MEMO

Onderwerp	**Informatievoorziening n.a.v. cyberaanval gemeente Hof van Twente**
Datum college	zsm
Datum advies	10 december 2020
Afdeling	OWO Bedrijfsvoering
Steller / van	A. van der Weide
Bijlagen	geen

Met dit memo informeer ik u over de status van onze ICT beveiliging in relatie tot de geconstateerde cyberaanval bij de gemeente Hof van Twenthe.

Vorige week werd bekend dat de gemeente Hof van Twente is getroffen door een cyberaanval. Alle gegevens op de servers en de back-up zijn voor de gemeente ontoegankelijk gemaakt. Veel gegevens zijn onbruikbaar / vernietigd en het gaat veel tijd kosten om de complete ICT-infrastructuur weer aan het draaien te krijgen. Volgens De Volkskrant wil de criminele groepering € 750.000 om de bestanden weer vrij te geven. De Informatiebeveiligingsdienst voor Gemeenten (IBD) ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy. De IBD informeert gemeenten over dreigingen en incidenten op het vlak van informatiebeveiliging en adviseert over te treffen maatregelen. Zo ook over de cyberaanval bij de gemeente Hof van Twente.
De gemeente Hof van Twente onderzoekt nu met de politie, leveranciers en forensisch onderzoekers de exacte omvang en oorzaak van de cyberaanval. De IBD onderhoudt nauw contact met de gemeente en informeert andere gemeenten zodra er meer informatie beschikbaar is. De oorzaak van de cyberaanval mag vanwege het lopende onderzoek niet gedeeld worden. De IBD heeft al wel diverse maatregelen geadviseerd die gemeenten kunnen treffen om de technische beveiliging te verbeteren/borgen.

De afdeling OWO Bedrijfsvoering en met name het team Informatisering en Automatisering onderhoud nauw contact met de drie gemeentelijke informatieveiligheidsfunctionarissen (CISO's), de Informatie Beveiligingsdienst van de VNG (IBD). Daarmee borgen wij dat maatregelen op tijd bekend zijn en doorgevoerd kunnen worden op onze ICT omgeving voor de drie gemeenten.

Hoe schatten wij ons eigen risico in?
Risicoloos door het leven gaan…..kan dat? Neen, helaas niet en dat geldt ook voor de digitale wereld waarin onze gemeenten (OWO)verbonden zijn.

Het risico van een cyberaanval is een gegeven, en ja dit kan ons (jammer genoeg) ook overkomen. Uiteraard doen wij er alles aan om het risico te beperken. Beheersingsmaatregelen en procedures worden toegepast, beveiligingsmiddelen voor ons netwerk zijn ingericht. Daarnaast zijn medewerkers opgeleid om beveiligingsbewust met de hen toevertrouwde bedrijfsmiddelen om te gaan. Wij hebben ons geconformeerd aan de Baseline Informatiebeveiliging Overheid (BIO), welke de controls en maatregelen beschrijft

die minimaal benodigd zijn om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie(systemen) te waarborgen. De maatregelen die wij daarvoor moeten hanteren en hebben doorgevoerd bieden dan ook een bepaalde zekerheid van risicobeheersing.

Het is zoals de IBD al aangeeft: "*Er is op dit moment geen indicatie dat de situatie aanleiding geeft voor aanvullende maatregelen bij andere gemeenten. Indien het onderzoek dit wel uitwijst zal de IBD hier advies over geven."* En dan zullen ook wij daarop direct de noodzakelijk geachte maatregelen en controles alsnog doorvoeren.

Uiteraard zijn er in de achterliggende week al wel activiteiten ontplooid om de beheersing van het risico op de lokale situatie in de OWO gemeenten en ons netwerk te borgen. Over deze te ondernemen maatregelen wordt conform de instructies van de IBD in select gezelschap gecommuniceerd en er vinden werkzaamheden plaats om de beveiliging van onze systemen te borgen. U zult begrijpen dat wij om veiligheidsredenen inhoudelijk verder niet op dit voorval en de specifieke maatregelen in kunnen gaan.