Informatieclassificatie Vlaamse overheid (Vo-ICR)

Veiligheidstesten

Minimale maatregelen

Team Informatieveiligheid| Digitaal Vlaanderen

Dit is een document voor publiek gebruik

AGENTSCHAP
DIGITAAL VLAANDEREN
HAVENLAAN 88 BUS 60, 1000 BRUSSEL

KORTE SAMENVATTING

Dit document beschrijft wat de Vlaamse overheid verstaat onder verschillende praktijken die de veiligheid van (software) code bewaken. Specifiek gaat het over:

- **Code review**: het controleren van code op veiligheidsproblemen tijdens de ontwikkelings- en testfases
- **"Vulnerability scans":** het testen op kwetsbaarheden in een toepassing en haar onderliggende infrastructuur
- Incidenten of waarschuwingen die voortkomen uit **security mechanismen**, zoals "Intrusion Detection/Prevention Systems" of next-generation netwerk sensoren
- **Penetratietesten**: het testen op kwetsbaarheden in toepassingen en websites in productie
- **Responsible Disclosure**: publiekelijk de vraag stellen aan white hat hackers om kwetsbaarheden te zoeken in toepassingen en websites die in productie staan

In deze oplijsting zit een logische, chronologische volgorde, wat ook in lijn ligt met het concept van Security by Design.

Voor elk van deze praktijken brengen we in kaart:

- welke risico's ze afdekken
- wat we exact onder elk van deze praktijken verstaan
- in welke omgeving toepassingseigenaars of -beheerders deze moeten uitvoeren
- tegen welke scope deze tests moeten gebeuren
- welke tools je kunt gebruiken

Ook geven we aan hoe de (toepassings)eigenaar omgaat met het oplossen van gevonden kwetsbaarheden. Hierbij is risico-appetijt de basis.

Het is essentieel om binnen de (eigen) organisatie de rollen en verantwoordelijkheden duidelijk af te lijnen om tot een effectief beheer van kwetsbaarheden te komen. Het uitvoeren en inrichten van veiligheidstesten is hierin slechts de eerste stap. Elke entiteit kan zelf beslissen hoe ze zich hiervoor organiseert. In het hoofdstuk Rollen en verantwoordelijkheden geven we hier wel een aanzet voor.

INHOUD VAN DIT DOCUMENT

Situering van het document

Dit document maakt deel uit van de begeleidende documentatie in context van het generieke informatieclassificatieraamwerk (ICR) van de Vlaamse overheid (Vo) op initiatief van het Stuurorgaan Vlaams Informatie- en ICT Beleid.

Doel van het document

Dit document geeft scope aan van welke praktijken toepassingseigenaars moeten ondernemen om de veiligheid van hun (software) code op orde te hebben. Het legt op welke praktijken ze hiervoor moeten toepassen, de frequentie ervan en wanneer ze gevonden kwetsbaarheden moeten oplossen.

Verspreiding van het document

Dit document is voornamelijk voor intern gebruik en bevat informatie die mag gedeeld worden met personen verbonden aan de Vo en zijn diensten leveranciers.

Het document mag gedeeld worden met derden onder de richtlijnen openbaarheid van bestuur van de Vlaamse regering.

Vrijwaring

Dit document geeft de huidige status en daaraan gerelateerde informatie binnen het project weer. Gelieve de auteur of de bevoegde project begeleiders te contacteren om zich ervan te vergewissen dat u de laatst gevalideerde versie van dit document in handen heeft.

Eigenaar

Voorzitter werkgroep informatieveiligheid | Digitaal Vlaanderen

security@vlaanderen.be

Classificatie

Dit document valt onder de vertrouwelijkheidsklasse 1 (Publiek) en mag toegankelijk zijn voor iedereen.

Dit document valt onder integriteitsklasse 2. De organisatie heeft **geen directe hinder** indien de informatie gewijzigd wordt door onbevoegden en de **dienstverlening blijft gegarandeerd**. Maar bijsturing van de criteria en/of maatregelen is aangewezen.

Historiek

Datum	Auteur	Opmerkingen

v.0.1	31 maart 2020	Beau Janssens	Eerste versie
v.0.2	13 mei 2020	Beau Janssens	Tweede versie na input van verschillende gesprekspartners (binnen HFB, Onderwijs & Vorming, AIV)
v.0.3	16 juli 2020	Beau Janssens	Derde versie na bijkomende aligning en input
v.0.4	20 oktober 2020	Beau Janssens	Finale draft ter goedkeuring, na bijkomende feedback belanghebbenden

Bronnen en verwijzingen

https://owasp.org/www-project-top-ten/

https://cve.mitre.org/

https://www.exploit-db.com/search?q=

INHOUDSOPGAVE

WELKE RISICO'S DEKKEN WE AF?

