UGent beleid voor gecoördineerde bekendmaking van IT-kwetsbaarheden[1]

Het is voor medewerkers en studenten van de UGent, alsook voor derden extern aan de UGent **toegelaten** actief kwetsbaarheden in de beveiliging van de ICT-infrastructuur van de UGent op te sporen, voor zover dat gebeurt **in overeenstemming met de bepalingen** van voorliggend (door het bestuur goedgekeurd) beleid voor gecoördineerde bekendmaking van IT- kwetsbaarheden.

De UGent kan **incentives** of beloningen voorzien (campagnegewijs of permanent, eventueel voor een afgelijnde scope) voor wie kwetsbaarheden meldt overeenkomstig voorliggend beleid. De UGent zal geen beloningen uitkeren aan medewerkers of studenten van de UGent voor melding van kwetsbaarheden op systemen of toepassingen onder hun eigen beheer.

Opsporen van kwetsbaarheden mag enkel met goede bedoelingen gebeuren. De UGent zal geen sancties opleggen of juridische stappen ondernemen tegen wie zich houdt aan de regels van dit beleid en geen illegale acties onderneemt.

De **scope** van dit beleid omvat **de IT-infrastructuur van de UGent met uitzondering van** websites, toepassingen, systemen, etc. die **expliciet uitgesloten** worden. De directie ICT zal op de centrale helpdesksite aangeven wat buiten de scope van dit beleid valt en dus niet in aanmerking komt voor onderzoek op kwetsbaarheden. Actief zoeken naar kwetsbaarheden in informatiesystemen die uitgesloten worden van de scope van dit beleid is ongeoorloofd en kan leiden tot sancties en/of gerechtelijke vervolging.

De UGent engageert zich om meldingen van kwetsbaarheden naar best vermogen te (laten) verwerken en op basis van risicoanalyse passende remediëring te voorzien, zowel in door DICT centraal beheerde infrastructuur als in decentraal beheerde infrastructuur. In het geval van een potentieel datalek of ander incident met vertrouwelijke informatie of persoonsgegevens worden betrokkenen (en indien nodig autoriteiten) op een gepaste manier op de hoogte gebracht.

De UGent behoudt zich het recht voor om een tussenpersoon of coördinator aan te duiden en/of een centraal technisch platform (beheerd door de directie ICT) in te zetten waarop eventueel ook beloningen voor het opsporen en melden van kwetsbaarheden worden aangeboden, met als doel een constructieve relatie tussen de partijen tot stand te brengen en te behouden, of eventueel de anonimiteit van de deelnemer waarborgen.

Overeenkomstig het reglement voor correct gebruik van de ICT-infrastructuur van de Universiteit Gent[2], dragen alle ICT-beheerders (zowel die van de directie ICT als die van andere directies binnen de centrale administratie en die van faculteiten en vakgroepen) zelf de **verantwoordelijkheid voor de beveiliging** van de systemen en toepassingen die onder hun bevoegdheid vallen. Zij moeten daarom voor die systemen en toepassingen actief kwetsbaarheden (laten) opsporen en (laten) remediëren.

Door ICT-beheerders van de UGent kan naar dit beleid verwezen worden om in bepaalde websites, toepassingen, systemen gericht naar kwetsbaarheden te laten zoeken, door andere UGent medewerkers, door UGent studenten of door derden extern aan de UGent.

[1] Coordinated Vulnerability Disclosure Policy (CVDP)
[2] https://codex.ugent.be?regid=REG000157

Addenda

1. Wederzijdse verplichtingen

De directie ICT (DICT) zal dit beleid, de scope van toepassing en de uitzonderingen daarop duidelijk communiceren. Op de centrale helpdesksite van DICT zal gepubliceerd worden:

- Instructies hoe gevonden kwetsbaarheden moeten gemeld worden.
- Welke toepassingen of systemen niet in aanmerking komen voor onderzoek op kwetsbaarheden en dus buiten de scope van dit beleid vallen.
- Welke incentives of beloningen er zijn, eventueel specifiek voor bepaalde toepassingen of systemen (bv. een bug bounty programma met een eventuele beloning of een vermelding in een responsible disclosure “Hall of fame”).

