Memo

Datum
4 juni 2024

Van
Artikel 5.1 lid 2 Woo
@uwv.nl

Aan
[Naam]

Onderwerp
Beantwoording vragen FG

De Functionaris Gegevensbescherming (FG) heeft een aantal vragen gesteld over de opzet en werking van de risico-mitigerende maatregelen naar aanleiding van het incident op 4 mei waarbij via 1 werkgeversaccount 150.000 CV's zijn ingezien en/of gedownload.

In deze memo worden deze vragen puntsgewijs beantwoord.

1. Welke in 2019 benoemde maatregelen zijn doorgevoerd?
   Hadden deze het beoogde effect en zoniet waarom niet en zijn daar nog aanvullende maatregelen op genomen?
   Welke maatregelen zijn niet doorgevoerd en waarom niet?

De volgende maatregelen zijn ingevoerd:

- **Resetten wachtwoorden werkgevers.**
  In 2019 was e-herkenning nog niet ingevoerd en hadden werkgevers een eigen werk.nl-account. Na het incident zijn de wachtwoorden van alle accounts direct gereset.
- **Invoeren e-Herkenning.**
  Het werkgeversdeel van werk.nl is daarna beter afgeschermd doordat het gebruik van e-herkenning niveau 3 (substantieel), dat een screening kent door 1 van de 6 geautoriseerde e-herkenningsorganisaties. (Uittreksel KVK, persoonsgegevens en legitimatie teken bevoegde, en evt. persoonsgegevens en legitimatie van gebruiker).
- **Mogelijkheid om NAW-gegevens en persoonlijke gegevens af te schermen.**
  Werkzoekenden hebben de mogelijkheid om hun NAW en andere persoonlijke gegevens af te schermen bij het publiceren van hun CV in de cv-database die alleen toegankelijk is voor werkgevers. Daarmee kunnen werkgevers alleen via werk.nl contact met hen opnemen. Ongeveer één derde van de werkzoekenden maakt hier gebruik van.
- **Er is een logging-monitoring (LOMO) systeem ingericht.**
  Iedere dag wordt een LOMO-rapportage gegenereerd en iedere werkdag wordt deze bekeken en beoordeeld door een coördinator Informatie Beveiliging & Privacy (IB&P) en bij afwijkende aantallen opgevraagde Cv's, patronen of geografische oorsprong van de inlog wordt dit besproken in het IB&P team in de dagelijkse stand-up. Daarnaast wordt er bij het opvragen van meer dan 2000 CV's binnen 24 uur een melding verzonden naar de coördinator IB&P.
  Bij afwijkende patronen wordt nader onderzocht of dit om regulier gebruik gaat (met name uitzendbureaus hebben soms bulk vacatures waarbij ze in 1 keer heel veel mensen werven) of om mogelijk misbruik.
  Er zijn geen normen voor het onderkennen van misbruik, de professionele inschatting van de coördinator IB&P en het team is leidend voor onderzoek en maatregelen bij mogelijk misbruik.

De volgende maatregelen zijn overwogen maar niet ingevoerd:

- **Het aanbrengen van een limiet voor het aantal te bekijken Cv's.**
  De onlinedienstverlening van UWV is beschikbaar voor alle werkgevers in Nederland. Wat voor uitzendbureaus normaal gedrag is, is voor de lokale Mkb'er uitzonderlijk.
  Er is geen objectieve maatstaf beschikbaar voor wat "normaal" gebruik van de cv-database is, daarmee is het complex om een grens te stellen aan het aantal in te zien Cv's. Tevens kan het inzien van kleine aantal Cv's, dat niet relevant is voor een vacature ook gezien worden als misbruik en dit voorkom je met een limiet niet.

