Vrijwaringsverklaring inzake de uitvoering van een PEN-test

Disclaimer
Het uitvoeren van een PEN-test (zoals gedefinieerd in het beschrijvend document kan risico's voor u meebrengen. Zorg er derhalve voor dat u zich door UWV en uw eigen IT-verantwoordelijken en/of IT-leveranciers goed laat informeren.

Aandachtspunten voor het uitvoeren van een PEN-test:

- *Laat het onderzoek niet op uw productieomgeving uitvoeren.*
- *Heeft u geen andere productie-like omgeving, vraag bij uw IT-verantwoordelijken na wat de mogelijkheden zijn om een productie-like omgeving tot stand te brengen. Het testen kan inhouden (niet-limitatief) dat UWV achterdeuren en/of bepaalde malafide software probeert te installeren en/of het netwerk van de omgeving scant. Door een afgeschermde omgeving beschikbaar te stellen; reduceert u eventuele nadelige gevolgen.*
- *Tijdens het onderzoek is het mogelijk dat kwaadwillenden ook de omgeving "onderzoeken". Probeer daarom uw omgeving tijdens het onderzoek actief te monitoren en houd hierbij rekening dat niet alle activiteiten van UWV afkomstig hoeven te zijn.*
- *Omdat er tijdens een onderzoek mogelijk veel vreemde data en software wordt geïnstalleerd waardoor de omgeving niet betrouwbaar meer is, geldt het advies om de beschikbaar gestelde omgeving, direct na het onderzoek, offline te halen. U kunt deze het beste voor (eventuele) forensische doeleinden veilig opslaan óf volledig opschonen.*

De ondergetekenden:

1. Uitvoeringsinstituut werknemersverzekeringen (UWV), gevestigd en kantoorhoudend aan de La Guardiaweg 94-114 te (1043 DL) Amsterdam, ingeschreven in het Handelsregister van de Kamer van Koophandel onder nummer 34360247, te dezen rechtsgeldig vertegenwoordigd door Gerben Rozendaal, hoofd Inkoop, hierna te noemen: "**UWV**"

   en

2. <Volledige bedrijfsnaam>, gevestigd te <straat en nummer (postcode) te plaats>, ingeschreven in het Handelsregister van de Kamer van Koophandel onder nummer <invullen> te dezen rechtsgeldig vertegenwoordigd door de <invullen>, <directeur> <invullen>, hierna te noemen: "**de Onderzochte Partij**".

samen te noemen: "**Partijen**".

Overwegende dat:

A. De Onderzochte Partij een inschrijving heeft ingediend voor de UWV aanbesteding arbodienstverlening (hierna te noemen: "**Offerteaanvraag**").
B. UWV overweegt de opdracht uit deze Offerteaanvraag onder te brengen bij de Onderzochte Partij.
C. UWV door middel van een zogenaamde PEN-test een onderzoek wenst te (laten) doen naar de informatiebeveiliging binnen de door de Onderzochte Partij te leveren diensten c.q. het door Onderzochte Partij beheerde syste(e)m(en).
D. Het doel van de PEN-test is om:
   - inzicht te krijgen in de risico's en kwetsbaarheden van de te onderzoeken diensten/syste(e)m(en) te bezien of deze voldoen aan het overeengekomen beveiligingsniveau;
   - de beveiliging van de te leveren diensten/het te leveren syste(e)m(en) te verbeteren.
E. De in het kader van de PEN-test door UWV te verrichten testwerkzaamheden mogelijkerwijs schade tot gevolg zouden kunnen hebben.
F. De PEN-test – onder meer gelet op het bepaalde in artikel 138ab Wetboek van Strafrecht– alleen kan geschieden met toestemming van de Onderzochte Partij.
G. Dit document een beperkte vrijwaring bevat ten behoeve van UWV tegen eventuele aansprakelijkheden voor schade als gevolg van een PEN-test.
H. Partijen hun afspraken in verband met de uitvoering van de PEN-test in deze vrijwaringsverklaring vastleggen.