De bedoeling van al deze oefeningen is om kwetsbaarheden te identificeren. Gelet op de aard van de oefeningen is niet te voorspellen welke kwetsbaarheden naar boven komen. Deze kunnen betrekking hebben op alle drie kwaliteitskenmerken van informatie: vertrouwelijkheid, integriteit en beschikbaarheid.

Het is wel zo dat bij bijvoorbeeld penetratietesten de scope zo te bepalen is, dat er een focus ontstaat op één bepaald soort kwetsbaarheid. Dit kan ook specifiek het doel zijn van een test: het beoordelen van één specifiek risico. Dit doe je in overleg met je specialist Informatieveiligheid.

De vuistregel is dat hoe vroeger je een kwetsbaarheid identificeert, hoe makkelijker én hoe goedkoper het is om ze op te lossen.

Alle (best) practices en technieken die in dit document beschreven staan, zijn onderhevig aan risicoanalyses. Elke kwetsbaarheid moet je analyseren in haar context en op basis van die analyse bepalen hoe je ermee omgaat. De kwetsbaarheid moet ook effectief uitbuitbaar ('exploitable') zijn en een reëel risico vormen. Het is aan elke (toepassings)eigenaar om te beslissen welke kwetsbaarheden zij oplossen. Voor eventuele restrisico's geldt dat er een risicoaanvaarding nodig is.

Rapportering over de gevonden kwetsbaarheden gebeurt uiteraard binnen de eigen entiteit volgens de daar geldende procedures. Van zodra er kwetsbaarheden geïdentificeerd zijn die impact kunnen hebben op andere entiteiten, moet dit duidelijk gecommuniceerd worden. Bij gedeelde infrastructuur bijvoorbeeld moet duidelijk zijn, wie welk issue moet oplossen.

Bijvoorbeeld: Je laat een penetratietest afnemen op je toepassingen die gebruik maakt van een bouwsteen van Het Facilitair Bedrijf. Als er in die bouwsteen kwetsbaarheden zijn, moet de eigenaar van die bouwsteen het probleem oplossen. Je lost enkel kwetsbaarheden op over domeinen waar je zelf voor verantwoordelijk bent.

DE DETAILS OVER CODE REVIEW

Wat is het?

Met code review bedoelen we alle manuele/geautomatiseerde controles die je kunt doen om de veiligheid van de code van een toepassing te controleren. Afhankelijk van de fase waarin je ontwikkeling zich bevindt, is een ander soort review nodig. Deze reviews gebeuren in de ontwikkel-, test- of acceptatieomgeving.

Je hebt statische en dynamische code reviews:

- **Statische reviews** gebeuren op niet-gecompileerde broncode – in essentie dus code zonder context.
- **Dynamische reviews** gebeuren op code die in een context geplaatst is, bijvoorbeeld in een test- of acceptatieomgeving waar je kunt zien hoe de code zich in een proces gedraagt.

Behalve deze twee testen, kun je met andere testen tijdens het ontwikkelproces (unit testing of acceptatietesting bijvoorbeeld) ook de veiligheid in een toepassing testen. Dit kun je manueel in een testscenario of automatisch doen.

Het objectief is risico's te identificeren en te analyseren welke risico's je moet/kunt mitigeren.

In welke omgeving doe je code review?

- Statische code reviews doe je in de ontwikkelomgeving. Dit is een controle op kwetsbaarheden in een abstracte context
- Dynamische code reviews doe je in de test- en/of acceptatieomgeving. Dit is een controle op kwetsbaarheden in een functionele context

Hierbij is het belangrijk veiligheid en functionaliteit aan elkaar te koppelen. Het moet niet enkel veilig zijn, het moet ook werken.

Wat?

- Code review focust op kwetsbaarheden die voorkomen in de "OWASP top 10" (zie link op p.3)
- Je kunt ook specifieke dreigingen checken, bijvoorbeeld gebaseerd op gepubliceerde kwetsbaarheden. Deze kun je bijvoorbeeld vinden op https://www.cvedetails.com/ of https://www.exploit-db.com/search?q=
- Je maakt een **risico-afweging** van welke kwetsbaarheden je moet oplossen. Het streefdoel is dat je zoveel mogelijk kwetsbaarheden oplost in de mate van het financieel/projectmatig haalbare
- Ook al naargelang je risico-appetijt kun je bepaalde kwetsbaarheden meenemen naar een volgende fase in de ontwikkeling
- Je zorgt ervoor dat dit proces deel uitmaakt van je quality assurance op nieuwe ontwikkelingen
- Je promoveert je code pas naar een volgende fase als alle kwetsbaarheden die je wilt oplossen volgens je risico-appetijt, opgelost zijn

Welke tools?

