Welkom

VVSG Ronde van Vlaanderen

mei-juni 2021

#VVSGronde

vvsg
AGENTSCHAP BINNENLANDS BESTUUR
Vlaamse overheid
Belfius
elia Elia Group
ethias
fluvius.
MATEXI Welkom in de buurt.
proximus
RASSCHAERT ADVOCATEN

Welkom

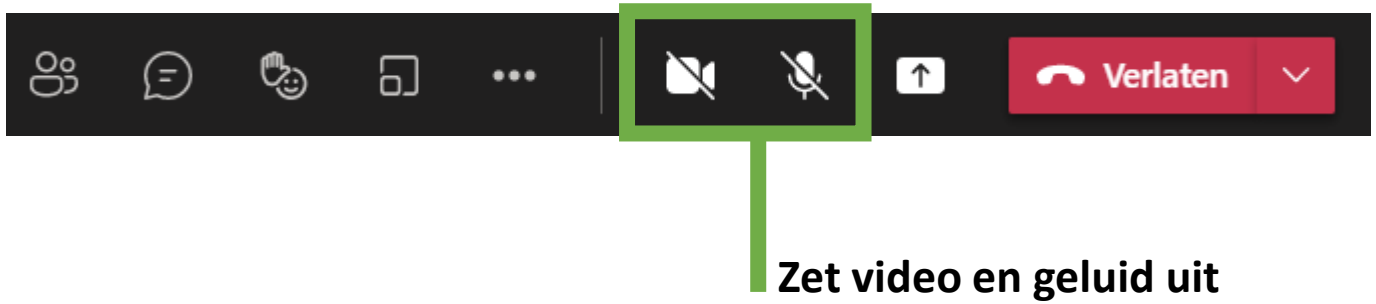
- ✓ **Het webinar start om 13 uur**
- ✓ Via Microsoft Teams
- ✓ Volg bij voorkeur via **Microsoft Teams app**
- ✓ Of via je browser **(Chrome, Firefox, Safari of Edge)**
- ✓ Stel vragen **via de chat.** Vermeld dan ook even je naam en lokaal bestuur.

Welkom! Enkele praktische afspraken

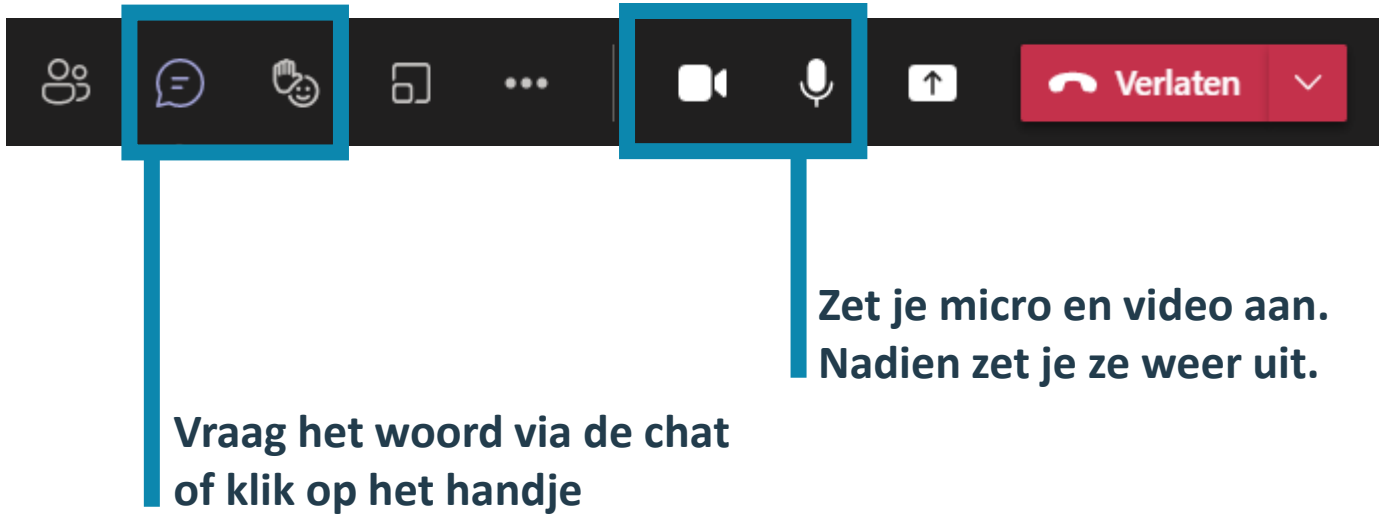
- ✓ **Het webinar start om 13 uur**
- ✓ Via Microsoft Teams
- ✓ Volg het bij voorkeur via de **Microsoft Teams app**
- ✓ Of via je browser **(Chrome, Firefox, Safari of Edge)**
- ✓ Stel je vragen **via de chat.** Vermeld dan ook even je naam en lokaal bestuur.