Bezoekadres
La Guardiaweg 116
1043 DL Amsterdam

- **De NAW en persoonlijke -gegevens afschermen van de complete cv-database.**
  Op werk.nl staan zowel Cv's met als zonder NAW-gegevens, de client maakt hierin zelf de keuze. Op een CV met NAW-gegevens staat de volgende informatie: naam, geslacht, geboortedatum, adres, postcode, woonplaats, e-mail (telefoonnummer indien client dit aangeeft). Op een cv waarbij de NAW-gegevens zijn afgeschermd kan de cliënt ervoor kiezen om het telefoonnummer zichtbaar te maken op het cv.
  Na het incident in 2019 is overwogen om de NAW en persoonlijke gegevens van alle CV's in de cv-databank af te schermen, er is besloten dit niet te doen. UWV heeft de wettelijke taak om de arbeidsmarkt transparant te maken voor werkzoekenden en werkgevers (Wet SUWI). In 2019 is de afweging gemaakt dat het afschermen van alle NAW-gegevens grote impact zou hebben op het dienstverleningsaanbod aan werkgevers, en daarmee zouden we de eigen keuze van de client om de gegevens te publiceren niet respecteren.
  In 2024 is deze afweging anders uitgevallen en heeft UWV wel besloten om voorlopig alle NAW-gegevens af te schermen. Onderzocht zal worden wat hiervan de impact is op werkzoekenden en werkgevers.

- **Real time monitoring.**
  Er is gekozen voor het logging en monitoringsysteem zoals eerder beschreven. Voor real-time monitoring is destijds de inschatting gemaakt dat dit technisch moeilijk realiseerbaar was, doorlooptijd van deze wijziging zou langdurig zijn. Het idee was dat de bovengenoemde maatregelen sneller tot het gewenste resultaat zouden leiden.
  Daarnaast zou om dit effectief te laten zijn een UWV-medewerker en een medewerker van de IT-leverancier 24/7, 365 dagen per jaar beschikbaar en bereikbaar moeten zijn. Een vorm van redundantie zou ingebouwd moeten worden zodat als deze medewerker om wat voor reden dan ook niet beschikbaar is, de monitoring alsnog doorgaat.

2. Hoe was de monitoring precies ingeregeld ten tijde van het incident?
   Wat was de trigger/drempelwaarde?
   Was het een procesmatige afspraak om iedere dag in te loggen?
   Of kreeg iemand een alert of een automatisch bericht vanuit het systeem?
   Wat was de afgesproken actie bij een exceptie?

Dagelijks wordt een rapportage gegenereerd en deze wordt iedere werkdag ingezien en beoordeeld door de coördinator IB&P. Hierin staan het aantal opgevraagde Cv's per gebruikersaccount en de geografische locatie van de inlog. Indien via een account meer dan 2000 Cv's worden opgevraagd binnen 24 uur wordt er een melding verstuurd naar de coördinator IB&P en de afdeling databeheer. Zij kunnen dan beoordelen of dit regulier gebruik is of mogelijk misbruik.

Op zaterdag 4 mei is 2 keer een melding verzonden dat de grens van 2000 opgevraagde Cv's is overschreden. (Hiervan zijn screenshots beschikbaar) Deze zijn op maandagmorgen 6 mei gezien door een medewerker van UWV.

Op maandagmorgen 6 mei, de eerste werkdag na 4 mei is de ontdekt dat er een groot aantal Cv's op werk.nl is opgevraagd door het account van 1 werkgever, dit is besproken in de stand-up van team IB&P en is direct actie ondernomen. Het werkgeversaccount is geblokkeerd en er is een onderzoek gestart naar het incident. Na de eerste bevindingen in dit onderzoek is op 8 mei besloten om hier een UWV-incident van te maken en is een voorlopige melding bij de Autoriteit Persoonsgegevens gedaan.

Conclusies

Geconcludeerd kan worden dat het systeem heeft gewerkt zoals beoogd. Het account waarmee het misbruik heeft plaatsgevonden heeft ingelogd via e-herkenning, op de eerste werkdag na het incident is het misbruik direct onderkend, is het account geblokkeerd en is een onderzoek gestart. Tevens kan geconcludeerd worden dat deze maatregelen het misbruik niet hebben kunnen voorkomen.

Real time monitoring had dit mogelijk gedeeltelijk voorkomen, maar nooit helemaal. Er is prioriteit gegeven aan het implementeren van e-Herkenning. Het blijft mogelijk om meer Cv's in te zien dan strikt noodzakelijk, dit is inherent aan de functionaliteit cv-databank. UWV heeft in 2019 besloten dit rest-risico te accepteren, de huidige situatie laat zien dat UWV opnieuw moet kijken naar aanvullende maatregelen.