- De Vlaamse overheid legt geen specifieke tools op. Het team Informatieveiligheid kan wel advies verlenen
- Dit is een dienst die je kunt afnemen binnen het raamcontract

Enkele tools die hiervoor bestaan zijn Twistlock, of HP Fortify en HP WebInspect. Binnen verschillende entiteiten zijn er al andere tools in gebruik. De tool is enkel het middel; het belangrijkste is dat de controle op de code gebeurt.

Scope?

- Alle online toepassingen
- Alle websites
- Alle intern ontsloten toepassingen (enkel toegankelijk voor geauthenticeerde gebruikers op het Vlaamse overheid-netwerk)

Wat met externe code of toepassingen?

- **Ingekochte toepassingen**
  - Hierbij is het belangrijk om na te gaan dat de leverancier deze praktijk toepast. Dit kun je contractueel indekken en deel laten uitmaken van de risicoanalyse van het contracteringsproces. Contacteer hiervoor de Aankoopcentrale
  - Afhankelijk van de risico-appetijt van de entiteit, kun je deze controle grondig uitvoeren en expliciet de bewijslast van de leverancier analyseren en beoordelen; of vertrouwen op de contractuele clausules
  - Deze check doe je vóór je de code of de toepassing inkoopt of installeert. Hier geldt ook het principe dat hoe vroeger je je ervan vergewist dat het oké is, hoe makkelijker het verloop van het proces

- **Open source code**
  - Ook bij open source code en toepassingen is het belangrijk om deze controles uit te voeren
  - Zeker bij open source is dit een gesprek dat je moet voeren met de community die instaat voor het onderhouden van de code
  - Deze check doe je vóór je de code of toepassing uitrolt of installeert
  - In dit soort opzet is zo'n controle natuurlijk heel moeilijk afdwingbaar. Zelfs zonder deze afdwingbaarheid, kun je proberen bepaalde controles uit te voeren en de feedback te bezorgen aan de community, in zoverre de voorwaarden dit toelaten

Ook voor ingekochte code, of open source code gebeurt dit soort oefening in de ontwikkel-, test- of acceptatieomgeving.

DE DETAILS OVER "VULNERABILITY SCANS"

Wat is het?

Met "vulnerability scans" doelen we op (geautomatiseerde) scans van een toepassing en haar onderliggende infrastructuur. Deze gaan op zoek naar onder andere op kwetsbare varianten van infrastructuurcomponenten die niet de juiste patches hebben geïnstalleerd. Ze kunnen ook gekend kwetsbare instellingen opsporen. Dit is een scan die meestal op regelmatige intervals gebeurd, bijvoorbeeld één keer per maand.

De waarschuwingen en opgespoorde issues die hieruit voortkomen, behandel je als een security incident. Deze controles staan beschreven in het Beleidsdocument "Incident beheer".

Als je diensten afneemt van een Security Operations Center (SOC), kun je dat in deze context beheren. Dit zal ook helpen om heel kort op de bal te spelen als er een issue is met een grote reikwijdte. Een snelle reactie op een melding of incident zorgt voor een risicoreductie en heeft budgettaire voordelen.

In welke omgeving doe je vulnerability scans?

- Als de acceptatieomgeving op exact dezelfde manier is ingericht als de productieomgeving, kunnen "vulnerability scans" gebeuren in de acceptatieomgeving vóór een gewijzigde architectuur live gaat, bijvoorbeeld in parallel met integratietests. Dit geldt dan enkel voor testen in het kader van een wijziging
- Als dat niet zo is, kun je "false positive" kwetsbaarheden vinden en moet je sowieso dezelfde oefening nog eens opnieuw doen in productie. Of kun je bepaalde reële kwetsbaarheden niet vinden omdat de context anders is. Dit is een verlies van tijd, energie en geld

- Recurrente testen gebeuren in de productieomgeving. Deze gebeuren met de reguliere producten die op de markt beschikbaar zijn volledig automatisch

Wat?