Welkom! Enkele praktische afspraken

Tijdens vergadering



Het woord vragen?



Cyberveiligheid, zoveel meer dan IT

West-Vlaanderen | dinsdag 4 mei 2021

Gunter Schryvers | Audit Vlaanderen

Tomas Coppens | VVSG

Het grotere geheel

Hoe prioritair is cyberveiligheid?

Het grotere geheel

Bron: VRT NWS, 25/1/20

Gemeentediensten van Willebroek slachtoffer van cyberaanval: "Hackers vragen betaling in bitcoins"

De gemeentediensten van de Antwerpse gemeente Willebroek zijn het slachtoffer geworden van een cyberaanval. De hackers vragen een betaling in bitcoins, meldt de gemeente op haar website.

Cyberaanval op Kuurne heeft grote gevolgen: geen gemeenteraad en ook identiteitskaarten uitreiken kan niet

18/11/2020 om 13:37 door Kris Van

Het Centrum voor Cybersecurity België (CCB) waarschuwt Belgische bedrijven die gebruik maken van Microsoft Exchange Servers voor een systeemkwetsbaarheid.

Bij talloze computerservers van bedrijven, organisaties en overheidsdiensten wereldwijd zijn sinds januari hackers binnengedrongen, zo bericht Microsoft. Het bedrijf vond een reeks kwetsbaarheden in zijn Exchange-servers. Dat zijn e-mailservers die door duizenden bedrijven en organisaties worden gebruikt. Ook Belgische organisaties maken gebruik van dit product en zijn mogelijks slachtoffer.

DILBEEK - **De cyberaanval die de gemeentelijke dienstverlening in Dilbeek al bijna een week in grote problemen brengt, wordt mee onderzocht door experts van de Federal Computer Crime Unit.**

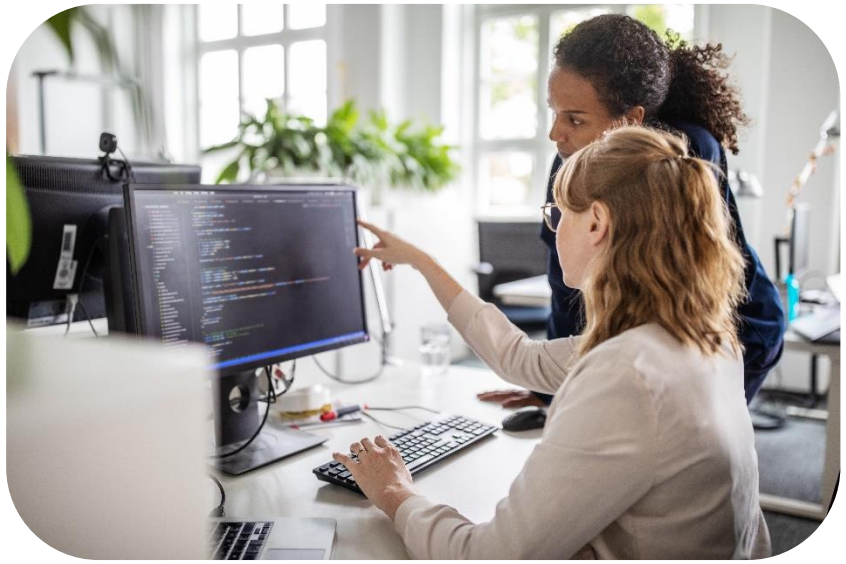
Burgemeester Willy Segers (N-VA) laat weten dat er een klacht tegen onbekenden wordt neergelegd bij de politie na de cyberaanval die de gemeentelijke serveromgeving vorige week zwaar heeft getroffen. ...

