Gedragscode 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 richt zich op bedrijven die aanbieders zijn van openbare telecommunicatienetwerken en/of –diensten;
- Hetgeen afgesproken in deze code laat wettelijke verplichtingen onverlet;
- Bedrijven die deze gedragscode onderschrijven, beogen met de Gedragscode Responsible Disclosure te voorzien in de behoefte aan transparante informatie voor derden omtrent de bij het bedrijf geldende procedure van responsible disclosure.

Definities

a. Een melding betreft het door een melder aan een bedrijf op verantwoorde wijze melden van een vermoedelijke beveiligingsprobleem;
b. De melder is de persoon of instantie die een melding doet;
c. Het bedrijf is een aanbieder van openbare telecommunicatienetwerken en/of –diensten;
d. 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;
e. Een klant betreft degene waarmee het bedrijf een zakelijke overeenkomst heeft voor het beheren van infrastructuur of ICT-systemen;
f. Op verantwoorde wijze melden houdt in dat de melder het beveiligingsprobleem of kwetsbaarheid meldt via het proces zoals dat door het betreffende bedrijf wordt gehanteerd en dat bekend wordt gemaakt via de respectievelijke corporate websites

1. Aanleiding

Voor telecombedrijven staat het vertrouwen in dienstverlening bovenaan. Ieder bedrijf heeft een eigen verantwoordelijkheid om beveiliging op een passende wijze te waarborgen. De sector werkt daarnaast tevens aan gezamenlijke initiatieven die bijdragen aan het vergroten van de beveiliging. Telecomdiensten zijn voor hun continuïteit afhankelijk van complexe ICT-systemen. De privacy van gebruikers en klanten van bedrijven is van groot belang, net als de vertrouwelijkheid van communicatie en informatie. Daarom moet voorkomen worden dat onbevoegden toegang krijgen tot de infrastructuur van bedrijven of de gegevens van gebruikers en klanten. Om dit te voorkomen investeren bedrijven veel in de veiligheid van hun infrastructuur. Daarnaast controleren bedrijven 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 willen telecombedrijven het makkelijker maken voor derden om vermoedelijke beveiligingsproblemen te melden. Hiermee hoopt de sector problemen sneller te herstellen en te voorkomen dat informatie in de verkeerde handen valt.

Deze gedragscode is van dusdanig generieke aard dat deze ook voor andere bedrijven dan telecombedrijven toepasbaar is. Wel kunnen er verschillen 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 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 kunnen rapporteren aan het desbetreffende bedrijf.

Met het onderschrijven van deze gedragscode hanteert het bedrijf de volgende richtlijn voor responsible disclosure:

2.1 De uitgangspunten

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

2.2 De procesafspraken voor een melding

a. Het bedrijf zorgt ervoor dat een kwetsbaarheid op een toegankelijke manier gemeld kan worden, bijvoorbeeld via een herkenbaar mailadres zoals cert@<domein bedrijf> of security@<domein bedrijf>.
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 het bedrijf.
c. De melding mag anoniem worden gedaan.
d. Het bedrijf streeft ernaar dat de melding op een beveiligde manier gedaan kan worden, bijvoorbeeld met de versleutelingstechniek PGP.
e. Indien de melding de systemen van een klant van het bedrijf betreft, zal het bedrijf 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 het bedrijf bemiddelen met en tussen melder en de klant.
f. Het bedrijf (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. Het bedrijf 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 het bedrijf 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. Het bedrijf 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
Het bedrijf 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
Het bedrijf 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 tot stand gekomen binnen Nederland ICT en van toepassing op alle bedrijven die de gedragscode hebben onderschreven. Wijzigingen in deze code komen tot stand op instigatie van de initiatiefnemers van deze code. De gedragscode zal 6 maanden na de ondertekening door de initiatiefnemers van deze code worden geëvalueerd.

De gedragscode treedt in werking op datum 1 november 2013 en geldt voor onbepaalde duur. De gedragscode kan door een deelnemer ten aanzien van zijn eigen betrokkenheid worden opgezegd met inachtneming van een opzegtermijn van 1 maand.

Gedragscode november 2013

De initiatiefnemers:

Koninklijke KPN N.V.
Vodafone Libertel B.V.
T-Mobile Netherlands B.V.
Tele2 Nederland B.V.
UPC Nederland B.V.
Ziggo N.V.