Project Cyberveilige Gemeenten

# Traject Ethisch Hacken 2023

## Globaal analyserapport

vvsg howest hogeschool

## Inhoud

Deel 1

# Project Cyberveilige Gemeenten

## Project Cyberveilige Gemeenten

In 2020 startte het Project Cyberveilige Gemeenten, een initiatief van de Vlaams minister van Binnenlands Bestuur, Bestuurszaken, Inburgering en Gelijke Kansen. Het project had als doel de cyberveiligheid bij steden en gemeenten te verhogen en was een samenwerking tussen het Agentschap Binnenlands Bestuur, Digitaal Vlaanderen, Audit Vlaanderen en de Vereniging van Vlaamse Steden en Gemeenten.

Lokale besturen zijn een gegeerd doelwit voor cyberaanvallen. Een aanval kan tot verregaande maatschappelijke gevolgen hebben en raakt niet alleen de burger en medewerkers van het bestuur, maar zorgt ook voor grote imago- en financiële schade. Dat bleek onder meer uit de recente cyberincidenten waarbij de digitale dienstverlening gedurende enkele dagen, weken of zelfs maanden werd verhinderd.

## Traject Ethisch Hacken

Daarom is het van belang dat een lokaal bestuur cyberveiligheid hoog op de agenda plaatst en in actie schiet. Het Project Cyberveilige Gemeenten streeft daarnaar aan de hand van 3 luiken:

- Inspirerende webinars en infosessies
- Een toolkit cybersecurity
- Het Traject Ethisch hacken

Het Traject Ethisch Hacken is een samenwerking met Howest, Hogeschool West-Vlaanderen: derdejaarsstudenten Cyber Security Professional testen kosteloos de cyberveiligheid van lokale besturen. In dit globaal analyserapport wordt een overzicht gegeven van bevindingen en verbeterpunten uit het traject, uitgevoerd tijdens het najaar van 2023.

Daarnaast kunnen lokale besturen als aanvulling beroep doen op de ICT-veiligheidsaudits met cofinanciering via de Vlaamse overheid.

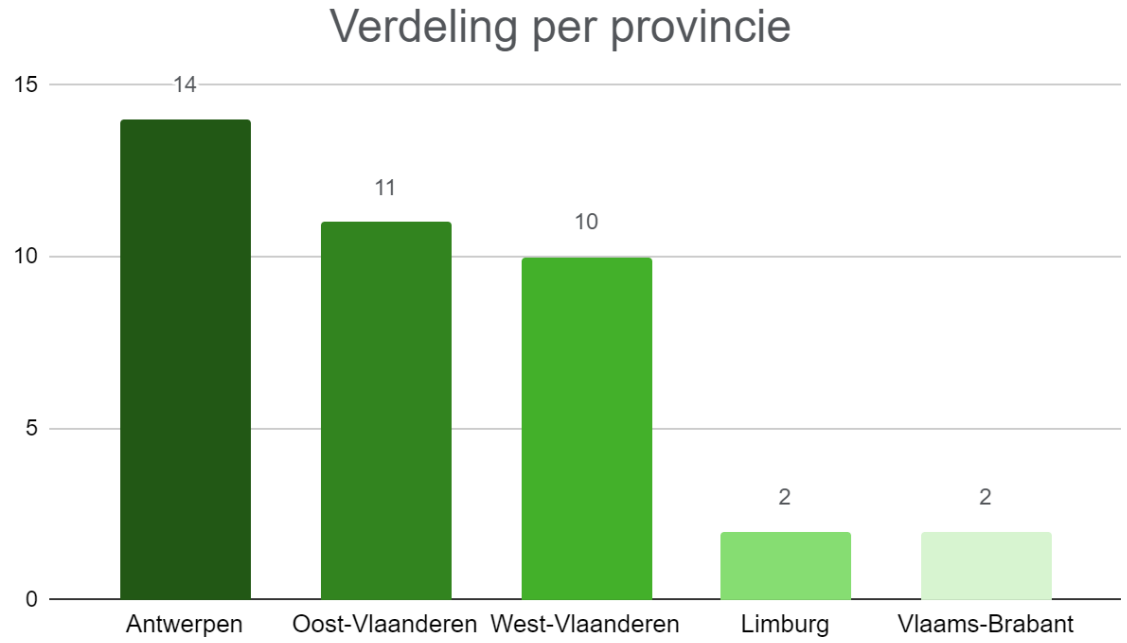
## Reikwijdte van het traject

In totaal schreven **40** steden en gemeenten zich in voor dit traject, waarvan **39** steden en gemeenten daadwerkelijk zijn ingestapt. Dit rapport beschrijft de resultaten van de 39 besturen die in 2023 doorgelicht werden.

Howest hogeschool en de VVSG bedanken de 39 geteste steden en gemeenten en ethische hackers voor hun constructieve samenwerking in het kader van dit project. Dit globaal rapport is een anonieme samenvatting van de individuele rapporten, die de studenten overmaakten aan de lokale besturen op het einde van de testperiode. In dit rapport worden zowel resultaten als de aanbevelingen meegenomen.

