MANAGEMENTSAMENVATTING
EXTERN ONAFHANKELIJK ONDERZOEK NAAR MOGELIJKE INBREUK IN SYSTEMEN VAN BIJ12.
Uitgevoerd door Sogeti (onderdeel van CAP Gemini)
16 maart 2021

1. Managementsamenvatting

BIJ12 heeft Sogeti gevraagd een securityonderzoek uit te voeren op de omgeving van BIJ12 beheerd door Atos. Het onderzoek is gestart op 14-01-2021 en is uitgevoerd door ethical hackers / PEN testers van Sogeti.

Aanleiding voor het uitvoeren van dit onderzoek is de wens om te signaleren of er hacks hebben plaatsgevonden op de applicaties en onderliggende systemen. Dit onderzoek is geen forensisch onderzoek en is verricht vanuit het perspectief van een (ethical) hacker. Er is onderzocht of er verdachte zaken zoals een backdoor, script of onverklaarbare open poorten aanwezig waren op de systemen. De onderzoeker heeft het onderzoek uitgevoerd met de hoogste rechten en heeft daarbij ook de productiesystemen onderzocht. Ook heeft de onderzoeker verschillende penetratie testen uitgevoerd op de applicaties en systemen om inzichtelijk te krijgen welke kwetsbaarheden mogelijk misbruikt kunnen worden om toegang tot de systemen te krijgen.

Samenvatting

Na afronding van het onderzoek is de securityspecialist tot de volgende conclusies gekomen.

Het onderzoek laat zien dat er geen sporen van misbruik gevonden zijn op de onderzochte systemen.

De beschikbare logs van de omgeving van BIJ12 beheerd door Atos waren erg beperkt. Op basis van de beschikbare logs is gezocht op verdachte situaties, deze zijn niet gevonden. Het is aan te raden om meer logging toe te voegen op de productie omgeving.

De verschillende systemen en applicaties zijn onderzocht op de aanwezigheid van backdoors, deze zijn niet gevonden.

De onderzoeker heeft onderzoek gedaan naar de Advanced Web Statistics. Op basis van de gemaakte HTTP(S) requests en specifieke downloads van bestanden is er geen bewijs van misbruik gevonden.

De onderzoeker heeft blackbox penetratie testen uitgevoerd aan de “buitenkant” van de applicaties, er zijn geen kritieke vulnerabilities gevonden die tot misbruik van onderliggende systemen konden leiden.

Een onderzoek achteraf kan nooit uitsluiten dat ergens inbreuk zou zijn gepleegd door een hacker die alle sporen daarvan volledig zou hebben gewist, maar bovenstaande bevindingen maken het zeer onwaarschijnlijk dat er op deze systemen inbreuk is gepleegd.

Het is aan te raden om in de toekomst met regelmaat vulnerability assessments en penetration testen te laten doen. Ook is het aan te raden om het patch management op te zetten.

De onderzochte applicaties zijn wisselend in kwaliteit, het is aan te raden om te onderzoeken welke applicaties opnieuw gebouwd of aangepast moeten worden. Dit onderzoek is inmiddels gestart bij BIJ12.

Lopende het onderzoek is er samen met de BIJ12 architect, applicatie eigenaren en beheerders een helder en compleet overzicht opgesteld van de BIJ12 applicaties en systemen beheerd door Atos (en buiten Atos, maar deze zijn buiten scope van dit onderzoek). Op grond van de prioriteitsstelling uit deze lijst heeft het onderzoek plaatsgevonden.