Beste Griffie,

De VVD Rijswijk heeft de volgende vragen die zij aan het College wil stellen

Digitaal Kwetsbaar: Apache Log4j
Enige dagen geleden kwam het nieuws naar buiten bij het NCSC dat er een serieus ernstig digitaal lek bestaat waarbij bedrijven en overheden gevaar zouden lopen. Persoonsgegeven en kritieke data zouden hiermee op straat kunnen komen, met alle gevolgen van dien.

- Is het College bekend met deze digitale lek?
Antwoord: Ja

- Maakt onze gemeente gebruik van systemen waarbij een dergelijk lek kan plaatsvinden?
Antwoord: Ja

- Wat heeft het College gedaan om de persoonsgegevens en de data in de gemeentelijke systemen veilig te stellen?
Antwoord:
Voor zover bekend wordt de kwetsbaarheid tot nu toe alleen misbruikt voor cryptomining (de rekenkracht van de geïnfecteerde systemen wordt gebruikt om nieuwe cryptovaluta te 'oogsten') en voor het installeren van ransomware (bij ransomware wordt de data op het geïnfecteerde systeem versleuteld en daarmee onbruikbaar. Tegen betaling van losgeld wordt de data weer ontsleuteld).

Er zijn grofweg drie acties uitgevoerd om de systemen hiervoor veilig te stellen:
1. Alle servers met een verbinding naar internet zijn gescand op de kwetsbaarheid. Daar waar de kwetsbaarheid voorkwam zijn onmiddellijk maatregelen getroffen.
2. Er is een inventarisatie gestart van alle applicaties en systemen die de gemeente gebruikt. Gevraagd is of systemen kwetsbaar zijn en welke maatregelen nodig zijn om de eventuele kwetsbaarheid voor het systeem te verhelpen.
3. Er zijn technische maatregelen getroffen om pogingen tot misbruik van buitenaf te detecteren en te blokkeren.

- Heeft het College daarbij overwogen de systemen "offline" te halen en een digitale reparatie voor dit lek uit te voeren? Zo niet, waarom?
Antwoord:
Waar mogelijk wordt gelijk een reparatie uitgevoerd om de kwetsbaarheid te verhelpen. Indien een reparatie nog niet mogelijk is wordt op basis van een risico-inschatting bepaald welke andere maatregelen getroffen kunnen worden, zoals het isoleren of uitzetten van een systeem. In een enkel geval is besloten om een systeem, in afwachting van een reparatie van de kwetsbaarheid, voor de 'buitenwereld' af te sluiten.

- Welke maatregelen neemt het College om in de toekomst de digitale weerbaarheid voor zich zelf zo optimaal mogelijk te maken?
Antwoord:
Het verbeteren van de digitale weerbaarheid is een continu proces. De gemeente hanteert hierbij de uitgangspunten van de Baseline Informatiebeveiliging Overheid. Er wordt blijvend geïnvesteerd in de daarin voorgeschreven technische, procedurele en organisatorische maatregelen.