Alle deelnemende besturen ontvingen op het einde van de testperiode een gepersonaliseerd rapport met de gevonden aandachtspunten en aanbevelingen om de aanwezige kwetsbaarheden aan te pakken. **79%** van de geteste lokale besturen gaf aan met de resultaten aan de slag te kunnen gaan, **48%** is daar reeds mee begonnen.

# Deelnemende besturen




Deel 2

# Aanbod binnen het Traject Ethisch Hacken

## Aanbod binnen het Traject Ethisch Hacken

Howest werkte in samenspraak met de VVSG een aanbod uit op maat van lokale besturen. Binnen dit aanbod worden vijf standaarddelen voorzien, met daarnaast de keuze voor een optionele test.

Het standaardaanbod voor het Traject Ethisch Hacken 2023 bestond uit de volgende testen:

- Een Open-Source Intelligence Test waarbij informatie uit publieke bronnen wordt ingewonnen die het werk van hackers kan vergemakkelijken. Het kan hierbij onder andere gaan over gelekte inloggegevens en informatie over de netwerkstructuur of het hosten van websites. Uitgevoerd in **34** besturen.

- Een interne blackbox pentest waarbij de studenten zich aansluiten op het interne netwerk om kwetsbaarheden op te sporen in de systemen, netwerken, applicaties of webplatformen, zonder enige voorkennis. Uitgevoerd in **39** besturen.

- Een externe blackbox pentest waarbij de studenten zoeken naar kwetsbaarheden in de systemen zonder zich te verbinden met het interne netwerk. Uitgevoerd in **37** besturen.

## Aanbod binnen het Traject Ethisch Hacken

Daarnaast maken ook volgende elementen deel uit van de standaardaudit:

- Een gestructureerd interview met de functionaris gegevensbescherming (DPO) of verantwoordelijke informatiebeveiliging (CISO) op basis van een door Howest opgestelde vragenlijst, om inzicht te krijgen in de beveiligingsmaatregelen die het lokaal bestuur inzet. Uitgevoerd in **33** besturen.

- Een vragenlijst opgesteld door de Howest-lectoren en verspreid naar de lokale medewerkers door de studenten. De vragenlijst peilt naar het bewustzijn van ICT-veiligheidsrisico's, de aanwezige sensibilisering binnen het lokaal bestuur en de mate waarin de medewerkers goede praktijken toepassen. Ingevuld door **1086** medewerkers uit **34** besturen.

## Aanbod binnen het Traject Ethisch Hacken

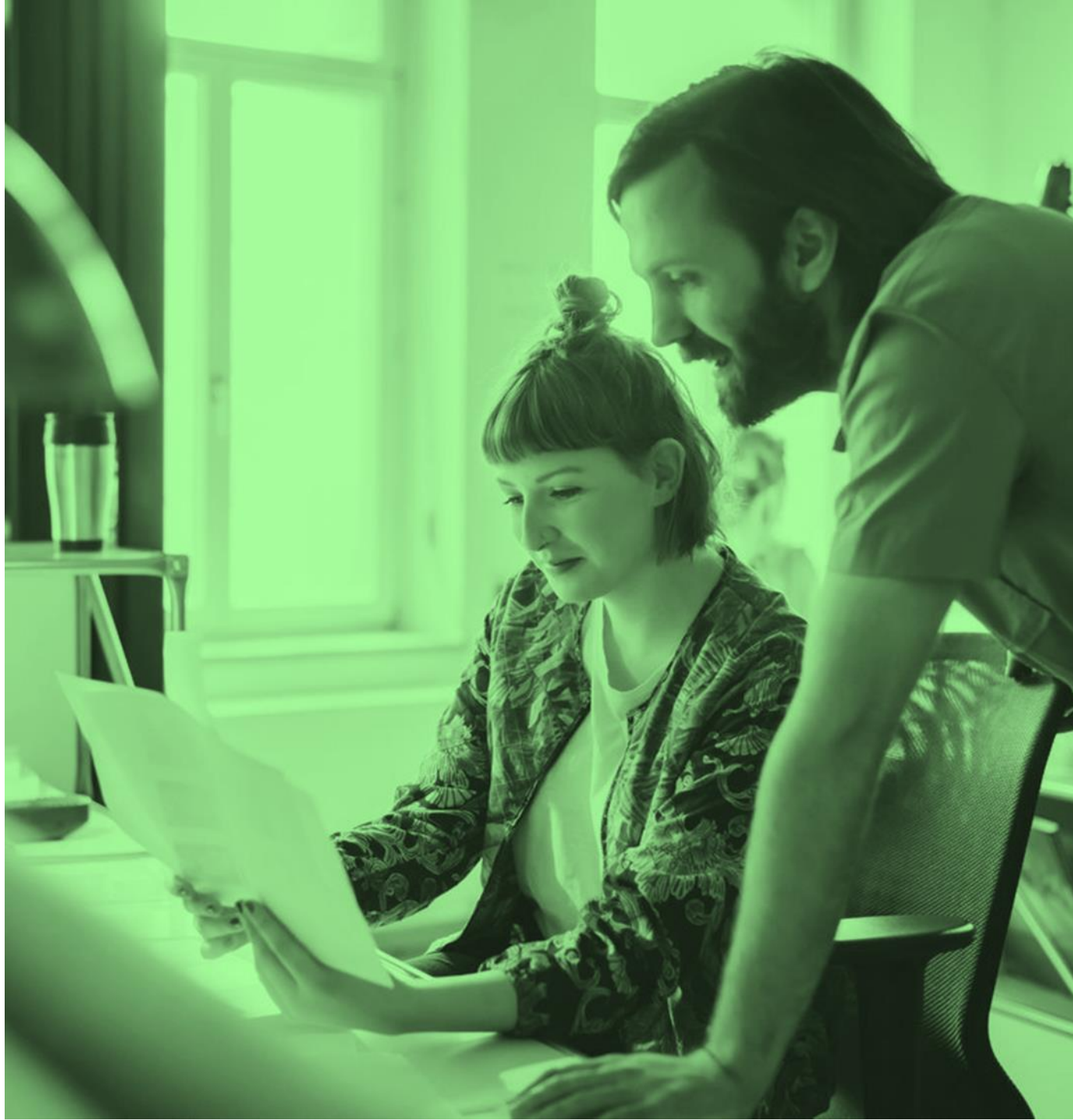
De deelnemende lokale besturen kunnen naast het standaardaanbod, opteren voor één van onderstaande optionele testen:

- Een social engineering campagne waarbij studenten kijken hoe medewerkers reageren op een phishingmail, impersonatie (waarbij de studenten onder een alias toegang proberen krijgen tot netwerken en systemen) of een USB-drop (waarbij gekeken wordt hoeveel medewerkers een USB die mogelijk malware bevat aansluiten). Uitgevoerd in **28** lokale besturen.

- Een camera security audit waarbij de studenten een test uitvoeren op een beveiligingscamera/beveiligingscamera's beheerd door het lokaal bestuur. Hierbij testen de studenten of de camera/camera's voldoende beveiligd is/zijn tegen een mogelijke cyberaanval. Uitgevoerd bij **8** lokale besturen.

Deel 3

# Bevindingen en aanbevelingen



De resultaten die de Howest-studenten beschrijven, tonen aan dat de deelnemende lokale besturen reeds diverse maatregelen nemen om de veiligheid van de aanwezige ICT-infrastructuur en bewaarde gegevens te waarborgen. Toch blijken een aantal belangrijke beschermingsmaatregelen niet ingevoerd, waardoor het risico op een cyberaanval of datalek groter is.

Bij **35** deelnemende besturen die een interne blackbox pentest lieten uitvoeren, zijn er meerdere kwetsbaarheden aangetroffen op het netwerk. Cybercriminelen kunnen hiervan gebruik maken om de desbetreffende steden en gemeenten te hacken.

Bij **11** besturen die een externe blackblox pentest lieten uitvoeren, zijn diverse kwetsbaarheden gedetecteerd, zoals bijvoorbeeld ontbrekende of incorrecte certificaten, information disclosure en onbeveiligde verbindingen.

De resultaten en aanbevelingen uit de studentenrapporten weerspiegelen grotendeels de bevindingen uit het globaal rapport ICT-veiligheidsaudits met cofinanciering van Audit Vlaanderen 2020-2022.

Eerst volgt een overzicht van de belangrijkste bevindingen, naar analogie van de bevindingen van Audit Vlaanderen. Vervolgens wordt er dieper ingegaan op de specifieke kwetsbaarheden en risico's die frequent terugkomen in de auditrapporten van de studenten, met enkele aanbevelingen om deze weg te werken.

**Bevinding 1: Onvoldoende beveiliging op niveau van de werknemer**

Wanneer personen in de organisatie te weinig beveiligingsmaatregelen nemen, geen cyberveilige houding aannemen en procedures onvoldoende volgen, is het voor een cybercrimineel mogelijk om op een relatief eenvoudige manier toegang te krijgen tot het gegevens of het netwerk van een lokaal bestuur.

**Bevinding 2: De ICT-omgeving is te weinig beschermd**

Ook het ICT-netwerk en de ICT-systemen zijn soms nog onvoldoende beveiligd bij lokale besturen. Door enkele extra beveiligingen in te voeren, verklein je het risico op een cyberincident.

**Bevinding 3: Een betrouwbare herstelprocedure ontbreekt**

Een cyberveilige omgeving bestaat niet alleen uit een hoge graad van bescherming, maar ook uit een procedure om dienstverlening te blijven garanderen of zo snel mogelijk herop te starten bij een cyberaanval. Gegevens moeten beschikbaar zijn of snel hersteld kunnen worden bij verlies, schade of diefstal. De kans dat een lokaal bestuur getroffen wordt door cybercriminelen is groot, ondanks mogelijk hoge beveiliging, daarom is een continuïteits- en herstelprocedure cruciaal.

