Traject Ethisch Hacken 2021

Globaal analyserapport

vvsg howest / we develop people

1. Project Cyberveilige Gemeenten

vvsg

Project Cyberveilige Gemeenten

Dat lokale besturen een gegeerd slachtoffer zijn voor cyberaanvallen bleek onder meer uit het incident in Willebroek (2020), Dilbeek (2020) en Hoeilaart (2021) waarbij de digitale dienstverlening gedurende enkele dagen werd lamgelegd.

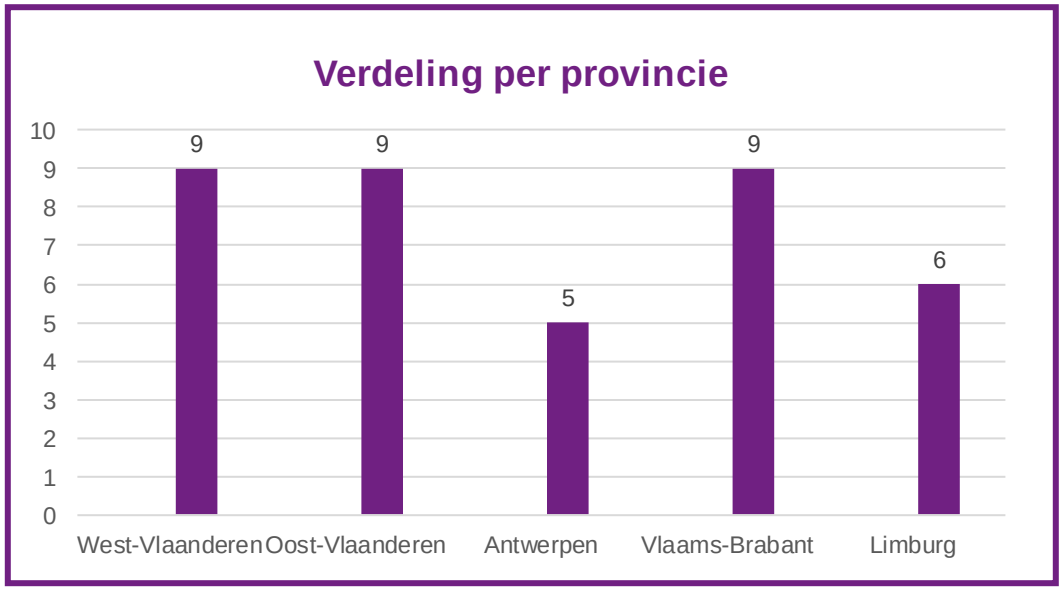
Om het hoofd te bieden aan dergelijke dreigingen besloot de Vlaamse Overheid in het voorjaar van 2020 om 2,18 miljoen euro te investeren in de cyberveiligheid van lokale besturen op voorstel van **minister Bart Somers**. Onder de noemer 'Project Cyberveilige Gemeenten' werden, in samenwerking met **Audit Vlaanderen** en het **Agentschap Binnenlands Bestuur**, diverse acties uitgewerkt die lokale besturen in staat moeten stellen om de veiligheid van hun IT-systemen op te krikken.

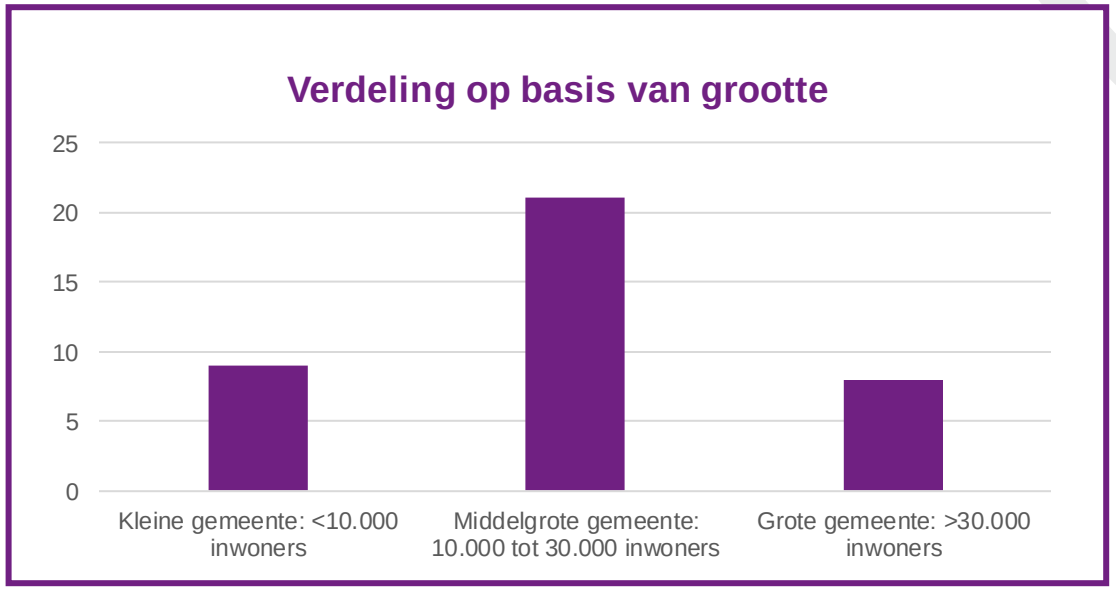
Om te bouwen aan cyberveilige steden en gemeenten is het natuurlijk van belang om eerst te weten waar de voornaamste kwetsbaarheden liggen. Als aanvulling op **de ICT-veiligheidsaudits met cofinanciering via Audit Vlaanderen** werd ook gekeken naar een mogelijke samenwerking met ethische hackers.