Als deelnemer aan dit beleid hou je je aan de volgende regels:

- Je valt enkel toepassingen en systemen aan die binnen de scope van dit beleid vallen.
- Je maakt de kwetsbaarheid niet openbaar en communiceert hier niet over met anderen tot bevestigd werd dat het probleem opgelost werd.
- Je maakt geen misbruik van de situatie: je doet enkel het minimum om te bevestigen dat de kwetsbaarheid aanwezig is. Je verwijdert, wijzigt, leest of kopieert niet meer data dan nodig is om het probleem aan te tonen.
- Je voert geen kwaadwillende aanvallen uit op externe systemen vanaf IT-infrastructuur van de UGent.
- Je wist alle gegevens die je verkregen hebt via de kwetsbaarheid meteen na de melding, in het bijzonder alle persoonsgegevens. Indien je zicht hebt gekregen op persoonsgegevens, dan moet je dit ook melden.
- Je mag de volgende handelingen niet toepassen:
  - opzettelijke pogingen om communicatie of netwerktraffiek te onderscheppen
  - plaatsen van malware of andere hacking tools
  - downloaden, kopiëren, wijzigen of verwijderen van data en/of wachtwoorden
  - aanbrengen van permanente of onomkeerbare veranderingen in een systeem
  - onnodig toegang nemen tot systemen of toegang delen met anderen
  - geautomatiseerde scans die de goede werking van toepassingen in productie storen
  - poging tot bruteforcing van toegang tot systemen
  - aanvallen of omzeilen van fysieke beveiliging
  - phishing, social engineering, spam versturen
  - (distributed) denial-of-service attacks

2. Voor geïnteresseerde deelnemers

Als je een kwetsbaarheid in de beveiliging van de ICT-infrastructuur van de UGent ontdekt, dan moet je die kwetsbaarheid zo snel mogelijk melden. Het uitbuiten van de kwetsbaarheid of ze verder bekend maken aan derden is verboden.

Meld eventuele gevonden kwetsbaarheden via het daartoe geëigende kanaal of IT-platform.
Precieze instructies zullen op de website van de helpdesk van de directie ICT (https://helpdesk.ugent.be) van de UGent gepubliceerd worden. Melding kan bv. gebeuren per e-mail aan de helpdesk van DICT eventueel met kopie aan de verantwoordelijke van het systeem, of via een daartoe geëigend elektronisch vulnerability disclosure of bug bounty platform aangeboden door DICT.

Je bevestigt bij het melden van een kwetsbaarheid dat je dit beleid voor gecoördineerde bekendmaking van kwetsbaarheden gelezen hebt en dat je werkt overeenkomstig de bepalingen ervan.

Zorg ervoor dat je zelf ook terug kan gecontacteerd worden.

Inlichtingen die je moet verstrekken bij de melding van een kwetsbaarheid zijn bijvoorbeeld: soort kwetsbaarheid, configuratiedetails, verrichte handelingen, gebruikte tools, data van de tests, bewijzen, IP-adres of URL van het getroffen systeem, screenshot, contactgegevens, enz.
Geef ook details over vertrouwelijke gegevens of persoonsgegevens van de UGent waartoe je eventueel toegang hebt gehad.

Voor elke fase van de afhandeling van meldingen zijn er indicatieve maximumtermijnen. Het versturen van een ontvangstbevestiging aan de deelnemer gebeurt normaal gezien binnen de week, het opvragen en meedelen van bijkomende informatie binnen de twee weken, de onderzoeken en het ontwikkelen van een oplossing en het antwoord aan de deelnemer binnen 2 maand, en de eventuele toekenning van een beloning of de toelating tot publicatie binnen de 3 maand.

De genoemde maximumtermijnen blijven flexibel, en kunnen ingekort of verlengd worden naargelang de complexiteit van de kwetsbaarheid, het aantal getroffen systemen, de dringendheid of de ernst van de situatie.

Publicatie van gevonden issues zal altijd worden toegestaan mits naleven van een onderling overeen te komen voldoende lang embargo (maximaal 3 maand).

3. Legal Fineprint

Dit beleid is van toepassing op de IT-infrastructuur van de UGent. Sommige delen van de IT-infrastructuur (bepaalde websites, toepassingen, toestellen, diensten, systemen, netwerken,…) kunnen expliciet uitgesloten worden en vallen dan buiten de toegelaten scope van gericht onderzoek. Infrastructuur van derden zoals door UGent gebruikte cloud oplossingen vallen altijd buiten de scope. Kwetsbaarheden in dergelijke toepassingen die het gevolg zijn van specifieke (fouten in) configuraties door de UGent vallen wel binnen de scope, tenzij anders bepaald.

De precieze scoping gebeurt voor centraal beheerde ICT door de directie ICT (DICT) en voor niet-centraal beheerde ICT door de verantwoordelijke IT-beheerder van andere directies, vakgroepen of faculteiten, in overleg met de directie ICT en wordt gepubliceerd op de helpdeskpagina's van DICT.