**Bevinding 4: De risico's moeten meer in kaart gebracht worden**

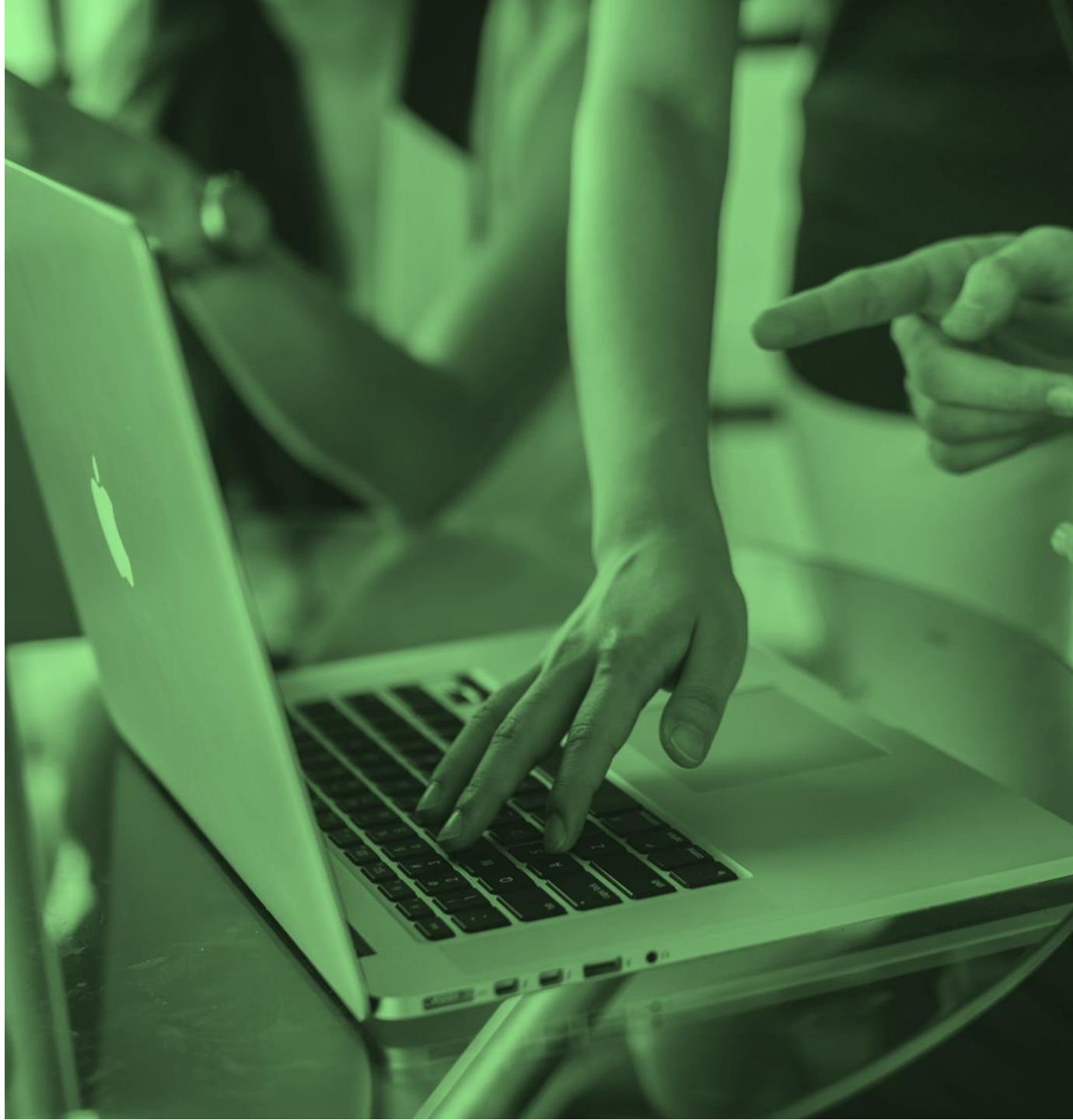
Een duidelijk zicht op de ICT-risico's maakt het uitvoeren van gerichte cybersecurity acties gemakkelijker. De toegepaste maatregelen zijn doelbewuster, je creëert een sterkere ICT-omgeving en bespaart op zinloze uitgaven.

**Bevinding 5: Beheersmaatregelen worden infrequent correct toegepast**

Niet enkel het hebben van goede procedures is belangrijk, ook de controle erop. Zorg dat de voorziene maatregelen steeds nageleefd worden, zorg dat je veiligheidsproces van begin tot einde in orde is, met een regelmatige check en evaluatie van de genomen stappen en gekozen soft- en hardware.

Bevinding 1

# Onvoldoende beveiliging op niveau van de medewerker



# Cyberveiligheid begint bij bewustzijn

1. Phishing

In **20** lokale besturen werd een phishingcampagne uitgevoerd: een onschadelijke e-mail leidde de werknemer naar een vervalste inlogpagina. 9% van de medewerkers klikte op de link in de e-mail. De phishingcijfers evolueren positief, maar nog te weinig medewerkers doen melding van een verdachte e-mail

2. Sensibilisering

**14** van de 31 ondervraagde medewerkers geeft aan dat er regelmatig (jaarlijks tot halfjaarlijks) een phishingtraining georganiseerd wordt.

