

Gedragcode DELTA

Responsible Disclosure

Reikwijdte

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

Definities

- Een melding betreft het door een melder aan DELTA melden van een vermoedelijk beveiligingsprobleem op een verantwoorde wijze;
- De melder is de persoon of instantie die een melding doet;
- DELTA is een aanbieder van openbare telecommunicatienetwerken en/of –diensten;
- Een beveiligingsprobleem of kwetsbaarheid is een (vermoedelijke) zwakte in of inbreuk op de beveiliging van de infrastructuur of ICT-systeem van het bedrijf en/of van de klanten;
- Een klant betreft degene waarmee het bedrijf een zakelijke overeenkomst heeft voor het beheren van infrastructuur of ICT-systemen;
- Op verantwoorde wijze melden houdt in dat de melder het beveiligingsprobleem of kwetsbaarheid meldt via het proces zoals dat door DELTA wordt gehanteerd.

1 Aanleiding

DELTA neemt veiligheid uiterst serieus. Voor DELTA staat het vertrouwen in dienstverlening bovenaan. DELTA heeft een eigen verantwoordelijkheid om beveiliging op een passende wijze te waarborgen. DELTA werkt daarnaast gezamenlijk met andere bedrijven in de telecomsector aan het vergroten van de beveiliging. DELTA is voor de continuïteit van dienstverlening afhankelijk van complexe ICT-systemen. De privacy van gebruikers en klanten van DELTA is van groot belang, net als de vertrouwelijkheid van communicatie en informatie. Daarom moet voorkomen worden dat onbevoegden toegang krijgen tot de infrastructuur van DELTA of de gegevens van gebruikers en klanten. Om dit te voorkomen

investeert DELTA veel in de veiligheid van de infrastructuur. Daarnaast controleert DELTA voortdurend op onregelmatigheden, zoals inbraakpogingen.

Incidenten kunnen diverse oorzaken hebben, zoals menselijke fouten, 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 DELTA het makkelijker maken voor derden om vermoedelijke beveiligingsproblemen te melden. Hiermee hoopt DELTA 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 bekende kwetsbaarheid waarvoor al een beveiligingsupdate bestaat eenvoudiger te dichten dan een nieuwe kwetsbaarheid die voor het eerst aan het licht komt. Ervaring met responsible-disclosure-programma's van internationale ICT-bedrijven leert dat het verhelpen van sommige nieuw ontdekte kwetsbaarheden van enkele maanden tot meer dan een jaar kan duren. De snelheid waarmee een kwetsbaarheid kan worden verholpen, kan dus sterk verschillen.

2 Responsible-disclosure-procedure

De intentie van deze procedure is het ervoor zorgen dat het voor derden helder is hoe zij op een verantwoorde wijze kwetsbaarheden in de beveiliging van de infrastructuur en ICT-systemen van DELTA kunnen rapporteren. Met het onderschrijven van deze gedragscode hanteert DELTA de volgende uitgangspunten en procesafspraken voor responsible disclosure:

2.1 De uitgangspunten

- DELTA zorgt voor een voor derden duidelijke proces en eigen meldpunt om beveiligingsproblemen en kwetsbaarheden te rapporteren. DELTA zorgt voor een bekendmaking van dit proces, bijvoorbeeld door het te plaatsen op de corporate website, eventueel met uitleg en randvoorwaarden.
- DELTA zorgt ervoor dat de procesafspraken op relevante plekken in de organisatie bekend zijn en worden nageleefd.
- De melder van een kwetsbaarheid en DELTA spreken af op welke termijn duidelijkheid geboden zal worden over de wijze waarop de kwetsbaarheid verholpen kan worden.
- De melder van een kwetsbaarheid en DELTA spreken af of en op welke wijze er publiciteit wordt gezocht

2.2 De procesafspraken voor een melding

- a. DELTA zorgt ervoor dat een kwetsbaarheid op een toegankelijke manier gemeld kan worden. Op de website delta.nl staan de stappen uitgelegd.
- b. De melder zelf moet duidelijk benoemen wat het onderwerp is en de melding moet vergezeld gaan van bewijsmateriaal ten behoeve van de handelingsperspectief voor DELTA.
- c. De melding mag anoniem worden gedaan.
- d. Indien de melding de systemen van een klant van DELTA betreft, zal DELTA de (contact)gegevens van de betreffende klant slechts dan afgeven om direct melden mogelijk te maken, wanneer hiervoor toestemming van de klant is verkregen. In alle andere gevallen zal DELTA bemiddelen met en tussen melder en de klant.
- e. DELTA (en/of de klant) informeert de melder over de termijn waarop de kwetsbaarheid verholpen zal zijn en maakt afspraken met de melder hoe eventueel de publiciteit wordt gezocht.

2.3 Het aangiftebeleid

- a. DELTA 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 kan DELTA ervoor kiezen toch 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 dan wel openbaar maken van (vertrouwelijke) gegevens.
- d. DELTA 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.

2.3 Het aangiftebeleid

DELTA bepaalt zelfstandig of een beloning wordt toegekend in geval van een melding, wat deze beloning inhoudt en onder welke voorwaarden dit gebeurt. In overleg met de melder wordt afgesproken of de melder wordt vermeld in de eventuele publicatie over de kwetsbaarheid.

3 Wijze van bekendmaking

DELTA heeft de beschikbare informatie die samenhangt met deze gedragscode in begrijpelijke bewoordingen en in toegankelijke vorm op één pagina op de corporate website van het bedrijf geplaatst. Deze informatie is beschikbaar voor alle klanten. Op de corporate website van het bedrijf is aangegeven dat het bedrijf de Gedragscode Responsible Disclosure hanteert. De gedragscode is ook te vinden op de corporate website van het bedrijf.

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 DELTA en worden gepubliceerd op delta.nl - op de reguliere webpagina voor het meldpunt beveiligingslekken.