Responsible disclosure - ethische veiligheidsmelding

Gemeente Sint-Gillis-Waas draagt cyberveiligheid hoog in het vaandel en tracht de nodige stappen te nemen om informatie en systemen veilig te houden. Ondanks deze voorzorgen, bestaat de kans dat een kwetsbaarheid opduikt of nog niet werd weggewerkt.

Daarom werkt gemeente Sint-Gillis-Waas graag samen met jou om de beveiliging van netwerken informatiesystemen te verbeteren. Wanneer een kwetsbaarheid in de systemen, uitrusting en producten van de organisatie gedetecteerd wordt, kunnen deelnemers ons dan ook hierover inlichten binnen het kader en de bepalingen van dit beleid voor de gecoördineerde bekendmaking van kwetsbaarheden (de zogeheten 'Responsible Disclosure Policy').

Concreet richt dit beleid zich op beveiligingskwetsbaarheden die misbruikt kunnen door derden met een kwaadwillig oogmerk of die de goede werking van onze producten, diensten, netwerk- of informatiesystemen kunnen verstoren. Deelnemers hebben de toestemming om informaticagegevens in het informaticasysteem in te voeren of proberen, zolang de bepalingen in dit beleid gerespecteerd worden.

Mocht er twijfel bestaan bij de opzet of bepalingen in deze responsible disclosure, is het steeds mogelijk om contact op te nemen met cyberveiligheid@sint-gillis-waas.be voor extra verduidelijking.

Wat valt zoal binnen deze responsible disclosure?

Deze responsible disclosure werd uitgewerkt door gemeente Sint-Gillis-Waas en is uitsluitend van toepassing op volgende website:

- www.sint-gillis-waas.be

Hoe meld ik een kwetsbaarheid?

1. Zodra een kwetsbaarheid ontdekt wordt, meld je dit zo snel mogelijk door je bevindingen te mailen naar cyberveiligheid@sint-gillis-waas.be en bevestig je dat je conform de Responsible Disclosure Policy hebt gehandeld en zult blijven handelen.
2. Optioneel: Versleutel je bevindingen om te voorkomen dat de informatie bij de gevonden kwetsbaarheid in verkeerde handen valt. Maak voor de overdracht bijvoorbeeld gebruik maakt van Transport Layer Security (TLS) of Secure Sockets Layer (SSL) , Secure Multipurpose Internet Mail Extensions (S/MIME) of Pretty Good Privacy (PGP) en beveilig met een paswoord of zip.-beveiliging.
3. Deel zeker ook je naam (of een pseudoniem mocht je dat verkiezen), mailadres en telefoonnummer mee, zodat we contact kunnen opnemen in kader van de opvolging bij de kwetsbaarheid.
4. Tracht steeds om zoveel mogelijk informatie te geven, zodat de kwetsbaarheid gereproduceerd en opgelost kan worden, zoals een beschrijving van de kwetsbaarheid, de soort kwetsbaarheid, configuratiedetails, het besturingssysteem, Data en tijdstippen van de tests, de uitgevoerde bewerkingen (via logs), de gebruikte tools, de data en tijdstippen van de tests, het IP-adres of de URL van het getroffen systeem, screenshots en andere relevante bijlagen of informatie,

Welke regels moet ik naleven?

Evenredigheid

Je verbindt je ertoe om evenredig te werk te gaan. Dat wil zeggen dat je de beschikbaarheid van de door het systeem geleverde diensten niet verstoort en geen gebruik maakt van de kwetsbaarheid buiten wat strikt noodzakelijk is voor het aantonen van het beveiligingsprobleem. Indien het probleem op kleine schaal is aangetoond, ga je niet verder.

Verboden acties

Je maakt geen gebruik van de volgende handelingen bij het testen:

- Kopiëren of wijzigen van gegevens, verwijderen van gegevens of het aanbrengen van veranderingen in een informaticasysteem
- Plaatsen van malware, zoals een virus, worm, Trojaans paard, ...
- Herhaaldelijk toegang verwerven tot het systeem of de toegang delen met anderen
- Gebruik van geautomatiseerde scantools
- Gebruik van zogeheten 'bruteforcing' voor toegang tot systemen of ‘denial-of-service aanvallen’, waarbij zeer grote hoeveelheden aan informatie naar een applicatie verstuurd worden, diefstal van paswoorden, social engineering technieken zoals phishing, vishing en spam of aanvallen op de fysieke beveiliging
- De installatie van een toestel dat het mogelijk maakt om communicatie die niet publiek toegankelijk is te onderscheppen, op te slaan of in te kijken
- Het met opzet onderscheppen, opslaan of kennisnemen van niet voor het publiek toegankelijke communicatie of van elektronische communicatie
- Het met opzet gebruiken, bijhouden, meedelen of verspreiden van inhoud uit niet voor het publiek toegankelijke communicatie of van gegevens van een informaticasysteem waarvan de deelnemer redelijkerwijze had moeten weten dat ze onwettig werden verkregen
- [...]