# Cyberveiligheid begint bij bewustzijn

3. Wachtwoorden

**59%** van de ondervraagde werknemers geeft aan de regels over het gebruik wachtwoorden te kennen

4. Bewustzijn

**43%** van de ondervraagde werknemers geeft aan altijd het scherm te vergrendelen bij verlaten van de werkpost

# Aanbevelingen

- Communiceer helder over een aanspreekpunt en meldingsprocedure voor verdachte e-mails, pop-ups of gedrag

- Organiseer voldoende trainingen en verhoog de bewustmaking onder medewerkers
  - (Her)bekijk de voorbije VVSG-webinars
  - Lees de tips van het Vo-CRT

- Evalueer je wachtwoordbeleid, zorg voor duidelijke en werkbare richtlijnen en herhaal deze regelmatig
  - Lees de tips van Safe On Web

Bevinding 2

# De ICT-omgeving is te weinig beschermd

# Een sterke muur om je ICT-systeem

1. Default wachtwoorden

In **33** van de 39 lokale besturen ontdekten de studenten default wachtwoorden

- Vooral op printers worden de standaard inloggegevens niet vervangen, maar ook op sommige belangrijke software

2. Oudere versies

In **22** lokale besturen werden verouderde systemen of toepassingen gevonden tijdens de pentesten. Deze worden minder of niet meer ondersteund en krijgen ook geen beveiligingsupdates. Hackers kunnen bij deze systemen misbruik maken van reeds gekende kwetsbaarheden.

# Een sterke muur om je ICT-systeem

3. Multi-factor authenticatie

**23** van de 39 lokale besturen gebruiken multi-factor authenticatie (MFA): gebruikers krijgen pas toegang tot een applicatie of website nadat ze zich twee of meer keer geauthentiseerd hebben.

4. Netwerksegmentatie

**25** van de 31 ondervraagde DPO's geeft aan dat er netwerksegmentatie geïnstalleerd is: het netwerk is opgeknipt in kleinere segmenten, wat ervoor zorgt dat cybercriminelen geen ongehinderde toegang hebben tot andere netwerksegmenten. Een incident is zo beperkt tot een afgeschermd deel van het netwerk.

# Een sterke muur om je ICT-systeem

## 5. Toegangs- en gebruikersbeheer

**23** van de 31 ondervraagde DPO's bevestigt dat er een IDM/ACM (Identity and Acces Management) ingevoerd is. Onrechtmatig gebruik van applicaties en digitale toepassingen, brengt risico's met zich mee. Een degelijk toegangs- en gebruikersbeheer zorgt ervoor dat enkel de juiste medewerkers toegang hebben en dat ze hun identiteit sterk moeten bewijzen.

## 6. Encryptie

Bij **14** van de 31 lokale besturen zijn kritieke gegevens sterk versleuteld wanneer ze via internet verzonden worden. Encryptie zet gegevens om in een onleesbare vorm zodat veilig gecommuniceerd kan worden over gevoelige informatie.

## Aanbevelingen

- Verander default wachtwoorden onmiddellijk en zorg dat elke toepassing of elk apparaat voldoende beveiligd is

- Update systemen zo snel mogelijk naar recente en ondersteunde versies

- Implementeer zoveel mogelijk multi-factor authenticatie
  - Lees de aanbevelingen van het Vo-CRT
  - Gemeente Grimbergen maakt digitale werkplek veilig met multifactorauthenticatie

- Verdeel je netwerk in kleinere segmenten
  - Laat je inspireren door de goede praktijk van stad Geel

