Zaaknummer: 30373-2021
Documentnummer: 30373-2021:551307

Raadsinformatiebrief

Onderwerp
Raadsinformatiebrief Informatiebeveiliging: een terugblik, ontwikkelingen en een voortuitblik

Datum
10 juli 2021

Geachte leden van de raad,

Deze raadsinformatiebrief heeft als doel om u bij te praten over de ontwikkelingen rondom informatiebeveiliging. Er wordt hierbij aandacht besteed aan wat er om ons heen gebeurt, wat dit betekent voor de gemeente en wat de gemeente mede naar aanleiding hiervan onderneemt.

Terugblik

Vorig jaar is het strategisch informatiebeveiligingsbeleid van de gemeente vastgesteld. Dit beleid vormt het zogenaamde kapstokbeleid voor het opstellen en de uitvoering van het tactische en operationeel beleid. Om invulling te geven aan het tactische en operationele beleid, is er eind vorig jaar een onderzoek uitgevoerd om de noodzakelijke maatregelen te bepalen. Tijdens dit onderzoek is vanuit het geldend normenkader voor informatiebeveiliging (Baseline Informatiebeveiliging Overheid) gekeken in hoeverre de gemeente voldoet aan de verplichte maatregelen uit dit normenkader.

Naast dit onderzoek is er eind vorig jaar ook een gemeentebrede risico inventarisatie- en evaluatie uitgevoerd. Tijdens deze analyse zijn de gemeentebrede risico’s rondom informatiebeveiliging in beeld gebracht.

Deze onderzoeken hebben geleid tot het informatiebeveiligingsplan dat geldt voor de jaren 2021 t/m 2023. Dit plan vormt een samenhangend pakket aan maatregelen om informatiebeveiliging binnen de gemeente goed te organiseren. Hiermee worden de grootste risico’s rondom informatiebeveiliging zo veel mogelijk beperkt en zijn informatie, (persoons)gegevens en de verwerking hiervan in goede handen.

Het informatiebeveiligingsplan is niet statisch. Dit is omdat ontwikkelingen snel gaan, kwaadwillenden steeds inventiever worden en tegelijkertijd de gemeente weerbaar moet blijven. Nieuwe dreigingen en kwetsbaarheden worden vanuit risicomanagement beoordeeld en er wordt vervolgens gekeken of deze een plek krijgen in het informatiebeveiligingsplan.

Ondanks alle beleidstukken en plannen is het helaas een feit dat 100% bescherming niet bestaat. Het is de taak van de gemeente om met de gegeven middelen informatiebeveiliging zo goed mogelijk te organiseren.

Wat gebeurt er om ons heen?

Dreigingsbeeld informatiebeveiliging
In het meest recente dreigingsbeeld informatiebeveiliging Nederlandse gemeenten van de Informatiebeveiligingsdienst zijn de meest actuele dreigingen rondom informatiebeveiliging beschreven. De belangrijkste uitkomsten uit dit dreigingsbeeld worden hier beneden kort beschreven.

Bedrijfscontinuïteit in het geding
Er kunnen verschillende redenen zijn waardoor de continuïteit van de dienstverlening en processen in gevaar kunnen komen. Het kan bijvoorbeeld gaan om brand, een grote stroomstoring of een hack. Vooral de laatste dreiging weet vaak het nieuws te halen, zowel binnen als buiten de overheid.

Integriteit van gegevens is niet gewaarborgd en vertrouwelijke gegevens in verkeerde handen
Er bestaat een risico dat iemand bewust of onbewust gegevens kan wijzigen, wissen of toevoegen. Dit kan bijvoorbeeld gebeuren omdat een kwaadwillende zich toegang heeft verschaft tot gegevens of omdat een medewerker gegevens verwerkt waarvoor de medewerker eigenlijk geen toegang nodig heeft voor de werkzaamheden. Een e-mail aan een verkeerd e-mailadres of iemand die te veel toegangsrechten heeft zijn voorbeelden van risico's die inbreuk kunnen maken op de integriteit en vertrouwelijkheid van gegevens.

Imagoschade en financiële schade
De eerdergenoemde risico's kunnen het vertrouwen in de gemeente schade. Het vertrouwen in de gemeente hangt onder meer samen met de manier waarop de gemeente omgaat met gegevens. Inwoners en ondernemers moeten er op kunnen vertrouwen dat de gemeente gegevens op een passende manier beschermt en plannen uitvoert zoals ze zijn afgesproken. Naast het risico van imagoschade kan de gemeente ook financiële schade ervaren. Dit kan bijvoorbeeld doordat de Autoriteit Persoonsgegevens een boete oplegt, omdat de gemeente onzorgvuldig omgaat met persoonsgegevens. Hiernaast kan een kwaadwillende die zich toegang heeft verschaft tot het gemeentelijk netwerk, of het netwerk zelfs platlegt, losgeld eisen met de dreiging dat de kwaadwillende geen toegang meer verschaft aan de gemeente tot data of de dreiging dat zij gegevens gaan publiceren.

Gegevens in verkeerde handen
Onze gemeente wordt geacht om als goed huisvader om te gaan met de gegevens die ze onder haar hoede heeft. Als de informatie in verkeerde handen komt zijn de mogelijke gevolgen voor inwoners en ondernemers vaak niet te overzien. Voorbeelden hiervan zijn identiteitsdiefstal, identiteitsfraude of imagoschade van een inwoner omdat bekend is gemaakt dat de inwoner een bepaalde uitkering of zorg ontvangt.

