

Veelgestelde vragen

Hieronder vind je antwoorden op de meest gestelde vragen die wij hebben ontvangen naar aanleiding van het recente datalek (tijdelijke hack van een e-mailaccount van een van onze medewerkers veroorzaakt door een phishing e-mail). Mocht je vraag of vragen 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 voordoeft 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.

Welke gegevens zijn er precies gehackt? Alleen e-mailadressen? Of ook andere gegevens?

Het betreft e-mailadressen en e-mails van één e-mailaccount. We voeren momenteel een grondig onderzoek uit naar de specifieke inhoud van het getroffen e-mailaccount en bijbehorende e-mails. Mocht blijken dat er gevoelige informatie of bijzondere persoonsgegevens zijn gelekt, dan zullen we de betrokkenen zo snel mogelijk persoonlijk informeren.

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.

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.

Zijn er bijzondere persoonsgegevens of gevoelige informatie uitgelekt?

De medewerker van het e-mailaccount is niet direct betrokken bij de uitvoering van de zorg, waardoor het risico op het lekken van persoonlijke of gevoelige informatie klein lijkt. We zijn momenteel bezig met een grondig onderzoek naar de specifieke inhoud van het getroffen e-mailaccount en de bijbehorende e-mails. Als er bijzondere persoonsgegevens en/of gevoelige informatie zijn gelekt, zullen we de betrokkenen zo snel mogelijk persoonlijk informeren.

Zijn de uitkomsten van het onderzoek bekend?

Het onderzoek heeft uitgewezen dat het datalek beperkt is gebleven tot de e-mailadressen en e-mails van één e-mailaccount. Het onderzoek naar de specifieke inhoud van het getroffen e-mailaccount en de bijbehorende e-mails is nog in volle gang. We stellen alles in het werk om het onderzoek zo snel mogelijk af te ronden.

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

Op dit moment onderzoeken we de inhoud van het getroffen e-mailaccount en e-mails. Zodra het onderzoek is afgerond en hierover meer duidelijkheid is, communiceren wij dit bij 'Nieuws' op onze website. Mocht hierbij gevoelige informatie of bijzondere persoonsgegevens geëkt zijn, dan zullen we de betrokkenen zo snel mogelijk persoonlijk informeren.

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. Mocht u een phishing mail van Combinatie Jeugdzorg ontvangen, dan willen wij hierover graag geïnformeerd worden. Controleer altijd het e-mailadres/ de domeinnaam van de afzender.

Welk e-mailadres is gecompromiteerd?

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: 11-10-2024