Raadsinformatiememo

Datum	woensdag 18 december 2019
Ons kenmerk	19.061465
Aan	De gemeenteraad en steunfractieleden
Kopie aan	
Van	Burgemeester M.J.P. van Kampen - Nouwen
Steller	Joep Boukens – CISO Gemeente Schagen
Onderwerp	Raadsinformatiememo Phishing mail vanuit de gemeente Schagen verzonden

Geachte dames en heren,

Naar aanleiding van het voorgevallen incident waarbij phishing e-mail vanuit de gemeente is verspreid, zowel intern als naar buiten toe wil ik u graag informeren over het voorval, de wijze waarop de gemeente heeft gehandeld en de maatregelen die getroffen zijn en gaan worden om de kans op herhaling zo klein mogelijk te maken.

Het voorval
Afgelopen maandag 16 december heeft een medewerker van de gemeente Schagen vanuit een externe partij (softwareleverancier) een phishing e-mail ontvangen. Omdat deze van een vertrouwd mailadres afkomstig was leek de mail legitiem. In dit geval was het mailadres van de afzender zelf 'gehackt'. De medewerker heeft vervolgens zijn inloggegevens afgegeven waardoor ook zijn e-mailaccount overgenomen kon worden. Vervolgens is eenzelfde e-mail vanuit zijn account gestuurd naar iedereen in zijn adresboek (sneeuwbaleffect).

De handelingswijze van de gemeente
Zodra bekend werd dat deze mail bij iedereen terecht is gekomen zijn direct in chronologische volgorde de volgende acties genomen:

- Het mailaccount en de toegang tot de digitale kantooromgeving van de betreffende medewerker is geblokkeerd;
- Alle medewerkers zijn per direct ingelicht en gewaarschuwd via sms en intranet;
- Via de griffie zijn ook alle raads- en commissieleden ingelicht;
- Uit alle interne mailboxen en de mailboxen van de raads- en commissieleden is met een script het betreffende mailtje verwijderd;
- Er is contact geweest met de softwareleverancier waar de mail in eerste instantie vandaan kwam:
    - Zij hebben aangegeven dit incident in onderzoek te hebben bij een externe partner;
    - De 'hackers' zijn hoogstwaarschijnlijk vooral uit geweest op inloggegevens;
    - De aanpak hoe zij hebben gehandeld is besproken.
- Er is contact geweest met de Informatiebeveiligingsdienst (IBD). Zij gaven aan dat gemeente Schagen niet de enige gemeente is geweest waarbij dit heeft gespeeld.
- Naar buiten toe is een publicatie geweest op de verschillende communicatiekanalen waarin de gemeente waarschuwt voor dit mailtje en instructies geeft hoe te handelen;
- Als preventieve maatregel heeft iedere medewerker van de gemeente Schagen zijn/haar wachtwoord moeten veranderen binnen 24 uur;

- Er is actief gemonitord op netwerkverkeer uit onlogische geografische locaties, dit geldt voor de accounts van de medewerkers van Schagen en ook voor de e-mailaccounts van de raads- en commissieleden;
- Een datalek is intern gemeld en het incident is opgenomen is het gemeentelijk incidentenregister.

Getroffen en te nemen maatregelen
Door snel te hebben gehandeld lijkt de schade zeer beperkt, naast imagoschade wat opgelopen is doordat dit incident de landelijke media heeft bereikt.

Incidenten als deze zijn nooit volledig uit te sluiten, maar de kans hierop kan wel tot een minimum worden beperkt. Hiervoor zijn al diverse technische en organisatorische maatregelen getroffen. Bewustwording onder het personeel is hier een zeer belangrijke factor in. Deze mail liep toevalligerwijs samen met een bewustwordingsactie rond phishingmail binnen de organisatie. Dit soort bewustwordingsacties zullen naar de toekomst toe nog verder worden geïntensiveerd. Daarnaast zijn en worden een aantal technische maatregelen genomen en onderzocht om risico's rondom phishing te verkleinen.

Namens het college van burgemeester en wethouders,
De portefeuillehouder,

Marjan van Kampen - Nouwen