Informatienota

Datum vergadering	:	30 januari 2024
Registratienummer	:	GZDGWB1148999/1165628
Informatienummer	:	IN004
Portefeuillehouder	:	Burgemeester
Bijlage(n)	:	-
Onderwerp	:	Informatieveiligheid voor de gemeenteraad

Onderwerp
Informatieveiligheid voor de gemeenteraad

Kennisnemen van
Het besluit dat de faciliteiten en mobiele apparatuur die raadsleden in bruikleen hebben van de gemeente conform de Baseline Informatiebeveiliging Overheid (BIO) op het minimaal noodzakelijke beveiligingsniveau gebracht zal worden.

Inleiding
De digitalisering en afhankelijkheid van digitale middelen nemen zowel binnen de maatschappij als binnen onze organisatie toe. Met deze digitalisering nemen ook dreigingen op het gebied van cybercriminaliteit toe. Het landelijke dreigingsbeeld vanuit het Nationaal Cyber Security Center (NCSC) en de Informatie Beveiligingsdienst Gemeenten (VNG/IBD) bevestigen deze toename en spreken van een onverminderde toename waarbij incidenten een hoge impact hebben op de bedrijfsvoering, dienstverlening en het imago van de organisatie.

Het dreigingsbeeld op informatiebeveiliging neemt ook voor de gemeente West Betuwe toe.
Dit is niet alleen voor de interne organisatie maar ook voor het bestuur van toepassing.

De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). Had voorheen iedere overheidslaag zijn eigen baseline, nu is er met gezamenlijke inspanning één BIO voor de gehele overheid. Alle overheidslagen zijn met ingang van 1 januari 2019 gestart met de invoering van de BIO. Ook onze gemeente werkt, om de weerbaarheid op het gebied van informatieveiligheid te versterken, aan de implementatie van de BIO. Dit doen we door technische en organisatorische maatregelen toe te passen. Daarnaast werken we continu aan bewustwording van onze medewerkers.

Collegeleden en medewerkers werken dagelijks binnen de digitale informatievoorziening (het netwerk) van de gemeente West Betuwe. Voor deze doelgroep zijn verschillende maatregelen zoals het gebruik van sterke wachtwoorden, multifactor authenticatie en beveiliging van mobiele apparaten al actief. Dit is centraal geregeld en in beheer bij de ICT-afdeling van onze bedrijfsvoeringsorganisatie BWB.

Voor gemeenteraadsleden en hun informatievoorziening waaronder mobiele apparatuur is deze beveiliging nog niet centraal geregeld. Dit vormt een risico, niet alleen voor de raadsleden of de

fracties zelf, maar ook voor de bedrijfsvoering van de gemeente. Het is de verantwoordelijkheid van het college om middelen beschikbaar te stellen die veilig zijn en om te zorgen voor een ordentelijk beheer op onder andere deze mobiele apparatuur.

Onze gemeente werkt op ICT-gebied nauw samen met de gemeenten Culemborg en Tiel. Onze digitale informatievoorzieningen zijn met elkaar verbonden. Hierdoor is het effect van een digitale inbreuk direct merkbaar bij meerdere gemeenten. Een inbreuk binnen de gemeente West Betuwe treft dus ook onze partners. In theorie kan een geslaagde phishing-aanval op een raadslid van West Betuwe dus impact hebben op de dienstverlening van gemeenten Culemborg en Tiel.

Kernboodschap
1.1 Digitale informatievoorziening van raadsleden
De digitale informatievoorziening van raadsleden is nog niet conform de landelijke Baseline Informatiebeveiliging Overheid (BIO) ingericht. Dit is wel nodig.
Raadsleden maken deels gebruik van dezelfde digitale informatiemiddelen als medewerkers. Waar informatiebeveiligingsmaatregelen binnen de organisatie voor medewerkers zijn ingericht is dit voor voorzieningen van de gemeenteraad nog onvoldoende geregeld. Omdat raadsleden en medewerkers deels gebruik maken van één omgeving (bijvoorbeeld e-mail (Outlook en Microsoft 365)) kan een inbreuk bijvoorbeeld middels phishing bij een raadslid invloed hebben op de bedrijfsvoering en dienstverlening van de gemeente.

1.2 Rechtspositiebesluit decentrale politieke ambtsdragers
Het Rechtspositiebesluit decentrale politieke ambtsdragers geeft aan dat een raadslid, wethouder of de burgemeester voor het uitoefenen van zijn functie informatie- en communicatievoorzieningen ter beschikking krijgt. In artikel 3.3.2 van dit besluit staat dat het college van burgemeester en wethouders informatie- en communicatiemiddelen beschikbaar stelt aan onder andere een raadslid. Het college is dus verantwoordelijk. Evenzo is het de verantwoordelijkheid van het college om deze middelen ordentelijk te beheren. Het voldoende beveiligen van deze middelen is een belangrijk onderdeel van dit beheer.

