gemeente harderwijk

Gemeenteraad Harderwijk
T.a.v. raadsfractie VVD
Postbus 149
3840 AC HARDERWIJK

datum: 16 november 2022
ons kenmerk: 02430000122785 / 02430000410838
uw brief van: 25 oktober 2022
uw kenmerk: 02430000408787
onderwerp: Beantwoording schriftelijke vragen conform artikel 32 van de organisatieverordening van de VVD over cyberaanvallen.

Geachte heer/mevrouw,

De VVD-fractie heeft op 25 oktober 2022 schriftelijke vragen ingediend over cyberaanvallen. In deze brief geven wij antwoord op de gestelde vragen.

Vraag 1:
Is het college bekend met het genoemde artikel en wat is de reactie van het college hierop?
Antwoord 1
Ja, het artikel sluit aan bij onze voortdurende aandacht die dit onderwerp heeft

Vraag 2:
Zijn er cijfers bekend van de afgelopen drie jaar over het aantal cyberaanvallen binnen onze gemeente, op de volgende gebieden:
- Totaal aantal cyberaanvallen;
- Ransomware-aanvallen;
- Phishing aanvallen;
- Cyberaanvallen op derden waarmee de gemeente samenwerkt?

Antwoord 2:
Eind 2021 hebben de drie gemeenten extra middelen beschikbaar gesteld om meer in controle te zijn en kwetsbaarheden inzichtelijk te maken en te mitigeren. Met deze middelen is onder meer tooling ingezet waarmee wij ook beter zicht krijgen op onze kwetsbaarheden en technisch aanvallen kunnen afslaan. Inzicht in aantallen is vanaf begin 2022 beschikbaar. Om hackers niet te voorzien van informatie over onze gedetecteerde beveiligingsincidenten delen wij deze aantallen niet openbaar.

EHZM werkt samen met de Informatie Beveiligings Dienst (IBD) van de VNG en ontvangt zeer regelmatig informatie omtrent kritieke kwetsbaarheden, deze meldingen worden gecontroleerd op aanwezigheid binnen EHZM en geëvalueerd.

organisatie eenheid: Meerinzicht
behandeld door: W.R. Mark
telefoonnummer: 085 1108 328
bijlage(n): 0

Havendam 56
Correspondentieadres:
Postbus 149
3840 AC Harderwijk
T 0341 411 911
F 085 110 8515
E info@harderwijk.nl
I www.harderwijk.nl
B NL44 BNGH 0285 0033 13

Waar noodzakelijk worden hier mitigerende acties op ondernomen.

Derden partijen zijn via (verwerkings)overeenkomsten contractueel verplicht om kritische kwetsbaarheden en datalekken te melden aan ons, daarnaast zijn de I-adviseurs, technisch applicatie beheerders en contractmanagers voortdurend in contact met deze partijen.

Vraag 3:
Welke stappen zet het college nu om deze cyberaanvallen tegen te gaan of te beperken?
Antwoord 3:
Technische maatregelen zijn de afgelopen jaren reeds genomen onze risico's te beheersen. In 2022 is er reeds extra budget vrijgegeven om extra veiligheidsmaatregelen te nemen en deze zijn ook ingezet. Eind 2021 is een vaste CISO (Chief Information Security Officer) aangenomen; tot dat moment was er een tijdelijke inhuur CISO beperkt beschikbaar.

Vraag 4:
Welke stappen wil het college in de toekomst zetten om deze cyberaanvallen tegen te gaan of te beperken?
Antwoord 4:
Beantwoord in vraag 6

Vraag 5: Welke middelen heeft het college nu extra nodig om de gemeente online veilig te houden/maken?
Antwoord 5:
Beantwoord in vraag 6

Vraag 6:
Kan de gemeente de aanpak cybercrime voldoende realiseren vanuit de bestaande budgetten of verwacht het college de aanpak te intensiveren met daaraan gekoppeld een verhoging van de beschikbare budgetten?
Antwoord 6:
In de praktijk moet er eerst een nieuwe kwetsbaarheid/bedreiging bekend worden voordat wij hierop reageren, wij zijn dus altijd reactief in geval van nieuwe kwetsbaarheden/bedreigingen. We hebben op dit moment in de begroting middelen opgenomen waarmee wij met de kennis van nu kunnen acteren, echter dat kan door ontwikkelingen in de cybercriminaliteit snel wijzigen.

Binnen EHMZ wordt er naast de technische maatregelen aandacht gegeven aan privacy en informatiebewustzijn door middel van o.a een specifiek introductieprogramma, alsmede een privacy en informatieveiligheids bewustwordingsprogramma en organiseren wij afdelingsspecifieke privacy en informatieveiligheid bijeenkomsten.

In zijn algemeenheid is informatiebeveiliging in orde houden/maken is een grote uitdaging. Wat vandaag veilig is kan morgen onveilig zijn en vraagt om continue aanpassingen, die ook worden uitgevoerd. Wij kunnen niet uitsluiten dat in de toekomst aanvullende middelen noodzakelijk zijn.

Vraag 7:
Hoe wordt de Raad actief op de hoogte gehouden van actuele ontwikkelingen op het gebied van online veiligheid binnen de gemeente Harderwijk en/of welke keuzes het college maakt om de online veiligheid te vergroten?
Antwoord 7:
Wij informeren regelmatig de betrokken wethouder (Wilco Mazier) omtrent het informatie-beveiligingsvraagstuk.

In geval van calamiteiten wordt afstemming gezocht met de wethouder en gemeentesecretaris en waar nodig informeren wij de raad. Daarnaast wordt op reguliere basis in P&C-cycles gerapporteerd over de stand van zaken omtrent informatieveiligheid en de eventueel benodigde extra investeringen.

Wij gaan er van uit dat wij u een helder antwoord hebben gegeven op uw vragen. Mocht u toch nog vragen hebben dan kunt u contact opnemen met de heer W.R. Mark van Meerinzicht. Telefoon: 085 1108 328.

Met vriendelijke groet,
Burgemeester en wethouders van Harderwijk

de heer J.P. Wassens
secretaris

de heer H.J. van Schaik
burgemeester