In samenwerking met Howest werd het **Traject Ethisch Hacken** opgestart, waarbij derdejaarsstudenten Toegepaste Informatica de cyberveiligheid van lokale besturen kosteloos doorlichten.

De reikwijdte van het Traject Ethisch Hacken in 2021

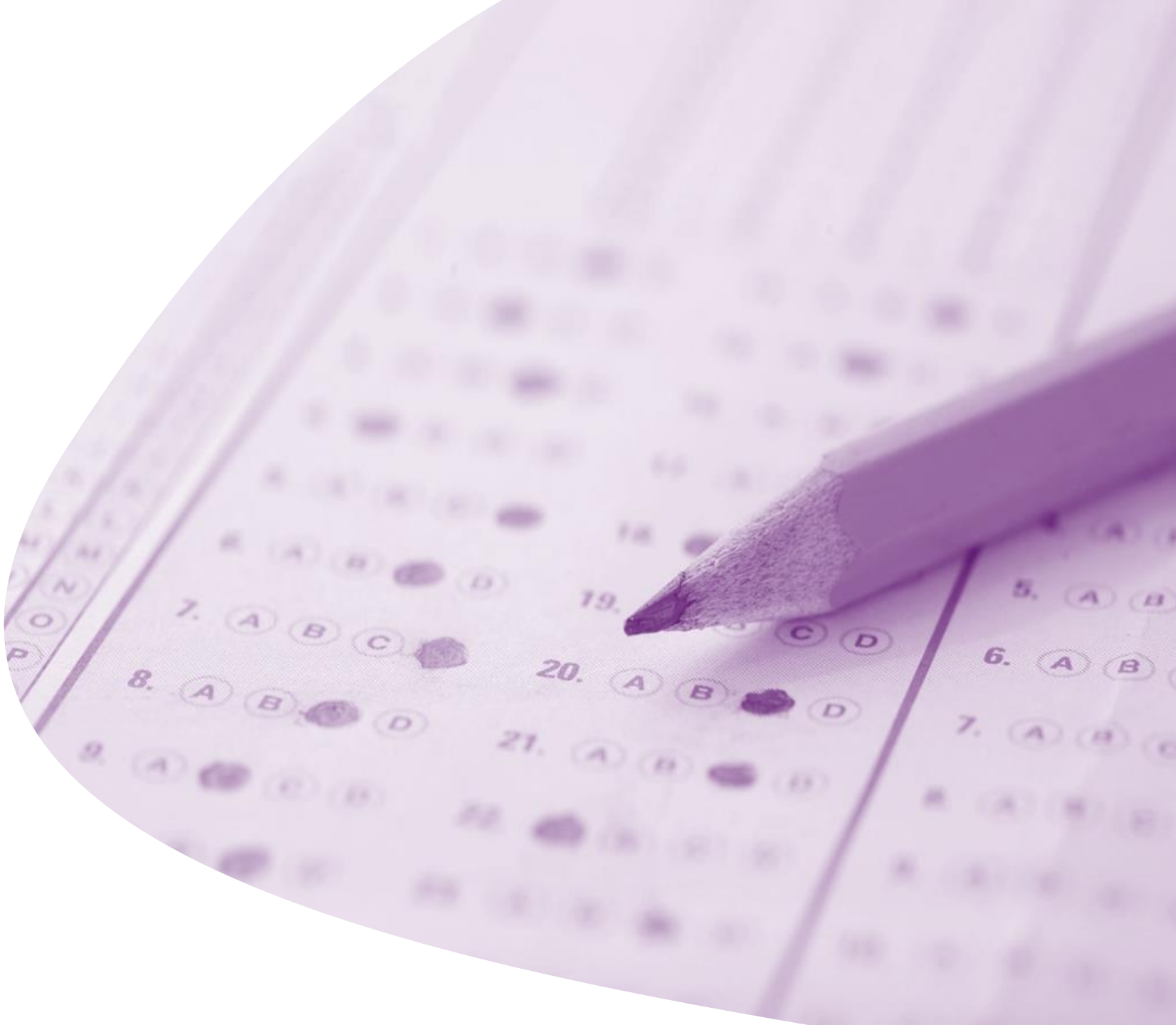
In totaal schreven er 40 steden en gemeenten zich in voor het Traject Ethisch Hacken, waarvan 38 steden en gemeenten daadwerkelijk konden instappen in het Traject Ethisch Hacken. Dit rapport beslaat de resultaten van de **38 besturen die in 2021 doorgelicht werden**.





Howest en VVSG bedanken de 38 geteste steden en gemeenten en ethische hackers voor hun constructieve samenwerking in het kader van dit project. Dit globaal rapport is een samenvatting van de individuele rapporten die de studenten overmaakten aan de lokale besturen op het einde van de testperiode, zowel naar resultaten als naar aanbevelingen toe.

2. Aanbod binnen het Traject Ethisch Hacken



vvsg

Aanbod 1/2

Howest werkte in samenspraak met VVSG een aanbod uit op maat van de lokale besturen. Binnen dit aanbod werden **vijf standaardtests** voorzien, met **een optioneel luik** voor lokale besturen waar de testperiode van 4 dagen voldoende was om een bijkomende test uit te voeren of waar de deelnemende lokale besturen een of meerdere testen uit het standaardaanbod lieten wegvallen.