1.3 Wereldwijde standaarden
Voor de beveiliging maken we gebruik van een wereldwijde standaarden. Microsoft Intune (voor Mobile Device Management) is een wereldwijde standaard voor de beveiliging van mobiele apparatuur. Voor de beveiliging van mobiele apparatuur kiest de organisatie daarmee een oplossing die nut en noodzaak inmiddels heeft bewezen. Deze oplossing is gebruiksvriendelijk en binnen de eigen organisatie al ingericht.

1.4 Beveiligingsmaatregelen zijn niet altijd even populair
Het nemen van maatregelen kan vaak het gevoel geven dat dit ten koste gaat van gebruiksvriendelijkheid en extra handelingen vereist. Informatiebeveiligingsincidenten ontstaan vaak vanuit het menselijke aspect. Om de menselijke verdedigingslinie te versterken, is bewustwording, houding en gedrag van bestuurders en medewerkers een belangrijke factor. Hierbij is het voorbeeldgedrag van het bestuur een belangrijk element.

Mobile Device Management (MDM) heeft primair als doel om mobiele apparaten in de zakelijke omgeving te beheren en te beveiligen. De nadruk ligt op het waarborgen van de veiligheid en beschikbaarheid van zakelijke informatie. Binnen onze gemeente wordt MDM ingezet om bedrijfsgegevens te beschermen, te voldoen aan de BIO, ons informatiebeveiligingsbeleid, en om zakelijke apps en diensten te beheren.

De inzet en het gebruik van MDM is strikt in overeenstemming met privacywetgeving, -regels en de BIO-richtlijnen. Om de privacy van gebruikers te waarborgen wordt een duidelijke scheiding gehandhaafd tussen de persoonlijke omgeving en apps van de gebruiker en de zakelijke omgeving van de organisatie.

1.5 Mobiele apparatuur is erg kwetsbaar en moet daarom worden beveiligd
Op mobiele apparatuur staat vaak veel vertrouwelijke- en persoonsinformatie. Daarnaast is deze apparatuur gevoelig voor verlies of diefstal. Als het apparaat onvoldoende is beveiligd en het in verkeerde handen terecht komt kan dit enorme nadelige gevolgen hebben voor betrokkenen en de organisatie. Daarom schrijft de BIO voor dat mobiele overheidsapparatuur moet worden beveiligd met een zogenaamde Mobiel Device Management oplossing. In ons geval is dit het toepassen van Microsoft Intune.

1.6 Een gestolen of verloren apparaat van een bestuurder is extra interessant
Politiek actieve personen zijn vanwege hun maatschappelijke rol voor onder andere de media extra interessant en daarmee kwetsbaarder. Een verloren of gevonden apparaat van een college- of raadslid zal meer impact hebben op de samenleving dan een mobiele telefoon van een scholier. Dit is een reden des te meer om een gestolen of verloren apparaat op afstand te kunnen wissen.

1.7 Bouwen aan Sterke Informatieveiligheid
Grote cyberincidenten zoals in Hof van Twente, Buren en recente aanval op 72 Duitse gemeenten op 3 november 2023, illustreren hoe belangrijk het is om als gemeenten de eigen informatieveiligheid op orde te hebben. Deze incidenten hebben niet alleen aanzienlijke schade toegebracht aan de betrokken gemeenten, maar hebben tevens geleid tot ernstige verstoringen van essentiële dienstverlening en het lekken van gevoelige informatie en persoonsgegevens van de inwoners.

Het beveiligen van digitale systemen is niet langer een keuze, maar een absolute prioriteit voor elke gemeente. Informatiebeveiliging is een voortdurend proces. Door de implementatie en regelmatige actualisatie van de noodzakelijke maatregelen op het gebied van informatiebeveiliging, kunnen we de kans en impact van dergelijke cyberincidenten minimaliseren. Een proactieve benadering vanuit de gemeenteraad en het bestuur is essentieel om te anticiperen op de voortdurend evoluerende dreigingen en de gemeentelijke systemen te beschermen tegen potentiële risico’s van cyberaanvallen.

