Federale Overheidsdienst Binnenlandse Zaken
Informatie- en Communicatiedienst

persbericht

25.05.2021

De FOD Binnenlandse Zaken heeft het hoofd geboden aan een cyberaanval en moderniseert zijn informatica-infrastructuur

Contactpersoon: Olivier Maerens **T:** 0475/363866

E-mail: olivier.maerens@ibz.fgov.be **F:**

- De FOD Binnenlandse zaken is het slachtoffer geworden van een complexe, geavanceerde en doelbewuste cyberaanval.
- Het gerechtelijk onderzoek naar de cyberaanval is gaande. De doelbewustheid en het verborgen karakter van de actor doen spionage vermoeden.
- In maart 2021 vond het Centrum voor Cybersecurity België (CCB) subtiele sporen van verdachte handelingen op het netwerk van de FOD Binnenlandse Zaken. Een grondige analyse toonde aan dat een aanvaller binnen kon dringen in april 2019. De FOD Binnenlandse Zaken en het CCB nemen deze situatie zeer ernstig.
- Beide diensten brachten de officiële instanties meteen op de hoogte en namen onmiddellijk actie om sporen van de aanvaller te verwijderen en de veiligheid te herstellen.
- De situatie is onder controle: het netwerk werd opgeruimd en de veiligheid hersteld. Omwille van het lopende onderzoek kunnen geen verdere details worden gegeven.

Wat vooraf ging

Begin dit jaar werd Microsoft op de hoogte gebracht van een reeks kwetsbaarheden in zijn Exchange-servers. Dat zijn e-mailservers die wereldwijd door duizenden bedrijven en organisaties worden gebruikt. Microsoft lanceerde op 2 maart updates om hun systemen weer te beveiligen. Ook de FOD Binnenlandse Zaken maakt gebruik van Microsoft Exchange servers en vroeg bijstand van het CCB. De FOD was net zoals duizenden bedrijven wereldwijd kwetsbaar geweest en er werden ‘achterpoortjes’ gevonden op het netwerk. Deze werden verwijderd, en de updates werden tijdig uitgevoerd, maar het CCB deed toch verdere monitoring.

Het is tijdens dit onderzoek dat de cyberexperten van het CCB subtiele aanwijzingen vonden van verdachte handelingen op het netwerk van de FOD. De eerste sporen dateren van april 2019, en wijzen op een zeer complexe en geavanceerde cyberaanval. De complexiteit van de aanval wijst op een actor die over omvangrijke cybercapaciteiten en middelen beschikt. De daders gingen doelbewust te werk, wat spionage doet vermoeden.

Naar een nieuw en veilig netwerk

Zodra de FOD op de hoogte was van deze aanval, werden het Nationale Crisiscentrum, de Gegevensbeschermingsautoriteit, de Federale Politie, het Federaal Parket, Veiligheid van de Staat, ADIV en de FOD Buitenlandse Zaken op de hoogte gebracht, volgens de richtlijnen die worden bepaald in het Nationale Cybernoodplan.

Het dossier is geopend door het Federaal Parket en het onderzoek wordt geleid door een Brusselse onderzoeksrechter. Er werd ondersteuning gevraagd van het CCB bij het volledig in kaart brengen van de omvang van de aanval en de remediering. Het CCB beschreef een plan van aanpak en ondersteunde de FOD bij de uitvoering ervan. Er werden dringende acties ondernomen: de toegang voor de aanvaller werd gestopt, malwares werden verwijderd en belangrijke informatie werd veilig gesteld.

De situatie wordt nog steeds opgevolgd. Om niets aan het toeval over te laten werden de systemen van IBZ opgeruimd om de veiligheid te herstellen.

IBZ moderniseert op dit ogenblik de volledig ICT infrastructuur om de beveiliging verder te optimiseren.

In het belang van het onderzoek kunnen er geen verdere details gegeven worden.

Leuvenseweg 1
1000 Brussel

T 02 488 10 00
F 02 488 19 68

info@ibz.fgov.be
www.ibz.be