

Digitale veiligheid is zo maar in geding

Er speelt veel bij de gemeente. De komende maanden staan er veel openbare vergaderingen op de planning en moet er over belangrijke dossiers een besluit worden genomen. Ook veel dossiers die de financiële huishouding onder druk zetten en waarbij pijnlijke keuzes nodig zijn. Dit is algemeen bekend.

Het is dus een lastige periode met veel spanning en werkdruk. Iedereen heeft er last van en is zoekende wat het beste is voor de gemeente en hoe de financiering geregeld kan worden. Er wordt veel intern overlegd door de ambtenaren, door het college en de raadsleden. Veel proefballonnetjes worden opgelaten en gedeeld met elkaar. Er wordt fysiek overlegd, gebeld, maar ook veel gemaïld om bestanden met elkaar te delen. Allemaal ideeën, maar daarnaast worden ook vertrouwelijke achterliggende stukken gedeeld om ook echt alles in ogenschouw te kunnen nemen.

En dan opeens, in alle drukte, ontvangt een medewerker een mail van de Algemeen Directeur met het verzoek zo snel als mogelijk te reageren op een vraag die hij stelt. In de snelheid leest de medewerker de mail en wilt deze gelijk beantwoorden. Tijdens het typen voelt de medewerker dat iets niet klopt en belt de Algemeen Directeur.

Gelukkig heeft de medewerker de mail niet beantwoord, want de mail bleek niet door de Algemeen Directeur te zijn verstuurd, maar door een cybercrimineel. Het beantwoorden had grote risico's met zich mee kunnen brengen. En wat blijkt, diverse ambtenaren en stakeholders hebben een gelijke mail ontvangen op naam en voornaam! Zelfs de foto van de Algemeen Directeur is zichtbaar, waardoor de mail betrouwbaar lijkt.

Een waargebeurd verhaal. Hoe gaat u hier mee om en realiseert u zich voldoende hoe snel het kan gaan dat informatie in verkeerde handen komt of sterker nog onbevoegde in onze systemen komen?

Vragen:

- 1) Heeft u een idee hoe de medewerker erachter kwam dat het niet klopte?
- 2) Wat moet de medewerker doen om erger te voorkomen?
- 3) Weet u waar u melding moet doen als u phishingmail (nepmail) ontvangt op uw gemeentelijke account?
- 4) Checkt u altijd het mailadres van de afzender?
- 5) Gebruikt u als raadslid voor uw gemeentelijke communicatie ook uw persoonlijke mail of alleen uw werkmail?
- 6) Hoe gaat u om met gevoelige informatie en vooral hoe deelt u deze informatie met collega's?
- 7) Moet er geïnvesteerd worden in informatiebeveiliging of mogen de dijken lager zijn?
- 8) Zijn binnen uw processen alle risico's bekend en wie heeft deze risico's geaccepteerd?