VERSLAG VAN DE SESSIE VAN DE RAAD DER GEMEENTE HAARLEMMERMEER OP DONDERDAG 3 SEPTEMBER 2020

Onderwerp: RKC-vervolgonderzoek informatiebeveiliging

Voorzitter: mw. C.F.M. van der Meij

De leden: dhr. M.L. Beusenberg, mw. R.F. Hussain, dhr. R. Kenselaar, dhr. H.C.M. Koning, mw. J. Koolmoes, dhr. P.C.I. Meijer, dhr. P.J.M. Schouten, dhr. H.P. Spijker, dhr. J.P.H. de Vries, dhr. H. Werner

Griffier: dhr. B Heerema

Portefeuillehouder: mw. W. Booij-van Eck

Insprekers: Geen

De VOORZITTER: Goedenavond dames en heren, het is inmiddels bijna 20.35 uur. Dat betekent dat we iets te laat beginnen met deze sessie. We hebben het vandaag over de nieuwe aanbeveling van de Rekenkamercommissie aan de raad op het gebied van informatiebeveiliging. We hebben anderhalf uur de tijd en het doel is die aanbeveling te bespreken en mee te geven aan het college wat we daarmee willen. Wie mag ik als eerste het woord geven? Dat zijn er twee tegelijk. Dames gaan voor, mevrouw Hussain, PvdA, gaat uw gang.

Mevrouw HUSSAIN: Dank u wel voorzitter. Als je online op zoek gaat naar de term 'informatiebeveiliging' vind je een scala aan informatie. Het is een brede definitie en het heeft uiteindelijk tot doel om de organisatie te beschermen, maar informatiebeveiliging is veel meer dan dat. Naast het verminderen van het risico op incidenten, biedt een goede informatiebeveiliging handvaten voor hoe je dient te handelen tijdens een incident, creëert het awareness in de organisatie en schept het vooral vertrouwen. Het is inderdaad een brede definitie en dat geeft aan waarom informatiebeveiliging zo belangrijk is voor onze organisatie. Daarbij is het van belang te onthouden dat eenieder binnen de organisatie een steentje hieraan dient bij te dragen. Ik denk ook dat het de leidraad dient te zijn bij de informatiebeveiliging van onze gemeente.
In 2016 heeft een onderzoek plaatsgevonden dat zich destijds enkel richtte op de maatregelen om de vertrouwelijkheid van informatie te garanderen. Ik gaf het net al aan, informatiebeveiliging is een breed begrip en omvat veel meer dan dat. Als je kijkt naar de uitkomsten van de aanbevelingen van destijds zie je dat her en der nog acties moeten worden genomen. Zo blijkt dat het bewustwordingsniveau in de gemeente nog laag is. De PvdA vindt het belangrijk dat dit bewustwordingsniveau binnen aanzienlijke periode stijgt en ook op niveau is. Hierbij verzoeken we het college om een structurele aanpak te creëren zodat het niveau behaald wordt, maar ook om te kijken naar de oorzaak van waarom het niveau nu zo laag is.

De VOORZITTER: De heer Meijer van Forza! heeft een interruptie.

De heer MEIJER: Dank u wel. Mevrouw Hussain zegt 'we willen graag dit en we willen graag dat', maar wat zijn uw eigen concrete plannen om dat te verbeteren? Ik zit al meer dan tien jaar in de raad en ik zie juist dat het heel erg vooruitgaat, zeker de laatste jaren. Dus wat vindt u dat er niet goed gaat en wat zou er verbeterd moeten worden? Even concreet graag.

Mevrouw HUSSAIN: Het gaat er niet om wat ik goed vind, het gaat erom dat de Rekenkamercommissie uitkomsten heeft neergelegd voor ons naar aanleiding van onderzoek waaruit blijkt dat heel veel dingen niet kloppen. Dat bespreken we ook vandaag en daarom kijken we naar het college voor wat het college kan doen. Uiteindelijk ligt er heel veel, waaronder een wettelijke verplichting, waaraan we straks moeten gaan voldoen.

De VOORZITTER: De heer Meijer. Is dat afdoende voor nu? Gaat u verder, mevrouw Hussain.

Mevrouw HUSSAIN: Dan ga ik verder met aanbeveling 3. Daar zie je dat de huidige organisatie kwetsbaar is. Dat hangt waarschijnlijk ook samen met het bewustwordingsniveau. Het is belangrijk dat op korte termijn heldere doelen worden geformuleerd en het is fijn om te zien dat er reeds actie is ondernomen door een wervingsproces te beginnen voor een vast dienstverband van een CISO. Daarnaast is het belangrijk dat er regelmatig een integrale audit of pentest op kwetsbaarheden wordt uitgevoerd. Door deze testen komen kwetsbaarheden sneller aan het licht. De afgelopen jaren hebben deze testen minimaal plaatsgevonden. Het is belangrijk dat deze testen vaker worden uitgevoerd. Fijn om te zien dat het initiatief reeds is genomen om jaarlijks een pentest uit te voeren.
Uit onderzoek bleek onder meer dat de ontwikkeling van monitoring en signalering van groot belang is zodat tijdig ingegrepen kan worden bij mogelijke aanvallen. Als je kijkt naar de tabel, zie je een lichte groei van incidenten. Voor nu wordt het uitbesteed aan KPN omdat het intern nog niet te organiseren valt. Is er wellicht zicht op mogelijkheden om dit straks wel intern te regelen? Of blijft uitbesteden in dit geval nog steeds de beste oplossing? We horen het graag.
Als je kijkt naar de voorgaande aanbevelingen en de uitkomsten daarvan, dienen er nog enkele acties genomen te worden ten aanzien van informatiebeveiliging in de gemeente. Het is dan ook zaak dat dit zo snel mogelijk gebeurt. Daarom omarmen we de twee nieuwe aanbevelingen van harte. Zo is het belangrijk dat de gemeente zo snel mogelijk voldoet aan de wettelijke verplichtingen van de BIO. Hoe en wanneer dat gaat gebeuren is nog niet nader gespecificeerd. De wettelijke verplichting geldt sinds 1 januari 2020. Daarom zien we graag zo spoedig mogelijk een plan van aanpak tegemoet en logischerwijs daarna een rapportage over de voortgang. Maar ook het ambitieniveau van de informatiebeveiliging voor 2020 en 2023 mag daarbij niet ontbreken. Op deze wijze zullen de doelen meetbaar zijn en krijgt eenieder meer zicht en grip op de informatiebeveiliging. Ik gaf het namelijk al eerder aan, eenieder dient zijn steentje daaraan bij te dragen voor de goede informatiebeveiliging. We horen graag van het college wanneer we dit kunnen verwachten. Dank u wel voorzitter.

De VOORZITTER: Dank u wel mevrouw Hussain, dan nu mijnheer De Vries, ChristenUnie-SGP.

