



Datum beantwoording: 30 maart 2023

Antwoord college/burgemeester

1. Hebben er bedrijven, die gevestigd zijn in de gemeente Duiven, (van maart 2021 tot heden) aangifte gedaan van datadiefstal en chantage door criminelen?

Antwoord: In de periode 1 maart 2021 tot en met 28 februari 2023 is er door 9 bedrijven aangifte gedaan van cybercrime/gedigitaliseerde criminaliteit. Het betrof: vijfmaal "overige horizontale fraude" (= fraude tussen inwoners of bedrijven onderling), tweemaal "fraude met betaalproducten" en tweemaal "cybercrime". De benamingen komen uit het politiesysteem.

2. Indien de vorige vraag met ja is beantwoord, hoeveel bedrijven én kunt u tevens aangeven om wat voor bedrijven het gaat?

Het waren negen verschillende bedrijven: softwareleveranciers en retailers. Het betreft oplichting, phishing, hacken van klantgebruikersaccounts, valsheid in geschrifte en installatie van ransom software.

3. Hoeveel inwoners van de gemeente Duiven hebben (van maart 2021 tot heden) aangifte gedaan van telefonische misleiding, afpersing, chantage en/of datadiefstal?

In bovengenoemde periode zijn er 273 registraties vastgelegd (inclusief bedrijven). Het betreft voornamelijk fraude met online handel (120x) en overige horizontale fraude (85x).

Een goed en compleet cyberbeeld ontbreekt echter. Veel cybercrime zaken worden niet in het basisteam maar in het Cybercrimeteam Oost Nederland opgepakt en afgehandeld. Daarnaast schamen veel bedrijven en personen zich dat zij slachtoffer geworden zijn van cybercrime/gedigitaliseerde criminaliteit en doen geen aangifte. Op het werkelijke aantal cybercrime/gedigitaliseerde criminaliteit zaken heeft de politie geen zicht.

4. Kan het College aangeven hoe de veiligheid van de digitale gegevens van onze inwoners, die opgeslagen is bij 1Stroom, is gewaarborgd?

De data van 1Stroom worden opgeslagen in twee geografisch gescheiden datacenters in Nederland. Het opslaan van desbetreffende data gebeurt op een intern netwerk van de RID, welke actief wordt beveiligd door een firewall. De opslag is niet publiekelijk te benaderen maar uitsluitend via afschermd systemen. Daarnaast worden op beide plekken backups gemaakt.

5. Wanneer zijn alle systemen van de gemeente gescand op veiligheid en of ze up-to-date zijn?

Het bewaken van de veiligheid gebeurt op meerdere manieren. Zo zijn er de meldingen van de Informatiebeveiligingsdienst van Nederlandse Gemeenten (IBD), het Nationaal Cyber Security Centrum (NCSC), de leveranciers, eventueel externe beheerders, bewakingssoftware e.d. Veel actoren zijn erbij betrokken, het gaat om continue processen.

Als het gaat om cloud toepassingen vindt afstemming en planning van updates plaats in samenwerking met de leverancier. Voor de on-premis (= op locatie) toepassingen vindt er afstemming met de RID plaats. Overigens wordt een update niet altijd om veiligheidsredenen geplaatst. Vaak gebeurt het ook om functionele wijzingen.

6. Als dat niet gebeurt is, waarom is dat niet gebeurd?

Zie antwoord 5. Het zijn continue processen.

7. Heeft het college een ethische hacker laten proberen om de systemen te hacken?

Wij hebben geen ethische hackers ingezet. We doen wel iets soortgelijks met een bedrijf dat op realistische wijze onze systemen test op kwetsbaarheden. Het voornemen is om deze zogenaamde penetratietesten voor de kerntoepassingen uit te breiden. Daarnaast hebben er kwetsbaarheidsonderzoeken plaatsgevonden.

8. Als dat niet gebeurd is, waarom is dat niet gebeurd?

Er zijn meer mogelijkheden om kwetsbaarheden op te sporen. Zie het vorige antwoord.

9. Hoeveel hackpogingen zijn op de diverse systemen geregistreerd vanaf 1 januari 2021?

Wanneer we het hebben over een gerichte, actieve hackpoging dan is er één geregistreerd sinds 1 januari 2021. Er worden - net zoals bij alle partijen - continu pogingen gedaan in de vorm van phishingmails en port-scanning, welke worden tegengehouden door onze spam-filter oplossingen en firewall.

10. Zijn er geslaagde hackpogingen geweest? Zo ja, welke informatie is er buit gemaakt?

De ene poging was niet geslaagd. Daarmee bedoelen we dat er geen toegang is verkregen tot onze Service Based Computing (Citrix) omgeving. Zonder toegang tot deze omgeving is er geen mogelijkheid om interne data in te zien.

11. Hoe ziet het beveiligingsbeleid eruit van de apparatuur die ambtenaren, colleges of andere mensen gebruiken die werkzaamheden uitvoeren voor onze gemeente? Hoeveel virussen zijn er aangetroffen en geblokkeerd en hoeveel apparaten zijn er gehackt geweest?

Het informatiebeleid in brede zin is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO). Dat is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). De apparatuur valt ook onder het BIO-regime. Daarnaast wordt gebruik gemaakt van een systeem van Service Based Computing, wat betekent dat er geen dataopslag op individuele computers plaatsvindt, maar 'er achter' op servers, die zich achter een geavanceerde beveiligingsmuur bevinden. Zoals eerder vermeld zijn er geen geslaagde hackpogingen geweest. Jaarlijks worden er wel tientallen virussen/malware geblokkeerd.

Ondertekening

Hoogachtend,
Burgemeester en wethouders van Duiven,

mr. drs. R.J. (Rutger) den Haan
secretaris

mr. H.B. (Huub) Hieltjes
burgemeester