- De scope van kwetsbaarheden waartegen je scant, leg je vast in overleg met de specialist informatieveiligheid van je entiteit. Dit leidt tot het instellen van parameters in de gebruikte tooling
- Je maakt een **risico-afweging** van welke kwetsbaarheden je moet oplossen
- Het streefdoel is dat je zoveel mogelijk kwetsbaarheden oplost in de mate van het financieel/projectmatig haalbare
- Als er rest-risico's zijn, moet de (toepassings)beheerder deze formeel laten aanvaarden door het top management, zoals beschreven staat in het Beleidsdocument "Risico beheer"

Welke tools?

- De Vlaamse overheid legt geen specifieke tools op. Het team Informatieveiligheid kan wel advies verlenen
- Dit is een dienst die je kunt afnemen binnen het raamcontract

Scope?

- Alle toepassingen en hun onderliggende infrastructuurcomponenten die zich binnen de verantwoordelijk van de Vlaamse overheid bevinden
- Deze toepassingen en hun infrastructuurcomponenten kunnen in eigen beheer zijn, of gelegeerd naar een leverancier.
- In het geval van uitbesteding, moet je contractueel afdekken dat de leveranciers deze controles uitvoert en dat de Vlaamse overheid inzicht krijgt in de resultaten en remediëring van de gevonden kwetsbaarheden. Hoe betrokken je hierin bent, hangt af van je risico-appetijt, zoals ook al hierboven besproken

DE DETAILS OVER SECURITY MECHANISMEN

Wat is het?

Verschillende praktijken kunnen hieronder vallen. Enkele van de meest bekende voorbeelden zijn:

- Intrusion Detection/Prevention Systems (IDS/IPS)
  - Deze technologieën installeer je om aanvallen, of ander ongewenst verkeer op te sporen (IDS), of uit je infrastructuur te weren (IPS)
  - De alerts die deze systemen genereren, kun je gebruiken om vast te stellen waar er zich in je architectuur kwetsbaarheden bevinden. Dit helpt om heel gericht controlemechanismen te ontwerpen en implementeren
  - IDS is een reactieve controle: je voert er geen actieve controle mee uit.
  - IPS is een preventieve maatregel: je bepaalt vooraf wie geen toegang kan krijgen tot je netwerk en
- Next generation network sensoren
  - De technologie is hierin uiteraard al fel geëvolueerd en de meeste omgevingen gebruiken tegenwoordig next-gen network sensoren[1]
  - Deze scannen permanent het netwerk op bepaalde patronen en gebeurtenissen om op basis daarvan gericht het event te kunnen behandelen als een potentieel security incident
  - Afhankelijk van de instellingen is dit een reactieve of preventieve controle

De waarschuwingen en opgespoorde issues die uit deze mechanismen voortkomen, behandel je als een security incident. Deze controles staan beschreven in het Beleidsdocument “Incident beheer”.

Als je diensten afneemt van een Security Operations Center (SOC), kun je dat in deze context beheren. Dit zal ook helpen om heel kort op de bal te spelen als er een issue is met een grote reikwijdte. Een snelle reactie op een melding of incident zorgt voor een risicoreductie en heeft budgettaire voordelen.

Deze diensten zijn geen veiligheidstest in de strikte zin van het woord. Wel kunnen ze helpen om bepaalde kwetsbaarheden te identificeren.

In welke omgeving installeer je deze security mechanismen?

- Als de acceptatieomgeving op exact dezelfde manier is ingericht als de productieomgeving, kun je deze mechanismen in de acceptatieomgeving implementeren
- Als je het in de acceptatieomgeving installeert, kan het gelden als een preventieve maatregel, omdat je voor een promotie naar productie bepaalde kwetsbaarheden kunt detecteren

- Dit soort security mechanismen installeer je sowieso in de productieomgeving

[1] Denk hierbij bijvoorbeeld aan tools van bijvoorbeeld Palo Alto of Darktrace.

Wat?

- De scope van kwetsbaarheden waartegen je scant, leg je vast in overleg met de specialist Informatieveiligheid van je entiteit. Dit leidt tot het instellen van parameters in de gebruikte tooling
- Je zorgt voor een aansluiting op het (security) incident proces
- Je maakt een **risico-afweging** van welke kwetsbaarheden je moet oplossen
- Het streefdoel is dat je zoveel mogelijk kwetsbaarheden oplost in de mate van het financieel/projectmatig haalbare
- Als er na de remediëring van een incident nog rest-risico's zijn, moet de (toepassings)beheerder deze formeel laten aanvaarden door het top management, zoals beschreven staat in het Beleidsdocument "Risico beheer"

Welke tools?

