Memo

Aan: **de leden van de gemeenteraad**

Van: **het college**

Datum: **1 november 2016**

Betreft: **verslag visitatiecommissie en penetratietest**

Medio 2015 heeft de visitatiecommissie Informatieveiligheid contact gezocht met de gemeente Leusden met de vraag of de gemeente Leusden vrijwillig wil meewerken aan een audit met betrekking tot informatieveiligheid in Leusden. Wij hebben hiermee ingestemd omdat Informatieveiligheid belangrijk is en wij ons graag laten toetsen om hiermee de informatieveiligheid te vergroten. De audit heeft plaatsgevonden in oktober 2015. Eind 2015 hebben we het definitieve verslag ontvangen. Bijgaand treft u het verslag aan. In het eerste kwartaal van 2016 ontvingen wij ook het verzoek van de Rekenkamer om een penetratietest op onze ICT omgeving te mogen uitvoeren. Ook hieraan hebben wij graag meegewerkt om reden dat wij door inzet van zogenaamde goede hackers echt inzicht krijgen in de kwaliteit van ICT veiligheid. Wij hebben besloten om de documenten, te weten het verslag van de visitatiecommissie, het rapport van de systeemtest en onze reactie op beide onderzoeken gezamenlijk aan u aan te bieden. Hieronder treft u onze reactie aan op beide documenten.

Penetratietest vanuit de rekenkamer

In opdracht van de Rekenkamercommissie Vallei en Veluwerand hebben onderzoekers van Hoffmann gedurende de maand maart 2016 een ICT beveiligingsscan ('Pentest') uitgevoerd op de infrastructuur van de gemeente Leusden. Deze scan is uitgevoerd op *de externe* infrastructuur en op de *interne* infrastructuren en systemen van de gemeente Leusden.
De *interne* pentest is uitgevoerd op locatie bij de gemeente Leusden. Daarbij is gekeken naar de mogelijkheden die een kwaadwillende heeft wanneer deze fysiek in het gebouw aanwezig is en bijvoorbeeld zijn laptop aansluit op het netwerk. Een ander scenario is die van een kwaadwillende die toegang heeft tot het interne netwerk van de gemeente Leusden door middel van het plaatsen van een virus of trojan (“achterdeur”).
Het *externe* onderzoek is uitgevoerd vanaf het internet en richt zich onder andere op de websites. Hierbij is het scenario gevolgd waarbij een kwaadwillende vanuit zijn eigen huis, of bijvoorbeeld een internetcafé, de systemen van de gemeente Leusden aanvalt.
Naast de technische testen is er in het kader van social enginering een phishing test uitgevoerd op de medewerkers en raadsleden van de gemeente Leusden.

Wij geven hieronder op hoofdlijnen de bevindingen van de onderzoeker aan en per bevinding geven wij onze reactie.

Interne penetratietest

- *Het is niet mogelijk directe toegang te krijgen tot het interne netwerk van de gemeente Leusden. In vergelijking met andere organisaties is het beveiligingsniveau in Leusden hoger dan gemiddeld.*

  Wij streven ernaar dit veiligheidsniveau als minimum te handhaven.

- *Er is een drietal kritieke kwetsbarheden geconstateerd in de beveiliging van printers/scanners. Zo was het voor onbevoegden mogelijk om inloggegevens te achterhalen die toegang geven tot onze kritieke systemen.*

  Wij hebben dit probleem dezelfde dag verholpen.

- *Er zijn incidentele kwetsbaarheden gevonden in de configuratie van systemen.*

  Wat betreft de aandachtspunten met de risicoclassificatie “Hoog” hebben wij alle aanbevelingen overgenomen. Gezien de consequenties voor het gebruik en beheer van onze applicaties en apparatuur is een acute aanpassing niet overal mogelijk en hebben wij de nodige acties in een planning opgenomen. De risico’s met de classificatie “Medium” zijn vooral het gevolg van het uitstellen van updates. Te snel installeren van updates levert het risico op dat updates niet juist blijken te zijn waardoor de continuïteit van de dienstverlening in het geding zou kunnen komen. Bij deze inschatting hebben wij alle zaken waar we een kritiek risico lopen direct verholpen. Voor zaken die in de planning staan en later worden uitgevoerd maken wij de inschatting dat er geen direct veiligheidsrisico is.

