Responsible Disclosure Policy

Bij Telenet vinden we de veiligheid van onze systemen en gegevens zeer belangrijk. Ondanks onze maatregelen om onze beveiliging te optimaliseren, kan het gebeuren dat er toch iets door de mazen van het net glipt. Mocht jij een beveiligingsprobleem ontdekken, dan bieden we jou de mogelijkheid om ons dit te melden op een verantwoorde manier. Wij werken graag met je samen om onze systemen beter te maken en onze klanten nog beter te beschermen.

Deze procedure dient voor het melden van:

- Vermoedelijke beveiligingsproblemen in onze producten en diensten, inclusief modem, Digicorder/Digibox, hotspot/homespot, websites, webgebaseerde toepassingen en mobiele apps, die kunnen worden misbruikt en kunnen leiden tot:
  - stelen van gevoelige data
  - ongeoorloofd veranderen of verwijderen van gevoelige data
  - beperken of onmogelijk maken van de toegang tot onze diensten
  - verstoren van de goede werking van ons netwerk, onze producten of diensten

Deze procedure dient **niet** voor het melden van:

- Vragen of klachten over de werking van onze producten, dienstverlening, facturatie, … Daarvoor verwijzen wij je vriendelijk door naar onze Klantenservice
- DDoS-aanvallen, brute force password guessing, social engineering-aanvallen, …
- Meldingen over virussen, phishing mail, spam mail, fraude, …

De spelregels

- Meld het vermoedelijke beveiligingsprobleem via de beveiligde pagina ‘Meld een beveiligingsprobleem’. Beschrijf het probleem in voldoende detail, en voeg het nodige bewijsmateriaal toe, zoals IP-adressen, log entries, screenshots, …
- Schrijf je melding in het Nederlands of Engels
- Als je liever anoniem blijft, dan hoef je geen contactgegevens achter te laten. Al kan het soms nodig zijn dat we je willen bereiken voor bijkomende informatie of om feedback te geven. In dat geval kan je eventueel een anonieme mailbox opgeven (bv. via Gmail of Hotmail)
- Meld je bevindingen alleen via deze procedure aan Telenet. Publiceer geen details over het beveiligingsprobleem via andere kanalen. Melding van het probleem via andere kanalen of media, ook vóór of na de melding aan Telenet via deze procedure en zelfs wanneer niet alle details worden vrijgegeven, zal aanzien worden als onverantwoord gedrag en kan alsnog leiden tot het neerleggen van een strafklacht
- Maak geen misbruik van het gevonden lek: verzamel alleen de nodige informatie om het bestaan ervan aan te tonen
- Verander of verwijder geen gegevens of systeeminstellingen
- Ga verantwoord om met eventuele gevonden gegevens: als je met een klein gedeelte kan aantonen dat er een beveiligingsprobleem is, ga dan ook niet verder

Responsible Disclosure Policy

Belangrijk!

Hou je voor het vaststellen van mogelijke beveiligingsproblemen altijd aan de wettelijke bepalingen. Toon geen beveiligingslekken aan door het uitvoeren van DDoS-aanvallen, brute force password guessing, social engineering-acties, het infecteren van systemen met malware, het scannen van onze systemen, … Die zullen aanzien en behandeld worden als gerichte aanvallen omdat ze zowel Telenet als haar klanten schade kunnen berokkenen. Telenet kan in dit geval niet garanderen dat je niet vervolgd wordt, aangezien het risico bestaat dat de officiële instanties de nodige maatregelen zullen nemen naar aanleiding van dergelijke aanvallen.

Onze belofte

- We geven zo spoedig mogelijk feedback op je melding, als je je contactgegevens hebt achtergelaten
- Mochten we nog bijkomende informatie nodig hebben, nemen we eventueel contact met je op, als dat mogelijk is
- We doen al het mogelijke om eventuele tekortkomingen zo snel mogelijk op te lossen, en houden je op de hoogte
- Afhankelijk van het mogelijk vastgestelde beveiligingsprobleem, kan Telenet autonoom beslissen over een mogelijke beloning. De inhoud en de omvang van deze beloning worden eenzijdig door Telenet bepaald, en geeft geen garantie op toekomstige beloningen
- Het volgen van bovenstaande spelregels garandeert dat Telenet tegen jou geen strafklacht bij de gerechtelijke instanties neerlegt