- De Vlaamse overheid legt geen specifieke tools op. Het team Informatieveiligheid kan wel advies verlenen
- Dit is een dienst die je kunt afnemen binnen het raamcontract

Scope?

- Deze mechanismen scannen aan de perimeter van je infrastructuur, of specifieker aan de perimeter van bepaalde toepassingen die bijzondere aandacht vergen. Dit kan gaan om de eigen infrastructuur, die van de centrale dienstverlening, of die bij een leverancier

Het is van het grootste belang om een heel duidelijk beeld te hebben van wie welke verantwoordelijkheid draagt binnen het landschap. Maak afspraken met de verschillende rollen die tussenkomen: toepassingseigenaar, beheerder, netwerkbeheerder, etc. en bespreek duidelijk wie welk soort meldingen gaat oplossen en hoe. Dit vermijdt discussies als er zich in productie incidenten voordoen.

DE DETAILS OVER PENETRATIETESTEN

Wat is het?

Bij een penetratietest vraag je een tester om kwetsbaarheden van een bepaalde toepassing te onderzoeken. Dit gebeurt met een vooraf bepaalde scope: welk(e) (deel van een) toepassing moet de tester benaderen en met welke aanvalsvectoren. Deze testen gebeuren in principe altijd in de productieomgeving.

Het kan hierbij een toegevoegde waarde zijn om te werken met een gecertificeerde tester. Wat echter belangrijker is, is dat er duidelijke afspraken zijn over testscenario's en de modaliteiten van de tets (scope, aanvalsvectoren, timing, etc.).

Een penetratietest is het strikte minimum dat je kunt doen aan veiligheidstesten. Deze test gaat heel wat kwetsbaarheden opvangen die de hierboven beschreven testen ook identificeren. Het is geen 1-op-1 vervanging ervan en het is een kostelijkere manier om hetzelfde te bereiken. Hoe vroeger je kwetsbaarheden identificeert, hoe makkelijker en goedkoper je ze kunt oplossen. Dit doe je door security (en bij uitbreiding privacy) standaard in je design mee te nemen – algemeen heet dit Security/Privacy by Design. Dit concept en hoe je dit kunt meenemen in je levenscyclus, staat ook beschreven in het Beleidsdocument "Ontwikkeling en gebruik van toepassingen".

In welke omgeving doe je penetratietesten?

- Als de acceptatieomgeving op exact dezelfde manier is ingericht als de productieomgeving, kan een penetratietest gebeuren in de acceptatieomgeving vóór een gewijzigde toepassing live gaat. Dit geldt dan enkel voor testen in het kader van een wijziging
- In deze omgeving doe je penetratie testen. Om de mogelijke impact op productie te beperken, kun je de timing wel zo voorzien dat het niet conflicteert met piekmomenten (bijvoorbeeld in een weekend, niet bij een maandafsluiting).

- Recurrente testen gebeuren in de productieomgeving

Wat?

- Er zijn drie soorten tests die je kunt doen:
  - **"White box"**: hierbij heeft de tester informatie over de manier waarop de toepassing is geïmplementeerd en over de interne werking van de organisatie (architectuur, organigram, etc.)
  - **"Black box"**: hierbij heeft de tester in principe geen, of bijna geen informatie over de toepassing of de organisatie
  - **"Grey box"**: hierbij krijgt de tester een deel van de informatie, maar niet zoveel als bij een white box
- Bij het testen houd je rekening met een bepaalde scope. In het zoeken naar mogelijke kwetsbaarheden, moet de penetration tester minstens rekening houden met deze aanvalsvectoren, kwetsbaarheden en technieken:
  - De OWASP top 10 kwetsbaarheden

- (D)DoS paraatheid
- Brute force attack paraatheid
- Buffer overflow/memory leak
- Check tegen gekende CVE reports (zie link op p.3)
- Credential hunting (default passwoorden, hardgecodeerde gebruikersnamen of wachtwoorden)
- Downgrade attacks die gebruik maken van verouderde protocollen
- Exploit servers
- Input errors
- Privilege escalation
- Zoeken naar niet-ondersteunde versies van programma's of systemen

Dit is een overzicht van de verschillende termijnen die je moet respecteren voor het uitvoeren van de tests en het remediëren van ontdekte kwetsbaarheden. Het zegt ook welk soort test je kunt uitvoeren in de gegeven context.