Dienstverlening van de gemeente niet beschikbaar en ontwrichting van alledaagse processen
Als gevolg van een crisis kunnen inwoners en ondernemers de dupe worden als de dienstverlening van de gemeente niet of verminderd beschikbaar is. Dit kan leiden tot licht

ongemak wanneer een inwoner diensten of producten een paar dagen later geleverd krijgt of zelfs serieuze maatschappelijke, economische en sociale gevolgen als er sprake is van uitval van meerdere dagen of nog langer.

Enkele voorbeelden van dichtbij en uit het nieuws
Dat bovenstaande aangehaalde risico's zich helaas ook in de praktijk manifesteren blijkt uit onderstaande voorbeelden.

Citrix-gate
Tijdens de zogenaamde Citrix gate heeft de organisatie geleerd dat er ten tijde van een crisis de juiste mensen worden betrokken en dat zij samen de juiste maatregelen bepalen en implementeren. Ook werd echter duidelijk dat een gedegen calamiteiten- en continuiteitsplan noodzakelijk zijn om nog beter op soortgelijke bedreigingen te kunnen reageren. Daar is en wordt aan gewerkt. De gevolgen van Citrix-gate waren beperkt. Het werken op afstand is gedurende een korte periode afgesloten en er zijn kosten voor het inhuren van externe deskundigheid gemaakt. De gemeenteraad is hierover eerder geïnformeerd via de raadsinformatiebrief met dagtekening 21 januari 2019.

Gemeente Hof van Twente
Eind vorig jaar hadden hackers de computersystemen van gemeente Hof van Twente platgelegd en eisten de hackers losgeld. De gemeente heeft ervoor gekozen om hier geen gehoor aan te geven maar om (samen met een andere grotere gemeente) een nieuw en mogelijk veiliger ICT-netwerk te bouwen. Dit heeft natuurlijk heel veel invloed (gehad) op de continuïteit van de dienstverlening aan inwoners en ondernemers.

Senzer
In maart dit jaar is werkbedrijf Senzer slachtoffer geworden van een netwerkinbraak. Senzer had de juiste preventieve maatregelen genomen waardoor de impact beperkt is gebleven. Hierdoor heeft deze inbraak heel minimaal tot geen invloed gehad op de processen binnen de gemeente. Na deze netwerkinbraak heeft Senzer zogenaamde "lessons learned" gedeeld zodat andere organisaties hier iets van kunnen leren.

Vooruitblik

Zoals in de terugblik is beschreven, is er een meerjaren informatiebeveiligingsplan opgesteld. Twee belangrijke onderdelen uit dit plan zijn hier beneden kort beschreven. Het gaat om 2 onderwerpen waarmee de meeste dreigingen uit het dreigingsbeeld kunnen worden voorkomen, voor zover dit natuurlijk mogelijk is met de gegeven middelen.

Programma voor verhogen van bewustzijn en kennis
Onbewust menselijk handelen is de belangrijkste bedreiging voor de informatievoorziening van onze gemeente. Investeren in het structureel verhogen van de kennis en het besef bij medewerkers dat informatiebeveiliging en privacy belangrijk zijn, is een effectieve maatregel om dreigingen het hoofd te bieden. Daarom is er een meerjaren programma ontwikkeld met als doel de gemeente een handreiking te bieden voor een structurele aanpak van het verhogen van de kennis en het bewustzijn binnen de gemeente. Hiermee verkleinen we de

risico’s op onrechtmatige en onveilige verwerking van persoonsgegevens en wordt een veilige informatievoorziening beter gewaarborgd.

Naast dit programma is er ook een communicatieplan voor informatiebeveiliging opgesteld. Op basis hiervan wordt elke maand over verschillende (vooraf gekozen) onderwerpen een bericht geschreven en gedeeld via het intranet. Naast deze berichtgeving wordt er ook gecommuniceerd als er buiten de organisatie een incident heeft plaatsgevonden waarvan de kans reëel is dat dit ook in onze gemeente kan gebeuren. Ook wordt er gecommuniceerd als er binnen de gemeente een incident heeft plaatsgevonden en dit incident zich ook bij andere personen in de gemeente voor kan doen.

<u>Continuïteitsmanagement</u>
Gezien de dreigingen en de frequentie waarmee ze in heel Nederland lijken te gebeuren voert de gemeente dit jaar nog een onderzoek uit om te bepalen in hoeverre de gemeente de zaken al op orde heeft zodat de gemeente in een crisissituatie in elk geval de meest kritieke processen kan opstarten. Hiernaast wordt er in beeld gebracht of de ondersteunende middelen (bijvoorbeeld ICT) voor deze kritieke processen tijdens een crisis adequaat genoeg zijn.
Na de zomer zal in de commissie een presentatie over dit onderwerp komen, waarin een en ander nog nader besproken zal worden.

Bijlagen
Geen

Hoogachtend,

Het college van burgemeester en wethouders,

gemeentesecretaris van Laarbeek	de burgemeester van Laarbeek
	
J.W.M. van de Ven	F.L.J. van der Meijden