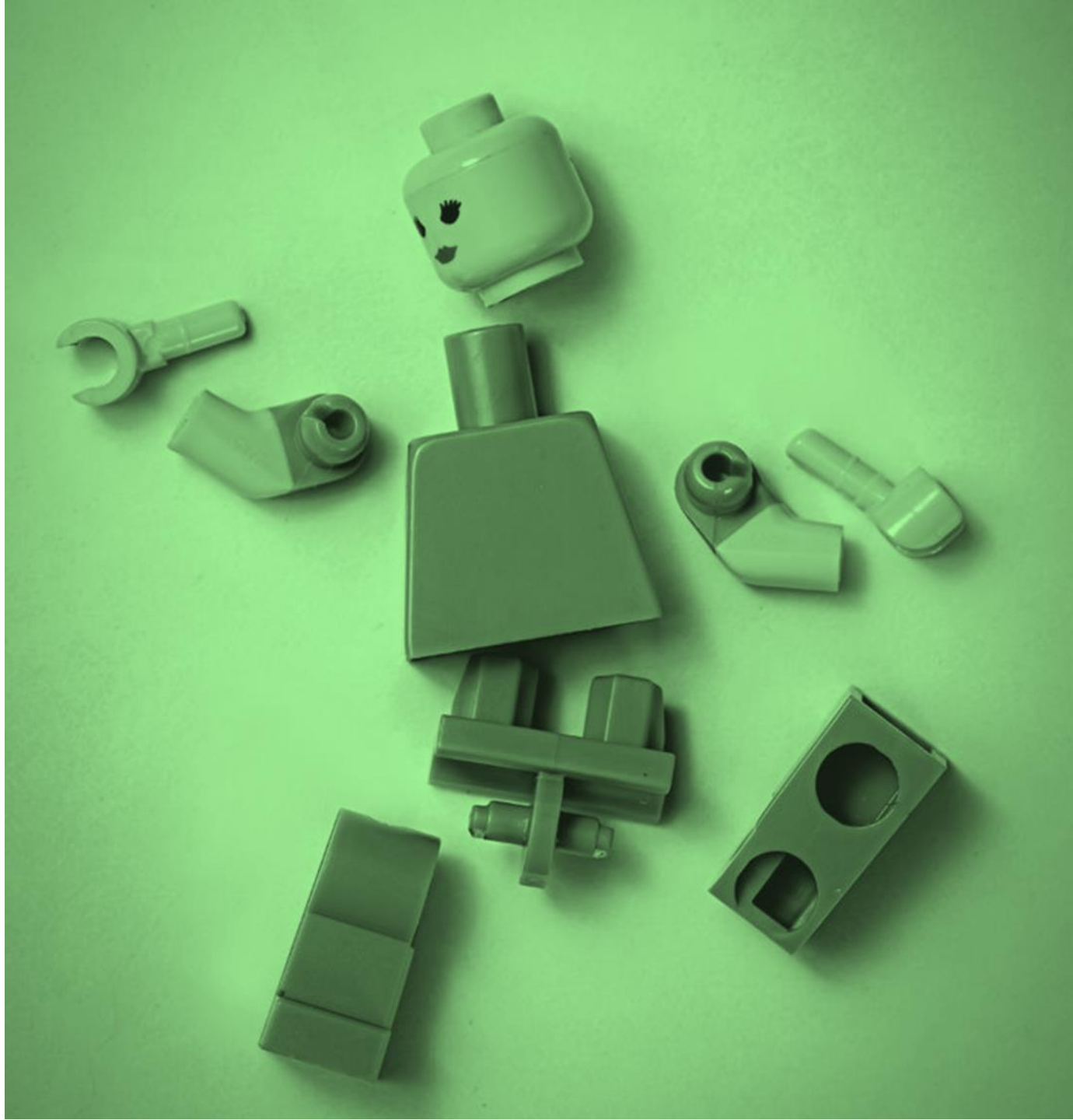
# Aanbevelingen

- Zorg voor een sterk toegangs- en gebruikersbeheer
  - Digitaal Vlaanderen geeft meer informatie over toegangsbeheer (ACM) en gebruikersbeheer (IDM)
  - Ontdek de procedure van gemeente Haacht
  - Binnenkort zal je als lokaal bestuur via het Vo-CRT een traject kunnen volgen voor de implementatie van deze Vlaamse bouwstenen

- Stel duidelijke richtlijnen op over het versleuteld verzenden van gevoelige gegevens
  - Meer informatie over encryptie en sleutelbeheer

Bevinding 3

# Een betrouwbare herstelprocedure ontbreekt



# Verzeker je continuïteit

1. Een bedrijfscontinuïteitsplan (BCP)

**12** van de 31 ondervraagde DPO's verklaart dat er een BCP opgemaakt is. Een bedrijfscontinuïteitsplan beschrijft maatregelen die een organisatie neemt om de dienstverlening zo goed mogelijk te beschermen, wanneer ze getroffen wordt door een incident.

2. Back-ups

**21** besturen hebben wel een formeel back-up plan, waarin uitgeschreven staat hoe de organisatie omgaat met back-ups van bestanden en ICT-systemen. Idealiter is dit gecombineerd met een disaster recovery plan (DRP): richtlijnen om de ICT-infrastructuur draaiende te houden, zelfs op het meest minimale niveau, bij een mogelijke ramp.

# Verzeker je continuïteit

## 3. Testen van back-ups

Ondanks een gedocumenteerd back-up beleid, worden bij slechts **14** besturen de back-ups regelmatig getest en geverifieerd**.** Een controle om te zien of de back-ups goed functioneren, is een belangrijke stap in het back-upbeleid.

## Aanbevelingen

- Maak zo snel mogelijk werk van een grondig BCP
  - Op deze pagina vind je een sjabloon
  - Binnenkort zal je beroep kunnen doen op het Vo-CRT om je hierbij te begeleiden

- Voorzie een goed herstelplan
  - Organiseer een crisisoefening cybercrime om medewerkers bewust te maken van het belang van een goed herstelplan

- Test en verifieer je back-ups op regelmatige basis
  - Lees de "Gouden regels" van het CCB

Bevinding 4

# Risico's meer in kaart brengen

# Een duidelijk overzicht brengt inzicht

1. Patching

**18** van de 31 ondervraagde DPO's geeft aan dat er een geformaliseerd patchingproces is voor kritieke infrastructuur. Een systematische aanpak voor identificeren, evalueren en toepassen van softwareupdates of "patches" is een grote hulp bij het ontdekken en rechtzetten van kwetsbaarheden in software en bij het verbeteren van IT-systemen.