Hoedanigheid/ Informatieklasse van de toepassing	**Frequentie**	**Kritische en Significante risico kwetsbaarheden oplossen binnen[2]**	**Grote en Gemiddelde risico kwetsbaarheden oplossen binnen**	**Kleine risico kwetsbaarheden oplossen binnen**	**Soort test**
Toepassingen die persoonsgebonden informatie bevatten (ongeacht de klasse)	Bij de release[3] van een nieuwe versie, of minstens 1 keer per jaar	2 werkweken	4 werkweken	Opnemen in een volgende release	Black box Grey box White Box
Klasse 3, 4 en 5 (Vertrouwelijkheid en/of Integriteit)	Bij de release van een nieuwe versie, of minstens 1 keer per jaar	2 werkweken	4 werkweken	Opnemen in een volgende release	Black box Grey box White Box
Klasse 1 en 2 (Vertrouwelijkheid en/of Integriteit)	Minstens 1 keer per 2 jaar	4 werkweken	6 werkweken	Opnemen in een volgende release	Grey box White Box

- Je maakt een **risico-afweging** van de gevonden kwetsbaarheden
- Hierbij hou je rekening met het feit of een toepassing naar het internet ontsloten is. Als deze toepassingen kwetsbaarheden hebben, los je deze altijd prioritair op en dit ongeacht hun informatieclassificatie
- De gegeven termijnen zijn maxima. Je kunt dus bijvoorbeeld een "fix" in een volgende release van je toepassing integreren, zolang deze binnen de verwachte oplostermijn past
- Het streefdoel is dat je zoveel mogelijk kwetsbaarheden oplost in de mate van het financieel/projectmatig haalbare volgens het hierboven beschreven schema

[2] De criticaliteit van een gevonden kwetsbaarheid bepaalt de penetration tester samen met de betrokken partijen (security team, toepassingseigenaar, etc.). Dit is altijd een inschatting van het reële risico dat het uitbuiten van deze kwetsbaarheid tot gevolg kan hebben.
Deze schalen bepaal je in lijn met het Beleidsdocument "Risico beheer".

[3] Voor de definitie van "Release" kun je terecht in het Beleidsdocument "Release en deployment beheer". Uiteraard is een release in het waterfall-concept anders dan in een Agile omgeving. Hier kun je rekening mee houden door bijvoorbeeld in een Agile omgeving, deze testen enkel te doen bij substantiële functionele of technische wijzigingen: bijvoorbeeld bij het toevoegen van nieuwe procesmodules, of het wijzigen van de opzet van de toepassingsarchitectuur.

- Als er na de remediëring nog rest-risico's zijn, moet de toepassingsbeheerder deze formeel laten aanvaarden door het top management, zoals beschreven staat in het Beleidsdocument "Risico beheer"
- Na het oplossen van kwetsbaarheden, moet je altijd een nieuwe test doen om er zeker van te zijn dat de kwetsbaarheden in productie opgelost zijn

Welke tools?

- Bij voorkeur gebeurt deze test door een gecertifieerd tester. Deze tester kan zelf bepalen welke tools nodig zijn om het gewenste resultaat te behalen
- Dit is een dienst die de Vlaamse overheid op dit moment alleen inkoopt en waarvoor geen interne medewerkers voorzien zijn
- Dit is een dienst die je kunt afnemen binnen het raamcontract

Scope?

- Alle online toepassingen
- Alle websites
- Alle intern ontsloten toepassingen (enkel toegankelijk voor geauthenticeerde gebruikers op het Vlaamse overheid-netwerk)
- Dit kan gaan om toepassingen of websites in eigen beheer, die van de centrale dienstverlening, of die bij een leverancier

Opmerking:	*Red & Blue teaming (samen ook wel Purple Teaming genoemd), is nog niet opgenomen in dit Beleidsdocument.* *De bedoeling van deze oefeningen in om de effectiviteit van een SOC of incident response team te testen in het geval er een aanval zou zijn. Het is dus het uitvoeren van een fictieve aanval.* *Entiteiten die deze oefeningen al willen uitvoeren, kunnen dit uiteraard doen in overleg met de nodige teams en instanties.*

DE DETAILS OVER RESPONSIBLE DISCLOSURE

Wat is het?

Bij Responsible Disclosure (RD) nodig je white hat hackers uit om kwetsbaarheden te melden op je toepassingen. De voorwaarde is hier wel dat de white hat hacker eventueel gevonden kwetsbaarheden niet actief uitbuit.

