Veelgestelde vragen datalek CJ

Hieronder vind je antwoorden op de veelgestelde vragen die wij hebben ontvangen naar aanleiding van het datalek. Mocht je vraag hiermee niet beantwoord zijn, stel deze dan via e-mail aan communicatie@combinatiejeugdzorg.nl.

Is het veilig om e-mails te ontvangen van Combinatie Jeugdzorg?
De e-mails van Combinatie Jeugdzorg zijn veilig. Het is echter altijd mogelijk, ongeacht deze hack, dat iemand zich voordoet als Combinatie Jeugdzorg. Daarom is het belangrijk te weten dat wij nooit via e-mail om persoonlijke wachtwoorden of inloggegevens vragen.

Is er een melding gedaan bij de Autoriteit Persoonsgegevens?
Ja, wij hebben het incident gemeld bij de Autoriteit Persoonsgegevens (AP) en we laten ons adviseren door de casemanager AP.

Is Z-CERT geïnformeerd?
Z-CERT, het expertisecentrum voor cybersecurity in de zorg, is geïnformeerd en blijft betrokken.

Hoeveel e-mailadressen zijn uitgelekt?
Er is één e-mailaccount met onderliggende mappen betrokken bij de hack. Dit heeft geresulteerd in de blootstelling van ruim 10.000 e-mailadressen en e-mails waarmee in het verleden is gecommuniceerd. Uit zorgvuldigheid hebben we ervoor gekozen om iedereen te informeren waarmee mailverkeer met dit e-mailaccount heeft plaatsgevonden.

Ik heb (al enige tijd) geen contact met Combinatie Jeugdzorg gehad/ ik ben (al lang) geen klant/cliënt meer van Combinatie Jeugdzorg. Hoe komt het dat mijn e-mailadres betrokken is bij de hack?
We hebben iedereen geïnformeerd die in het heden of verleden met het getroffen e-mailaccount contact heeft gehad. Uit zorgvuldigheid hebben we ook alle oude, niet recente contacten van dit e-mailaccount aangeschreven.

Welke gegevens zijn er betrokken bij het datalek? Alleen e-mailadressen? Of ook andere gegevens?
Het datalek betreft e-mailadressen en e-mails van één e-mailaccount van een medewerker die niet direct betrokken is bij de uitvoering van de zorg. Daardoor betreft het met name zakelijke contacten (90%). We zijn een onderzoek gestart naar de inhoud van het getroffen e-mailaccount en de bijbehorende e-mails om deze te checken op gevoelige en bijzondere persoonsgegevens. Dit onderzoek is inmiddels afgerond (zie vraag en antwoord hieronder).

Zijn de uitkomsten van het onderzoek bekend?
We hebben het onderzoek naar de specifieke inhoud van het getroffen e-mailaccount en de bijbehorende e-mails afgerond. Daaruit blijkt dat bij het datalek verschillende soorten gegevens mogelijk zijn gelekt:

- E-mailadressen en e-mails van alle betrokkenen bij het datalek waar mogelijk NAW-gegevens (naam, adres en woonplaats) en telefoonnummers in staan.
- Een klein aantal e-mailadressen en bijbehorende mails waar mogelijk gevoelige of bijzondere persoonsgegevens zijn gelekt.

Hoe worden betrokkenen op de hoogte gesteld van de resultaten van het onderzoek?

- Alle betrokkenen zijn via een e-mail geïnformeerd over het datalek op 8 oktober jl.
- In gevallen waar gevoelige of bijzondere persoonsgegevens mogelijk zijn gelekt, hebben we de betreffende personen individueel geïnformeerd en voorzien van specifieke informatie over hun situatie en de mogelijke risico's en gevolgen.
- Op 7 november hebben we alle betrokkenen nogmaals geïnformeerd n.a.v. de afronding van het verdere onderzoek.

Wat kunt u zelf doen?

Blijf alert op malafide e-mails waarin inloggegevens of wachtwoorden gevraagd worden, ook met Combinatie Jeugdzorg als afzender, en ga hier niet op in. Controleer altijd het e-mailadres/ de domeinnaam van de afzender. Mocht u een phishing mail van Combinatie Jeugdzorg ontvangen, dan willen wij hierover graag geïnformeerd worden.

Mocht u een mail krijgen vanuit een @combinatiejeugdzorg.nl mailadres met een link naar of een verzoek om een bestand te openen en/of opnieuw in te loggen bij een Microsoft-account van u, neem dan direct contact op met de ICT-support van uw organisatie.

Gaat het om een privé e-mailadres dan raden wij u aan om het volgende te doen:

- Reageer niet op de e-mail
- Open geen bijlagen
- Klik niet op links
- Markeer het bericht als spam in het e-mailprogramma
- Blokkeer de afzender
- Verwijder de mail.

Welk e-mailadres is gecomprimeerd?

Hierover kunnen wij geen verdere informatie verstrekken.

Van welk bedrijf was de phishing e-mail die de hack heeft veroorzaakt?

Hierover kunnen wij geen verdere informatie verstrekken.

Welke partij/ hacker zit hierachter en wat is het doel van deze partij?

We weten niet wie hierachter zit of wat het doel is van de hack. We hebben aangifte gedaan bij de politie die een onderzoek is gestart.

Welke maatregelen hebben jullie genomen?

Na het incident hebben we onmiddellijk maatregelen getroffen om herhaling te voorkomen. We hebben een externe partij ingeschakeld die gespecialiseerd is in cybercrime om onze systemen te onderzoeken. Op basis van hun feedback hebben we een aantal maatregelen direct doorgevoerd.

Laatst bijgewerkt: 07-11-2024