Het **standaardaanbod** voor het **Traject Ethisch Hacken 2021** 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 22 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 24 besturen.**

- Een **externe blackbox pentest** waarbij de studenten zoeken naar kwetsbaarheden in de systemen zonder zich te verbinden met het interne netwerk. **Uitgevoerd in 33 besturen.**

- 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 38 besturen.**

Aanbod 2/2

- **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 1429 medewerkers uit 37 besturen.**

- **Het optioneel luik** bestaat uit 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 35 lokale besturen.**

Bij **13 van de 38 deelnemende lokale besturen** werden de **vijf standaardtesten** uitgevoerd **inclusief het optioneel luik.**

Bij **1 van de 38 deelnemende lokale besturen** werd de **vijf standaardtesten** uitgevoerd **zonder het optioneel luik.**

Alle deelnemende besturen ontvingen op het einde van de testperiode een **gepersonaliseerd rapport** met de gevonden pijn- en aandachtspunten en aanbevelingen om de aanwezige kwetsbaarheden aan te pakken.

3. Bevindingen en verbeterpunten

Traject Ethisch Hacken 2021

vvsg

Inleiding

De resultaten en aanbevelingen die geformuleerd werden door de Howest-studenten laten zien dat lokale besturen reeds diverse maatregelen nemen om de veiligheid van de aanwezige ICT-infrastructuur en bewaarde gegevens te waarborgen, maar dat een aantal **belangrijke beschermingsmaatregelen onderbenut** blijven en reële risico's **onvoldoende afgedekt** worden.

Bij 24 besturen die **een interne pentest** lieten uitvoeren, zijn er meerdere kwetsbaarheden aangetroffen op het netwerk die uitgebuit kunnen worden door individuen of organisaties met een kwaadwillig oogmerk.

Bij **33 deelnemende lokale besturen konden er tijdens de externe pentesten** diverse kwetsbaarheden gedetecteerd worden zoals bijvoorbeeld ontbrekende of incorrecte certificaten, information disclosure en onbeveiligde verbindingen.

De **resultaten en aanbevelingen** uit de studentenrapporten weerspiegelen grotendeels de **bevindingen uit de thema-audits informatiebeveiliging 2017-2018 en 2020 van Audit Vlaanderen**. Het gaat hierbij over technische kwetsbaarheden als verouderde IT-systemen en zwakke of ontbrekende versleuteling. Daarnaast zijn er ook organisatiebrede aanbevelingen zoals de sensibilisering rond phishing en cyber-hygiëne, duidelijke afspraken rond toegangen en rechten en het opmaken van een business continuïteitsplan.

In het **overzicht van de bevindingen en verbeterpunten** wordt 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.

Overzicht bevindingen Traject Ethisch Hacken 2021

Bevinding 1: Actualisatie van systemen en toepassingen

- Het **up-to-date houden van systemen en toepassingen** is een belangrijke bouwsteen voor een cyberveilige organisatie, aangezien veiligheidsupdates beschermen tegen gekende kwetsbaarheden. Om hierop toe te zien is het van belang om een geformaliseerd patchingproces te hebben waar de frequentie en verantwoordelijkheden vastgelegd worden.

Bevinding 2: Zwakke wachtwoorden

- Vaak wordt na installatie vergeten om **standaardinstellingen**, en dus ook wachtwoorden, aan te passen ondanks dat deze makkelijk geraden kunnen worden zoals een login met ‘admin’ als wachtwoord. Ook zwakke wachtwoorden van gebruikers maken het eenvoudiger voor hackers om toegang te verkrijgen met geautomatiseerde technieken.

Bevinding 3: Toegangen en rechten

- Het is aangewezen om **toegangs- en gebruiksrechten voor gebruikers te beperken tot het strikt noodzakelijke.** Door deze goed af te bakenen en te monitoren kan voorzien worden in de nodige controle om onrechtmatige toegangen zoveel mogelijk te vermijden.

Bevinding 4: Technische beschermingsmaatregelen

- Technische beschermingsmaatregelen als **versleuteling en netwerksegmentatie** hebben een positieve impact op de veiligheid van de ICT-omgeving. Versleuteling zorgt ervoor dat communicatie en gegevens niet onderschept kunnen worden, terwijl netwerksegmentatie voorkomt dat besmettingen het volledige netwerk kunnen impacteren.

Overzicht bevindingen Traject Ethisch Hacken 2021

Bevinding 5: Phishing

- **Phishingaanvallen** waarbij men gebruikers probeert te overtuigen om op een link te klikken en/of hun gebruikersgegevens in te vullen, vormen een reële dreiging voor lokale besturen. Om het risico zoveel mogelijk te beperken is het belangrijk om in te zetten op manuele of automatische filtering en de nodige sensibilisering.

Bevinding 6: Sensibilisering

- **Het gedrag van medewerkers** is een belangrijke bouwsteen om netwerken, systemen en applicaties veilig te houden. Wanneer medewerkers en mandatarissen bewust zijn van de risico's die bepaalde acties en gewoonten met zich meebrengen en hun gedrag hieraan aanpassen, kunnen belangrijke kwetsbaarheden weggenomen worden.

Bevinding 7: Continuïteit en herstel

- Zelfs wanneer de nodige beveiligingsmaatregelen getroffen worden bestaat de kans dat een lokaal bestuur geconfronteerd wordt met cybercriminaliteit. In een dergelijke situatie is het cruciaal dat **de nodige continuïteitsmaatregelen** getroffen worden om de dienstverlening waar mogelijk operationeel te houden en de werking te herstellen.