De heer DE VRIES: Dank u wel voorzitter. In 2016 werd een aantal aanbevelingen gedaan door de Rekenkamercommissie naar aanleiding van het eerste onderzoek over de staat van de informatiebeveiliging in onze gemeente. Begin dit jaar keek de Rekenkamercommissie nog eens naar wat er van de plannen terecht is gekomen en als we het rapport doornemen, worden we niet laaiend enthousiast van de bevindingen. Toch heeft mijn fractie genoeg lichtpuntjes gezien om het vertrouwen te krijgen dat we de goede kant op gaan en het doel gaan bereiken. Met name vorig jaar zijn stevige stappen gezet. Er is een functionaris gekomen die deze materie grondig ter hand kon nemen en dat ook deed, de CISO. De wereldwijde Citrixproblemen van eind vorig jaar zijn mede daardoor aan de gemeentelijke deuren voorbijgegaan. Het college voldoet nog niet aan de Baseline Informatiebeveiliging Overheid, de BIO, dat heeft mijn collega Hussain al genoemd, maar het college is er wel naartoe op weg met de organisatie. De fractie van de ChristenUnie-SGP kan zich wel vinden in de door de RKC voorgestelde opdracht om heldere streefdata vast te stellen waarop dit doel is bereikt en hier ook regelmatig over te rapporteren. Ook vinden we het een goed voorstel voor de komende jaren aan te geven op welk niveau onze beveiliging moet zijn geregeld. Tot zover, dank u

wel.

De VOORZITTER: Dank u wel mijnheer De Vries. Dan gaan we nu naar mevrouw Koolmoes van HAP.

Mevrouw KOOLMOES: Dank u wel voorzitter. Mijn zoon was twaalf jaar oud toen hij ons wachtwoord wist te hacken. Hij is nu 28 en IT-specialist. Hiermee wil ik zeggen dat het voor een hele hoop jongeren, en ook volwassenen, kinderspel is om te hacken. Het nummer 1 gebruikte wachtwoord is nog steeds '123456'. En onze gemeente heeft nog steeds geen wachtwoordbeleid voor de medewerkers. Vandaag spreken we over een onzichtbare insluiper die via een achterdeur kan binnenkomen. We gaan praten over hoe we die deur op slot kunnen houden en hoe we de mensen binnen die deuren tegen cyberaanvallen kunnen beschermen. Ook al weten we dat beveiliging duur is om te onderhouden, het slaapt zoveel beter wanneer gevoelige informatie van onze inwoners netjes en veilig opgeborgen blijft achter versleutelde wachtwoorden en daarmee niet in handen kan komen van derden. Laten we hier als gemeente de aankomende tijd een prioriteit van maken.
Er waren vijf aanbevelingen gedaan die zijn opgevolgd, maar wel met de nodige kanttekeningen. En er was een geamendeerde wijziging in een beslispunt. Die is opgevolgd, al in 2016.
Dan ga ik naar aanbeveling 1. In aanbeveling 1 vragen we het college om de aanbevelingen van de RKC op te volgen. Dat doe ik dan bij dezen, voorzitter.
In aanbeveling 2 lezen we dat er in 2019 al veel modules werden aangeboden en campagnes in het rond gingen, maar ook dat de bewustwording in de organisatie nog erg laag was. Daarom is HAP erg blij te horen dat er nu sprake is van een structurele aanpak en dat medewerkers van genoeg plekken worden voorzien om terecht te kunnen met hun vragen. Het is al helemaal in deze tijd van digitalisering en thuiswerken van belang dat medewerkers het waarborgen van informatiebeveiliging ergens op hun prioriteitenlijstje hebben staan.
Aanbeveling 3, er is een interim-CISO. Maar interim kinkt erg tijdelijk. HAP beveelt van harte aan dat de CISO in dienstverband, en dus intern, aan ons verbonden blijft. Zo zorgen we ervoor dat de veiligheid en de stabiliteit wordt gewaarborgd. Gelukkig wordt hier nu ook werk van gemaakt.
Aanbeveling 4, het doen van pentesten. Ook hier maakte Tim van Essen zich in 2016 hard voor. 'Doe steeds opnieuw ethische testen om de pijnpunten in ons systeem te herkennen'. Fijn om te lezen dat dat ook goed opgevolgd is. Het is tenslotte ook een verplichting in de BIO.
Aanbeveling 5, monitoring en signalering; een keurig rapportcijfer. We zien wel de oplopende cijfers door de jaren heen. We hopen natuurlijk dat de komende cijfers van 2020 ons positiever gaan stemmen.
Moet Haarlemmermeer de meest informatieveilige gemeente van Nederland worden? Als het even kan wel. Hoe mooi is het als wij als voorloper een goed voorbeeld kunnen zijn voor andere gemeenten? Maar zien wij samenwerking met andere gemeenten wel als een toevoeging? Zijn wij juist niet uniek met Schiphol in ons midden en kan geen andere gemeente daarmee worden vergeleken? HAP ziet de samenwerking met gemeenten die nog sterker zijn in informatiebeveiliging wel zitten. Misschien een leuk debatpunt zo meteen.
HAP vraagt het college het ambitieniveau voor informatiebeveiliging voor de periode 2020-2023 concreet uit te werken via meetbare doelen en dit op te nemen in de planning-en-controlcyclus. Dat we in maart allemaal plotseling thuis moesten gaan werken, was een niet voorziene bijkomstigheid. Ik neem aan dat daardoor de voortgang van de informatiebeveiliging on hold is gezet. Of dat nu echt een verstandige keuze was? Daar kunnen we over twisten. Ik lees wel in het document dat we in maart 2020 nog niet aan alle normen hadden voldaan die wel verplicht waren in de BIO. Hoe kan de gemeente Haarlemmermeer verantwoorden dat we nog steeds niet aan die verplichte voorwaarden voldoen?
Al in maart 2016 zei mijn voorganger Tim van Essen 'Laat dit debat het begin zijn van een moderne en dynamische veiligheidsorganisatie'. Tot zover, voorzitter.

De VOORZITTER: Waarvoor dank. Dan gaan we door naar de heer Kenselaar van GEZOND Haarlemmermeer.

De heer KENSELAAR: Dank u wel voorzitter. Dat het thema Informatiebeveiliging, zeker sinds de Privacywet is geëffectueerd, een hot item is, behoeft inmiddels geen verdere uitleg meer. Ook hoeft niet te worden uitgelegd dat gemeenten hierin als lokale en regionale overheden een voorbeeldfunctie hebben of in elk geval zouden moeten hebben. Wat wel uitleg behoeft, is dat in 2016 een en ander aan aanbevelingen van de Rekenkamercommissie aan ons gemeentebestuur is gegeven en dat hierop toezeggingen zijn gedaan, maar dat deze voor het grootste deel maar gedeeltelijk zijn uitgevoerd. Je kunt het ook positief bekijken zoals de heer Meijer net al aangaf. Het gaat wel een stuk beter, dat zijn de dingen die wel zijn opgepakt. We moeten vooral niet willen dat we een hoofdrolspeler worden in een soort rip-off van de recente kaskraker 'Meet the Grapperhauses', waarin wij als voorbeeldinstantie achter de feiten aanlopen terwijl we van burger en bedrijf vragen alles uit de kast te trekken om binnen de AVG-wetgeving te blijven.
De factor mens wordt door de Rekenkamercommissie al uitgelicht. Hierbij werd samengevat aangegeven dat de medewerkers de protocollen met betrekking tot de Privacywet nog niet dusdanig in hun dagelijkse doen en laten op het werk hebben weten in te passen dat de datalekken en dergelijke zo veel als mogelijk tot het verleden zijn gaan behoren. Ook de grafiek in de aangereikte stukken liet zien dat het aantal informatiebeveiligingsincidenten juist toe- in plaats van afnam, een stijging van 2019 even niet meegenomen omdat dit jaar niet een-op-een met de drie voorgaande jaren is te vergelijken.
Vragen van de Rekenkamercommissie waren onder andere 'wil Haarlemmermeer de beste van de klas worden op het gebied van informatiebeveiliging worden of mag het iets minder?' en 'wat mag dat allemaal kosten?' Gezond Haarlemmermeer vindt sowieso dat op dit gebied elke overheidsinstantie ernaar zou moeten streven om de beste van de klas te zijn, alleen al vanwege die voorbeeldfunctie maar ook vanwege het vertrouwen dat je de inwoners moet kunnen bieden. Natuurlijk, Henny Huisman zei het al, er kan er maar een de winnaar zijn, maar laten we ernaar streven dat onze inwoners en hun gevoelige informatie in ieder geval niet de verliezers worden. Wat mag dit dan kosten? Feitelijk maakt het niet uit hoeveel geld je ertegenaan gooit, zo lang je niet eerst en vooral zorgt dat de factor mens alles zo vlekkeloos mogelijk uitvoert en nakomt. We hebben kunnen lezen dat hier echt wel aandacht voor is geweest, maar klaarblijkelijk ben je er niet met alleen een sticker op de deur of de vloer plakken en zo nu en dan het eens belichten als het uitkomt. Vooral hierin zal wat ons betreft dan ook geïnvesteerd moeten worden. En heus niet alleen met aankopen voor beveiliging, maar met educatie en diepere bewustwording en die door de Rekenkamercommissie aangehaalde Chief of Information Officer, ofwel de CISO. Zodat we aan de hand van deze persoon ook van reactief naar proactief kunnen gaan, voorkomen is in dit geval beter dan de fout ingaan. En als we dat voor elkaar hebben, kun je uiteindelijk zeggen 'ziezo, nu heeft een verdere investering in hardware, software en andere fysieke middelen echt zin, want de factor mens is ervan doordrongen dat dit ons echt verder gaat helpen'. Tot zover, dank u wel.