Bron: Het Nieuwsblad, 24/11/20

Het grotere geheel

- ✓ Dienstverlening stopt een week of langer (behalve wat zonder IT kan)
- ✓ Persoonsgegevens (inclusief sommige rijksregistergegevens, inkomensgegevens, vergunningsgegevens en subsidiedossiers) worden gestolen en online verspreid
- ✓ Vertrouwelijke mails worden bekend gemaakt in een delicate periode
- ✓ Vanuit een gecompromitteerde mailaccount van je bestuur worden mails verzonden naar anderen om hen op te lichten of aan te vallen
- ✓ Alles wat opgeslagen was, is plots weg (mails + bestanden + gegevens)
- ✓ Plots moet de hele ICT-omgeving helemaal opnieuw opgezet worden

Het grotere geheel

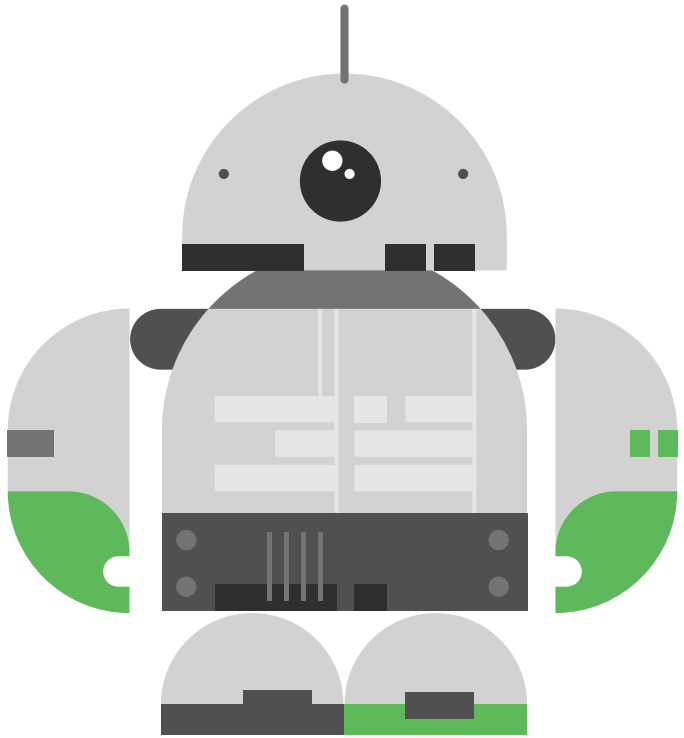


Waarom over gaan tot actie?

- ✓ Groeiende digitale dienstverlening
- ✓ Vertrouwelijke en gevoelige info
- ✓ Toenemende aandacht voor cyberveiligheid en privacy
- ✓ Risico op reputatie- en financiële schade
- ✓ Het aantal incidenten met een significante impact stijgt
- ✓ “Overheden moeten voorbeeld geven”

Enkele cyber security mythes

Vraagt cyberveiligheid om uitzonderlijke kosten en inspanningen?

