Schriftelijke vragen artikel 31.

Van:	: *Ingo Kehe (Blijf Stellingwarfs)*
Aan:	: College van burgemeester en wethouders
Datum:	: 31-05-2022
Onderwerp	: Omtrent ICT-beveiliging Gemeente Weststellingwerf:.

Inleiding:

Op 1 april werden de gemeenten Buren en Neder-Betuwe getroffen door een grote digitale hack. Honderdduizenden digitale bestanden (130GB) waren gestolen tijdens een ransomwareaanval begin welke worden aangeboden op het Dark web. De gemeente Buren meldde dat het gaat om o.a. 'gevoelige persoonsgegevens en vertrouwelijke informatie'. Criminelen claimen op het Dark web dat ze '5TB' aan gegevens hebben buitgemaakt. De hackers hebben naar eigen zeggen 'financiële informatie, contracten en gegevens van gemeentemedewerkers' buitgemaakt.

Het college wordt verzocht de volgende vragen binnen vier weken na indiening te beantwoorden:

Vraag:
Is de gemeente Weststellingwerf bekend met dit voorval?

Vraag:
Zo ja; welke ICT-maatregelen zijn er genomen om een dergelijke digitale dreiging tegen te kunnen gaan? En kunt u de veiligheid van de digitale gegevens van de Gemeente Weststellingwerf, haar medewerkers en haar inwoners (blijven) waarborgen?

Vraag:
Zo nee, is de gemeente Weststellingwerf ervan overtuigd dat dit onze gemeente niet kan overkomen? En hoe kunt u dit maatstaven?

Vraag:
Zijn we ons ervan bewust dat onze gemeente website een DANE-configuratiefout heeft ? ***1**
Zo nee, is de gemeente zich bewust dat hiermee alle gegevens van burgers openbaar zijn ?

Vraag:
Zijn we ons ervan bewust dat onze gemeente webserver www.weststellingwerf.nl *geen* Content-Security-Policy (CSP) actief heeft? ***2**
Zo nee, elke login via DigiD is hiermee onveilig. Beseft men dit?

Vraag:
Zo zijn er nog meer veiligheidsproblemen die simpel te herkennen en op te lossen zijn.
Wanneer gaat de gemeente hier maatregelen tegen nemen?

***1**

Info: DANE is een beveiligingsprotocol dat verder gaat dan het standaard HTTPS protocol in het beveiligen van de vertrouwensketen tussen server, Certificate Authority en gebruiker.

***2**

Info : Hiermee kan voorkomen worden dat kwaadaardige scripts of CSS-elementen worden geïnjecteerd of ingeladen, die bijvoorbeeld gebruikt worden om creditcard gegevens of andere persoonsgegevens te stelen, bezoekers te redirecten naar andere sites of (malafide) advertenties te tonen.
Ook is er een mogelijkheid tot rapportage, zodat je zicht kan houden op jouw policy en de overtredingen die plaatsvinden. Dit kan handig zijn om eventuele problemen te detecteren en op te lossen, en de website te veilig te houden.