Rapporteren van kwetsbaarheden in de ICT
Coordinated Vulnerability Disclosure

Spelregels

De gemeente Hof van Twente hecht veel belang aan de beveiliging van haar systemen. Ondanks alle voorzorgsmaatregelen blijft het mogelijk dat een zwakke plek in de systemen te vinden is. Wanneer een zwakke plek in één van onze systemen wordt ontdekt, vernemen wij dit graag van de ontdekker, zodat wij snel gepaste maatregelen kunnen nemen.

Het feit dat de gemeente Hof van Twente een Coordinated Vulnerability Disclosure beleid heeft, is geen uitnodiging om het bedrijfsnetwerk uitgebreid en actief te scannen om zwakke plekken te ontdekken. Wij monitoren zelf ons bedrijfsnetwerk.

Als een kwetsbaarheid in een van onze systemen wordt onderzocht, hou dan rekening met de proportionaliteit van de aanval.

Door het maken van een melding verklaart de ontdekker zich als melder akkoord met onderstaande afspraken over Coordinated Vulnerability Disclosure en zal de gemeente Hof van Twente de melding conform onderstaande afspraken afhandelen.

Wij vragen het volgende van de ontdekker:

- Mail uw bevindingen naar informatiebeveiliging@hofvantwente.nl. Versleutel de bevindingen indien mogelijk of verstuur de melding via beveiligde mail, om te voorkomen dat de informatie in verkeerde handen valt.
- Misbruik de zwakke plek niet door bijvoorbeeld:
    - Meer data te downloaden dan nodig is om de zwakke plek aan te tonen
    - Gegevens te veranderen of verwijderen
- Geef voldoende informatie om het probleem te reproduceren, zodat we het zo snel mogelijk kunnen oplossen. Meestal hoeft u alleen maar het IP-adres of de URL van het getroffen systeem en een omschrijving naar ons te sturen. Bij een uitgebreide zwakke plek is er misschien meer informatie nodig bijvoorbeeld een Proof of Concept.
- U verwijdert alle vertrouwelijke gegevens die u hebt verkregen in uw onderzoek, direct nadat wij de zwakke plek hebben opgelost.
- Wij vinden het altijd fijn als we hulp krijgen om een probleem op te lossen. Geef informatie over de zwakke plek die wij kunnen controleren. Vermijd dat uw advies neerkomt op reclame voor andere (beveiligings)producten.
- Laat uw gegevens achter zodat wij contact met u kunnen opnemen. Laat in ieder geval een e-mailadres of telefoonnummer achter.
- Dien de melding zo snel mogelijk in na ontdekking van de zwakke plek.

De volgende handelingen zijn niet toegestaan:

- U mag geen malware plaatsen op onze systemen noch op die van anderen.
- U mag de toegang tot het systeem niet “bruteforcen”. Dit betekent dat het eenvoudig moet zijn om met makkelijk en goedkoop verkrijgbare hardware en software een wachtwoord te kraken. Met dit wachtwoord kan men dan het systeem blootstellen aan gevaar.
- Het is alleen toegestaan om social engineering te gebruiken als het niet anders kan. Dit mag alleen als u aantoont dat medewerkers die toegang hebben tot gevoelige gegevens hier niet zorgvuldig mee om gaan. U moet legaal medewerkers hebben overgehaald om dit soort gegevens te geven aan personen die dat niet mogen krijgen. Het is niet toegestaan om medewerkers van de gemeente te schaden.
- Met wat u heeft gevonden mag u alleen aantonen dat de procedures en werkwijzen binnen de gemeente gebreken vertonen.
- U mag de informatie van het beveiligingsprobleem niet aan andere doorgeven voordat het probleem is opgelost.

- U mag alleen handelingen uitvoeren die echt nodig zijn om het beveiligingsprobleem aan ons te tonen en om aan ons te melden. U kunt ons een directory lijst geven, in plaats van een complete database te kopiëren. U mag nooit gegevens in het systeem wijzigen of verwijderen.
- U mag geen gebruik maken van technieken waarbij het gebruik en/of beschikbaarheid van het systeem of services verslechterd wordt (DoS-aanvallen).

Wat u mag verwachten:

- Als u aan al deze voorwaarden voldoet, doen wij geen strafrechtelijke aangifte. We spannen dan ook geen civielrechtelijke zaak tegen u aan.
- Als u zich niet aan deze voorwaarden heeft gehouden, kunnen wij een gerechtelijke zaak tegen u aanspannen.
- We behandelen de melding vertrouwelijk. We delen uw persoonlijke gegevens alleen met anderen als u daar toestemming voor heeft gegeven. Ook delen we de gegevens als we dat van de wet moeten doen of dat het door een rechterlijke uitspraak verplicht is.
- Gemeenten delen hun ervaringen met elkaar. Daarom delen we de ontvangen melding altijd met de Informatiebeveiligingsdienst voor gemeenten (IBD).
- U blijft anoniem als ontdekker van de zwakke plek. Als u wilt dat wij uw naam vermelden, dan doen wij dat.
- Binnen 2 werkdagen krijgt u een ontvangstbevestiging.
- Binnen 5 werkdagen krijgt u van ons een reactie met een beoordeling van de melding.
- We gaan het door u gemelde beveiligingsprobleem zo snel mogelijk oplossen. We willen u over het verloop goed op de hoogte houden. We willen er niet langer dan 90 dagen over doen om het probleem op te lossen. We zijn wel vaak afhankelijk van anderen.
- Nadat het probleem is opgelost, kunnen we samen beslissen of het probleem bekend gemaakt wordt en hoe we dit communiceren.
- Wij kunnen u een beloning geven voor uw onderzoek, maar zijn hiertoe niet verplicht. De vorm van deze beloning staat niet van tevoren vast en wordt door ons per geval bepaald. Of we een beloning geven en de vorm waarin dit gebeurt, hangt af van de zorgvuldigheid van uw onderzoek, de kwaliteit van de melding en de ernst van de zwakke plek.