De VOORZITTER: Ja ziezo. Dank u wel mijnheer Kenselaar, dan EEN Haarlemmermeer, Mijnheer Spijker.

De heer SPIJKER: Dank u wel voorzitter, allereerst dank aan de Rekenkamercommissie. Ze hebben weer een goed rapport aangeleverd dat aanzet tot actie ondernemen. Wat betreft informatiebeveiliging in deze tijd, dat is natuurlijk van groot belang. Er is aan alle oude aanbevelingen deels voldaan, maar voorzitter, het is nog absoluut niet acceptabel. EEN Haarlemmermeer pleit voor een strategische keuze waarbij wordt ingezet op investeren in een krachtige informatiebeveiliging. Dus college, pak die

handschoen op en zet die ambitie in naar een hoger niveau alstublieft. Want de gemeente is absoluut niet gebaat bij een aanval van verkeerde hackers, en daarmee doel ik niet op een jong speels inbrekertje, maar op een misdadige partij die de data van de gemeente wil misbruiken.

De VOORZITTER: U zag hem al aankomen, u krijgt een interruptie van Forza!, mijnheer Meijer.

De heer MEIJER: U zegt dat een beetje denigrerend mijnheer Spijker, over een minderjarig jongetje, maar die jongen die de grote DDoS-aanval heeft ingezet, was veertien jaar. Die heeft grote universiteiten platgelegd in Nederland en veel gemeenten in Nederland. Hij heeft ook geprobeerd om Haarlemmermeer binnen te komen en dat is gelukkig niet gelukt omdat wij wel 's avonds nog wakker waren. Dus het zijn vaak juist mensen waar je het niet van verwacht, dus ook jongetjes van veertien, vijftien jaar die dit beroepsmatig ook doen en het ook leuk vinden en vaak ook binnenkomen, niet alleen bij de gemeente, maar ook bij andere overheidsinstanties. Daar moet u wel goed rekening mee houden.

De VOORZITTER: Mijnheer Meijer, de volgende keer een vraag.

De heer MEIJER: Bent u het met mij eens, mijnheer Spijker?

De heer SPIJKER: Mijnheer Meijer, deels ben ik het met u eens, leeftijd maakt niet uit, daar heeft u volkomen gelijk in want het maakt niet uit of iemand veertien is of 88. Dat is om het even. Die zullen er misschien ook nog wel zijn, maar het gaat erom dat ik zei 'speels'. Ik zei als je het voor de gein doet, als je vriendje zegt 'kijk, we kunnen de gemeente Haarlemmermeer platgooien', of je bent een – laat ik het voorzichtig zeggen – grootmacht ergens op deze aardbol en je hebt gegevens van onze gemeente/Schiphol nodig, is dat een heel ander verhaal. Maar u heeft gelijk, leeftijd speelt geen rol daarin.
Dan zeg ik 'zorg voor een beter bewustzijn onder alle medewerkers en officiële gebruikers van de gemeente en zorg voor duidelijke richtlijnen, communicatie en feedback'. Als allerbelangrijkste aspect vindt EEN Haarlemmermeer dat we moeten voldoen aan de BIO want die wordt weer meerdere maken aangehaald, zeker op het gebied van meer risicomanagement.
Ook wij als gemeenteraad, dan pak ik zelf maar even de handschoen op, hebben een voorbeeldrol op het gebied van informatiebeveiliging dus wij staan zeker open voor nieuwe beleidskaders en krachtige veiligheidsprotocollen.
Dan de stelling 'moeten we de informatiebeveiliging uitbesteden aan externe partijen?' Ja, als wij de kracht niet in huis hebben, zullen we die moeten inhuren. Dat is logisch want we moeten absoluut investeren om inderdaad de beste van de klas te worden want ja, dat is heel, heel, heel belangrijk.
Dat was het voor de eerste termijn. Dank u wel.

De VOORZITTER: Dank u wel mijnheer Spijker. Dan mijnheer Schouten, GroenLinks.

De heer SCHOUTEN: Dank u wel voorzitter. Als eerste dank aan de Rekenkamercommissie voor het heldere rapport dat zij heeft opgeleverd. Het rapport Bewustwording als sleutel uit 2016 en dit vervolgrapport laten goed zien waar we staan. De gemeente is goed op weg, maar we zijn er nog niet. GroenLinks onderschrijft de conclusies en de aanbevelingen van het rapport.
De aanbevelingen:
Aanbeveling nr. 1, laat nog beter zien in de P&C-cyclus wat de doelen zijn, hoe die behaald zullen worden en laat zien dat ze zijn behaald. Wat kostte het en wat levert het op? Voldoen we al aan de COBIT/CMMI maturity level 2 die het college als doel heeft gesteld in 2016? En wanneer gaan we voldoen aan de wettelijke verplichte BIO-normen?
Aanbeveling nr. 2, inzetten op bewustwording. Niet eenmalig studeren voor een certificaat voordat je

je laptop ophaalt, maar regelmatig actualiseren en herhalen. Goed om te lezen dat eind vorig jaar opnieuw is ingezet op een hogere bewustwording door allerlei programma's en tools in te zetten.
Aanbeveling nr. 3, de organisatie rond de informatiebeveiliging moet goed worden opgetuigd. De tijdelijk ingehuurde CISO en twee privacy- en securitymedewerkers krijgen een permanente positie binnen de organisatiestructuur en gaan fulltime voor de gemeente aan de slag. Dit belooft veel goeds.
Aanbeveling nr. 4, voer regelmatig integrale audits en penetratietesten uit. Dit moet echt beter, systemen, processen en de IT-organisatie moeten regelmatig onder de loep genomen worden.
Aanbeveling nr. 5, zorg voor goede signalering en monitoring. Houd je systeem in de gaten zodat je snel kunt schakelen bij incidenten. Dit is een vrij ingewikkelde, technische bezigheid en het is goed te lezen dat KPN hiervoor wordt ingezet. 100% veilig bestaat niet, dat is onbetaalbaar en onwerkbaar. In de slotbeschouwing van het rapport wordt de vraag gesteld of de gemeente wel in staat is om zelfstandig de informatiebeveiliging op orde te krijgen. Ook een goede vraag voor de CISO. Niet zelf het wiel opnieuw uitvinden, maar met vergelijkbare gemeenten samenwerken. Tot zover, voorzitter.

