TLP:AMBER

Tim Abang
verslag week 49

TLP:AMBER

Over dit document

Dit document

Dit document is opgesteld door Tim Abang. Wij zijn het beveiligingsafdeling van het Programma Realisatie Digitale Ondersteuning COVID-19 bij de Directie Informatiebeleid van het Ministerie van Volksgezondheid, Welzijn en Sport.

Tim Abang is continu op zoek naar dreigingen en kwetsbaarheden om oplossingen te vinden voordat ze een probleem worden. Daarom helpen we met het bewaken van de omgevingen, uitvoeren van testen, het maken van allerhande risico-inschattingen, voeren dreigingsanalyses uit, onderzoeken, toetsen in de praktijk en bewaken de systemen om aanvallen te onderkennen. We delen informatie en oplossingen waar het maar verantwoord kan om de veiligheid te dienen.

Waar oplossingen nog niet bestaan bouwen wij deze, zoals de Kwetsbaarheden Analyse Tool. Bij beveiligingsincidenten doen wij de opvolging, forensisch onderzoek en voeren root cause-onderzoeken uit met het doel herhaling te voorkomen en problemen in de kiem te smoren. We delen kennis met een simpele missie: onze gezamenlijke digitale veiligheid te vergroten. (Hulp)vragen, tips, observaties of opmerkingen? 5.1.2e Ordobeheer.nl

Rubricering: Traffic Light Protocol

In de informatiebeveiliging wordt gewerkt met het Traffic Light Protocol (TLP). Dit zijn internationale uniforme afspraak aan de hand van de kleuren van het verkeerslicht. Het geeft aan hoe vertrouwelijk informatie is en of deze gedeeld mag worden met andere personen of organisaties.

• TLP:RED. Deze informatie heeft de hoogste vertrouwelijkheid. Deze mag niet met andere personen of organisaties worden gedeeld. Vaak zal deze informatie mondeling worden doorgegeven. In veel gevallen ook niet via e-mail of op papier, maar het kan natuurlijk wel.

TLP:AMBER. Deze informatie mag alleen binnen de eigen organisatie worden gedeeld met mensen voor wie toegang noodzakelijk is. Dit is op een 'need to know'-basis binnen de eigen organisatie.

• TLP:GREEN. Deze informatie is beschikbaar voor iedereen binnen de gemeenschap, waarop ze gericht is. Dat betekent dat het nuttig kan zijn en daarmee gedeeld kan worden op basis van 'nice to know'. Er is geen restrictie tot de eigen organisatie.

• TLP:WHITE. Deze informatie is niet vertrouwelijk en kan openbaar worden gedeeld.

Dit document is gerubriceerd als TLP:AMBER.

Inhoudsopgave

Over dit document....2
Dit document....2
Rubricering: Traffic Light Protocol....2
Week rapportage 5 t/m 11 december....4
Hoofdpunten week....4
CSPO Office....4
Blue Team....4
Red Team....5
Q&A....5
KAT....6
Geïdentificeerde risico's en kwetsbaarheden....6

TLP:AMBER

Week rapportage 5 t/m 11 december

Hoofdpunten week

Hier worden de belangrijkste lopen en uitgevoerde zaken van Tim Abang opgesomd.

Algemeen beeld

Er is een relevant lek in Log4j, een onderdeel van de software van de Apache Foundation, aangetroffen. Door dit lek zijn diverse andere producten getroffen. Voor RDO blijft de impact beperkt tot Zammad, de helpdesktool en Calvin (de monitoringtool van KAT). Het lek werd op vrijdag 11 december 2021 bekend en de risico's zijn dezelfde dag gemitigeerd.

CSPO Office

- Jurist gezocht en gevonden voor Tim Abang/KAT
- Profiel security liaisons naar projecten is uitgewerkt
- Er is organisatie rond de helpdesk opgezet.
- Analyse op spoedtest.nl-rapportage van het forensisch onderzoekbureau worden afgerond.
- Wordt aangestuurd op de gezamenlijke wens van RDO Beheer en Tim Abang om de functiescheiding te realiseren per 1 januari.
- Rapportage onderzoeksbureau is binnen en geanalyseerd voor de Tim Abang rapportage.
- Er loopt een risico-inschatting voor de Kort Verblijf Derde Landen. De Ministeriële Regeling is geanalyseerd.
- Ondersteuning bij GGD Contact voor versnelling ontwikkeling.
- Er loopt contact met 5.1.2e voor oplossen dataproblemen.
- Er wordt gewerkt aan inlog met DigiD voor BRBA.
- Er is uitleg geschreven over risico-overwegingen met betrekking tot het vervangen UZI-pas door DigiD-login.
- Stelselbewaking testaanbieders loopt. Er is een testaanbieder met complianceproblemen aangetroffen. Hierop wordt geacteerd.
- Van opsporingspartner het signaal gekregen dat het lijkt dat de intensiteit van fraude iets lijkt af te nemen. Belangrijkste oorzaak volgens hun vermoeden is de toch wel grote pakkans.