Bevinding 8: Leveranciersrelaties

- Lokale besturen werken vaak samen met **externe toeleveranciers** voor het aanleveren en veilig houden van IT-systemen en toepassingen. Een vergaande samenwerking kan een positieve zaak zijn, maar het is daarbij cruciaal dat er **duidelijke afspraken zijn voor taken en verantwoordelijkheden** en dat deze ook opgevolgd worden

Bevinding 1: Actualisatie van systemen en toepassingen

Het **up-to-date houden van systemen en toepassingen** is een belangrijke bouwsteen voor een cyberveilige organisatie, aangezien veiligheidsupdates beschermen tegen gekende kwetsbaarheden. Om hierop toe te zien is het van belang om een geformaliseerd patchingproces te hebben waar de frequentie en verantwoordelijkheden vastgelegd worden.

- Verouderde systemen en toepassingen werden bij een meerderheid van lokale besturen gevonden tijdens de pentesten. Bij **27 besturen** ging het hierbij bovendien over systemen en toepassingen die ondertussen minder of niet meer ondersteund worden door de leverancier en dus geen beveiligingsupdates meer krijgen in de toekomst. Verouderde systemen zorgen ervoor dat hackers misbruik kunnen maken van reeds gekende kwetsbaarheden.

- Uit de **38 interviews** met de bevraagde DPO's of CISO's blijkt dat slechts **15 lokale besturen** reeds beschikken over een geformaliseerd patchingproces voor infrastructuur die essentieel is voor de werking en dienstverlening van het lokaal bestuur. In de overige steden en gemeenten kon geen of slechts een beperkt patchingproces voorgelegd worden, terwijl dit een belangrijke hulpmiddel is om erop toe te zien dat systemen en toepassingen de nodige patches krijgen.

- Een uitgewerkte inventarisatie van IT-gerelateerde objecten zoals servers, routers, computers en printers kan eveneens een belangrijk hulpmiddel zijn om ervoor te zorgen dat systemen en toepassingen niet vergeten worden doorheen de tijd. In **18 van de 38 deelnemende lokale besturen** is er sprake van een inventaris die de levensloop van IT-gerelateerde objecten bijhoudt, maar toch zijn er ook meerdere lokale besturen waarbij dit hulpmiddel afwezig of onvolledig is.

Aanbevelingen uit de studentenrapporten

- **Wanneer verouderde versies van systemen aangetroffen worden, dienen deze zo snel mogelijk geüpdatet te worden naar de meest recente versie**. Het is belangrijk dat hierrond duidelijke afspraken gemaakt worden en verantwoordelijkheden worden toegewezen, zowel voor intern als met externe dienstenleveranciers.

- **Maak werk van een geformaliseerd patchingproces.** Zeker voor infrastructuur die een belangrijke rol speelt in de werking en dienstverlening van het lokaal bestuur, indien een dergelijk document nog niet aanwezig is. Een uitgewerkt proces kan helpen om de bovenvermelde aanbeveling in de praktijk te brengen en een duidelijk referentiekader te creëren voor lokale medewerkers en externe leveranciers. Een geautomatiseerd updateproces kan hierop een waardevolle toevoeging zijn.

- **Werk een omvattende inventarisatie van IT-gerelateerde objecten uit en tracht deze zo volledig mogelijk te maken,** door bijvoorbeeld actuele informatie per asset toe te voegen en licentiegegevens te integreren. Op zich draagt een dergelijke inventarisatie niet actief bij aan het patchingproces, maar het zorgt ervoor dat het lokaal bestuur weet welke systemen en toepassingen de nodige aandacht dienen te krijgen.

- **Laat de IT-omgeving op geregelde tijdstippen testen via professionele netwerkscans of ICT-veiligheidsaudits** om zo verouderde systemen en toepassingen op te sporen die mogelijk over het hoofd werden gezien.

Bevinding 2: Zwakke wachtwoorden

Vaak wordt na installatie vergeten om standaardinstellingen, en dus ook **wachtwoorden**, aan te passen ondanks dat deze makkelijk geraden kunnen worden zoals een login met ‘admin’ als wachtwoord. Ook zwakke wachtwoorden van gebruikers maken het eenvoudiger voor hackers om toegang te verkrijgen met behulp van geautomatiseerde technieken.

