To: 5.1.2e [5.1.2e @rivm.nl]
From: 5.1.2e
Sent: Sun 2/7/2021 3:10:45 PM
Subject: FW: Stand van zaken loggin Covid-systemen -CIMS-
Received: Sun 2/7/2021 3:10:45 PM

Hoi 5.1.2e

Zie hieronder ter info.

Gr,
5.1.2e

From: 5.1.2e <5.1.2e @rivm.nl>
Sent: zaterdag 6 februari 2021 14:58
To: 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e 5.1.2e 5.1.2e <5.1.2e @rivm.nl>
Cc: 5.1.2e <5.1.2e @rivm.nl>
Subject: Stand van zaken loggin Covid-systemen -CIMS-

All,

Inleiding
Hierbij een statusupdate m.b.t. het loggen van systeemevents van de bij de CIMS applicatie betrokken servers. Tevens meld ik storing aan het SIEM waardoor een deel van de logging niet aanwezig is.

Er is inmiddels een lijst van bijna 70 servers waarvan de systeemeigenaren hebben aangegeven dat het in verband met CIMS/Covid-19 noodzakelijk is de acties van beheerders/gebruikers/databases op deze systemen te monitoren, periodiek over het gebruik te rapporteren en alarmen bij onverwacht gebruik (of misbruik) in te richten
BI is verzocht om de logs van deze servers naar het SIEM te sturen. Dit is voor hun een flinke klus, en daarna volgt nog het inrichten van het SIEM. Ik verwacht niet dat dit voor medio maart gereed is, als alle gevraagde functionaliteiten al mogelijk zijn.

In deze lijst zijn de systemen van de API gateway / Clientportaal niet opgenomen. Daar heb ik deze week een overleg over.

De status op dit moment is:
Er zijn **drie systemen aangesloten op het SIEM**. Dat zijn de Linux systemen waarop de databases geplaatst zijn en de SFTP server. Functioneel beheerder 5.1.2e krijgt elke zondag een rapportage waarin staat wie er met verhoogde rechten op de systemen is ingelogd en wat voor commando die heeft uitgevoerd. Dit is nadrukkelijk geen applicatielog van de Oracle database. Daar wordt door Ordina op gelogd. Het is onbekend of zij alleen loggen om het systeembeheer van informatie te voorzien of dat ze ook loggen om misbruik te detecteren.

Storing SIEM:
Sinds **vrijdagmorgen 01:20 zijn er door onbekende oorzaak door het SIEM geen logs meer opgeslagen**. Op 06-02- 14:00 heb ik getracht wat processen op diverse systemen te herstarten. Helaas zonder resultaat. Maandagmorgen kunnen we een ticket met hoge prioriteit bij de leverancier indienen.

Verdere aandachtspunten:
De API gateway is gebouwd op het openshift platform. Het SIEM kan standaard niet mee omgaan. Het is onbekend in hoeverre het bv mogelijk dat het SIEM wel de logs opslaat, echter zonder hierover te rapporteren.

Omdat het SIEM niet in staat is langdurig events doorzoekbaar op te slaan. (de kracht van het SIEM zit in real-time analyse en correlatie). Heeft het NCSC ons aangeboden tijdelijk een extra sensor met opslagcapaciteit te leveren. Deze hebben ze speciaal voor ons gebouwd. De planning is dat deze eind deze week wordt geplaatst. Daarna zal deze de event informatie van de linux systemen waar de databases op staan gaan opslaan. Mogelijk kan deze ook ingezet worden om de logs van de Oracle applicatie op te slaan. E.e.a. blijft echter best-effort. Er is bij het NCSC ook geen ervaring met deze manier van opslaan en analyse.

Tot slot een opmerking over Splunk: ik was blij verrast donderdag tijdens de CIMS demo al een SPLUNK instantie te zien. Ik heb daarna direct contact opgenomen om te kijken of die ons nu al kon helpen, maar het bleek dat er een gratis versie met zeer beperkte mogelijkheden te zijn. Dat is helaas geen oplossing voor de logproblematiek.

Met groet,

5.1.2e