De VOORZITTER: Dank u wel. Dan de heer Koning van het CDA.

De heer KONING: Dank u wel voorzitter, we danken de Rekenkamercommissie voor het vervolgonderzoek Informatiebeveiliging. De vraag dringt zich echter op 'is het glas nu halfvol of halfleeg?' In elk geval kan vastgesteld worden dat het college elke aanbeveling van de raad heeft opgepakt, maar dat het nog niet klaar is met alles. Maar er is ook niet opgedragen dat het allemaal in vier jaar af moest. Zo moet de wettelijk verplichte BIO nog ingevoerd worden, die op 1 januari jl. verplicht is geworden. Het college maakt dit ondergeschikt aan een risicogestuurde werkwijze. Ongetwijfeld nuttig, de Rekenkamercommissie onderschrijft dit, maar het voldoen aan een wettelijke verplichting dient voorop te staan. Overigens is mij gebleken dat die BIO in nog geen enkele gemeente is ingevoerd.
Dan het verhogen van de bewustwording ten aanzien van de informatiebeveiliging. Er is een verplichte cursus opgelegd als voorwaarde voor het verkrijgen van een laptop en er zijn diverse campagnes gevoerd. Er is een nieuwe actie, waarbij het halen van een certificaat verplicht is en er worden opnieuw campagnes gevoerd om het e-bewustzijn te verhogen. Bovendien is er een interne website gemaakt met specifieke informatie over informatiebeveiliging. Mijn fractie oordeelt dat er voldoende inspanning is geleverd. Als de coronacrisis een ding heeft geleerd, is het wel dat Nederlanders ontzettend moeilijk zijn te motiveren om evidente maatregelen op te volgen. Dat komt deels doordat alles veel te vrijblijvend is, maar in de relatie werkgever-werknemer kan het verplichtend worden opgelegd en dat is ook gebeurd. Maar dat betekent natuurlijk niet dat iedereen intrinsiek van de noodzaak overtuigd is.
De information security officer is een interim-functie die vooralsnog bij Info Plus is ondergebracht. Het advies was echter deze functie als een strategische staffunctie te positioneren zodat deze een organisatiebreed mandaat zou krijgen. Inmiddels is besloten deze functie bij de corporate controller onder te brengen zodat ook aan deze voorwaarde volledig is voldaan. Voor het overige heeft het college zich voldoende ingespannen om aanbeveling 3 te realiseren.
Aanbeveling 4, voer regelmatig een integrale audit of penetrationtesten uit. Ik wist niet wat dat laatste was, dus ik heb dat opgezocht op internet en ben tot de conclusie gekomen dat daar toch vrij eenvoudig voldoende vrijwilligers voor te vinden zijn. Het is bovendien verplicht op grond van de BIO, maar de Rekenkamercommissie spreekt van een bescheiden aantal niet-integrale audits en pentesten in aanvulling op wat de gemeente verplicht is. We concluderen hieruit dat de gemeente dus wel aan de wettelijke verplichtingen voldoet.
Aanbeveling 5, investeren in de ontwikkeling van monitoring en signalering. Deze dient om te voorkomen dat alleen reactief wordt gereageerd. Door het uit te besteden bij de KPN meent mijn fractie dat adequaat is gereageerd. Aan de geamendeerde aanbeveling is volledig voldaan.
Kortom, mijn fractie is best tevreden over wat de afgelopen periode is gerealiseerd. Het is nu eenmaal

taaie materie waarbij het zeer moeilijk is om de juiste mensen te werven. Dus wat het CDA betreft, is het glas voller dan de Rekenkamercommissie concludeert. Over de twee nieuwe aanbevelingen kan ik kort zijn, die zullen we overnemen.
Dan nog een kritisch geluid richting de Rekenkamercommissie. In de slotbeschouwing staat 'Tijdens dit onderzoek bekroop de RKC de vraag of de gemeente geheel zelfstandig de informatiebeveiliging op orde kan krijgen. We hebben dit in dit vervolgonderzoek niet expliciet onderzocht.' Mijn fractie vindt dit niet kunnen. De Rekenkamercommissie moet zich beroepen op feiten en bevindingen en niet op gevoelens die hen bekruipen. En dat terwijl het vervolgonderzoek juist heeft aangetoond dat er op veel vlakken vooruitgang is geboekt. Eigenlijk zeg je 'we betwijfelen of jullie dit wel aan kunnen', zonder dit onderzocht te hebben en een organisatie kan zich heel moeilijk verdedigen tegen dergelijke gevoelens. Daarom moet het vermeden worden.
Dan de stellingen. Stelling 1, of we zo veel mogelijk moeten uitbesteden. In de brief van 9 februari 2018 staat dat vrijwel alle generieke IT-voorzieningen in de afgelopen jaren aan marktpartijen zijn uitbesteed. Voor onze Info Plus resteert dan slechts een regiefunctie.
Stelling 2, informatiebeveiliging is wel een thema voor de gemeenteraad, maar op afstand. Wij moeten overtuigd worden dat het naar behoren is geregeld.
Stelling 3. Wij hoeven echt niet de meest informatieveilige gemeente van Nederland te worden want dit kost al genoeg.
Stelling 4. We moeten meer samenwerken met andere gemeenten. Als dit nuttig en noodzakelijk is dan wel, maar ik waarschuw: we hebben al een keer een volledig uitgewerkt voorstel gehad om met Haarlem samen te werken. En ook met Amstelveen. Maar dat is toen door de raad afgeschoten en samenwerking geeft altijd gedonder over de wederzijdse financiële bijdragen en over de prioriteiten. Kijk maar naar Zandvoort-Haarlem en kijk maar naar Aalsmeer-Amstelveen. Het is gewoon stammenoorlog. Bovendien ontstaat zo een nieuwe bestuurslaag waar over alles overlegd moet worden. Onze voorkeur heeft het om het op eigen kracht te doen, doeltreffend, en niet de samenwerking met een andere gemeente te zoeken.

De VOORZITTER: Gaat u afronden, mijnheer Koning?

De heer KONING: Ja, dit is mijn laatste zin. Stelling 5, de gemeenteraad heeft volgens ons geen voorbeeldfunctie op het gebied van informatiebeveiliging. Tot zover, dank u wel.

De VOORZITTER: Dank u wel mijnheer Koning. De Rekenkamercommissie is hier vanwege de coronamaatregelen uiteraard niet aanwezig maar zal ongetwijfeld op afstand meekijken en mag reageren op uw punten op het rapport. Ik heb nog drie partijen die zich nog niet gemeld hebben. Inmiddels heeft er zich een daarvan wel gemeld, mijnheer Meijer, Forza!

