

**BIJLAGE A aan Dienstverleningsovereenkomst**

Security Audit - Howest Security Project **Scope Document**

*Demival v.z.w.*

|  |  |
| --- | --- |
| **Versie document** | *1.0* |
| **Opgesteld op:** | *17/10/2025* |
| **Naam auditeur 1** | *Sam Wolfs* |
| **Naam auditeur 2** | *Guust Taillieu* |

**DIT DOCUMENT IS VERTROUWELIJK**

De informatie in dit document is vertrouwelijk, geheim, juridisch beschermd en enkel bedoeld voor de betrokken ontvangers. De informatie kan niet gepubliceerd of verspreid worden zonder voorafgaande schriftelijke toestemming.

Inhoudstafel

Versiegeschiedenis 3

Contactgegevens 3

Voorwoord 4

1. Methodologie 5

2. Gedragscode 6

Definiëring van de scope 7

1. Algemene afspraken 7

Planning 7

Rapportering en aanvullende bepalingen 7

2. OSINT 8

3. Externe blackbox pentest 9

Toegestane externe scope 9

Regels voor pentesten 9

Post-exploitatie 9

4. Interne blackbox pentest 10

Toegestane interne scope 10

Regels voor pentesten 10

Post-exploitatie 10

5. Optionele testen 11

6. Bevraging medewerkers en DPO/CISO-interview 13

7. Handtekeningen ………………...13

Versiegeschiedenis

1. *17/10/2025 - Initieel ontwerp van het scopedocument in samenspraak met de partner*

Contactgegevens

* **Auditeurs Howest**
  1. Sam Wolfs  
     sam.wolfs@student.howest.be  
     +32 471 83 00 29
  2. Guust Taillieu  
     guust.taillieu@student.howest.be

+32 496 07 70 61

* **Vertegenwoordigers opdrachtgever**
  1. *Lokaal bestuur, DPO  
     Joe Pesci  
     joe.pesci@contoso.org  
     +32 13 14 15 16*
  2. *Lokaal bestuur, IT diensthoofd  
     John Smith  
     john.smith@contoso.org  
     +32 13 14 15 16*

Voorwoord

Dit document beschrijft de scope van de geplande ICT-veiligheidsscan. Het document geeft de toegestane testomgevingen, de te gebruiken technieken en andere praktische afspraken voor de uitvoering van de audit weer. De auditeurs engageren zichzelf om de nodige voorzorgen te nemen, zodat niet afgeweken wordt van deze vooraf vastgelegde scope.

**Het scope document is enkel geldig indien deze gekoppeld wordt aan een ondertekende dienstverleningsovereenkomst.** Alle aanpassingen aan de scope moeten gedocumenteerd en schriftelijk goedgekeurd worden door de klant alvorens deze in werking kunnen treden.

# Methodologie

Om de kwaliteit van de audit te verzekeren, zal de onderstaande methodologie gevolgd worden. Deze methodologie is gebaseerd op de Penetration Testing Execution Standard (PTES), de Penetration Testing Framework en de OWASP Testing Guide, met aanpassingen en aanvullingen door de auditeurs.

**Samenvatting van de verschillende fases binnen de penetration test:**

1. **Open-source intelligence test (OSINT):**   
   Open-source intelligence bestaat uit het verzamelen van potentieel waardevolle informatie over een doelwit aan de hand van publiek beschikbare bronnen. Deze informatie kan gebruikt worden om extra focus te leggen binnen de audit.
2. **Scanning en enumeratie:**De auditeurs achterhalen welke live systemen aanwezig zijn op het netwerk via host discovery en verzamelen bijkomende informatie over deze systemen, zoals de besturingssystemen en softwareversies. Dit is de eerste actieve fase binnen de audit waarbinnen ‘kwaadwillig’ verkeer gedetecteerd kan worden.
3. **Analyse van kwetsbaarheden:**

Op basis van de verzamelde informatie, gaan de auditeurs op zoek naar specifieke zwakheden in systeemsoftware. Dit omvat een scan op publiek gekende kwetsbaarheden (CVE) en het testen van applicaties zoals websites op veelvoorkomende fouten via een fuzzing proces.