Je bepaalt hierbij enkel de scope (bijvoorbeeld: de website www.vlaanderen.be en alle sub-sites hiervan) die ze mogen onderzoeken. Zij proberen op eigen initiatief welke aanvalsvectoren mogelijk zijn. Bij het vinden van een kwetsbaarheid, melden ze dit aan ons (via een externe partij) en verbindt de overheid zich ertoe deze kwetsbaarheid op te lossen.

Een compensatie voor de gevonden kwetsbaarheden is mogelijk. In tegenstelling tot een penetratietest, is de scope van RD veel breder: er zijn minder beperkingen in de scope van wat de white hat hacker kan testen en ze kunnen ook meer aanvalsvectoren gebruiken. Sowieso gebeurt dit op de productieomgeving.

Een white hat hacker mag binnen de context van Responsible Disclosure een gevonden kwetsbaarheid niet publiek maken, tenzij de Vlaamse overheid haar verplichtingen voor een tijdige oplossing niet naleeft. Dit moet de Vo expliciet opnemen in het contract met de white hat hacker, en/of het platform dat we hiervoor gebruiken.

In diezelfde context zorg je er ook voor dat er een duidelijke code of conduct bestaat en bevestigd is door alle betrokken partijen. Dit moet op juridisch sluitende manier moeten gebeuren.

In welke omgeving doe je aan responsible disclosure?

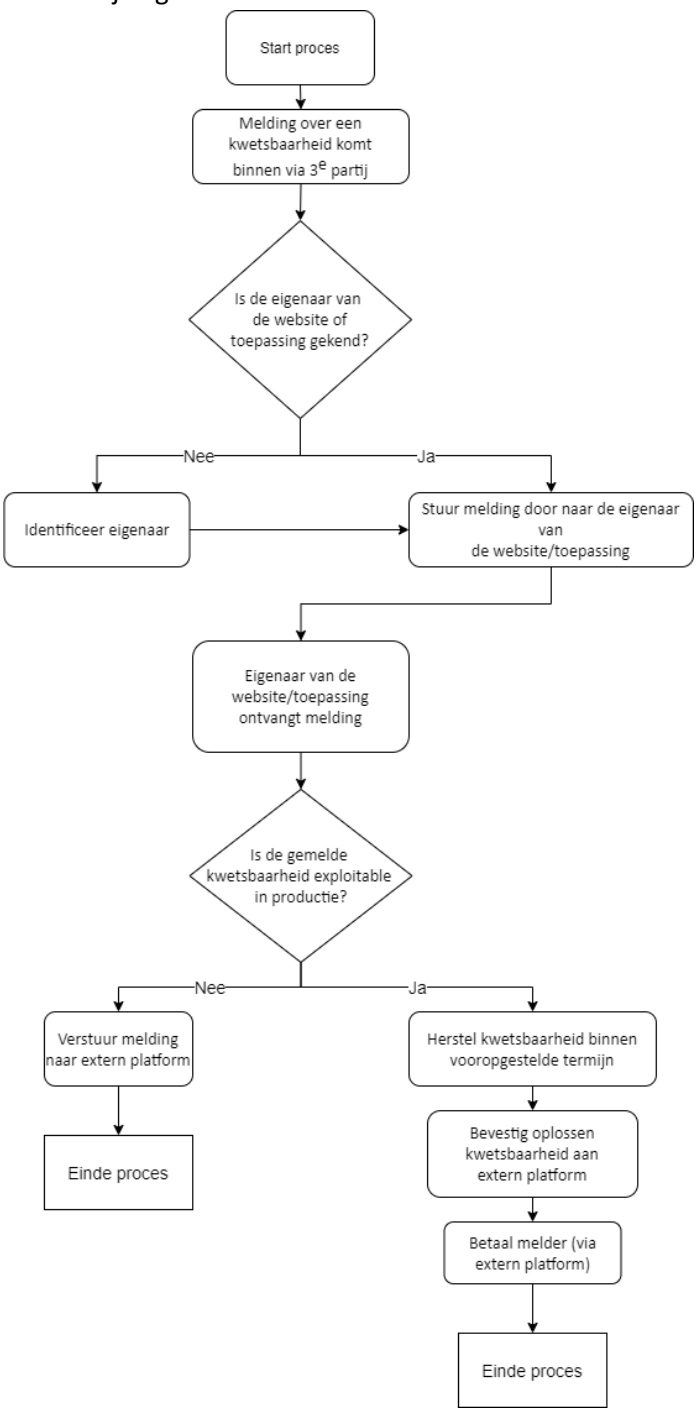
- Omdat dit soort oefening open staat voor mensen buiten onze organisatie, zonder hen extra rechten op onze toepassingen te geven, kan dit enkel in de productieomgeving.