De heer MEIJER: Dank u voorzitter. Laat ik beginnen te zeggen dat ik het heel erg knap vind dat de heer Koning zijn hele spreektijd kan vullen met dit onderwerp. Ik kreeg deze sessie onder ogen en dacht 'dat gaat helemaal mis natuurlijk', maar toen las ik het Rekenkamerrapport en dacht ik 'ja, gaat het nou slecht, kan het beter?' Ja, het kan altijd beter natuurlijk. Maar zoals ik net ook al zei, in ogenschouw nemend wat hier tien jaar geleden gebeurde en hoe het nu gaat, is mijn fractie is erg tevreden. Ik denk dat we een ding vergeten en ik ga het toch aanstippen, dat is ons eigen gedrag. Hoe we zelf omgaan met onze mobiele telefoons en onze laptops. De fractievoorzitters hebben laatst een kleine inkijk daarin gehad van een expert die ook bij onze gemeente nu werkzaam is. Als je ziet hoe makkelijk je gehackt kan worden… Ik geef een voorbeeld: de secretaresse van Carel Brugman kreeg op vrijdagavond een mailtje 'wil je even € 6 miljoen over maken op dit en dit adres, dat moet vanavond nog weg'. Als je niet beter weet, denk je 'mijn baas vraagt wat, dan doe ik het'. Maar toen ze naar de bovenste lijn keek, stond daar geen Carel Brugman, maar iets van, ik kan dat niet uitspreken, maar een heel andere extensie. Zo makkelijk kan het gaan. Daar heb ik zelf ook wel eens last van, dat je

een e-mail binnenkrijgt en je opent hem, dan blijkt het een phishing-e-mail te zijn. Jullie krijgen allemaal de informatie nog een keer van deze expert, dat is heel interessant om een keer mee te maken. Ik heb het al eerder gezegd, er is een externe DDoS-aanval geweest en er zijn universiteiten die miljoenen euro's hebben moeten betalen om hun gegevens terug te krijgen. Er is ook gebleken dat onze gemeente heel interessant is voor Russische hackers. Dat heeft met name te maken met wat er op Schiphol gebeurt, met rechtszaken tegen Oekraïne en het ongeluk dat boven Oekraïne is gebeurd. Ik denk dat een stukje bewustwording bij ons allen geen kwaad kan.
Heb ik dan nog kritiek? Ja natuurlijk heb ik kritiek, dat kan altijd. Er worden nu externe mensen ingevlogen en dat kost meestal meer dan wanneer je ze in eigen huis hebt. Die kosten weet ik nu niet precies, maar die krijgen we vast nog wel eens te horen.
Wij onderschrijven de conclusies van de Rekenkamercommissie zeer zeker. Ik denk dat we echt op de goede weg zijn en daar wil ik ook mijn complimenten voor uitdelen, ook aan de mensen die ons veilig houden en zorgen dat onze problematiek niet op straat komt te liggen.
Verder hoeven we echt niet de nr. 1 gemeente te worden als het gaat om veiligheid. Wel veiligheid op straat, maar dat is een ander onderwerp. Ik denk dat de gemeente goed bezig en dat het, als we zo doorgaan, wel goed komt. Dank u wel voorzitter.

De VOORZITTER: Dank u wel mijnheer Meijer. Ik zie nog een hand, mijnheer Beusenberg, SRH.

De heer BEUSENBERG: Dank u wel voorzitter. Ik kan heel kort zijn. Ik heb er totaal geen verstand van maar het enige dat ik wil weten van de wethouder is: worden we als raadsleden beschermd tegen aanvallen van buitenaf? Ook ik was bij die informatieve sessie en ik schrok daar…

De VOORZITTER: Ik wil daar even op reageren, dat was geen informatieve sessie, dat was informatie in het seniorenconvent. Ik wil dat graag even meegeven.

De heer BEUSENBERG: O sorry, dan was het informatie in het seniorenconvent, maar het komt op hetzelfde neer. Het ging over dat er van alle kanten aanvallen van buitenaf komen en daar was ik wel een beetje van geschrokken. Maar ik was vergeten te vragen of we als raadsleden beschermd zijn tegen die aanvallen van buitenaf en of dat dan ook gecoördineerd wordt binnen de gemeente om te zorgen dat wij veilig ons werk kunnen blijven uitoefenen. Dat was het, voorzitter.

De VOORZITTER: Dank u wel mijnheer Beusenberg. Ik zal daar alvast even op reageren omdat er net van links wordt gezegd dat er sowieso in oktober een informatieve sessie plaatsvindt over dit onderwerp, sterker nog, op 1 oktober a.s. Mijnheer Werner, u bent als laatste aan de beurt. VVD.

De heer WERNER: Dank u wel voorzitter. De VVD-fractie wil de Rekenkamercommissie bedanken voor het heldere vervolgonderzoek naar de informatiebeveiliging. Vijf aanbevelingen uit het rapport uit 2016 zijn zo goed als ongewijzigd met een amendement door het college en de raad overgenomen. Het rapport geeft helder en duidelijk weer waar wel en niet aan is voldaan. Nu kan ik, net als mijn collega's al die aandachtspunten 1 tot en met 5 nog een keer langslopen, maar het lijkt me niet echt zinvol omdat het meeste daarover al is gezegd.
Het rapport toont aan dat er door het college stappen in de goede richting zijn gezet in de afgelopen jaren. De VVD-fractie vindt het van belang dat juist in een tijd waarin steeds meer digitaal gaat, zaken op orde zijn. In de bestuurlijke reactie op het rapport van de Rekenkamercommissie lezen we dat het college zaken serieus oppakt. Zo zal de interim-CISO in vaste dienst treden en zal er begin 2021 een nieuw geactualiseerd beleidsdocument aan de raad worden aangeboden. Hiermee geeft het college aan de nieuwe aanbevelingen van de Rekenkamercommissie ter harte te nemen.
Ik heb nog wel een paar vragen aan het college. Wanneer is begin 2021 voor wat betreft het nieuwe beleidsdocument? Kunnen we daar een datum of een kwartaal voor krijgen?

Wanneer komt de CISO in vaste dienst, want ik denk dat dat een belangrijke is. En wanneer denkt het college te voldoen aan de wettelijke richtlijnen van BIO? Dat was onze inbreng. Dank u wel.

De VOORZITTER: Dank u wel mijnheer Werner. Dan kijk ik naar mijn rechterzijde, naar de portefeuillehouder, mevrouw Booij.

