Stappenplan bij mailhack

Versie: 4 juni 2025

Auteur: Adfiz

Inleiding

Bij een cyberaanval is het van het grootste belang om snel en adequaat te handelen om de toegang tot het account te blokkeren en schadelijke e-mails te minimaliseren. Tegenmaatregelen dienen direct te worden genomen, stakeholders en klanten moeten worden geïnformeerd.

Dit stappenplan heeft betrekking op een de situatie van een mailhack. Een mailhack is soort cybercrime waarbij een e-mailaccount wordt gehackt, waarna de aanvaller toegang heeft tot communicatie, wachtwoorden of gebruikt maakt van het account om anderen te misleiden.

Indien er bij de hack ook sprake is van een inbreuk op persoonsgegevens onder de privacywetgeving moet je snel handelen. Eerst documenteer je het incident, inclusief aard en omvang. Daarna bepaal je of je binnen 72 uur melding moet maken bij de Autoriteit Persoonsgegevens. In sommige gevallen moet je ook betrokkenen informeren. Meer informatie vind je hierover op de website van de Autoriteit Persoonsgegevens.

Onderstaand stappenplan is gebaseerd op de praktijkervaring van één van de Adfizleden. Voor meer informatie over Cybercrime kijk op het Adfiz Kennisportaal: Cyberrisico's

Stappenplan bij mailhack

Stap 1: Neem contact op met systeembeheer voor volgende acties:

- Wijzigen wachtwoord voor alle systemen (zowel eigen systemen als van partners). Dat is een actie voor jezelf en de systeembeheerder
- Beëindigen alle actieve sessies
- Uitschakelen eventuele schadelijke e-mailregels.
- Laten opsporen besmette bestand
- Verwijderen besmette bestand

Stap 2: Overleg met systeembeheerder over vervolgstappen:

- Lokaliseren alle uitgaande pishingmails: naar wie zijn deze e-mails verzonden?
- Opstellen en versturen waarschuwingsmail naar getroffen ontvangers (zie voorbeeld tekst in de bijlage).
- Laten opstellen mailing bestand (.xls en .csv) met 'Naam', 'Mail' en 'Telefoonnummer' van de betrokkenen.
- Overweeg bij een omvangrijke hack om eventueel andere communicatiemiddelen te gebruiken. Let bij de inzet van socials op de impact van het reputatierisico.

Stap 3: Neem telefonisch contact op met belangrijkste stakeholders;

- Verzekeraars o.a. op grond van een samenwerkingsovereenkomst
- (Zakelijke) Klanten

Stap 4: Evalueer het proces

- Wat ging er goed, wat kan er beter?
- Bepaal eventuele nieuwe technische en organisatorische veiligheidsmaatregelen
- Bespreek deze met het team

Stap 5: Voer nieuwe veiligheidsmaatregelen door (*bijvoorbeeld*):

- Scherp de alertheid binnen het kantoor aan voor verdachte e-mails en het klikken op (noodzakelijke) links
- Aanscherpen beveiliging voor openen van links en documenten
- Organiseren bewustwordingssessie en training om medewerkers te wapenen voor toekomstige dreigingen.

BIJLAGE 1: Voorbeeld waarschuwingsmail naar klanten

Belangrijke waarschuwing: Nepmail uit naam van < naam kantoor >

Beste relatie,

Lees onderstaande mail volledig!

Onlangs is er een nepmail verstuurd die afkomstig lijkt te zijn van < naam kantoor >.

Wij wijzen je erop dat deze mail **niet van ons afkomstig is.**

Na deze ontdekking hebben we direct met onze systeembeheerder geschakeld en het achterliggende bestand onklaar gemaakt. Ondanks deze actie vragen wij u alert te blijven.

Wat te doen?

- **Heeft u een mail van ons ontvangen, maar deze nog niet geopend?** Verwijder deze dan direct.

- **Heeft u wél de mail wel geopend en op de link geklikt? Neemt u dan direct deze maatregelen:**
  - Wijzig dan onmiddellijk het wachtwoord van uw e-mailadres
  - Neem contact op met uw IT- afdeling of systeembeheerder om verdere risico's uit te sluiten en eventuele inbraak te achterhalen.

In het algemeen raden wij u aan sterke wachtwoorden aan en het wachtwoord voor één dienst te gebruiken. Het kan lastig zijn om veel unieke wachtwoorden te onthouden; u kunt overwegen een passwordmanager te gebruiken.

Het kan zijn dat na dit incident ons mailadres door uw mailserver wordt gezien als spam. Het is daarom belangrijk dat u het algemene emailadres van < naam kantoor > niet te markeren als spam.

Wij nemen uw veiligheid zeer serieus. Samen met onze IT-specialisten werken wij voortdurend aan het beveiligen van onze systemen en het voorkomen van misbruik. Heeft u vragen of twijfels, neem dan gerust contact met ons op. Wij helpen u graag verder.

Neem contact op met < naam> , <mailadres> , <telefoonnummer >.

Met vriendelijke groet,

BIJLAGE 2: Voorbeeld bericht informeren klanten en relaties bij cyberincident

Attentie: Mailhack < naam kantoor >

Beste relatie,

Helaas moeten wij u berichten dat wij / één van onze leveranciers is getroffen door een cyber aanval.

Getroffen maatregelen

We hebben per direct na de ontdekking van het incident externe deskundigheid ingeschakeld. Met deze deskundigheid hebben is het systeem hersteld. Tegelijkertijd zijn aanvullende maatregelen getroffen om het systeem te beveiligen.

<Indien van toepassing: “Omdat het cyber-incident ook persoonsgegevens bevat, hebben wij het incident gemeld bij de Autoriteit Persoonsgegevens”>.

Gevolgen voor onze cliënten en relaties

De aanval heeft mogelijk gevolgen gehad voor onze klanten en relaties. Gedurende een periode heeft de aanvaller toegang gehad tot data. We hebben niet precies kunnen vaststellen welke data het precies betreft.

Dossiers zijn <wel/niet> inhoudelijk ingezien. Ook is er < geen/wel > toegang geweest tot financiële informatie of BSN-gegevens.

Aanbeveling voor onze cliënten

We hebben maatregelen getroffen om de impact van het incident zo veel mogelijk te beperken. Desondanks vragen we u om extra alert te zijn op ongewone zaken. Let daarom op als u ongewone e-mails met een instructie tot het klikken op een link of het openen van bijlagen ontvangt.

Contact

Wij betreuren het zeer dat dit incident heeft plaatsgevonden. We kunnen ons voorstellen dat u vragen heeft over dit bericht. In dat geval kunt u contact opnemen met < naam contactpersoon/ naam Functionaris Gegevensbescherming> via mailadres < ….> of telefoonnummer <…>.

Met vriendelijke groet,