1. **Exploitatie kwetsbaarheden:**

Indien kwetsbaarheden gedetecteerd worden, zullen de auditeurs proberen om deze te gebruiken om informatie in te winnen of toegang tot het systeem te verkrijgen. Op basis van het bijhorende risico - zoals een mogelijk systeemcrash – kunnen de auditeurs zich beperken tot een basis ‘proof-of-concept’.

1. **Post-exploitatie:**Via de gecompromitteerde systemen, bijvoorbeeld door middel van opgeslagen inloggegevens, proberen de auditeurs om verder toegang te verkrijgen binnen het huidige (escalatie van privileges) of andere systemen (pivoteren).
2. **Rapportering**

**Opmerking**: Op basis van de beschikbare tijd en goedgekeurde scope kunnen bepaalde testen beperkt of niet uitgevoerd worden. De methodologie zal licht aangepast worden aan elke audit, zodat deze ingepast kan worden binnen de bepaalde scope en timing.

**Voor meer info:**

* Penetration Testing Execution Standard: <http://www.pentest-standard.org/index.php/Main_Page>
* Penetration Testing Framework: <http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html>
* OWASP testing guide: <https://www.owasp.org/images/1/19/OTGv4.pdf>

# Gedragscode

Van de auditeurs wordt verwacht dat zij zich professioneel, rechtsgeldig, eerlijk en ethisch gedragen, en dat zij steeds handelen in het belang van de klant terwijl ze hun werkzaamheden in opdracht van Howest uitvoeren. Deze gedragscode reikt enkele richtlijnen aan voor de verwachte zakelijke gedragscode van Howest studenten en ander betrokken personeel bij de ICT-veiligheidsprojecten. Indien de auditeurs onzeker zijn of hun gedrag of dat van andere betrokken auditeurs tegemoetkomt aan deze code, dienen zij hun coach of leidinggevende te contacteren.

* The auditeurs verzekeren dat ze over de nodige goedkeuringen voor hun testactiviteiten beschikken (dit aan de hand van een ondertekende projectovereenkomst) en dat deze gebeuren binnen een legaal juridisch kader. Zij treden niet buiten de scope die samen met de klant vastgelegd werd binnen het scope document.
* De auditeurs beperken hun dienstverlening tot hun expertiseveld, en zijn eerlijk en rechtuit over de beperkingen van hun ervaring en scholing. Dit omvat zowel tools als technieken en technologieën.
* De auditeurs zullen nooit wetend gebruik maken van software die verkregen weerhouden werd op illegale of onethische wijze.
* De auditeurs nemen alle voorzorgen om de risico’s van hun acties voor de dienstverlening, systemen en netwerken van de klant te beperken.
* De auditeurs zullen nooit informatie van de klant verzamelen, overhandigen, verkopen of doorsturen naar een derde partij zonder eerst schriftelijk toestemming te vragen. Private informatie is en blijft privaat en de vertrouwelijkheid van confidentiële informatie wordt niet geschonden. De auditeurs zullen de informatie alleen gebruiken voor de vooraf goedkeurde doeleinden, met kennis en toestemming van de klant.
* The auditors behouden een transparante relatie met de klant en zullen relevante informatie die gevonden werd tijdens de testactiviteiten op de systemen of netwerken van de klant communiceren. Transparantie houdt in dat de klant steeds op de hoogte is van wat er gebeurt en welke acties ondernomen dienen te worden in kader van de veiligheid van het systeem of netwerk.
* The auditeurs gedragen zich steeds ethisch en professioneel, met respect voor de rechtsgeldigheid van hun acties.
* De auditeurs zijn zich ervan bewust dat bij elke vorm van onethisch gedrag Howest de nodige sancties zal opleggen aan de auditeurs.

**Opmerking:** Indien een deel van deze code indruist tegen bestaande lokale wetgeving en regelgeving, zijn alleen de secties van deze code die overeenstemmen met de bestaande wetten en regelgeving van toepassing. Wetgeving die specifiek geldt binnen de jurisdictie van de klant heeft voorrang waar bepalingen binnen deze code niet overeenstemmen.

