Motie vreemd aan de orde van de dag

‘Hack Meierijstad!’

De raad van Meierijstad in vergadering bijeen op donderdag 20 december 2018,

constaterende dat:

- een waterdichte beveiliging van de informatie- en datasystemen van de gemeente Meierijstad van zeer groot belang is,
- het vertrouwen van inwoners bevestigd en versterkt wordt als die beveiliging is aangetoond,
- maatregelen kunnen en moeten worden genomen als juist wordt aangetoond dat die beveiliging niet optimaal is.

overwegende dat:

- gemeenten Eindhoven en Den Haag deze controles lieten uitvoeren door zogeheten ethische hackers (zie: https://www.computable.nl/artikel/nieuws/overheid/6518825/250449/den-haag-schakelt-ethische-hackers-in.html),
- dit idee navolging verdient in Meierijstad,
- de afsluiting van de twee jaar durende harmonisatie daarvoor een mooi moment is.

verzoekt het college om:

- een actie, vergelijkbaar met het Haagse voorbeeld te ontwikkelen en te houden in de eerste helft van 2019,
- hierover vooraf en na afloop te communiceren met de gemeenteraad en het publiek en daarbij verantwoording af te leggen over de resultaten van de actie en eventuele reparatie- of verbeteracties

en gaat over tot de orde van de dag.

Namens ‘Hart voor Schijndel’, D66

Laurens van Voorst Marrik van Rozendaal

Bijlage: bijzonderheden en kanttekeningen

Bijlage: bijzonderheden en kanttekeningen

Om een exacter beeld te schetsen van de voorgestelde actie, hieronder wat gedachten over doelen, vectoren en randvoorwaarden. Deze lijst is mogelijk niet compleet, maar helpt bij de ideevorming.

Doelen:
- bescherming tegen gevaren van binnen;
- beschermen tegen gevaren van binnen (fysiek toegang tot het gebouw - geen medewerker);
- beschermen tegen gevaren van binnen (toegang tot remote werken met medewerker gegevens);
- beschermen tegen gevaren van binnen (fysieke toegang en toegang tot systemen met medewerkers gegevens).

Opties voor aanvangssituatie:
- de hackers weten niets van de systemen en moeten alles zelf uitzoeken;
- grove omgevingsschets wordt gegeven zodat informatievergaring niet te veel tijd kost;
- details van systeeminformatie wordt gegeven, zodat de systemen echt goed getest worden.

Randvoorwaarden:
- vooraf garanties voor geheimhouding door hackers;
- hackers dienen VOG te overleggen;
- nadere voorwaarden rond type inschrijvers (studenten, bedrijven, zzp-ers, particulieren?);
- meldingsplicht van gevonden lekken en andere onvolkomenheden;
- monitoring door professionals;
- vooraf bepalen wat er gebeurt met resultaten;
- vooraf vaststellen wie verantwoordelijk is voor gevonden omissies en het realiseren van reparaties.