Ziggo BV
Postbus 43048, 3540 AA Utrecht
0900–1884 (€ 0,10 per minuut) | www.ziggo.nl

Gedragscode Responsible Disclosure

Reikwijdte

- Deze gedragscode richt zich op de procedure voor het melden van vermoedelijke beveiligingsproblemen en het verantwoord openbaar maken daarvan (hierna: responsible disclosure)
- Deze gedragscode is van toepassing op zowel Ziggo als de melder van een beveiligingsprobleem of kwetsbaarheid.
- Hetgeen afgesproken in deze code laat wettelijke afspraken onverlet

Definities

a. Een **melding** betreft het door een melder aan Ziggo melden van een vermoedelijke beveiligingsprobleem, om het probleem op een verantwoorde wijze kenbaar te maken.
b. De **melder** is de persoon of instantie die een melding doet.
c. **Ziggo** is een aanbieder van openbare telecommunicatienetwerken en –diensten.
d. Een **beveiligingsprobleem** of **kwetsbaarheid** is een (vermoedelijke) zwakte in of inbreuk op de beveiliging van de infrastructuur of ICT-systeem van Ziggo en/of van de klanten.
e. Een **klant** betreft degene waarmee Ziggo een (zakelijke) overeenkomst heeft voor het beheren van infrastructuur of ICT-systemen.

1. Aanleiding

Ziggo neemt veiligheid zeer serieus. Het vertrouwen in dienstverlening staat bovenaan. Incidenten komen helaas voor. Ziggo heeft een eigen verantwoordelijkheid om beveiliging op een passende wijze te waarborgen. Ziggo werkt daarnaast gezamenlijk met andere bedrijven in de Telecomsector aan het vergroten van de beveiliging. Ziggo is voor de continuïteit van haar dienstverlening afhankelijk van complexe ICT-systemen. De privacy van gebruikers en klanten van Ziggo is van groot belang, net als de vertrouwelijkheid van communicatie en informatie. Daarom moet voorkomen worden dat onbevoegden toegang krijgen tot de infrastructuur van Ziggo of de gegevens van gebruikers en klanten van Ziggo. Om dit te voorkomen investeert Ziggo veel in de veiligheid van haar infrastructuur. Daarnaast controleert Ziggo voortdurend op onregelmatigheden, zoals inbraakpogingen.

Incidenten kunnen diverse aanleidingen hebben, zoals een menselijke fout, externe factoren als stroomuitval of kwetsbaarheden in een ICT-systeem. In sommige gevallen worden kwetsbaarheden voortijdig opgemerkt door derden. Met een responsible disclosure procedure wil Ziggo het makkelijker maken voor gebruikers om vermoedelijke beveiligingsproblemen te melden. Hiermee hoopt Ziggo problemen sneller te herstellen en te voorkomen dat informatie in de verkeerde handen valt.

Er kan verschil ontstaan in de wijze van opvolging van meldingen. Zo is een kwetsbaarheid die reeds eerder is ontdekt en waartegen een update bestaat eenvoudiger te dichten dan een kwetsbaarheid die voor het eerst aan het licht komt. Ervaring met responsible disclosure programma's van internationale bedrijven leert dat het soms tot meer dan zes maanden kan duren voordat sommige nieuw ontdekte kwetsbaarheden adequaat zijn verholpen.

2. Responsible disclosure procedure

Een responsible disclosure procedure is het hebben van procesafspraken zodat het voor derden helder is hoe zij op een verantwoorde wijze kwetsbaarheden in de beveiliging van de infrastructuur en ICT-systemen kunnen rapporteren aan Ziggo.

Met het onderschrijven van deze gedragscode hanteert Ziggo de volgende uitgangspunten en procesafspraken voor responsible disclosure:

2.1 De uitgangspunten

a. Ziggo zorgt voor een voor derden duidelijke proces en eigen meldpunt om beveiligingsproblemen en kwetsbaarheden te rapporteren. Ziggo zorgt voor een bekendmaking van dit proces, bijvoorbeeld door op de Ziggo website een bericht te plaatsen met uitleg en randvoorwaarden.
b. Ziggo zorgt ervoor dat de procesafspraken op relevante plekken in de organisatie bekend is en wordt nageleefd.
c. De melder van een kwetsbaarheid en Ziggo spreken af op welke termijn duidelijkheid geboden zal worden over de wijze waarop de kwetsbaarheid verholpen zal worden.
d. De melder van een kwetsbaarheid en Ziggo spreken af of en op welke wijze er publiciteit wordt gezocht zodra zicht is op welke wijze de kwetsbaarheid is verholpen.