2. Inventaris

**17** besturen hebben een inventaris met de locatie van hun IT-gerelateerde objecten, maar die inventaris bevat niet alle actuele informatie. Een actuele inventaris ondersteunt niet alleen bij het beheren van kosten en middelen en bij het plannen van updates en vervangingen, maar vereenvoudigt ook het beveiligingsbeheer. En met een goede inventaris determineer je sneller welke infrastructuur geraakt is door een mogelijke cyberaanval.

# Een duidelijk overzicht brengt inzicht

3. Testing

Bij **16** lokale besturen gebeuren er regelmatig penetratietesten op kritieke systemen en infrastructuur. Deze testen brengen de zwakke plakken in het IT-systeem aan het licht en helpen om gericht acties te ondernemen om de veiligheid te verhogen.

4. Monitoring

**22** lokale besturen beschikken over een monitoringssysteem. Cyberaanvallen blijven vaak lang onopgemerkt, waardoor zelfs back-ups geïnfecteerd raken. IT-diensten hebben vaak te weinig tijd of capaciteit om logbestanden te controleren op onregelmatigheden. Automatische monitoring waarschuwt onmiddellijk bij bepaalde gebeurtenissen, zoals een toename van dataverkeer op specifieke locaties in het netwerk.

# Aanbevelingen

- Organiseer een sterk kwetsbaarhedenbeheer
  - Lees de aanbevelingen van het Vo-CRT
  - Vul het self-assesment in van het CCB
  - Laat je inspireren: risicomanagement door stad Gent
- Maak werk van patchmanagement
  - Lees de factsheet van Nederlandse Informatiebeveiligingsdienst (IBD)
- Stel een zo breed mogelijke inventaris op en houd die actueel
  - Zo pakt gemeente Niel het aan

# Aanbevelingen

- Test en check je IT-systemen regelmatig
  - Creëer een kader voor ethische hackers met een "beleid voor responsible disclosure"
  - Bestel een ICT-veiligheidsaudit met co-financiering door de Vlaamse overheid

- Installeer automatische monitoring
  - Ontdek hoe stad Wervik het aanpakt

Bevinding 5

# Toepassen van beheersmaatregelen

# Naar een effectieve en efficiënte uitvoering

1. Camerabeheer

Bij **23** van 31 lokale besturen is het duidelijk bepaald wie toegang heeft tot de camera en beelden. De camera's zijn goed afgeschermd, maar bij 25% van de geteste besturen konden studenten echter toegang krijgen tot een of meerdere camera's.

2. Externe dienstverleners

Slechts **7** deelnemers controleren externe dienstverleners om ervoor te zorgen dat ze zich aan de vastgestelde SLA's houden. Het zeker weten van welke ondersteuning je van een leverancier kan verwachten bij onverwachte situaties, is een belangrijk onderdeel van je cyberveiligheidsgevoel. Maak steeds duidelijk welke verantwoordelijkheden bij het lokaal bestuur liggen en welke bij externe partners.

# Naar een effectieve en efficiënte uitvoering

## 3. Bewaarbeleid logs

Bij **6** deelnemende besturen bestaat er een beleid voor het bewaren van eigen logs. Gebeurtenissen die belangrijk zijn voor de beveiliging of analyse van verstoringen, worden vastgelegd in een logbestand. Met het naleven van de procedure voor het inkijken en bewaren van deze logs, verhoog je de controle op je organisatie.

# Aanbevelingen

- Maak werk van organisatiebeheersing
  - Praktijk Wevelgem
  - Praktijk Sint-Niklaas
  - Praktijk Aalter

- Zorg voor goed afgeschermde camera's en toegang tot de beelden
  - Niet enkel de toegang is belangrijk, maar realiseer een verantwoord camerabeleid

- Controleer de SLA met je leveranciers
  - Betrek je leveranciers ook bij een crisisoefening cybercrime

- Stel een beleid op voor het inkijken en bewaren van logbestanden
  - Lees de aanbevelingen van de Kruispuntbank van de Sociale Zekerheid