Verklaren dat:

Artikel 1 - Voorwerp van deze vrijwaringsverklaring

1. UWV wenst een PEN-test uit te voeren, zoals beschreven in Bijlage I - Het onderzoek van deze vrijwaringsverklaring.
2. De Onderzochte Partij laat UWV vrij in de wijze waarop deze zal proberen de in Bijlage I - Het onderzoek beschreven computernetwerken en/of systemen binnen te dringen, dan wel in de wijze waarop gepoogd wordt gegevens aan deze computernetwerken en/of systemen te onttrekken. Dit met uitzondering van methoden waarvan het UWV op voorhand redelijkerwijs bekend moet zijn, dat die de voornoemde systemen en aangeboden diensten onbereikbaar maken, zoals *denial of service-attacks*. Evenmin is het UWV toegestaan om wijzigingen aan te brengen in de systemen en data die het aantreft, zodra het in de systemen is binnengedrongen.

Artikel 2 - Toestemming

1. De Onderzochte Partij geeft UWV hierbij toestemming voor het uitvoeren van een PEN-test zoals bedoeld in het eerste lid van artikel 1.
2. De Onderzochte Partij is zich ervan bewust dat de werkzaamheden van UWV zijn gericht op het identificeren van kwetsbaarheden in de beveiliging van de geleverde diensten, het geautomatiseerde systeem, de gegevens, bedrijfsgebouwen of enig ander goed dat aan de Onderzochte Partij toebehoort of door hem wordt beheerd. Dit alles met het oogmerk om doeltreffende maatregelen te kunnen treffen ten aanzien van deze kwetsbaarheden en om, zo nodig, de beveiliging in overeenstemming te brengen met het tussen Partijen overeengekomen niveau.

Artikel 3 - Uitvoering van de PEN-test

1. UWV zal de Onderzochte Partij vooraf door middel van een aankondiging informeren over de periode waarin de PEN-test zal plaatsvinden.
2. De Onderzochte Partij zal de ontvangst van deze aankondiging bevestigen.
3. De personen die de contacten over de uitvoering van de PEN-test onderhouden zijn voor:
   UWV: <invullen>
   Onderzochte Partij: <invullen>
4. De Onderzochte Partij kan UWV om gewichtige redenen met een gemotiveerd verzoek vragen een PEN-test waarvoor toestemming is verleend te staken. UWV schort in een dergelijk geval de testwerkzaamheden op en Partijen treden in overleg. Afhankelijk van de uitkomst van het overleg zet UWV de testwerkzaamheden, al dan niet in gewijzigde vorm, voort of staakt het die werkzaamheden.

Artikel 4 - Beschikbaar stellen van resultaten PEN-test

De resultaten van de PEN-test worden door UWV vastgelegd in een concept rapportage. Na afstemming van de concept rapportage met de Onderzochte Partij, stelt UWV de rapportage definitief vast. UWV is gerechtigd om de rapportage beschikbaar te stellen aan derden, waaronder auditors, indien dit noodzakelijk is om de beveiliging van de dienst adequaat te waarborgen of vereist is om verantwoording af te leggen.

Artikel 5 - Aansprakelijkheid

1. UWV is niet aansprakelijk voor schade die ontstaat als gevolg van diens werkzaamheden op grond van de PEN-test, indien en voor zover deze werkzaamheden vallen binnen de reikwijdte van Bijlage I - Het onderzoek en de desbetreffende werkzaamheden ook overigens zijn verricht conform het bepaalde in deze vrijwaringsverklaring. De Onderzochte Partij vrijwaart UWV dan ook tegen aansprakelijkheden dienaangaande, met name ingeval een derde UWV zou aanspreken wegens schending van een of meer van de artikelen 161sexies, 161septies, 351, 351bis, 138ab en 138b van het Wetboek van Strafrecht en voor zover dit niet in strijd is met de wet.
2. Voor zover UWV wel aansprakelijk is, is de hoogte van de aansprakelijkheid beperkt tot een bedrag ad € 100.000,- (honderdduizend euro).

Artikel 6 - Beperking vrijwaring

De vrijwaring als omschreven in artikel 5.1 ziet niet op schade die is ontstaan door opzet, bewuste roekeloosheid of een ernstige beroepsfout van UWV bij het uitvoeren van de PEN-test door UWV.