2.2 De procesafspraken voor een melding

a. Kwetsbaarheden kunnen op een toegankelijke manier gemeld worden. Zie de Ziggo website voor een stap-voor-stap uitleg: https://www.ziggo.nl/klantenservice/meldpunt-beveiligingslekken
b. De melder zelf moet duidelijk benoemen wat het onderwerp is en de melding moet vergezeld gaan van bewijsmateriaal ten behoeve van het handelingsperspectief voor Ziggo.
c. De melding mag anoniem worden gedaan.
d. Ziggo streeft ernaar dat de melding op een beveiligde manier gedaan kan worden, bijvoorbeeld met de versleutelingstechniek PGP.
e. Indien de melding een klant van Ziggo betreft, zal Ziggo de (contact)gegevens van de betreffende klant slechts dan afgeven (om direct melden mogelijk te maken), wanneer hiervoor expliciete toestemming van de klant is verkregen. In alle andere gevallen zal Ziggo bemiddelen met en tussen melder en de klant.
f. Ziggo (en/of de klant) heeft contact met de melder over de termijn waarop de kwetsbaarheid verholpen zal zijn en maakt afspraak met de melder hoe eventueel de publiciteit wordt gezocht.

2.3 Het aangiftebeleid

a. Ziggo zal niet tot aangifte overgaan indien de melder geen misbruik heeft gemaakt van de gevonden kwetsbaarheid en niet voortijdig de publiciteit is gezocht.
b. Als blijkt dat voor of na de melding door de melder misbruik is gemaakt, kunnen de procesafspraken voor responsible disclosure niet worden gevolgd en zal Ziggo aangifte doen.
c. Onder misbruik van de kwetsbaarheid valt onder meer het bemachtigen van gegevens (anders dan nodig is om kwetsbaarheid aan te tonen), manipulatie van informatie, wijziging van de netwerkconfiguratie en het kennis nemen van (vertrouwelijke) gegevens.
d. Ziggo hoeft de procesafspraken voor responsible disclosure niet te volgen als blijkt dat de aanvaller zich middels social engineering naar binnen heeft gepraat of wanneer het een Denial of Service aanval betreft.

2.4 Het beloningsbeleid
Ziggo bepaalt zelfstandig of een beloning wordt toegekend. Voorwaarde hiervoor is dat er een terechte melding is gedaan met een vernieuwend en substantieel karakter binnen de voorwaarden van deze gedragscode. In overleg met de melder wordt afgesproken of de melder wordt vermeld in een eventuele publicatie over de kwetsbaarheid.

3. Wijze van bekendmaking
Ziggo heeft de beschikbare informatie die samenhangt met deze gedragscode in begrijpelijke bewoordingen en in toegankelijke vorm op één pagina op de website van Ziggo geplaatst. Ziggo geeft duidelijk aan waar de informatie op de website te vinden is. Deze informatie is beschikbaar voor alle klanten.

Op de website van Ziggo is aangegeven dat Ziggo de Gedragscode Responsible Disclosure hanteert. De gedragscode is ook te vinden op de website van Ziggo.

De meldinstructie en gedragscode is via de volgende link te vinden:
https://www.ziggo.nl/klantenservice/meldpunt-beveiligingslekken

4. Slotbepalingen

De gedragscode is van toepassing op alle personen en/of organisaties die de gedragscode hebben onderschreven. Wijzigingen in deze code komen tot stand op initiatief van Ziggo en worden gepubliceerd op de reguliere Ziggo webpagina voor het meldpunt beveiligingslekken. De gedragscode zal 6 maanden na in gebruikname worden geëvalueerd.