- *Geconstateerd is dat de gemeente Leusden gebruik maakt van voorspelbare en relatief eenvoudige wachtwoorden.*

  Dit is een bewuste keuze waarbij wij hebben overwogen dat sterke wachtwoorden moeilijker zijn te onthouden waardoor medewerkers onbedoeld zouden kunnen worden gestimuleerd deze wachtwoorden ergens te noteren. Het noteren van wachtwoorden zouden wij een ongewenste ontwikkeling vinden die nog grotere risico’s met zich meebrengt. Toch nemen wij de aanbeveling over door een herziening van ons wachtwoordbeleid mee te nemen met de verplichte implementatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Externe penetratietest

- *Tijdens de externe penetratietest zijn geen vertrouwelijke gegevens aangetroffen.*

  Wij zijn zeer gelukkig met dit resultaat en streven ernaar dit ook zo te houden. Tegelijkertijd realiseren wij ons dat 100% veiligheid helaas niet bestaat.

- *Leusden maakt gebruik van niet versleutelde verbindingen bij met name loginformulieren op de websites www.leusden.nl en raadsplein.leusden.nl. Aanvallers zouden hierdoor logingegevens kunnen bemachtigen.*

  Wij hebben de betreffende aanbevelingen overgenomen. Op deze punten vindt
  afstemming plaats met onze leveranciers en worden de noodzakelijke maatregelen getroffen om de risico's af te dekken.

Social Engineering (phishing test)

- *De resultaten van de phishing actie laten zien dat een groot deel van de medewerkers van de gemeente Leusden niet alert genoeg is op het herkennen van phishing. Ruim 30% heeft zijn/haar logingegevens afgegeven op een website die buiten het domein van de gemeente Leusden ligt.*

  Wij realiseren ons dat de menselijke factor een cruciale rol speelt bij de beveiliging van informatie en dat training van medewerkers noodzakelijk is om risico's en gevaren te herkennen. Wij hebben over deze actie van de rekenkamer reeds intern gecommuniceerd. In het najaar zullen we een bewustwordingscampagne voeren.
  Wij nemen alle aanbevelingen mee met de verplichte implementatie van de Baseline Informatiebeveiliging Nederlandse gemeenten (BIG)

WiFI

- *Op de draadloze netwerken van de gemeente Leusden zijn geen belangrijke bevindingen gedaan.*

  Wij streven ernaar deze situatie te handhaven.

Door het uitvoeren van deze test hebben wij zicht gekregen op een aantal risicovolle plekken in onze ICT omgeving. Wij hebben deze acute veiligheidsrisico's gerepareerd. Daarnaast nemen wij ook alle aanbevelingen van de rekenkamer over. Het is wel belangrijk te beseffen dat deze test een momentopname is. Bij volgende tests zullen er weer nieuwe risico's worden geduid omdat kwaadwillenden steeds modernere en verfijndere technieken tot hun beschikking hebben. Daarom is het jaarlijks laten uitvoeren van een penetratietest essentieel..

U heeft reeds de openbare oplegnotitie van de rekenkamercommissie toegestuurd gekregen. Een meer uitgebreid rapport ligt voor u ter inzage bij de griffier. De reden hiervan is dat in het rapport gedetailleerd wordt ingegaan op de architectuur van onze ICT systemen. Het is uit veiligheidsoverwegingen zeer ongewenst dat deze gegevens bij een grotere groep bekend worden.

Verslag VNG visitatiecommissie Informatieveiligheid

Het college kijkt terug op een open en leerzaam gesprek met de commissie. De VNG heeft deze commissie ingesteld om de bewustwording bij gemeenten met betrekking tot Informatieveiligheid te vergroten, eventuele manco's bloot te leggen en te stimuleren dat gemeenten van elkaar leren. De commissie doet de volgende aanbevelingen.

- *Breng scheiding aan in de rollen van CIO en CISO.*

  Deze scheiding is aangebracht. Wij hebben een medewerker aangesteld die voor 24 uur per week de rol van CISO vervult. De rol van CIO is binnen een andere functie belegd. De afgelopen periode is een aantal concrete maatregelen genomen:
  - Persoonsgegevens worden binnen de gemeente en Larikslaan2 niet meer per mail verstuurd maar via een beveiligde omgeving;
  - Er worden geen onbeveiligde USB-sticks meer gebruikt in situaties waarbij met gevoelige informatie wordt gewerkt;
  - De beperkte inlogmogelijkheden van externe medewerkers zijn nog verder ingeperkt;
  - Voor het Sociaal Domein (gemeente en Larikslaan 2) is tijdelijk een informatieadviseur aangesteld die de informatiearchitectuur in beeld brengt. Er is speciale aandacht voor privacy en informatieveiligheid en er is een aantal aanvullende maatregelen genomen, zoals een privacy scan bij LL2.

