

## Memo

onderwerp : Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten  
2023-2024  
datum : februari 2023  
zaaknummer : Z/23/104786/201601593  
van afdeling/ambtenaar : IBP/Philippe Hermans  
aan afdeling/directie/bestuur : Algemeen Bestuur GR 1Stroom

## Inleiding

De cybercriminaliteit is in onze samenleving niet meer weg te denken. Dagelijks vinden er incidenten plaats die ons allen veel ongemak bezorgen. Deze incidenten nemen jaarlijks toe.

Ook als gemeenten zijn we een potentieel doelwit. We hebben een grote verantwoordelijkheid om onze informatievoorziening te beveiligen en veilig te houden. De Baseline Informatiebeveiliging Overheid (BIO) beschrijft de controls en maatregelen die minimaal benodigd zijn om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie(systemen) te waarborgen.

We staan er niet alleen voor. De Informatiebeveiligingsdienst (IBD), onderdeel van de Vereniging van Nederlandse Gemeenten ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy.

## Digitale weerbaarheid

Informatiebeveiliging is een proces van plannen, uitvoeren, controleren en bijstellen (Plan-Do-Check-Act). We groeien in volwassenheid van informatiebeveiliging. De focus verschuift van reageren op incidenten naar het herkennen en voorkomen van incidenten.

Een digitaal weerbare gemeente kan potentiële incidenten vroegtijdig signaleren en de gevolgen ervan beperken, omdat de juiste maatregelen zijn getroffen. Als de basis door implementatie van de BIO op orde is, verhoogt dit de digitale weerbaarheid van gemeenten.

De IBD brengt jaarlijks een rapportage uit met daarin het actuele dreigingsbeeld over de informatiebeveiliging en benoemd de grootste risico's voor gemeenten van dit moment. Deze risico's verhogen de kans tot hoge herstelkosten, reputatieschade en minder vertrouwen in de overheid. Als bijlage is de rapportage *Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten 2023 → 2024* bijgevoegd.

## Succesfactoren

Zoals in het document benoemd wordt zijn de BIO en de AVG het vertrekpunt. We beschikken over veel gegevens en werken met veel applicaties en verschillende processen. Om de weerbaarheid te vergroten en de kans op een incident of crisis te verkleinen worden 6 succesfactoren benoemd: financiën, techniek, eigenaarschap management, organisatie, samenwerkingsverbanden en de factor mens. Ze beïnvloeden elkaar en voor het meest effectieve resultaat moeten ze in samenhang worden opgepakt. Deze factoren worden in samenwerking door RID en 1Stroom bewaakt.

## **Actuele Situatie**

De rapportage van de IBD schets het actuele dreigingsbeeld van de Nederlandse gemeenten. Hieronder wordt de actuele situatie van 1Stroom beschreven aan de hand van de benoemde succesfactoren.

### Financiën:

Vanuit de VNG is geadviseerd om jaarlijks een vast budget voor Informatiebeveiliging en privacy te reserveren en minimaal uit te gaan van 10% van het ICT-budget. De RID heeft op dit moment onvoldoende zicht op hoeveel budget er voor informatiebeveiliging gereserveerd is. N.a.v. de VNG-brief van Zanen, Cyberalert, eind 2021 is het ICT-budget wel verhoogd.

Daarnaast heeft in opdracht van de gemeenten Duiven, Westervoort en Zevenaar ICT-adviesbureau M&I/Partners onderzoek gedaan naar de robuustheid van de huidige ICT-samenwerking met RID de Liemers. Uit het rapport volgt het advies om de huidige ICT-samenwerking met RID de Liemers voort te zetten en te intensiveren, zodat zij de deelnemende organisaties op een adequate wijze kan ondersteunen op het gebied van informatisering en automatisering. De gemeenschappelijke regeling SDL, waar de RID onder valt zal hierover communiceren. Hierop vooruit lopend wordt vanuit beide colleges een kennisgeving naar de gemeenteraden gestuurd over dit toekomstscenario en de (mogelijke) financiële consequenties daarvan. Als winstwaarschuwing wordt nu afgegeven dat er bij de RID extra middelen nodig zullen zijn.

### Techniek:

De kans om slachtoffer te worden van een aanval met ransomware (oftewel gijzelsoftware) is sterk toegenomen. Het is van belang dat de basismaatregelen op orde zijn. Dit was ook de strekking van de VNG-brief van Zanen. Een aantal maatregelen zijn direct opgepakt en voor andere maatregelen zijn middelen beschikbaar gesteld. Door de transitie RID kunnen deze pas in 2023 worden uitgevoerd. Een belangrijke maatregel hierbij is de netwerksegmentering. Wat betreft monitoring & response neemt 1Stroom deel aan een landelijk traject van aanbesteding o.l.v. de VNG en ondersteund door de IBD. Hierdoor is het mogelijk om de kennis en kunde te benutten en inkoopvoordeel te behalen. Een eerder ingezet traject met de KPN is daarom vorig jaar beëindigd. In 2023 wordt een crisis(cyber) oefening gehouden i.s.m. OOV met de focus op continuïteit.

### Eigenaarschap management:

Voor de borging wordt regulier overleg gevoerd met de portefeuillehouders en de directie. Een belangrijke taak is het bewustzijn onder bestuurders, managers en medewerkers te vergroten. De afgelopen jaren is hier minder aandacht voor geweest. 1Stroom doet hiervoor momenteel mee met het project Troje van de provincie Gelderland. In deze cyberchallenge wordt onderzocht hoe de deelnemende gemeenten er wat betreft cyberveiligheid voor staan. De aanbevelingen/bevindingen verwachten we maart 2023. Op basis van de bevindingen kan het bewustzijnstraject daarna gericht worden ingevuld.

### Organisatie:

1Stroom heeft een gecombineerde functionaris gegevensbescherming (FG) en chiel i information security officer (CISO). Met een privacy officer (PO), de juridisch adviseur op privacygebied die geen FG is, is het hele taakveld binnen de organisatie gedekt. Binnen 1Stroom wordt deze rol per onderwerp ingevuld. Voor verdere versterking van de informatiebeveiliging is de wens om deze rol meer specifiek en regulier in te vullen. De FG/CISO maakt onderdeel uit van het beveiligingsoverleg de Liemers (1Stroom, Zevenaar, RID, RSD en de MGR). De positie van de CISO en FG in deze regionale samenwerking is essentieel en zal verder verstevigd worden.

#### Samenwerkingsverbanden:

Hiermee wordt elke samenwerking bedoeld waarbij persoonsgegevens betrokken zijn. In onze organisatie is goed ingeburgerd dat we dan gebruik maken van de standaard verwerkersovereenkomst van de VNG. Hierdoor waarborgen we de informatiebeveiliging en privacy. Sinds begin 2022 worden bij de aanschaf van nieuwe applicaties ook de informatiebeveiliging en privacy vragen meegenomen.

#### De factor mens:

Een belangrijke succesfactor is de mens. Het bewustzijn van de medewerkers is daarom een belangrijke bouwsteen voor informatiebeveiliging en privacy. We moeten er rekening mee houden dat de investering in bewustwording extra inzet zal vragen van 1Stroom. Zoals in het document wordt vermeld is het belangrijk dat incidenten snel herkend en erkend worden. Zo is bijvoorbeeld het meest voorkomende datalek dat e-mail naar de verkeerde ontvanger verzonden wordt. Naast digitaal bewustzijn zullen technische maatregelen, zoals de doorontwikkeling van Microsoft 365 ons daarbij helpen. Het bewustzijnstraject zal later dit jaar na de aanbevelingen van het project Troje opgepakt worden.