Wat?

- Dit soort oefening is een **aanvulling** op een penetratietest, geen vervanging ervoor. Het biedt namelijk een ander perspectief om te testen: de testscenario's liggen niet vast en bieden dus meer ruimte om aanvalsvectoren te ontdekken
- Dit proces verloopt via een derde partij met wie wij in contact staan via een afzonderlijk beschreven proces
- Een melding van een kwetsbaarheid handel je af als een veiligheidsincident, waarbij de urgentie afhangt van het risico gekoppeld aan de gemelde kwetsbaarheid. Hiervoor kun je dezelfde termijnen hanteren als voor penetratietesten
- De premies die we uitbetalen aan de white hat hacker bij een als uitbuitbaar bewezen kwetsbaarheid:
  - € 100 voor een kwetsbaarheid die voorkomt in de OWASP Top 10
  - Voor andere kwetsbaarheden, een ad hoc te bepalen vergoeding

Welke tools?

〉 Dit proces verloopt via een derde partij met wie wij in contact staan via een afzonderlijk beschreven proces
Hier is een high level beschrijving:



Scope?

- Alle online toepassingen, die in scope van de oefening zijn geplaatst door de deelnemende partijen. Deze lijst deelt de Vo mee aan het platform
- Alle websites, die in scope van de oefening zijn geplaatst door de deelnemende partijen. Deze lijst deelt de Vo mee aan het platform
- Dit kan gaan om toepassingen of websites in eigen beheer, die van de centrale dienstverlening, of die bij een leverancier

Elke entiteit kan voor zichzelf bepalen welke delen van hun online dienstverlening ze in of out of scope willen hebben. Daarbij is het dus belangrijk te begrijpen dat deelname niet verplicht is voor alle entiteiten. Hoe meer entiteiten deelnemen, hoe groter de kostenefficiëntie.

Een aparte aanpak om kwetsbaarheden op te lossen (scope, timing) per entiteit is ook mogelijk. Dit verhoogt uiteraard de complexiteit en de kostprijs.

WANNEER MOET ER IETS GEBEUREN?

Visueel samengevat is dit de samenvatting van de verschillende fases en soorten testen en wanneer wat kan/moet gebeuren. Sommige praktijken kun je in verschillende fases ondernemen; dit kan eenmalig of als controlemechanisme dat fouten in een vorige fase gecorrigeerd zijn.

Dezelfde regels gelden voor

- eigen toepassingen en infrastructuur
- de centrale dienstverlening,
- diensten, (open) source code, toepassingen of infrastructuur die je bij een leverancier inkoopt

Omgeving	Soort test die je uitvoert	Frequentie
Ontwikkeling (development)	Statische code reviews	Vóór promotie naar een volgende omgeving
Test	Dynamische code reviews	Vóór promotie naar een volgende omgeving
Acceptatie	Dynamische code reviews	Vóór promotie naar een volgende omgeving
	Vulnerability scans	Op regelmatige basis, bijvoorbeeld maandelijks
	Penetratietesten	Volgens Informatieklasse
Productie	Vulnerability scans	Op regelmatige basis, bijvoorbeeld maandelijks
	Netwerk scanning	Permanent
	Penetratietesten	Volgens Informatieklasse
	Responsible Disclosure	Permanent

ROLLEN EN VERANTWOORDELIJKHEDEN

Volgende rollen en verantwoordelijkheden werden vastgelegd op basis van een klassiek RACI model.

	Uitvoeder (Responsible)	**Aansprakelijke** (Accountable)	**Raadpleging** (Consultable)	**Informeren** (Informed)
Identificeren kwetsbaarheden	Toepassingseigenaar	(Toepassings)eigenaar	DPO(*) CSO(*)	-
Oplossen kwetsbaarheden	Beheerders (intern aan de Vo, of extern)	(Toepassings)eigenaar	DPO(*) CSO(*)	-
Inschatten en antwoord formuleren op geïdentificeerde risico's	(Toepassings)eigenaar en beheerders	(Toepassings)eigenaar	DPO(*) CSO(*)	In geval van kwetsbaarheden die breder zijn dan de eigen entiteit: Leden van het Stuurorgaan Vlaams Informatie en ICT beleid

DPO: Data Protection Officer
CSO: Chief Security Officer
(*) delegatie aan veiligheidsconsulent is mogelijk