8. Er is onvoldoende aandacht voor het beveiligingsbewustzijn van medewerkers.
Oplossingsrichting: Door middel van awareness zorgen dat medewerkers op de hoogte zijn van het juiste veilige gedrag bij het gebruik van de applicatie.

DigiD

De vier openstaande bevindingen op het gebied van DigiD normen zijn:

1. Er is onvoldoende controle op mogelijke invoer op de website, met het risico op het uitvoeren van hackopdrachten binnen de website.
Oplossingsrichting: Meer controle op het plaatsen van mogelijk kwaadaardige bestanden door kwetsbare onderdelen te migreren naar een veiliger platform.
2. De standaardinstellingen van [REDACTED].
Oplossingsrichting: De missende beveiligingsinstellingen worden alsnog ingesteld.
3. De omgang met [REDACTED] is onvoldoende beschreven en bekend.
Oplossingsrichting: De procedure voor de omgang met [REDACTED] wordt conform de richtlijnen van de norm opgesteld en gecommuniceerd.
4. Er draait verouderde software op de [REDACTED].
Oplossingsrichting: Onderzoeken van de specifieke verouderde software en zorgen dat alle software binnen de scope van DigiD ook daadwerkelijk beheerst wordt.