Vraag gemeenteraad:

Welke nadelen zijn er aan het gebruik van privé-accounts?

Antwoord:

Algemeen:
Raadsleden zijn politieke ambtsdragers. Politieke ambtsdrager hebben gezien hun taken en verantwoordelijkheden bij uitstek veel politiek-vertrouwelijke en privacygevoelige informatie. Deze informatie moet beschermd worden conform de geldende wet- en regelgeving. Voor gemeenten is de Baseline Informatiebeveiliging Overheid (BIO) het kader. Dit kader geldt ook voor politieke ambtsdragers.

De BIO geeft de normen aan waar wij als openbaar bestuur aan moeten voldoen. Met de aangeboden dienst (raad e-mailadres) weet u dat u als politiek ambtsdrager voldoet aan deze normen. De gemeenteraad is zelf verantwoordelijk om te voldoen aan de BIO.

Het gebruik van privé e-mailadressen is weliswaar niet expliciet verboden, maar wordt vanwege veiligheidsrisico's in het openbaar bestuur sterk afgeraden.

Nadelen aan het gebruik van privé e-mailadres.
Om goed antwoord te geven op deze vraag is het verstandig om dit te plaatsen in het perspectief van het huidig dreigingsbeeld. We schetsen hieronder drie scenario's.

- **Identiteit**
  Uw identiteit is op internet een zeer waardevol element. Met het overnemen van uw identiteit kan uw imago schade oplopen, uw partij imagoschade, de raad imagoschade of de gemeente imago schade oplopen.
  De gemeente heeft om u hiervoor te beschermen een aantal maatregelen geeffectueerd. Dit betreft een wachtwoordbeleid, tweefactor authenticatie maar ook beveiligingsinstellingen in Outlook. Deze instellingen worden aangebracht om de informatie te beschermen en het kwaadwilligen onmogelijk cq lastiger te maken. ICT kan verdachte inlogpogingen detecteren. Bij een privé email wordt u geacht al deze instellingen zelf aan te brengen en ook te beheren (conform de BIO).
- **Datalekken**
  Ter waarborging van de privacygevoelige informatie die opgeslagen zit in mailboxen heeft de gemeente allerlei overeenkomsten gesloten om dit goed te beschermen. Een privé mailbox heeft deze mogelijkheid veelal niet dan wel wordt de metadata van deze mailbox verhandeld voor advertenties.
- **Hack(pogingen)**
  De taak van de afdeling ICT is er mede voor om zoveel mogelijk de gegevens te beschermen tegen hackpogingen en eventueel snel actie te ondernemen. Bij een privé mailaccount heeft het team ICT hierin geen rol en dient u zelf actie te ondernemen.

Waarom is het onverstandig om mail door te sturen naar uw eigen prive e-mail?
Bij het standaard doorsturen van uw raads email naar uw prive email ontstaat de situatie dat u zelf moet zorgen dat u voldoet aan de normen van de BIO. Dit is gelijk aan de situatie dat u ervoor zou kiezen uitsluitend uw prive email te gebruiken.
Wij ontraden het doorsturen om de volgende redenen.

a. Het verlaat de veilige omgeving van de gemeente en gaat naar een wellicht onveiligere omgeving.
b. De Amerikaanse grote technologiereuzen ontraden doorsturen steeds meer. Immers bij automatisch doorsturen wordt dit langzaam maar zeker als spam of ongewenste email

beschouwd. Hiermee kunnen wij dus ook niet meer garanderen dat alle doorgestuurde email in de juiste postbus terechtkomt.

c. Bij het beantwoorden van email heeft de gemeente bepaalde controls ingericht zodat de ontvanger zeker weet dat u het afkomstig van de gemeente Woerden. Deze controls zijn niet standaard ingericht op uw prive email. Dat betekent dat een inwoner niet zeker weet dat u de verzender bent van een bepaald email bericht.

Waarborg:

- Vanwege de bijzondere positie van raadsleden zorgen wij voor scheiding tussen het college en de raad. Zo heeft het college geen mogelijkheid om uw agenda te zien. Ook geldt de ambtelijke richtlijn **niet** dat de gemeentesecretaris/ college ingeval van nood mail bekeken mag worden. Met de griffie gaan we nog een protocol opstellen om voor deze noodsituaties een proces af te stemmen.

Overzicht problemen gebruik prive mailaccounts:

Loggen
Als de gemeente de e-mailberichten voor raadsleden direct doorstuurt naar een ‘extern’ mailadres heeft zij geen controle meer over verder doorgestuurde berichten/informatie. Het externe e-mailverkeer kan niet worden gelogd.

Datalekken
De gemeente heeft geen controle over de privé-omgeving van een raadslid. Wordt hij/zij gehackt dan ontstaat er een datalek. Met formele samenwerkende partijen heeft de gemeente verwerkersovereenkomsten met veiligheidswaarborgen en controlemogelijkheden. Met raadsleden bestaan dergelijke overeenkomsten niet. Ook is verkeer moeilijk te traceren. Komt de e-mail bij de verkeerde ontvanger dan is het moeilijk te traceren als er ingewikkelde wegen worden gebruikt om mail te versturen.

Beveiliging door wachtwoord
De BIO-verplichting om een wachtwoord regelmatig te veranderen, kan voor de privé-IT/mailomgeving niet worden gecontroleerd.

Tweefactor authenticatie
Om het hacken van een mailaccount te voorkomen, werken we met extra beveiliging door SMS of gebruik van een authenticator-app op de mobiele telefoons. Dit maakt de toegang tot een account veel lastiger. Veel mailprogramma's bieden wel die functionaliteit maar wij kunnen deze niet verplichten voor de raadsleden op privé-accounts.

Veiligheid e-mail
Het Transport van e-mail gaat via het internet. Dat geeft veel mogelijkheden tot het onderscheppen van de berichten, zeker als de berichten onvoldoende beveiligd zijn.
Er zitten dus vele zwakke schakels in het transport van e-mail.
Meer info over veiligheid email **https://www.iusmentis.com/beveiliging/email/**

Filters en instellingen Microsoft 365
Microsoft doet steeds meer aan ‘security by design’. Dit betekent dat alle verdachte mails automatisch in spam of quarantaine gezet worden. Het automatisch doorzenden van mails wordt hierdoor steeds slechter ondersteund en zal tot gevolg hebben dat de mails niet doorgestuurd worden naar het mailadres van het raadslid maar terechtkomen in spam of quarantaine.

Afzender

Bij het eventueel verder doorsturen van mail ontstaat er een wijziging in afzender, namelijk uw eigen raads e-mailadres. Bij uw eigen privé of partij email adres zal een dergelijke e-mail betrouwbaarder lijken omdat u de afzender bent. Bij phising kan je vaak aan de afzender direct zien dat het bericht niet klopt. Dit is nu minder duidelijk zichtbaar.
Hiermee ontstaat dan het risico dat de ontvanger niet twijfelt aan de inhoud en dit als betrouwbaar opent en minder attent is op phising en spam.