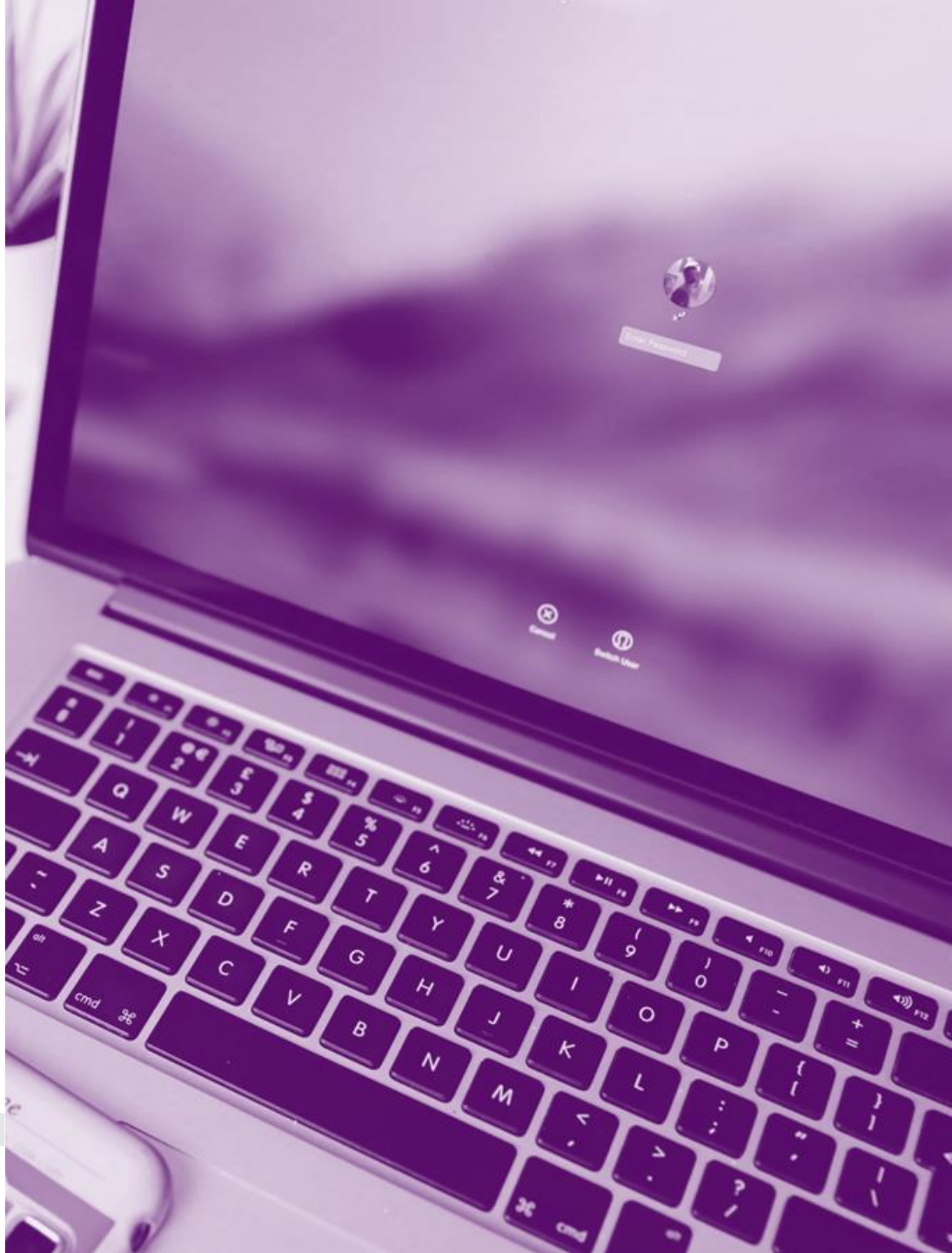
- In **13 besturen** werden er zwakke wachtwoorden aangetroffen tijdens de pentesten. Bij **5 besturen** bleek er geen login te zijn of een automatische login voor een of meerdere systemen en toepassingen aanwezig te zijn.
- In een beperkt aantal gevallen gaven de **standaardwachtwoorden of ontbrekende wachtwoorden toegang tot administrator-accounts met hoge privileges.** De impact varieert sterk: in sommige gevallen kunnen studenten enkel gegevens inkijken of manipuleren, terwijl andere toegangen de mogelijkheid bieden om belangrijke instellingen te wijzigen.
- Ook het regelmatig hernieuwen van wachtwoorden is een belangrijke beveiligingsmaatregel om ongeoorloofde toegangen te vermijden. De **Open-Source Intelligence Testen** door de studenten bevestigen het belang van deze aanbeveling, aangezien bij **er bij 4 van de 22 lokale besturen die deze test liet uitveren** mailadressen van medewerkers werden gevonden die ooit deel uitmaakten van een datalek.

Bevinding 2: Zwakke wachtwoorden

- Uit de gesprekken met de DPO's of CISO's kwam naar boven dat een gedocumenteerd wachtwoordbeleid aanwezig is in **30 van de geteste besturen. Bij 8 lokale besturen** wordt aangeven niet of nog niet te beschikken over een volledig uitgewerkt wachtwoordbeleid met minimumvereisten.

    - De aanwezigheid van **een gedocumenteerd wachtwoordbeleid** is echter niet voldoende om de veiligheid van wachtwoorden te garanderen. De regels die hierin vervat zitten, moeten ook bijdragen tot een voldoende hoge complexiteit.

- De vereiste minimale lengte varieert sterk naar gelang het lokaal bestuur, **van 0 tot 20 tekens.**



Aanbevelingen uit de studentenrapporten

- **Kijk systemen en toepassingen na op standaardwachtwoorden** en zorg bij de installatie of introductie van nieuwe systemen en toepassingen er voor dat inloggegevens gewijzigd worden naar wachtwoorden met een hoge complexiteit of dat een wachtwoord ingesteld wordt indien afwezig.

- **Hanteer een sterk wachtwoordbeleid** in het lokaal bestuur en dwing dat waar mogelijk af bij zowel technische als gewone gebruikersaccounts. Kijk hiervoor bijvoorbeeld naar de aanbevelingen van Safe on Web, waar men wachtwoorden of zinnen van minstens 13 tekens met een combinatie van cijfers, hoofdletters en speciale tekens aanraadt. Zorg er ook voor dat gebruikers hun wachtwoorden periodiek aanpassen, want ook sterke wachtwoorden kunnen gekraakt worden.

- Indien sterke wachtwoorden niet voor alle toepassingen en systemen afgedwongen kunnen worden, is een belangrijke rol weggelegd voor **sensibilisering bij gebruikers**, al dan niet op basis van reeds bestaand campagnemateriaal.

Bevinding 3: Toegangen en rechten

Het is aangewezen **om toegangs- en gebruiksrechten** voor gebruikers te beperken tot het strikt noodzakelijke. Door deze goed af te bakenen en te monitoren kan voorzien worden in de nodige controle om onrechtmatige toegangen zoveel mogelijk te vermijden.