Kwetsbaarheidsonderzoek op websites, toepassingen, toestellen, diensten, systemen of netwerken die uitdrukkelijk uitgesloten werden, kan leiden tot sancties of gerechtelijke vervolging van de deelnemer. Informatiesystemen van derden zijn altijd uitgesloten van het toepassingsgebied. De directie ICT of de verantwoordelijke IT-beheerder moet vooraf aangesproken worden in geval de scoping onvoldoende duidelijk is of indien er daarover twijfel is bij potentiële deelnemers.

Opzettelijke pogingen om communicatie die niet toegankelijk is voor het publiek of pogingen om elektronische communicatie te onderscheppen, op te nemen of er kennis van te nemen is uitdrukkelijk verboden. Dit verbod slaat niet op de inhoud van communicatie die op strikt toevallige wijze door deelnemers wordt bekomen in het kader van het opsporen van kwetsbaarheden.

Het is de deelnemer verboden informaticagegevens waarvan hij of zij redelijkerwijs kan aannemen dat deze illegaal verkregen zijn, te gebruiken, bij te houden, te onthullen of bekend te maken.

Het is tevens verboden om een toestel te installeren of te laten installeren dat het onderscheppen, kennisnemen of opnemen van communicatie die niet toegankelijk is voor het publiek, mogelijk maakt. Een dergelijk toestel mag wel gebruikt worden voor academisch onderwijs of onderzoek in een strikt gecontroleerde netwerkomgeving en met de toestemming van alle deelnemers aan de communicatie.

Elke deelnemer verbindt zich ertoe om bij zijn acties het evenredigheidsbeginsel na te leven, d.w.z. de beschikbaarheid van de door het systeem geleverde diensten niet te verstoren en geen gebruik te maken van de kwetsbaarheid buiten wat strikt noodzakelijk is voor het aantonen van het beveiligingsprobleem. Indien het probleem op kleine schaal is aangetoond, moet niet verder worden gegaan.

Gegevens van de UGent, waaronder eventuele persoonsgegevens, mogen door de deelnemer enkel verwerkt worden voor zover strikt noodzakelijk voor het aantonen van de informaticakwetsbaarheid. De gegevens mogen niet langer dan noodzakelijk bijgehouden worden. De deelnemer moet aan de UGent melden over welke (categorieën van) gegevens het precies gaat, motiveren waarom ze eventueel verder verwerkt zijn en erop toezien dat deze gegevens tijdens deze periode veilig worden bewaard.

De deelnemer mag de ingezamelde informatie niet delen met derden of verspreiden onder derden, zonder de uitdrukkelijke toestemming van de UGent.

Dit beleid heeft niet tot doel de opzettelijke kennisneming van de inhoud van informatica-, communicatie- of persoonsgegevens mogelijk te maken. Dergelijke kennisneming mag slechts toevallig en incidenteel plaatsvinden in het kader van het opsporen van kwetsbaarheden in de betrokken infrastructuur en technologieën.

De UGent verbindt zich ertoe om voorliggend beleid voor gecoördineerde bekendmaking te goeder trouw

uit te voeren en de deelnemer die de voorwaarden ervan naleeft noch burgerrechtelijk noch strafrechtelijk te vervolgen.

In hoofde van de deelnemer mag er geen sprake zijn van bedrieglijk opzet, het oogmerk om te schaden, of de wil om gebruik te maken van of schade te veroorzaken aan het bezochte systeem of aan de gegevens ervan.

Wat betreft de instrumenten die een inbreuk in verband met informaticagegevens mogelijk maken, kan de deelnemer dergelijke instrumenten uitwerken, bezitten of ter beschikking stellen in het kader van de deelname aan een beleid voor de bekendmaking van kwetsbaarheden. Die acties zijn niet onwettig, zolang ze worden gerechtvaardigd door legitieme doeleinden met betrekking tot het opsporen van kwetsbaarheden met de toestemming van de organisatie van de verantwoordelijke van het betrokken informaticasysteem.

Elk verzoek om een beloning buiten de voorwaarden bepaald door voorliggende beleid of het eventuele bug bounty platform dat de technische en administratieve aspecten van het beloningsprogramma coördineert, kan worden gelijkgesteld met (een poging tot) het plegen van strafrechtelijke inbreuken (bv. afpersing).

De eventuele bekendmaking van de kwetsbaarheid moet gecoördineerd en gesynchroniseerd gebeuren tussen de partijen, om de UGent of andere betrokkenen voldoende tijd te geven om het probleem aan te pakken.

Referenties en bronnen:

CCB gids over het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden (2020)
“Deel I: Goede praktijken” en “Deel II: Wettelijke aspecten”

ENISA Good Practice Guide on Vulnerability Disclosure (November 2015)

NCSC Coordinated Vulnerability Disclosure: de Leidraad (Oktober 2018)