- *Informatieveiligheid beter verankeren in de portefeuille van de wethouder*

  Wij hebben deze aanbeveling overgenomen door wethouder J. Overweg te benoemen tot bestuurlijk verantwoordelijke voor de informatieveiligheid. Informatieveiligheid is vast onderdeel van het werkoverleg met de wethouder. Dit geldt zowel voor het overleg met de CISO als voor het overleg met de medewerkers binnen het Sociaal Domein.

- *Laat het topmanagement werken aan bewustwordingscampagnes.*

  Deze actie staat gepland voor het najaar van 2016. In het voorjaar is de aandacht gericht op het nemen van fysieke – en organisatorische maatregelen om de basis voor Informatieveiligheid te versterken. Bewustwording bij de medewerkers is echter een belangrijk onderdeel. Het onderzoek van Hoffman toont aan dat de mens de kwetsbare factor is waar het gaat om informatieveiligheid. Om die reden zullen wij in het najaar een interne informatiecampagne starten om de bewustwording te vergroten.

- *Afspraak maken met leveranciers over Informatieveiligheid*

  Dit advies zullen wij overnemen. Wij zullen met onze leveranciers in contact treden over dit onderwerp.

- *Versterken GIP structuur*

  Inmiddels is het GIP overgegaan in het Kernteam. De CISO is lid van het Kernteam. Het Kernteam richt zich op het informatiebeleid in brede zin en op de uitvoeringsagenda. Informatieveiligheid is een belangrijk onderdeel van het informatiebeleid en daarmee ook van het Kernteam.

- *Opstellen jaarplan Informatieveiligheid*

  In het kader van de ICT samenwerking met de gemeenten Bunschoten, Nijkerk, Putten en Leusden is besloten tot een gezamenlijke aanpak voor informatieveiligheid. De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) nemen wij hierbij als uitgangspunt. Hierin staat waaraan gemeenten op het gebied van informatieveiligheid minimaal moeten voldoen. Naast technische zaken zoals firewalls, virusscanning, logging en detectie, is er ook aandacht nodig rond de procedures en afspraken. Hierbij is het essentieel om rollen te beleggen binnen de organisatie en afspraken te maken over wie doet wat en bij wie kan je terecht met vragen over beveiliging, de security officer bijvoorbeeld. Deze moet bekend zijn en benoemd, zodat duidelijk is wie verantwoordelijk is voor de beveiliging. Daarnaast moeten er afspraken zijn over wie welke informatie mag zien en waarom. Hiermee slaan we twee vliegen in één klap. Hiermee voldoen we aan de landelijke richtlijn en de BIG is ook een gestructureerde aanpak waarmee we een Informatieveiligheidsplan maken.

Wij zijn blij dat wij vrijwillig hebben meegewerkt aan het interview met de auditcommissie en het verzoek van de rekenkamer om een penetratietest te mogen uitvoeren op ons ICT netwerk. Hiermee is een aantal risico’s blootgelegd dat wij anders nog niet in beeld hadden gehad. Wij zullen ook in de toekomst jaarlijks een penetratietest laten uitvoeren omdat informatie en informatieveiligheid van steeds groter belang zullen worden. Het onderzoek leert ons ook dat de menselijk factor per definitie de zwakste schakel is waar het gaat om informatieveiligheid. Wij hebben daarom direct een aantal maatregelen genomen en zijn aanvullend gestart met aandacht te besteden aan bewustwording bij ons personeel. Dir is een permanente actie.

Hiermee hopen wij u voldoende te hebben geïnformeerd over de penetratietest, het gesprek met de auditcommissie Informatieveiligheid en de naar aanleiding hiervan genomen maatregelen.

Wilt u deze onderwerpen bestuurlijk behandelen dan vragen wij u dit in samenhang te doen. Om die reden hebben wij de rapporten van beide onderwerpen gelijktijdig aangeboden.