Blue Team

- Opbouw SOC wordt uitgewerkt. Basis rolverdeling en taakomschrijving staan. Eerste profielen zijn aangemaakt. Rol in incidentmanagementproces beschreven.
- Er is een lopende discussie over rechtenbeheer. Voor github is er weerstand vanuit CoronaCheck, omdat zij dit zelf willen doen. Het ontbreekt echter aan documentatie, procedurele borging en het voldoen aan standaarden, zoals de BIO.
- Er is een risicoinschatting op begeleid zelftesten uitgevoerd (FMEA).
- Proces QR-codes blokkeren opnieuw aangepast aan huidige situatie en loopt.
- Komende week worden alle projecten – voor zover mogelijk qua medewerking – aangesloten op de KAT-monitoring.
- Overleg met RDO Beheer: er komt toevoeging van objecten buiten VWS op beschikbaarheid en certificaten. Middel wordt Nagios. Nagios wordt aangesloten op KAT.

Red Team

- Security Codereviewer is toegevoegd aan het team.
- Pentest CoronaCheck is afgerond.
- Eerste versie pentest Curacao Health App afgerond. Ontwikkelaars krijgen nu de kans verbeteringen door te voeren.
- Er is lopend overleg met IGJ, OM om toch detectie te kunnen uitvoeren op eigen systemen.
- Risico's (breed) voor touristenroute geïnventariseerd en samengevat.
- Er is een sourcecode analyse gaande over de rogue scanner app.
- Er loopt een onderzoek op verzoek van de BVA

Q&A

- Change Management proces wordt beschreven.
- Incident rapportage Spoedtest.nl wordt gefinaliseerd. Foutmodi worden op basis hiervan gedestileerd.
- Profiel voor kwaliteitsreviewer wordt gemaakt. Doel hierbij is kwaliteit van de broncode borgen waar Software Improvement Group tekort schiet.
- Contractverlening voor de Software Improvement Group aanstaande.
- De Algemene Rekenkamer heeft vragen gesteld over rechtenbeheer bij CoronaCheck. Deze waren al aangekondigd in het eerste werkbezoek, waarbij toen is aangekondigd dat er vooral interesse was in het omgaan met accounts op Github.

- Gesprek met Algemene Rekenkamer over monitoring van testaanbieders.
- Er loopt een uitvraag welke QA-testers er momenteel lopen.
- Er wordt inhuur van testers geregeld voor in eerste instantie GGD Contact.
- Er is een auditor gevonden die over de projecten kan meekijken en aan KAT kan toevoegen om deze werkzaamheden in het ISMS van KAT te gaan borgen.

KAT

- Analistenrol voor KAT is uitgezet. Dit traject met de inhuurdesk verloopt moeizaam.
- Er zijn frontenders gevonden en een backender voor de opschaling naar SOC-monitoring.
- DPIA is in de afrondende fase.
- Er is een communitymanager gevonden en komende week wordt de uitvraag gedaan.
- Aanmeldingen via website openkat.nl hebben geleid tot het plannen van een afspraak. Er is een plan om bijdrage meteen concreet te maken.
- Opschaling naar alle RDO-projecten voor KAT.
- Er hebben upgrades aan de VM's van KAT plaatsgevonden.
- Nieuwe functionaliteit KAT naar productie:
  - Bevindingen die niet meer aangetroffen zijn, worden automatisch verwijderd. Daarmee is het beeld reëler. Dit was een technisch ingewikkeld probleem om te realiseren. Voor het SOC is dit belangrijk, omdat een alarm dat optreedt ook automatisch kan verdwijnen.
  - Nieuwe boefjes zijn verbeterd.
  - Shortcuts voor livegang zijn allemaal inmiddels vervangen met de coderewrite.

Monitoring testaanbieders

Er worden deze week 29 testaanbieders gemonitord door de Kwetsbaarheden Analyse Tool (KAT). Van deze aanbieders zijn er zeven die niet gebruik maken van de infrastructuur van Stichting Open Nederland. Deze afgelopen week heeft opvolging gevonden op meerdere ernstige lekken:

Kritiek

- Een gevonden kwetsbaarheid in Elementor 2.7.4

Hoog

- Elementor Page Builder Plugin niet up-to-date
-

Medium

- Openstaande database poorten
- HSTS onjuist geconfigureerd (meerdere)
- CSP onjuist geconfigureerd (meerdere)

Overige bevindingen

Er zijn in totaal 122 medium bevindingen, 67 lage en 340 informationals aangetroffen en gemeld.

Oplossen

De bevindingen bij vijf van de zeven testaanbieders zijn opgelost en geverifieerd. Bij twee moet de verificatie op het moment van schrijven nog plaats vinden. Er worden nieuwe boefjes toegevoegd, waarbij het waarschijnlijk is dat er nieuwe bevindingen gaan komen.