Consequenties
De implementatie van passende maatregelen zorgt ervoor dat we kunnen voldoen aan wet- en regelgeving. Belangrijker nog is dat dit de veiligheid en continuïteit van onze producten, diensten en digitale middelen waarborgt, wat resulteert in kostenbesparingen voor de beheerorganisatie, vereenvoudiging van beheerwerkzaamheden, verhoogde productiviteit van gebruikers en de mogelijkheid om nieuwe applicaties en technologieën beschikbaar te stellen.
Het gebruik van nieuwe technologieën, zoals Single Sign-On (eenmalig inloggen in verschillende applicaties met één wachtwoord), optimaliseert en vereenvoudigt het inlogproces. Applicaties zoals Outlook, Word, Excel, PowerPoint, Topdesk en gemeenteoplossingen (GO) zijn dan met een druk op de knop op een veilige en gecontroleerde manier beschikbaar. Dit bevordert de efficiëntie en maakt een naadloze toegang tot belangrijke applicaties veilig en eenvoudig.

Het ontbreken van een MDM-installatie betekent dat de gemeenteraad zich afsluit van de gemeentelijke organisatie en beperkt wordt in het gebruik van nieuwe digitale middelen en ontwikkelingen op het gebied van informatiebeveiliging en digitalisering. Dit heeft tot gevolg dat het college niet in staat is de veiligheid en continuïteit van de aangeboden digitale middelen aan raads- en commissieleden te waarborgen.

Het is van cruciaal belang dat de gemeenteraad MDM implementeert om toegang te krijgen tot en te profiteren van de nieuwste digitale middelen en om de veiligheid en betrouwbaarheid van onze informatiesystemen te versterken. Hierbij is het voorbeeldgedrag van de raads- en commissieleden een belangrijk element.

Beveiliging van mobiele apparaten (MDM)
Vanaf maandag 27 februari 2024 kan men alleen nog werken met de Microsoft omgeving inclusief de zakelijke email als MDM op de juiste manier op de iPad geïnstalleerd is. De synchronisatie van niet-beveiligde apparaten wordt dan geblokkeerd. De toegang tot de zakelijke mailomgeving blijft wel beschikbaar via webmail op ”https://webmail.bvowb.nl/”. Let op: Dit is geen automatische synchronisatie, maar vereist regelmatig inloggen in combinatie met twee-factor-authenticatie (2FA).

Sterk wachtwoord
Sterke wachtwoorden zijn van essentieel belang voor het beschermen van gevoelige informatie en het voorkomen van identiteitsdiefstal. Momenteel zijn sterke wachtwoorden nog niet geïmplementeerd voor raads- en commissieleden. Vanaf begin volgend jaar streven we ernaar deze sterke wachtwoorden in te voeren. Dit betekent dat wachtwoorden maximaal 1 jaar geldig zijn en minimaal 12 karakters moeten bevatten, inclusief 1 hoofdletter, 1 kleine letter, 1 getal, en 1 vreemd teken.

2Factor authenticatie
Twee-factor-authenticatie (2FA) is een essentiële beveiligingsmaatregel. In tegenstelling tot alleen een wachtwoord, voegt 2FA een extra verificatiestap toe aan het inlogproces. Zelfs als het wachtwoord wordt blootgesteld, is er nog steeds een extra stap vereist, een eenmalige code op een telefoon of iPad. Dit maakt het voor kwaadwillenden aanzienlijk moeilijker om toegang te krijgen tot gevoelige informatie,

waardoor 2FA een noodzakelijke stap wordt om onze digitale identiteit en systemen te beschermen tegen cyberdreigingen.

Financiën
Het toepassen van beveiligingsmaatregelen voor de gemeenteraad heeft verder geen financiële consequenties. De basisinrichting is immers al gerealiseerd en licenties zijn beschikbaar.

Communicatie
Eind januari 2023 is tijdens een raadinformatiebijeenkomst een toelichting gegeven op de maatregelen die genomen moeten worden om de gemeenteraad op hetzelfde beveiligingsniveau te krijgen als de rest van de organisatie.

Vervolg
We streven ernaar om Microsoft Intune (Mobile Device Management (MDM)) in januari 2024 geïmplementeerd te hebben. In samenwerking met de ICT-afdeling worden inloopmomenten georganiseerd voorafgaand aan de raadsvergaderingen, waar raadsleden de mogelijkheid hebben om de installatie van Microsoft Intune uit te voeren. Raadsleden kunnen aan de hand van een handleiding deze installatie ook zelf uitvoeren.

Bijlage(n)
n.v.t.

Suggestie ter afhandeling
Voor kennisgeving aannemen

Burgemeester en wethouders van de gemeente West Betuwe,

de gemeentesecretaris,	de burgemeester,
Philip Bosman	Servaas Stoop