Artikel 7 - Looptijd
Deze vrijwaringsverklaring treedt in werking op het moment van ondertekening door alle Partijen en heeft de duur van <zes (6) maanden> en heeft betrekking op het totale onderzoek (zoals beschreven in Bijlage I – Het onderzoek), inclusief hertesten.

Aldus op de laatste van de hierna genoemde data ondertekend:

Namens UWV, genoemd onder 1:

Naam: Gerben Rozendaal
Functie: Hoofd Inkoop
Datum: <invullen>
Plaats: Amsterdam

Namens de Onderzochte Partij, genoemd onder 2:

Naam: <invullen>
Functie: <invullen>
Datum: <invullen>
Plaats: <invullen>

Bijlage I - Het onderzoek

Het onderzoek staat gepland in de periode van <begindatum invullen> tot en met <einddatum invullen>.
Er dient rekening gehouden te worden met mogelijke aanpassing van deze periode door mogelijke vertragingen in het voortraject dan wel uitloop van werkzaamheden. De uitvoering zal gedaan worden door de pentesters van het UWV Security Operations Center.

In scope zijnde van dit onderzoek is:

- De webapplicatie die wordt aangeboden op https://<XXX>
- De mobiele applicatie behorende bij de <XXX> oplossing voor UWV. Deze zal uit de *Google Play Store/Apple App Store* gehaald worden door de onderzoekers zelf. Met de optie een test versie op te vragen bij de Onderzochte Partij in de vorm van een APK bestand.
- De mogelijke *API endpoints* die betrokken zijn bij de werking van zowel de web als de mobiele applicatie. Deze hosts worden automatisch in scope geplaatst ook al zijn deze op een andere IP adres te benaderen dan eerder is aangegeven.
- Mogelijke subdomeinen of *API endpoints* die betrokken zijn bij de werking van de applicatie. Deze hosts worden automatisch in scope geplaatst.
- De nadruk tijdens het onderzoeken ligt op:
    - Het verkrijgen van data die normaal niet toegankelijk mag zijn, bijvoorbeeld die van andere gebruikers.
    - Het verkrijgen van verhoogde rechten binnen de webapplicatie.
    - Het verkrijgen van toegang tot andere gebruikersaccounts of administratieve accounts door fouten in de applicatie logica.
    - Het onderzoek wordt gedaan vanuit het perspectief dat er géén account beschikbaar is én het perspectief dat er wél een account beschikbaar is.
- Het uitvoeren van exploits op de webserver of onderliggende OS laag om zo toegang tot gegevens of het systeem te krijgen.
- Het uitvoeren van een poort scan op alle betrokken hosts.
- Openstaande poorten, die niet direct gebruikt worden voor het functioneren van de applicatie worden wel onderzocht om een risico inschatting te kunnen maken.
- Onderzoek naar de mobiele applicaties (Android en iOS app's) hoort bij de webapplicatie. Indien tijdens dit onderzoek extra hosts worden geïdentificeerd, die direct invloed hebben op de applicatie, dan worden deze hosts ook in scope geplaatst. Bijvoorbeeld *API endpoints*.

<u>NIET</u> in scope zijnde van dit onderzoek is:

- Uitvoeren van DOS of DDOS aanvallen om de continuïteit/beschikbaarheid te onderzoeken.
- *Social engineering* of andere *phishing* activiteiten.
- Cyberaanval richting andere accounts, gebruikers en/of klanten die niet bij dit onderzoek betrokken zijn.
- Uitvoeren van grootschalige brute force aanvallen (>10.000 verzoeken op functies in de applicatie of een URL om middels brute force toegang te krijgen tot specifieke gegevens).

Uitvoering
In het geval dat voor het onderzoek gebruik gemaakt moet worden van bestaande/eigen UWV-accounts, worden de volgende accounts mogelijk gebruikt:

- <invullen>
- <invullen>
- <invullen>
- <invullen>

In andere gevallen waar inloggegevens vereist zijn kunnen deze in latere e-mail-correspondentie (via Zivver) gedeeld worden.