Update SGBO-IV GAL

5.1.2.e

14-10-24

« waakzaam en dienstbaar »

Opdracht SGBO-IV GAL

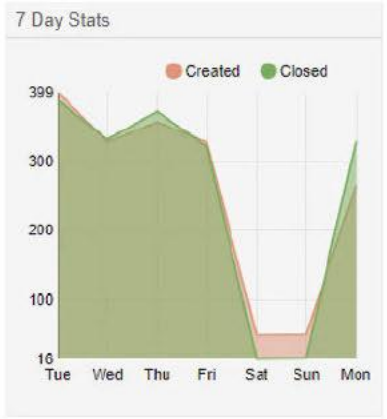
In de opdrachtbeschrijving voor het NSGBO staat het volgende:

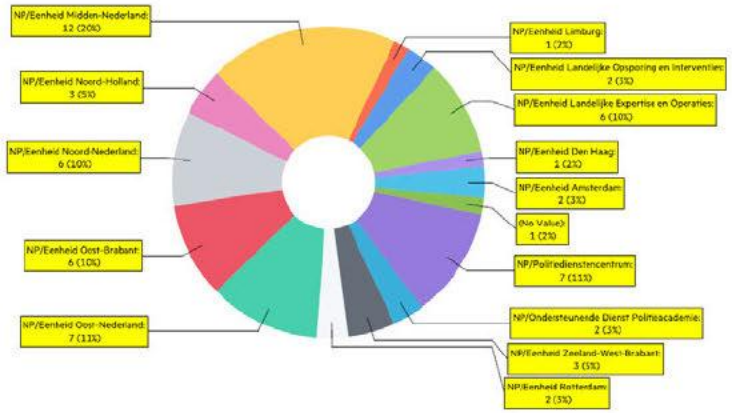
SGBO IV zal de aanbevelingen vanuit de 5.1.1.b,5.1.2.c,5.1.2.i opvolgen en de 3e partij begeleiden die een second opinion op het forensisch onderzoek zal uitvoeren & de getroffen maatregelen zal valideren.

+ ondersteuning NSGBO/ SGBO-PDC

De aanbevelingen zijn uitgewerkt door het SGBO-IV in adviezen welke zijn goedgekeurd door de KL.

Huidige situatie





- Aantal Phishingmail meldingen
- Vandaag 265

- Afgelopen 72 uur 56 meldingen bij het loket

Maatregel 1

Geadviseerde maatregel #1 -5.1.1.b,5.1.2.c,5.1.2.i

Advies vanuit IV

De voorgestelde maatregelen worden omarmd. Dit advies wordt overgenomen omdat dit conform vigerend beleid is. Een nadere analyse is nodig als het gaat om de voorbereiding voor het verder aanscherpen van maatregelen binnen dit beleid. Oplevering van dit plan in 2 weken.

Status maatregel:

- 5.1.1.b,5.1.2.c,5.1.2.i
- De inventarisatie van 5.1.1.b,5.1.2.c,5.1.2.i zijn is afgerond. Onderscheid is gemaakt tussen Hoog, Laag, Midden risico. Op basis daarvan worden vervolg stappen in gang gezet.
- Huidige inzicht 5.1.1.b,5.1.2.c,5.1.2.i : Vraagt om aanpassingen of risico acceptatie van systeemeigenaren. Systeemeigenaren zijn cq worden hier over benaderd
  - 5.1.1.b,5.1.2.c,5.1.2.i
  - 5.1.1.b,5.1.2.c,5.1.2.i 5.1.1.b,5.1.2.c,5.1.2.i
- 5.1.1.b,5.1.2.c,5.1.2.i

Maatregel 2

Geadviseerde maatregel #2 - 5.1.1.b,5.1.2.c,5.1.2.i

Advies vanuit IV

Analyse 5.1.1.b,5.1.2.c,5.1.2.i Een analyse wordt uitgevoerd of hier onvoorziene neveneffecten kunnen zijn voor de operatie. Oplevering van de analyse binnen een periode van 5 weken.

Status maatregel:

- Opdracht omschrijving scherp gesteld. Nog nader verifiëren vanuit de techniek
- PVA is gereed. Op basis van het PvA impact voor business bepalen mbt effect bij activeren.
- Gezien overige openstaande activiteiten heeft deze tav de Politie omgeving een lagere prioriteit gekregen.
- LMS heeft een eerste quickscan opgeleverd.

Maatregel 3

5.1.1.b,5.1.2.c,5.1.2.i

Advies vanuit IV

Het 5.1.1.b,5.1.2.c,5.1.2.i echter het belang wordt gezien om dit beleid aan te scherpen. Dit wordt via de lijn CISO en dienst IV opgepakt.

Status maatregel

- Aanscherping van het beleid gevraagd aan CISO/ Sector IB. Beleid ontvangen. Op basis hiervan zal een impact analyse worden opgesteld tav de technische uitvoerbaarheid.
- 5.1.1.b,5.1.2.c,5.1.2.i
- 5.1.1.b,5.1.2.c,5.1.2.i Hiermee voldoen we daar aan de geadviseerde maatregel.
- Nog uitlopen welke overige domeinen deze instelling moeten krijgen. Overzicht van alle domeinen wordt opgevraagd, 5.1.1.b, 5.1.2.c, 5.1.2.i om goed te checken welke nog open staan.

Maatregel 4

Geadviseerde maatregel #4 – 5.1.1.b,5.1.2.c,5.1.2.i

Advies vanuit IV

Het SOC van de Politie volgt reeds alle geadviseerde maatregelen op.

Status maatregel

- Vanuit onderzoek 5.1.1.b,5.1.2.c,5.1.2.i ontbreekt is besloten om deze omgevingen nog extra te monitoren en terug te kijken in de logging
- Voor een aantal systemen/omgevingen is reeds logging opgeleverd voor nader onderzoek

Maatregel 5

Extra maatregel #5 – 5.1.1.b,5.1.2.c,5.1.2.i tref maatregelen

Status maatregel

- 5.1.1.b,5.1.2.c,5.1.2.i
- 5.1.1.b,5.1.2.c,5.1.2.i
- Alle informatie is aangeleverd. 5.1.1.b,5.1.2.c,5.1.2.i
- Verdere uitwerking van de maatregelen vraagt om een projectmatige aanpak buiten het SGBO-IV

Second opinion

Opdracht: begeleiden van de 3e partij die een second opinion op het forensisch onderzoek zal uitvoeren & de getroffen maatregelen zal valideren.

Opdracht 3e partij:

- Toetsen bevindingen SOC
- Aanbevelingen geven op de gestelde maatregelen

Status:

- Eerste rapport opgeleverd via het SOC. Wordt nader beoordeeld door techniek.
- Onderzoek loopt nog verder door
- Eerste bevindingen op de maatregelen hebben geen nieuwe inzichten opgeleverd

Overige maatregelen

Opdracht: Tref of versnel andere relevante security maatregelen

Status:

- Inventarisatie loopt
- 5.1.1.b,5.1.2.c,5.1.2.i .
- De toegang tot diverse portals is dichtgezet.
- Phishing knop binnen Politie en PA volledig aangezet.
- Phishing knop LMS is in voorbereiding. Wordt volgende week woensdag geïmplementeerd.
- Aangifte is namens 5.1.2.e gedaan
- Medewerkers waarvoor dit van toepassing is worden van een 5.1.1.b,5.1.2.c,5.1.2.i

Openstaande vragen

Vragen:

- Opdracht van NSGBO om het visitekaartje terug te brengen tot minimale vulling
  - *HICTT brengt15-10 een memo in het SGBO-IV voor een stappenplan*