Wethouder BOOIJ: Dank u wel voorzitter. Ik zat nog even te schrijven. Misschien kan ik daarmee beginnen, mijnheer Werner. De interim-CISO die we nu hebben is niet per definitie de CISO die we in dienst gaan nemen. We gaan een CISO in dienst nemen en we zijn heel hard aan het zoeken, maar zoals de meesten van u wel weten, zijn de goede ICT-jongens heel moeilijk te pakken te krijgen. Nee, dat moet ik anders zeggen, voor mensen die in de ICT werken en heel goed zijn, zijn er heel veel kapers op de kust. We zijn heel hard aan het zoeken en wie weet kunnen we nog iets met deze CISO, dat we die kunnen houden. Maar dat evenzo dat u niet teleurgesteld bent als we volgende week iemand anders aangenomen blijken te hebben.
De informatie waar u naar vroeg over het nieuwe rapport over het informatiebeleid krijgt u in Q1 2021.
Maar laat ik even beginnen, want dat vergeet ik nu bijna in mijn enthousiasme, met de Rekenkamercommissie te bedanken voor dit onderzoek. We leren er elke keer weer van. De aanbevelingen hebben we, zoals de meesten van u ook zeiden, grotendeels opgevolgd want we zitten inmiddels alweer een tijdsbestek verder.
GroenLinks vroeg net wanneer het afgerond was en wanneer we de BIO dan gingen doen. Die vorige hebben we laten liggen omdat we overgegaan zijn op de BIO. Die bevat achttien hoofdstukken en 114 risicobeperkende maatregelen dus u begrijpt dat je dat niet in twee weken voor elkaar krijgt.
Daarnaast, dat zeiden sommigen van u ook, hebben we heel hard ingezet op 'wat is het meest urgent en waarvan vinden we zelf dat we het als eerste moeten doen?' Want je kunt daar natuurlijk ook keuzes in maken. En daarnaast hebben we ingezet op het risico beperken en op die beveiliging want dat vonden we heel erg belangrijk. U zei allemaal al dat je ziet dat het aantal aanvallen – laat ik het zo maar noemen, mijnheer Meijer – omhooggaat. Terecht dat u zegt 'er zijn veel meer aanvallen dan alleen maar van een hacker'. Andere mogendheden, het zou u verbazen hoeveel mensen graag in Haarlemmermeer zouden willen inbreken om zo op die manier bij onze partners terecht te komen, want daar ben je natuurlijk zo. En u zegt ook terecht, mijnheer Meijer, u heeft daar zelf verantwoordelijkheid in. Dat zei mijnheer Beusenberg ook. Op het moment dat u hier binnen bent, wordt u beveiligd door ons internet en onze firewalls en dat soort dingen, onze security. Daar zorgen we voor. Maar op het moment dat u zelf denkt dat u die mail wel kunt openen waarvan u niet weet waar die vandaan komt, ligt dat toch echt aan u. Ik kan u vertellen dat ik deze afgelopen week en een phishing-e-mail heb gekregen, een ransom-e-mail/sms heb gekregen, smishing heet dat geloof ik, en als laatste gecatfished ben voor het eerst van mijn leven. Mijn tante uit Amerika deed zich voor als zeer bezorgd en wilde mij wel een fortuin toekennen. Hartstikke leuk natuurlijk, alleen heeft mijn tante in Amerika geen fortuin dus ik zou niet weten hoe ze eraan komt. Het was de eerste keer dat ze zoiets deed. Maar zo makkelijk gaat dat. Onverwacht kun je iets binnen krijgen waarvan je denkt 'o wat leuk, mijn tante uit Amerika', en dan kom je er gaandeweg achter dat het helemaal niet zo is. Dat gebeurt ook met de e-mails die u krijgt. U weet natuurlijk allemaal dat ze steeds professioneler worden en dat betekent voor ons dat we heel sterk hebben ingezet op die bewustwording van ons allemaal want u heeft daar zelf ook wel degelijk een rol in, het is niet zo dat u achterover kunt leunen en denken 'die gemeente regelt dat wel'. U bent zelf ook verantwoordelijk voor wat u binnenhaalt. Sommigen van u zeiden dat ook al, we doen allemaal, ook wij als college, trainingen en we zitten op een percentage van 90% van mensen die regelmatig de nieuwe trainingen volgen. Dat is best veel, want die 10% zijn mensen die thuiszitten vanwege zwangerschapsverlof of langdurige ziekte. Dus dat is een respectabel aantal want ook in onze organisatie is doorgedrongen van die bewustwording, dat je ook zelf verantwoordelijk bent voor die veiligheid, en dat je dat niet alleen over kunt laten aan al die mensen die er ontzettend veel verstand van hebben waarvan we er gelukkig veel hebben in de gemeente,

maar dat je dat ook zelf moet doen.

De VOORZITTER: U krijgt een interruptie van mevrouw Koolmoes van HAP.

Mevrouw KOOLMOES: Dank u wel voorzitter. Ik heb er toch moeite mee dat u zegt dat we daar zelf verantwoordelijk voor zijn want als je aan het werk bent en je hebt een werkmail, denk ik dat je toch ook een beetje beschermd moet worden door de werkgever en dat het niet altijd je eigen verantwoordelijkheid is als er dan wat gebeurt. Uiteraard wel voor je privé-e-mail.

De VOORZITTER: Moment want ik zie nog twee interrupties op hetzelfde onderwerp. Mijnheer Meijer van Forza!

De heer MEIJER: Ik wil even reageren op mevrouw Koolmoes. Volgens mij maakt u zelf een e-mail-account aan. Dat doet de gemeente niet voor u en daar bent u zelf verantwoordelijk voor. De e-mailtjes die de gemeente naar u stuurt, komen naar het adres dat u zelf heeft aangemaakt. Dus dan kun je Gmail hebben of Hotmail of ik weet niet wat, maar daar zijn ook gradaties in qua veiligheid. Daar is de gemeente niet voor verantwoordelijk.

De VOORZITTER: Mevrouw Koolmoes wil even reageren op mijnheer Meijer, vermoed ik.

Mevrouw KOOLMOES: Dank u wel voorzitter. Ik denk dat we elkaar verkeerd begrijpen. Ik heb natuurlijk privé-e-mail die je zelf aanmaakt, maar vaak als je bij een bedrijf komt te werken, gebruik je daar een bedrijfse-mail die het bedrijf voor je aanmaakt en die e-mail is niet de verantwoording van degene die hem gebruikt, blijkbaar.

De VOORZITTER: Ik wil even terug naar de wethouder.

Wethouder BOOIJ: Ik ben dat niet met u eens, we proberen aan de voordeur of achterdeur, dat is maar net aan welke kant je binnenkomt, zo veel mogelijk af te vangen. Daar hebben we systemen voor. U heeft zelf in het document kunnen lezen dat we deals hebben met KPN en weet ik veel wie allemaal en wat er allemaal tussen zit. We doen pentesten, meer dan een, we doen audits en we volgen al die aanbevelingen op die in dat ding staan, maar op het moment dat u denkt dat u van mijnheer Meijer een hartstikke leuke e-mail binnenkrijgt en mijnheer Meijer vraagt u om door te klikken omdat u een uitnodiging krijgt voor een feest en u checkt niet of die e-mail wel van mijnheer Meijer is, dan bent u wel degelijk zelf in control want ik kan dat er niet voor u uithalen. Dat is wat er nu gebeurt, intern ook, dat je een e-mail krijgt van iemand die je kent, waarvan je denkt 'die ken ik, daar werk ik al heel lang mee', en dan klik je ongemerkt door. En dan is het al te laat want dan heb je de poort al open gezet en dat is waar u zelf bewust van moet zijn.

De VOORZITTER: Ik ga u onderbreken en ik ga naar mijnheer Beusenberg. Dat is wat mij betreft het laatste over dit onderwerp en daarna wil ik de wethouder vragen terug te gaan naar de vragen die er nog liggen. Mijnheer Beusenberg.

De heer BEUSENBERG: Dank u. Die uitleg van de wethouder begrijp ik, maar dan is mijn vraag: wordt daar vanuit de gemeente ook op toegezien of is het louter eigen verantwoordelijkheid?

De VOORZITTER: Dank u wel mijnheer Beusenberg. Mevrouw Booij.