# Definiëring van de scope

## Algemene afspraken

### Planning

|  |  |  |
| --- | --- | --- |
| **Test** | **Timing** | **Testlocatie** |
| OSINT | 1 okt - 17 okt | Op afstand |
| Externe Blackbox pentest | 3 nov – 5 nov | Op afstand |
| Interne Blackbox pentest | 6 nov / 7 nov | Op locatie (Demival in Deinze) |
| Bevraging medewerkers | 10 nov - 16 nov | Op afstand |
| Bevraging beveiligings-verantwoordelijke | 10 nov – 16 nov | Op afstand |
| Social Engineering | 18 nov | Op locatie (Demival in Deinze) |

De planning kan aangepast worden in de loop van het project mits akkoord per mail tussen beide partijen.

### Rapportering en aanvullende bepalingen

* **Deadline voor rapportering:** 12/12/2025
* **Aanvullende bepalingen:**
* Alle gevonden kwetsbaarheden die als kritiek omschreven kunnen worden op basis van hun risico en mogelijk impact zullen meteen gerapporteerd worden aan de klant. Onbelangrijke zaken zullen gecommuniceerd worden via teams en belangrijke zaken via mail.
* Acties die een impact kunnen hebben op het bedrijf moeten minimum een halve dag op voorhand goedgekeurd worden. Zolang dit niet is gebeurd, ondernemen we geen actie.
* Persoonsgegevens zullen niet worden vermeld in het uiteindelijke rapport.
* Het finale rapport zal overhandigd worden aan Wim Verleysens via mail als een versleutelde pdf.

## OSINT

Dit is de fase vooraleer de auditeurs overgaan tot verkenning, ook gekend als *footprinting* en *reconnaissance*. Men vergaart publiek beschikbare informatie over het netwerk en de apparaten, maar evenzeer over de organisatie en haar medewerkers. Deze fase is perfect legaal en kan door iedereen buiten de organisatie uitgevoerd worden.

Actieve acties en aanvallen maken **geen** deel uit van deze fase.

De enige vereiste informatie voor dit luik van de scope is de naam of het domein van de klant.  
De vermelde domeinen zijn GEEN beperking voor de OSINT fase vermits hierbij enkel publieke informatie wordt gezocht. Ze worden enkel als richtlijn gegeven voor de auditor(s).

* De mogelijke OSINT-doelwitten zijn:
  + - * *demival.be* en alle sub domeinen
      * *Sociale-media accounts*

## Externe blackbox pentest

Dit is een veiligheidsaudit die buiten het netwerk van de klant wordt uitgevoerd. Deze kan enkeluitgevoerd worden op extern toegankelijke doelwitten die omschreven staan in dit document.

Doelwitten die niet door de klant zelf beheerd worden - zoals een webapplicatie die gehost wordt door Combell of een mailserver op Office365 - kunnen **enkel getest worden indien de klant zelf toestemming verkrijgt van de respectievelijke partner**. Het verkrijgen van deze toestemming is de verantwoordelijkheid van de opdrachtgever. De auditors opereren te goeder trouw dat deze verkregen is voor alle doelwitten opgenomen in de scope. Indien er nog geen toestemming is van de hosting partner, dient dit hieronder vermeld te worden en kunnen de auditors slechts pentesten op het gehost domein als zij schriftelijk (bv. per mail) de bevestiging van de hosting partner toegestuurd krijgen.

### Toegestane externe scope

* **Web applicaties**
* *www.demival.be*
* **Systemen**
* *1.2.3.4: Firewall*
* *2.3.4.5: VPN*

### Regels voor pentesten

* Denial of service exploits zijn **verboden**
* Alle tools waarvan de gegevens niet worden gedeeld met een 3e partij zijn toegestaan.
* Bruteforcing is enkel toegestaan software die beheerd worden door Demival zelf.
* Code execution is toegestaan na goedkeuring van een verantwoordelijke binnen Demival.

### Post-exploitatie

Post-exploitatie houdt de acties in die men onderneemt nadat men toegang wist te verschaffen tot een systeem of applicatie. In deze fase bestaat het risico dat bedrijfs- of zelfs persoonlijke gegevens zichtbaar zijn.

