Gecoördineerde bekendmaking

het juridische en compliance kader

Marilyn Vandermarliere – General Counsel, Intigriti

Intro

Marilyn Vandermarliere

General Counsel - Intigriti

Inhoud

Juridische en compliance overwegingen CVDP

- Begrippen
- Is dat allemaal wel legaal?
- Beslissingsfase
  - Redenen om voor VDP te kiezen
  - Argumenten om Board te overtuigen
- Implementatiefase
  - Mogelijke bezorgdheden en aandachtspunten
- Uitvoeringsfase
  - Publieke bekendmaking
  - Bounties
  - Wat als er iets misgaat

VDP

CVDP

Beleid voor gecoördineerde bekendmaking

- Uitnodiging om te testen
- Afspraken over vertrouwelijkheid, melden, scope,…
- Gewoonlijk op een website of ander platform
- Eventueel met onafhankelijke coördinator (bv. CSIRT of Platform)

Ethisch hacken

- Beveiligingsproblemen opsporen
- Met of zonder toestemming
- Melding
- Doel: ICT security verbeteren

BBP

Bug Bounty Programma

- CVDP met vergoeding (geld, swag, reputatiepunten)

Is dat allemaal wel legaal?

Verdrag van Boedapest

- Toegang tot computersysteem of onderdeel daarvan zonder toestemming: strafbaar feit (art. 2)
- LS mag koppelen aan intenties

België

- Externe hacking (art. 550 bis Sw.)

  Intentie irrelevant
- Interne hacking (art. 550 ter Sw.)

  Bedrieglijk opzet of oogmerk om te schaden

Klokkenluiderswet

NIS Wet art. 62/1 & 62/2

Beschermd: **Feiten noodzakelijk voor melding** aan CSIRT


Bedrieglijk opzet /oogmerk om te schaden


Organisatie asap informeren


Verder gaan dan nodig


Openbaar maken zonder toestemming CSIRT

Waarom een CVDP?

Vanuit een juridisch en
compliance perspectief

INTIGRITI

Van onbeheerst risico naar best practice

Traditionele bezwaren

- Illegaal
- In het vizier komen van hackers
- Bijkomend risico creëren, toegang verlenen tot gegevens
- Geen afdwingbare voorwaarden

Evolutie naar

- Waardering
- Best practice
- Get hacked before you get hacked
- Juridische drivers

Onrechtstreekse drivers

GDPR

ISO normen

NIS I

DORA

AI Verord

Rechtstreekse drivers

Cyber Resilience Act

- Digitale producten
- Verplicht CVDP

Klokkenluiderswet

- Recht om te testen en melden
- Melding aan CSIRT als voorwaarde

NIS II

- LS streven om problemen weg te nemen, waaronder strafrechtelijke aansprakelijkheid
- Nationaal beleid voor CVD – CSIRST als coördinator