- Bij de pentesten werden er bij **20 lokale besturen** te ruime toegangen en gebruikersrechten aangetroffen voor interne gebruikers. Hierbij gaat het bijvoorbeeld over gedeelde mappen met gevoelige informatie voor het volledige netwerk tot te uitgebreide lees- en schrijfrechten voor gastaccounts.

- Een **identity en access management systeem** dat helpt om correcte authenticatie te garanderen en het beleid rond toegangsrechten uniform toe te passen, werd gerapporteerd in een meerderheid van de DPO-CISO interviews. Maar bij **6 lokale besturen** werd er nog geen beroep gedaan op een systeem dat het beheer van rechten en toegangen vereenvoudigt.

- **Tweestapsverificatie of 2FA** die een bijkomende authenticatiestap voorziet om toegangen extra te beveiligen, werd reeds in **17 van de 38 bevraagde besturen** voorzien..

Aanbevelingen uit de studentenrapporten

- **Zorg voor een gestandaardiseerde procedure die helpt bij het toekennen en intrekken van toegangen en rechten**. Wanneer er een vast proces is voor een medewerker die in dienst treedt, die de dienst verlaat of veranderd van dienst voor het toekennen van gebruikersrechten bij nieuwe applicaties, kan vermeden worden dat onbevoegde personeelsleden en externen toegang krijgen tot gevoelige informatie.

- **Een periodiek nazicht van toegangen en rechten** kan ook dienen als extra beheersmaatregel.

- **Versterk de huidige aanpak met een identity and access management systeem.** Duidelijke processen zijn een belangrijke eerste stap, maar voor de concrete toepassing kan het interessant zijn om gebruik te maken van een sluitend beheerssysteem, zoals **ACM-IDM** (het Toegangs- en Gebruikersbeheer van de Vlaamse Overheid).

- **Zet, indien nog niet aanwezig, in op tweestaps- of multifactorauthenticatie als extra beveiligingslaag, g**ecombineerd met een sterk afgedwongen wachtwoordbeleid en een sluitend beheer van toegangen en rechten. Zo kan deze technologie gevoelige informatie en systemen veilig houden.

Bevinding 4: Technische beschermingsmaatregelen

Technische beschermingsmaatregelen als versleuteling en netwerksegmentatie hebben een positieve impact op de veiligheid van de ICT-omgeving. Versleuteling zorgt ervoor dat communicatie en gegevens niet onderschept kunnen worden, terwijl netwerksegmentatie voorkomt dat besmettingen het volledige netwerk kunnen impacteren.

- In **13 van de 38 deelnemende besturen** werden tijdens de pentesten communicatieprotocollen gedetecteerd die onvoldoende of niet geëncrypteerd zijn, zoals HTTP in plaats van het veiligere HTTPS, die het zo mogelijk maken voor hackers om mee te luisteren of verzonden gegevens te onderscheppen.

- Wanneer men gevoelige informatie opslaat die niet actief gebruikt wordt, is het veiliger om dit te doen met de nodige encryptie zodat deze enkel geraadpleegd kan worden met een unieke sleutel. In realiteit gebeurt dit echter zelden bij de geteste besturen. De DPO-CISO interviews wijzen immers uit dat slechts **5 van de 38 lokale besturen** deze praktijk consequent toepassen voor gevoelige informatie. Wanneer studenten peilden naar het gebruik van versleuteling voor het verzenden van dergelijke informatie via het internet, gaven **12 besturen** aan dit reeds toe te passen.

- Uit de DPO-CISO interviews blijkt ook dat het merendeel van de lokale besturen reeds stappen heeft gezet om het netwerk op te delen in segmenten. In **18 van de 38 bevraagde lokale besturen** voorziet men reeds een extra beveiligingslaag, zoals een Demilitarized Zone voor systemen met een hoog risico.

Aanbevelingen uit de studentenrapporten

- **Vervang verouderde encryptie-methoden** zoals HTTP of verouderde communicatieprotocollen door hedendaagse, veiligere varianten zodat aanvallers geen vertrouwelijke informatie kunnen ontsleutelen en bekijken. Evalueer ook om de zoveel tijd of de gehanteerde methodes en gebruikte algoritmes nog steeds voldoende sterk zijn.

- **Maak werk van een lokaal beleid rond versleuteling, met aandacht voor zowel het opslaan als het versturen van gevoelige informatie en informatiedragers als USB's.** Bekijk welke IT-apparatuur het best versleuteld wordt - bijvoorbeeld door de aanwezigheid van gevoelige informatie - en kies voor een versleutelingsprogramma met een voldoende encryptiesterkte.

- **Een extra beschermingsmaatregel kan bestaan uit de investering in netwerksegmentatie en segregatie**, zodat de schade bij een cyberaanval zoveel mogelijk ingeperkt wordt. Zorg er ook voor dat servers en andere apparaten die toegankelijk moeten zijn van buiten het interne netwerk, in een gedemilitariseerde zone geplaatst worden.

Bevinding 5: Phishing

Phishingaanvallen waarbij men gebruikers probeert te overtuigen om op een link te klikken en/of hun gebruikersgegevens in te vullen, vormen een reële dreiging voor lokale besturen. Om het risico zoveel mogelijk te beperken is het belangrijk om in te zetten op manuele of automatische filtering en de nodige sensibilisering.