* Bij het verkrijgen van gegevens waarmee we mogelijks andere zaken kunnen gaan testen mogen we enkel actie ondernemen bij goedkeuring van een verantwoordelijke binnen Demival.
* Verkregen informatie mogen we niet misbruiken. Dit omvat het publiceren, aanpassen of verwijderen van de data.

## Interne blackbox pentest

Dit is een veiligheidsaudit die uitgevoerd wordt binnenin het te testen netwerk. Alleen systemen waarvoor toestemming verleend werd door de klant maken deel uit van de scope.

Hiervoor kan gewerkt worden met een whitelist (die expliciet de mogelijke doelwitten oplijst), een blacklist (die expliciet oplijst welke doelwitten niet tot de scope behoren), of geen lijst (denk aan het integrale Wi-Fi netwerk voor gasten).

### Toegestane interne scope

*<Dis>*ToegestaneIP ranges op netwerk X (Bv. wandcontactdoos in de vergaderzaal X of VPN Y):

*<Dis>Toegestane IP ranges op netwerk Y*

*<Dis>Toegestane applicaties*

**Notities:**

* De webapplicatie van het intranet is gevoeliger voor scans.

### Regels voor pentesten

* Denial of service exploits zijn **verboden**
* Alle tools waarvan de gegevens niet worden gedeeld met een 3e partij zijn toegestaan.
* Bruteforcing is enkel toegestaan software die beheerd worden door Demival zelf.
* Code execution is toegestaan na goedkeuring van een verantwoordelijke binnen Demival.

### Post-exploitatie

Post-exploitatie houdt de acties in die men onderneemt nadat men toegang wist te verschaffen tot een systeem of applicatie. In deze fase bestaat het risico dat bedrijfs- of zelfs persoonlijke gegevens zichtbaar zijn.

* Bij het verkrijgen van gegevens waarmee we mogelijks andere zaken kunnen gaan testen mogen we enkel actie ondernemen bij goedkeuring van een verantwoordelijke binnen Demival.
* Verkregen informatie mogen we niet misbruiken. Dit omvat het publiceren, aanpassen of verwijderen van de data.

## Optionele testen

### Phishing mail campagne

Phishing aanval

Phishing gebeurt met behulp van de tools van de een partner van Howest namelijk de firma Outkept ([www.outkept.com](http://www.outkept.com/)). De klant gaat ermee akkoord om op vraag van de auditors bepaalde toegangen (bv. poorten, IP adressen) te openen die enkel en alleen door de tools van Outkept zullen gebruikt worden om de phishing campagne te kunnen uitvoeren.

Tijdens een phishing aanval ontvangt een of meerdere medewerkers frauduleuze e-mails die als doel hebben om de auditeurs toegang te verschaffen tot de IT-omgeving of persoonlijke- en bedrijfsgegevens.

De phishing doelwitten kunnen enkel via een zogenaamde whitelist (expliciete en restrictieve lijst van doelwitten) worden gedefinieerd.

**Toegestane phishing doelwitten worden als een digitale lijst (bv. Excel) aan de auditors bezorgd.**  
*De bovenstaande lijst zou nog geleverd moeten worden.*

*<Noot: deze lijst kan – tot op het ogenblik van de uitvoering van de phishing - op elk moment ingeperkt worden mits afstemming tussen beide partijen>*

## 6.Bevraging medewerkers en interview beveiligingsverantwoordelijke

De survey en het interview kunnen bij verschillende sleutelprofielen binnen de organisatie van de klant uitgevoerd worden, zolang de bijhorende voorwaarden gerespecteerd wordt.

* *Bv. De data wordt geanonimiseerd*
* *Bv. Vooraleer de vragenlijst uitgestuurd wordt of het interview met de lokale DPO uitgevoerd wordt, brengen de auditeurs persoon X op de hoogte*
* *…*

## 7.HANDTEKENINGEN

**Voor de organisatie:**

Volledige naam:

Functie:

**HOWEST:**

Daniel DuSeuil  
Onderzoekscoördinator Howest