Indien je de hulp van een derde wenst bij de uitvoering van je onderzoek, dan kan dit enkel mits de derde vooraf kennisneemt van dit beleid en de voorwaarden evenzeer strikt naleeft.

Vertrouwelijkheid

Zonder voorafgaande en uitdrukkelijke toestemming mag je de informatie die je vergaard hebt binnen het kader van dit beleid in geen geval verspreiden met of onder derden. Het gaat hierbij zowel over informatica-, communicatie- als persoonsgegevens. Je maakt de kwetsbaarheid ook niet openbaar totdat deze gecorrigeerd werd en wist de gegevens die verkregen werden via de kwetsbaarheid meteen na de melding.

Uitvoering te goeder trouw

Er is geen sprake van bedrieglijk opzet, het oogmerk om te schaden, of de wil om gebruik te maken van of schade te veroorzaken aan de bezochte systemen of daaraan gerelateerde gegevens.

Publiceren over kwetsbaarheid

Indien je, nadat de kwetsbaarheid is verwijderd, over de kwetsbaarheid wil publiceren, vragen we om dit minstens één maand voor de publicatie te melden en ons de mogelijkheid te geven hierop te reageren. Ons identificeren, rechtstreeks of onrechtstreeks, in een publicatie kan slechts na uitdrukkelijk akkoord.

Verwerking van persoonsgegevens

Tenzij nodig om het bestaan van een kwetsbaarheid te bewijzen, mag je als deelnemer in geen geval

persoonsgegevens raadplegen, ophalen of opslaan. Het is echter wel mogelijk dat je als deelnemer, al dan niet toevallig, toegang krijgt tot persoonsgegevens die worden opgeslagen, verwerkt of overgedragen in het betrokken systeem tijdens het opsporen van kwetsbaarheden. Indien dit zich voordoet of er sprake is van een eventueel verlies van persoonsgegevens, vragen we om het onmiddellijk te melden via privacy@sint-gillis-waas.be. Bij het verwerken van dergelijke gegevens verbind je je ertoe om de wettelijke verplichtingen op het gebied van de bescherming van persoonsgegevens [1] en de voorwaarden van dit beleid na te leven.

[1] Europese Verordening nr. 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (AVG Algemene Verordening Gegevensbescherming).

Wat beloven wij?

- Indien je de bovenstaande voorwaarden van de Responsible Disclosure Policy respecteert en geen andere inbreuken hebt begaan, ondernemen wij geen juridische stappen tegenover jou.
- We reageren op meldingen binnen een redelijke termijn - indien mogelijk binnen de 10 werkdagen - met onze beoordeling van de melding en eventueel een verwachte datum voor een oplossing.
- Meldingen worden vertrouwelijk behandeld en je persoonsgegevens worden zonder je toestemming niet gedeeld met derden, tenzij dit noodzakelijk is om een wettelijke verplichting na te komen.
- Als dank voor elke melding, bieden we de mogelijkheid om vermeld te worden in onze online 'Hall of Fame'. Daarin wordt je naam (of pseudoniem), het aantal gevonden kwetsbaarheden en een verwijzing naar een of meerdere van je sociale en/ of websitelinks vermeld.
- Voor zover mogelijk en rekening houdend met de kosten en de bestaande kennis trachten we zo snel mogelijk een oplossing uit te werken, in functie van de ernst van de risico's die gebruikers van de betrokken systemen lopen.
- Je wordt minstens eenmalig op de hoogte gebracht van de resultaten van ons eigen onderzoek naar aanleiding van je melding en het gevolg dat hieraan gegeven wordt.
- We hebben het recht om meldingen van een lagere kwaliteit te negeren.
- Neem bij twijfel over de toepasbaarheid en modaliteiten van dit beleid altijd eerst contact op via cyberveiligheid@sint-gillis-waas.be, om expliciet toestemming te vragen.

Toepasselijk recht en duur

Het Belgisch recht is van toepassing op geschillen in verband met de uitvoering van dit beleid. De regels zijn toepasselijk vanaf 12 oktober 2023, tot ze eventueel worden gewijzigd of opgeheven door gemeente Sint-Gillis-Waas. Deze wijzigingen of opheffingen worden bekendgemaakt op onze website en zijn automatisch van toepassing 30 dagen na bekendmaking.

Hall of Fame

Naam	E-mail of sociale media	Meldingen
Vinit Lakra	www.linkedin.com/in/vinithacker	1
Hritom Bhattacharya	www.linkedin.com/in/hritom-bhattacharya-b0a3861a4	1