Hoe implementeren

Vanuit een juridisch en compliance perspectief

INTIGRITI

CVDP als toetredingsovereenkomst

Bepalen van (contractuele) voorwaarden

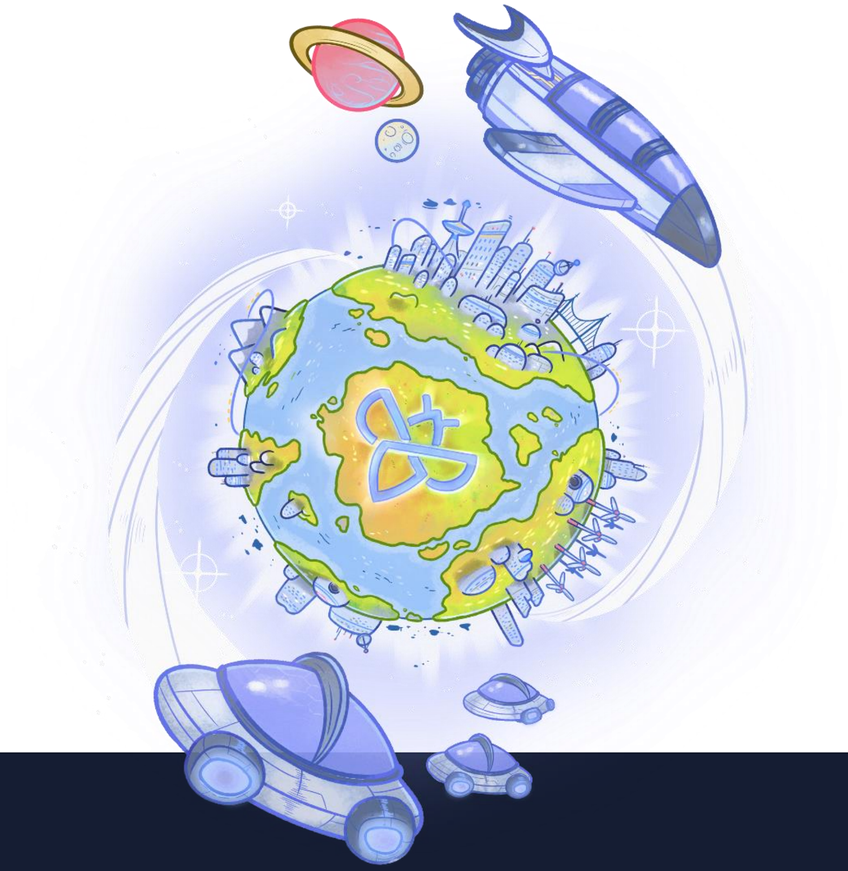
Vrij om al dan niet deel te nemen

Basis inhoud CVDP:

- Scope

- Do’s en don’ts

- Rapportagemodaliteiten



Strafbaarstelling en schade

- Strafbaar in de meeste landen, bij gebrek aan toestemming
- Klokkenluiderswet

Inhoud CVDP:

Toestemming / Safe harbour (quid quo pro)

Uitdrukkelijk verzoek tot analyseren en doordringen van beveiligingsbarrières

Vrijwaring tegen strafrechtelijke aansprakelijkheid

Vrijwaring tegen aanspraken van derden

Beperking/ uitsluiting aansprakelijkheid (volledig / *de minimis* / cap / onrechtsreekse)

Beperking/ uitsluiting aansprakelijkheid voor onrechtstreekse schade

(Intellectuele) eigendomsrechten

Bevoegd om een systeem in scope te stellen?

- Eigenaar systeem
- Uitbater systeem: Verifieer licentiebeperkingen
- Interne bevoegdheid (niet: individuele medewerker security dpt)

Inhoud CVDP:

- Scope
- Third-party systemen buiten scope
- Verhouding met conflicterende service voorwaarden

Handelsgeheimen en vertrouwelijkheid

Organisatie

Inhoud CVDP:

- Vertrouwelijkheidsplicht
- Afspraken over publieke bekendmaking
- Kwetsbaarheid =  en melden

Hacker

- Beschermd door Klokkenluiderswet

Conflicterende belangen & insider info

Inhoud CVDP:

- Uitgesloten deelnemers
- Conflicterende belangen

Samenspel met andere overeenkomsten (insider info)

GDPR – toegang to persoonsgegevens

- Geen verwerkingsdoel
- Mogelijk (accidentele) verwerking

GDPR – toegang to persoonsgegevens

Bezorgdheden

- Rechtsgrond
- Verwerker / verantwoordelijke
  - Controller 2 controller; of
  - CVDP als verwerkersovereenkomst
- Toegang van buiten de EU
- Interne toegang
- Inbreuk m.b.t. persoonsgegevens/meldingsplicht?

- **Inhoud CVDP:**
  - Algemene afspraken en instructies (bv. verbod om te browsen/ downloaden)
  - Toegang van buiten EU?
  - Verplicht om toegang tot PII te melden
  - Eventueel: Checks art. 28 GDPR

Verdere uitvoering

Publieke bekendmaking

- Erkenning
- Afspraken in CVDP
  - Timing
  - Vereist akkoord
  - Inhoud en vermeldingen
- Intellectuele eigendom en vertrouwelijkheid
  - Eigenaar systeem
  - Hacker

Bounties

- Sancties en embargoes
- Facturatie en fiches
- Platformen to the rescue

Wat als er iets misgaat?

Kwetsbaarheid = aanwezig

Quid quo pro: *safe harbour* als best practice

Good faith hacker: Complexiteit foutaansprakelijkheid

Bad faith hacker

- Strafrechtelijke aansprakelijkheid
- Burgerrechtelijke aansprakelijkheid

BCP / DRP

(Cyber) verzekering

- Foutloos
- Dekking aangestelden

Vragen?

INTIGRITI

Thank you

Marilyn.vandermarliere@intigriti.com