vvsg

Deel 4

# Trends

Trends

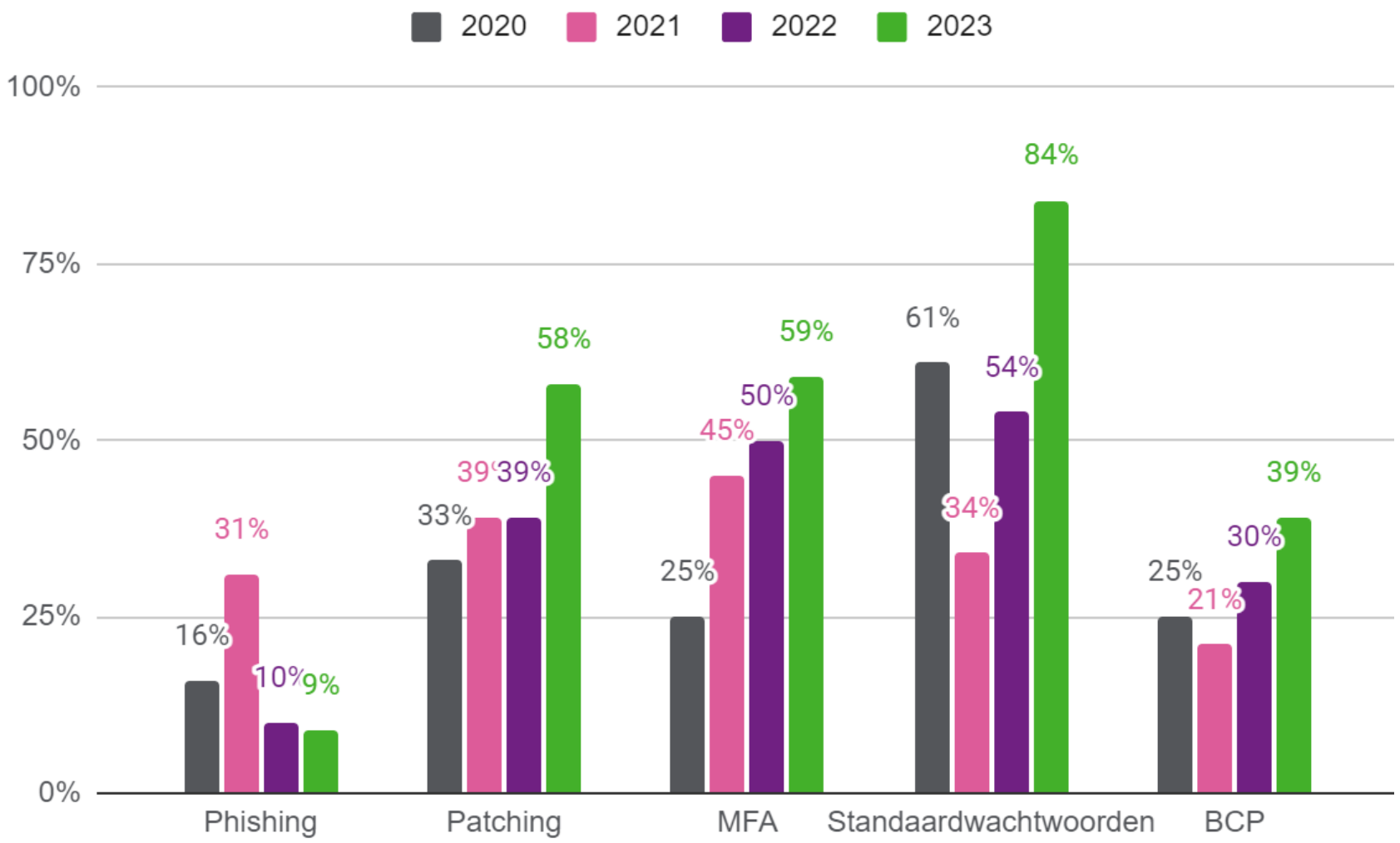
Een groot deel van de Vlaamse lokale besturen nam de voorbije jaren deel aan het Traject Ethisch Hacken.

Enkele testen en maatregelen zijn vergeleken met de vorige rapporten:

- Hoeveel procent van de deelnemers klikt op een link in een phishingmail?
- Hoeveel procent van de deelnemende besturen heeft een geformaliseerd patchingproces voor kritieke infrastructuur?
- Hoeveel procent maakt gebruik van multi-factor authenticatie?
- Bij hoeveel procent van de lokale besturen werden standaardwachtwoorden aangetroffen?
- Hoeveel procent heeft al een bedrijfscontinuïteitsplan?

Het volgende diagram geeft een overzicht. Daaruit blijkt dat de cijfers van 2023 telkens de beste zijn, behalve bij het aantreffen van default wachtwoorden.

## Trends


2020
2021
2022
2023
100%
75%
50%
25%
0%
16%
31%
10%
9%
33%
39%
39%
58%
25%
45%
50%
59%
61%
34%
54%
84%
25%
21%
30%
39%
Phishing
Patching
MFA
Standaardwachtwoorden
BCP

Deel 5

# Contact

Contact

# Vragen?

- VVSG
  - Charlotte De Mullier, Ward Van Hal
  - Project Cyberveilige Gemeenten
- Howest
  - kurt.schoenmaekers@howest.be
  - Opleiding Cybersecurity Professional
- Vo-CRT
  - cyberresponse@vlaanderen.be
  - Cyber Response Team Vlaanderen
- CCB
  - info@ccb.belgium.be
  - Centrum voor Cybersecurity België
- Audit Vlaanderen
  - ICT-veiligheidsaudits

Contact

Vereniging van Vlaamse Steden en Gemeenten
Bischoffsheimlaan1-8, 1000 Brussel

www.vvsg.be
cyberveiligheid@vvsg.be