- In **35 lokale besturen** werd een phishingmailcampagne uitgevoerd waarbij de studenten een frauduleuze, doch onschadelijke mail opstelden met een URL die leidt naar een geloofwaardig uitziende, maar vervalste inlogpagina. Gemiddeld klikte **31% van de medewerkers** naar wie een mail verstuurd werd, op de link en vulde in totaal **19% van de medewerkers zijn of haar gegevens in op de inlogpagina.**
- **In 6 van de 35 besturen** konden de phishingmails geen slachtoffers maken.
- In de vragenlijst naar **1429 medewerkers uit de 35 deelnemende lokale besturen,** geven **60 medewerkers** aan dat ze automatisch zouden klikken op een link in een onverwachte mail van een bekend contact.
- Bij **360 van de 1429 bevraagde medewerkers** die de vragenlijst invulden, werd aangegeven dat hun lokaal bestuur voorziet in training rond phishingmails om de 6, 12, 24 of 60 maanden. Toch verklaren **1029 van de 1429 bevraagde medewerkers** dat er binnen hun lokaal bestuur geen training wordt voorzien.

Aanbevelingen uit de studentenrapporten

- **Voorzie geregeld in phishingtraining binnen het lokaal bestuur,** waar medewerkers leren hoe ze phishingmails kunnen herkennen en welke stappen ze dienen te nemen wanneer ze met deze cyberdreiging geconfronteerd worden. Probeer medewerkers ook actief te betrekken tijdens dergelijke vormingsmomenten - bijvoorbeeld met interactieve oefeningen - zodat de lessen uit de training in de praktijk worden gebracht.

- **Zorg voor een duidelijk aanspreekpunt en bijhorende meldingsprocedure voor medewerkers** die een mogelijke phishingaanval detecteren en zorg er ook voor dat hierrond frequent gecommuniceerd wordt. Het is belangrijk om in te zetten op een bedrijfscultuur waar medewerkers phishing intern durven te signaleren, ook wanneer het misschien gaat over een vals alarm.

  - Deze aanbeveling kan gekoppeld worden aan het AVG (Algemene Verorbering Gegevensbescherming) en het informatieveiligheidsplan. In dit geval moet er een incidentenprocedure of register worden bijgehouden wanneer iemand toch in de val van een phishing zou trappen.

    - Sensibiliseringsmateriaal i.v.m. de gevaren van phishing kan je terugvinden binnen de **Toolkit Cybersecurity van VVSG.**

- **Organiseer geregeld een phishingtest in het lokaal bestuur** om te kijken of de aanwezige automatische of manuele filtering erin slaagt om mails met een kwaadwillig oogmerk te weren uit de inbox van medewerkers. Voorzie indien nodig bijkomende technische beheersmaatregelen.

Bevinding 6: Sensibilisering

Het **gedrag van medewerkers** is een belangrijke bouwsteen om netwerken, systemen en applicaties veilig te houden. Wanneer medewerkers en mandatarissen bewust zijn van de risico's die bepaalde acties en gewoonten met zich meebrengen en hun gedrag hieraan aanpassen, kunnen belangrijke kwetsbaarheden weggenomen worden.

- Uit de vragenlijst naar **1429 lokale medewerkers** blijkt dat zij in zekere mate **bewust zijn van goede praktijken** zoals het vergrendelen van de werkcomputer bij het verlaten van het werkstation, het versnipperen van gevoelige informatie alvorens deze weg te gooien of aparte wachtwoorden voor werk en privé. Maar dat de concrete toepassing varieert sterk.

- De verdeelde resultaten uit de vragenlijst geven aan dat lokale besturen in bewustmaking voorzien, zoals toelichtingen bij het wachtwoordbeleid, posters, phishingtraining of mails met aandachtspunten voor informatiebeveiliging, maar dat de frequentie sterk verschilt.

- Zo geeft **48% van de medewerkers** aan regelmatig mails met aanbevelingen te ontvangen, terwijl **13%** aangeeft toelichtingen te krijgen tijdens vergaderingen i.v.m. het gebruik van de werkcomputer. Slechts **6%** van de medewerkers geeft aan gesensibiliseerd te worden a.d.h.v. posters op de werkvloer.

Bevinding 6: Sensibilisering

Aanbevelingen uit de studentenrapporten

- **Hanteer een mix van sensibiliseringspraktijken**, zodat medewerkers meermaals en via diverse methodes gewezen worden op het belang van een goede cyberhygiëne. Wanneer medewerkers bijvoorbeeld na een toelichting over het gebruik van de werkcomputer deze boodschap ook terugvinden op de werkvloer in de vorm van een poster, kan dit de retentie bevorderen. Het bestaand campagnemateriaal van onder andere **CCB**, **Safe on Web** en de **Cyber Security Coalition** kan hierbij helpen.

- **Zorg ervoor dat sensibilisering een aangehouden engagement is**. Het is belangrijk dat cyberveiligheid meermaals onder de aandacht van medewerkers wordt gebracht. Van bij de werving tot de indiensttreding, met periodieke herhalingen voor wie reeds langer werkt bij het lokaal bestuur.

- **Kader sensibiliseringsacties binnen een organisatiebrede aandacht voor cyberveiligheid.** Sensibilisering dient voorzien te worden voor alle lagen van het lokaal bestuur, met gerichte training voor wie dagdagelijks werkt met persoonsgegevens, maar ook initiatieven voor algemene medewerkers. Betrokkenheid van directie en diensthoofden kan de impact van deze inspanningen versterken.

    - De twee laatste aanbevelingen kunnen gekoppeld worden aan het AVG (Algemene Verorbering Gegevensbescherming), het informatieveiligheidsplan en de taken van een DPO (Data Protection Officer) binnen een lokaal bestuur.

Bevinding 7: Continuïteit en herstel

Zelfs wanneer de nodige beveiligingsmaatregelen getroffen worden bestaat de kans dat een lokaal bestuur geconfronteerd wordt met cybercriminaliteit. In een dergelijke situatie is het cruciaal dat de **nodige continuïteitsmaatregelen** getroffen worden om de dienstverlening waar mogelijk operationeel te houden en de werking te herstellen.