Wethouder BOOIJ: Nee hoor mijnheer Beusenberg, zoals ik al zei, we hebben allerlei systemen die een heleboel dingen eruit kunnen halen. Als je echt een grote aanval krijgt, zoals waar mijnheer Meijer

het net over had, hebben we daar al een heel goed systeem voor dat ons daar ver van tevoren voor waarschuwt, of in ieder geval op tijd voor waarschuwt. We hebben ook een aantal dingen zo ingericht en dat doen we ook in samenwerking, we halen namelijk ook die ervaringen op bij andere gemeenten. Onze CISO is een samenwerking aangegaan met de CISO's in de provincie om ervaringen uit te kunnen wisselen met elkaar en om elkaar te kunnen helpen. Bijvoorbeeld grote Citrixaanvallen, mijnheer Meijer zei het al, daar hadden wij geen last van omdat onze CISO daar al van tevoren iets op had bedacht voor als zoiets zou gebeuren. Ik kan u dat wel uitleggen, maar het is heel technisch. Misschien zal hij dat zelf doen want 1 oktober a.s. krijgt u van hem als raad diezelfde lezing en informatieve bijeenkomst over wat beveiliging is en wat wij doen en wat u zelf kunt doen. Natuurlijk zien we daarop toe, maar ik kan niet zien wat u allemaal binnenkrijgt en soms glippen ze erdoor.

De VOORZITTER: Wethouder Booij, mag ik u onderbreken en vragen nu terug te gaan naar de vragen die er nog liggen, onder meer over het uitbesteden, het plan van aanpak en het stellen van doelen.

Wethouder BOOIJ: Ja, het plan van aanpak en het stellen van doelen hebben we al beschreven in een eerdere nota en dat staat ook in ons antwoord op de aanbevelingen van de Rekenkamer. En nu ben ik het eerste onderwerp kwijt, wat zei u nou?

De VOORZITTER: Er zijn verschillende vragen gesteld over 'moet het uitbesteed worden?'

Wethouder BOOIJ: O ja. We besteden al een heel groot deel uit en dat staat ook in het antwoord vermeld. Wethouder Horn, mijn voorganger, heeft al genoemd, in zijn brief uit 2018, dat we echt al heel veel uitbesteden en daar zijn we verder mee gegaan. Het zou zomaar kunnen zijn dat we dat straks nog meer gaan doen. Dat ontslaat ons niet van de plicht om wel zelf in control te blijven. We moeten zelf wel goed in de gaten houden wat er gebeurt met het werk dat we uitbesteden want je kunt het niet zo doen van 'doe jij het maar en ik leun achterover en het zal wel goed komen'. Zo werkt het niet. Er zit heel veel werk aan en we moeten dingen vernieuwen en we moeten die bewustwording op peil houden. U heeft van mij de afgelopen anderhalf jaar een aantal nota’s gekregen waarin ik u vraag om meerdere middelen voor nieuwe systemen, onder andere voor de beveiliging, en zo blijven we aan de gang.
Een van de stellingen is 'moeten we de veiligste gemeente van Nederland worden?' Ik denk dat dat een utopie is want op het moment dat we links de deur hebben dichtgedaan, weten ze rechts alweer onder die deur door te kruipen. We moeten continu alert zijn, continu op onze hoede zijn voor wat er om ons heen allemaal gebeurt. Dat betekent dat het heel fijn zou zijn als we op 90% zouden komen, maar of we de 100% ooit gaan halen? Dat denk ik niet. Ik denk dat we continu moeten blijven investeren in nieuwe systemen want zo snel gaat het, maar daar kom ik dan later wel weer bij u op terug met een nieuwe nota. Denk ik. Dank u wel.

De VOORZITTER: Dank u wel. We gaan naar de tweede termijn. We hebben nog ruimschoots de tijd maar de heer Koning heeft officieel geen spreektijd meer. Maar we kunnen kijken of we wat coulant kunnen zijn. Ik wil starten met de volgorde die we in de eerste ronde hadden. Dat is met mevrouw Hussain voor de tweede termijn, tenzij u zegt 'ik heb daar geen behoefte aan', dat is uiteraard ook mogelijk.

Mevrouw HUSSAIN: Op dit moment heb ik daar geen behoefte aan. De vragen waarmee ik zat, heeft de wethouder uitstekend beantwoord dus we kijken uit naar het volgende rapport en we kunnen het debat straks aangaan.

De VOORZITTER: Dank u wel. Mijnheer De Vries wilde nog wel graag reageren.

De heer DE VRIES: Ik wil zo meteen even met elkaar spreken over dat niveau van beveiliging want daar hebben diverse collega's wat over gezegd. Maar eerst vind ik het wel aardig om nog even de wethouder bij te vallen over 'waar ligt die verantwoordelijkheid?' Ik heb collega's horen vragen 'hoe word ik nu beveiligd?' En toen moest ik denken aan de bankpas. De banken doen er alles aan om ons banktegoed te beschermen, maar op het moment dat je je pincode in de portemonnee stopt waarin ook je bankpas zit, heb je een probleem met de bank. Dus in die zin heb je ook een eigen verantwoordelijkheid in dit verband en ook bij e-mailtjes die je krijgt.
Wat betreft het niveau van beveiliging. De veiligste gemeente van Nederland. Ik heb de heer Koning volgens mij horen zeggen dat dat onbetaalbaar is of het was mijnheer Schouten. Maar mijnheer Koning zei iets soortgelijks. Zeker als je de kosten bekijkt, vindt mijn fractie het niet zinvol om te streven naar het aller-, aller-, allerbeste beveiligingssysteem. Het streven zou moeten zijn: alles moet gewoon goed dicht zijn volgens de normen die ervoor staan. Dus de BIO met name. Dus het beste jongetje van de klas zijn is niet nodig, als maar wel alles gewoon veilig is. Wat vinden de collega's daarvan?

De VOORZITTER: Dank u wel mijnheer De Vries, even overleg met mijn linkerzijde, het is tweede termijn en we hebben nog drie kwartier dus ik zou die tijd vooral willen gebruiken voor debat en om op elkaar te reageren. Mevrouw Koolmoes.

Mevrouw KOOLMOES: Dank u wel voorzitter. Ik moet toch zeggen dat ik wat ik hier in de zaal proef allemaal nogal laf vind. 'We hoeven niet het veiligste jongetje van de klas te zijn, of de veiligste van Nederland'. Dat moeten we denk ik wel. We zijn niet te vergelijken met een gemeente als Groningen of Leeuwarden. Wij hebben een verhoogd risico met Schiphol in ons midden en ik denk echt dat we moeten streven naar het hoogst haalbare. En dan wordt er gezegd 'het kost zoveel', ja dus? Het is een heel gevaarlijk iets, dat hacken. Er kan heel gevaarlijke informatie op straat komen te liggen en het lijkt wel of men niet helemaal begrijpt hoe noodzakelijk het is dat we echt heel veilig zijn. Bij dezen.

De VOORZITTER: Dank u wel. Mijnheer Meijer wil daar graag op reageren.

De heer MEIJER: Ik denk dat iedereen wel begrijpt dat we veilig moeten zijn, maar ik begrijp niet zo goed wat Schiphol te maken heeft met ons raadhuis want daar praten we over. We praten niet over de veiligheid van Schiphol, maar over de veiligheid van onze ICT hier in Haarlemmermeer, in ons raadhuis. Dus ik vind dat die vergelijking helemaal niet opgaat. Je kunt wel het beste jongetje van de klas willen zijn, maar als het goed is, is het goed. En kan het beter? Ja het kan altijd beter, dat is altijd zo. Maar daar hangt ook een prijskaartje aan en zolang tegen ons wordt gezegd door de security experts dat we het goed doen, moeten we daar denk ik op vertrouwen. Bent u dat met mij eens?