- De gestructureerde interviews met DPO's en CISO's uit **38 lokale besturen** leren ons dat een volledig uitgewerkt business continuïteitsplan dat helpt bij het herstel van de dienstverlening binnen een redelijke termijn, slechts aanwezig is in **8 van de betrokken besturen**.

- Een back-up en herstelplan om systemen en data zo snel mogelijk terug operationeel te krijgen, werd in tegenstelling tot het business continuïteitsplan vastgesteld bij **meer dan de helft** van de bevraagde lokale besturen. Toch zijn er ook **6 besturen** die niet beschikken over een uitgeschreven plan en **5 besturen** die hun back-up en herstelplan nog niet volledig uitgewerkt hebben.

- In kader van een goede back-up en herstelstrategie is het ook van belang dat gemaakte back-ups periodiek getest worden. Deze praktijk wordt consequent toegepast bij **15 van 38 bevraagde lokale besturen.**

Aanbevelingen uit de studentenrapporten

- **Maak zo snel mogelijk werk van een business continuïteitsplan** zodat efficiënt opgetreden kan worden wanneer belangrijke dienstverlening uitvalt ten gevolge van een cyberaanval. Indien er reeds een plan voorhanden is, is het belangrijk dat dit plan ook jaarlijks geëvalueerd wordt om te verzekeren dat de beschreven informatie nog steeds courant is.

- **Zorg voor een volledig uitgewerkt back-up en herstelplan.** Voorzie binnen dit plan ook ruimte om de back-upstrategie en back-ups op geregelde tijdstippen te testen, zodat men in tijden van hoge nood niet tot de ontdekking komt dat de gemaakte back-ups niet bruikbaar zijn voor de herstelfase.

Bevinding 8: Leveranciersrelaties

Lokale besturen **werken vaak samen met externe leveranciers** voor het aanleveren en veilig houden van IT-systemen en toepassingen. Een vergaande samenwerking kan een positieve zaak zijn, maar het is daarbij cruciaal dat er duidelijke afspraken zijn voor taken en verantwoordelijkheden en dat deze ook opgevolgd worden.

- Bij **26 lokale besturen** worden afspraken over de rollen, verantwoordelijkheden en aansprakelijkheid inzake cyberveiligheid nog niet opgenomen in leveranciers-, derden- en partnerovereenkomsten.

- Het controleren van externe dienstverleners op het naleven van de vastgelegde servicelevel agreements (SLA's) blijkt een meer courante praktijk: **16 van de 38 bevraagde DPO's en CISO's** geeft aan dat er geregeld controles uitgevoerd worden om hierop toe te zien.

Aanbevelingen uit de studentenrapporten

- Wanneer er een grote afhankelijkheid is van externe software- en ICT-dienstenleveranciers - wat ook vaak het geval blijkt - is het belangrijk om **duidelijke afspraken te maken rond o.a. het actualiseren van systemen en toepassingen en het opvolgen bij storingen.** Het dient steeds duidelijk te zijn welke verantwoordelijkheden bij het lokaal bestuur en de externe partners liggen.

- Voorzie ook in **het nodige toezicht op de naleving van gemaakte afspraken**. Een goede vertrouwensrelatie wil niet zeggen dat er geen plaats is voor periodieke controles om problemen en misverstanden te vermijden.

4. Meer informatie

vvsg

Meer informatie

Het Traject Ethisch Hacken kadert binnen het Project Cyberveilige Gemeenten dat gecoördineerd wordt door de VVSG, met ondersteuning van de Vlaamse Overheid. Voor meer info bij het project en de verschillende luiken kan je terecht op **de VVSG website**. Op deze pagina zijn ook tools te vinden die gebruikt kunnen worden om de lokale aanpak te versterken, zoals een sjabloon voor een business continuïteits- en crisiscommunicatieplan en een inspirerende infosessies.

In de conclusie van dit analyserapport wordt verwezen naar de rapporten die Audit Vlaanderen uitwerkte in kader van de Thema-audits Informatiebeveiliging 2017-2018 en 2020. Beide documenten zijn te raadplegen op **de website van Audit Vlaanderen**. Audit Vlaanderen coördineert ook het aanbod van professionele ICT-veiligheidsaudits met cofinanciering in het kader van het Programma Cyberveilige gemeenten. **Hier** vind je meer informatie bij het aanbod en de bestelprocedure.

Voor diverse aanbevelingen uit dit analyserapport bestaan reeds goede praktijkvoorbeelden bij lokale besturen. **Op de website van de Vlaamse Overheid** staan een twintigtal praktijken die kunnen helpen bij het uitwerken van een eigen lokale aanpak.

Het Traject Ethisch Hacken kwam tot stand door een samenwerking met studenten Toegepaste Informatie van Howest. Voor meer informatie over de opleiding en de afstudeerrichtingen kan je terecht op **de website van de hogeschool.**

In het najaar van 2022 zal **een herhaling van het Traject Ethisch Hacken** plaatsvinden. Indien jouw lokaal bestuur hier graag deel van wil uitmaken, kan je dit reeds melden **via mail**. Het vervolgtraject zal formeel aangekondigd worden via de VVSG-kanalen.

Contact

Vereniging van Vlaamse Steden en Gemeenten
Bischoffsheimlaan1-8, 1000 Brussel
cyberveiligheid@vvsg.be

vvsg howest / hogeschool AGENTSCHAP BINNENLANDS BESTUUR AUDIT VLAANDEREN AGENTSCHAP FACILITAIR BEDRIJF