De VOORZITTER: Dank u wel. Misschien zouden we een keer kunnen proberen het beste meisje van de klas te zijn? Mevrouw Koolmoes, wilt u daar nog op reageren?

Mevrouw KOOLMOES: Natuurlijk wil ik daar wel op reageren. Schiphol is bij ons in de gemeente en ik denk dat we daarom alleen al interessant zijn, ook voor mensen die niet weten dat we heel weinig over Schiphol te vertellen hebben. Ik denk dat we een verhoogd risico hebben vergeleken met andere gemeenten. Ik vind echt dat we daar gewoon heel scherp op moeten zijn. En dat zijn we gelukkig, want het is zoals mijn collega mijnheer Koning zegt, ook waar dat niemand nogal die normen van de BIO al op orde heeft. Ik hoor net dat het er 114 zijn.
Ik wil wel meteen nog een vraag stellen. Het is jammer dat de Rekenkamercommissie hier vanavond niet is.

De VOORZITTER: Dan ga ik u even onderbreken want mijnheer De Vries wilde nog reageren op wat hiervoor werd gezegd. Onthoud uw vraag even. Mijnheer De Vries.

De heer DE VRIES: Ik had net het voorbeeld van de bank. Laat ik het voorbeeld van de fiets erbij halen. Je kunt je fiets niet op slot zetten, dan is de kans heel erg groot dat hij er niet meer is als je terugkomt. Je kunt hem gewoon met je wielslot op slot zetten, je kunt er ook nog een ketting omheen doen om hem aan een fietsnietje vast te zetten. Je kunt ook vier sloten eromheen hangen en je voorwiel nog op slot zetten, maar de vraag is of dat nu is wat je wilt als je terugkomt en je moet al die sloten weer weghalen en de vraag is of dat iets toevoegt aan het simpelweg op slot zetten. Dat is een beetje wat ik soms proef in beveiligingen. Soms kom ik software tegen waarvan ik denk 'nou jongens, kom op zeg, waarvoor is dit nu nodig, om zo veel drievoudige beveiliging te hebben?'

De VOORZITTER: Mijnheer De Vries, u krijgt twee interrupties van mevrouw Hussain en de heer Werner.

Mevrouw HUSSAIN: Ik heb niet direct een interruptie op mijnheer De Vries maar op mevrouw Koolmoes van HAP dus ik weet niet of mijnheer De Vries dan zijn bijdrage eerst af moet maken?

De VOORZITTER: Mevrouw Hussain, gaat u vooral door.

Mevrouw HUSSAIN: We hebben het hier over 'beste', maar wat is dat dan eigenlijk het beste? IT en technologie wordt zo snel weer ingehaald, voor je het weet als je up-to-date bent, is er misschien wel weer iemand ergens ons aan het aanvallen middels een hack of een botnet of een DDoS. Dus wat is het beste? Het gaat vooral om bewustwording, om het creëren van awareness, dat we erop voorbereid zijn zodat als iemand zo'n aanval zou willen plegen, we dat allemaal kunnen tegenhouden. Ik denk dat dat ook echt de leidraad moet zijn.

De VOORZITTER: De heer Werner, VVD.

De heer WERNER: Dank u wel voorzitter. Ik denk dat het zaak is dat we die BIO eerst op orde hebben. Dat is een wettelijke verplichting en ik neem aan dat als die wettelijke verplichting goed ingevuld wordt, je dan al het beste jongetje van de klas bent.

De VOORZITTER: Of het beste meisje. Mijnheer Spijker.

De heer SPIJKER: Dank u wel voorzitter. Ik wilde ervan maken 'laten we de verstandigste persoon van de klas worden'. Ik denk dat dat handiger is dan de beste, misschien dat je dan creatiever kunt omgaan met security.

De VOORZITTER: Dank u wel mijnheer Spijker. Wil iemand daarop reageren? Mijnheer Schouten.

De heer SCHOUTEN: Ik wil in het algemeen reageren. In de BIO staat niets over Schiphol. Schiphol heeft ook niets te maken met informatiebeveiliging die wij hier in Haarlemmermeer doen. We hebben het even over verantwoordelijkheden gehad tijdens de termijn van de wethouder. Firewalls en virusscanners doen voor 110% hun werk. Ze hebben zelfs zelflerende mogelijkheden om kwade dingen buiten te houden maar ze houden gewoon niet alles tegen. Daarom is aanbeveling nr. 2 zo belangrijk, die bewustwording. We moeten dit samen klaren. Mensen moeten altijd blijven letten op: waar klik je op, waar ga je naartoe, hoe ziet het eruit, waar komt het vandaan? Dan slaan we een goede slag met elkaar. We moeten het samen doen.

De VOORZITTER: Dank u wel daarvoor. Ik kijk nog een keer rond, zijn er nog mensen die willen reageren? Ja, mijnheer Meijer.

De heer MEIJER: Ik wil nog even reageren op wat de wethouder zei in eerste termijn, als mevrouw Koolmoes een uitnodiging voor een feestje van mij zou krijgen, kan zij hem wegklikken want dat is echt phishing. Toen u nog bij Forza! zat, hadden we altijd leuke feestjes, maar als u nu een uitnodiging van mij krijgt, dan gewoon wegklikken.

De VOORZITTER: Nou mevrouw Koolmoes, dat is misschien een tip die u ter harte kunt nemen, wilt u daarop reageren?

Mevrouw KOOLMOES: Op sommige dingen moet je gewoon niet reageren. Ik wil alleen nog reageren op mijnheer De Vries. Als ik een fiets zou hebben, zou ik hem waarschijnlijk in zo'n huisje doen met een slot erop en stroom erop. Want ik vind echt dat de hoogste veiligheidsgraad belangrijk is en echt het streven moet zijn. Dank u wel.

De VOORZITTER: Dank u wel. Ik kijk nog een keer rond en ik heb het gevoel dat alles wel zo'n beetje gezegd is. Ik heb een toezegging gehoord van de wethouder dat het opvolgrapport over de informatievoorziening in Q1 2021 komt en de tweede toezegging is dat we een informatieavond krijgen op 1 oktober a.s.

Wethouder BOOIJ: Dat is niet mijn toezegging, maar die wordt al georganiseerd.

De VOORZITTER: Precies. Ik dank u allen hartelijk voor deze bijeenkomst en sluit… Excuus, u heeft helemaal gelijk. U moest uw vraag onthouden.

Mevrouw KOOLMOES: Voorzitter, zoals ik al zei, de Rekenkamercommissie is er niet maar misschien kan schriftelijk mijn vraag worden beantwoord want ik wil heel graag weten waarom de BBN-schalen niet genoemd zijn en waarom die niet onderzocht zijn. Die zijn toch een basis van risico's met een drietal standaardbeveiligingsniveaus en ik was daar eigenlijk wel nieuwsgierig naar. Het zijn Basis Beveiligingsniveaus, BBN.

De VOORZITTER: Portefeuillehouder, kunt u die schriftelijk beantwoorden?

Wethouder BOOIJ: Mag ik die vraag schriftelijk beantwoorden want u overvalt me daar nu mee. Dan moet ik zoeken en doe ik dat liever even schriftelijk.

Mevrouw KOOLMOES: Natuurlijk. Prima.

Wethouder BOOIJ: Dank u.

De VOORZITTER: Oké. De volgende keer weer even via de voorzitter graag. Ik hoor een toezegging van de wethouder en sluit ik bij dezen nu wel definitief de vergadering. Dank u wel.