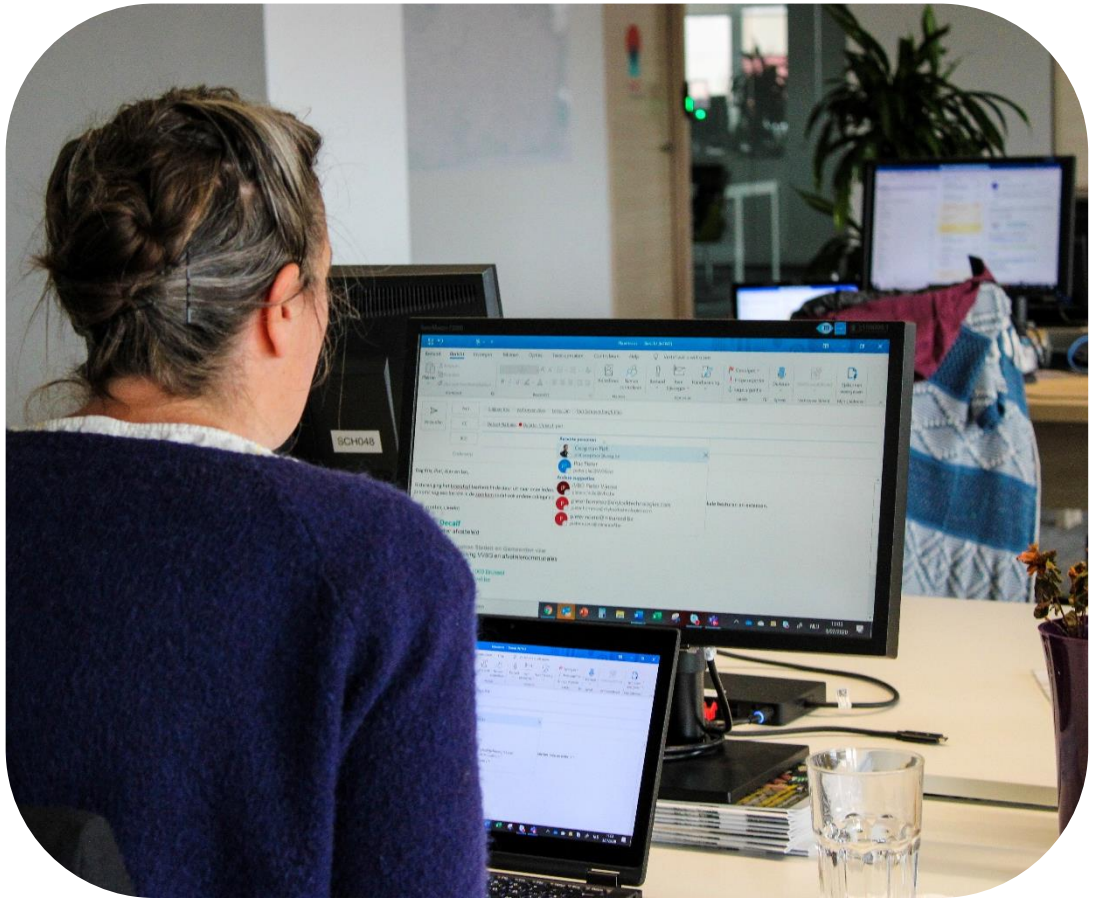


Poll: Hoe hoog schat je de kans in dat je lokaal bestuur dit jaar slachtoffer wordt van cybercrime?

- ✓ 0 tot 20%
- ✓ 20 tot 40%
- ✓ 40 tot 60%
- ✓ 60 tot 80%
- ✓ 80 tot 100%

Mythe: “Onze gemeente loopt geen direct risico.”

- ✓ Na al die jaren lijkt het vaak onwaarschijnlijk dat grote problemen zouden opduiken.
- ✓ Als men ziet welke ICT-systemen een bestuur gebruikt en wat daar jaarlijks voor wordt betaald, lijkt het snel alsof al veel inspanningen zijn geleverd.
- ✓ Af en toe gaat men ervan uit dat men door de implementatie van enkele (nieuwe) beveiligingsmaatregelen goed zit.
- ✓ Vaak groeit de aandacht voor cyberveiligheid wanneer een incident zich voordoet, intern of bij een collega-bestuur, maar die aandacht durft te verslappen.



Realiteit

- ✓ Tijdens de thema-veiligheidsaudit Informatieveiligheid 2020 kon men bij 5 op 6 lokale besturen **volledige controle** verwerven over het interne netwerk.
- ✓ Zowel in 2018 als 2020 tonen de auditresultaten aan dat bijkomende inspanningen geleverd moeten worden om de risico's voor informatiebeveiliging te beheersen.
- ✓ Tijdens de ICT-veiligheidsaudits met cofinanciering worden gemiddeld 5 en 1 **kwetsbaarheden met hoog risico** gevonden voor respectievelijk de interne en externe pentesten.
- ✓ Tijdens de pentesten in kader van het Traject Ethisch Hacken in samenwerking met Howest werden kwetsbaarheden gevonden bij 59 op 60 interne pentesten en bij 8 op 26 externe pentesten.

De risico's zijn meetbaar en reëel!

Mythe: “We beheersen de basis en moeten vooral verder innoveren”

- ✓ Vaak gaan aandacht en IT-budgetten naar nieuwigheden als E-Government, Internet of Things en nieuwe, interactieve websites.
- ✓ Nog te weinig wordt cyberveiligheid gezien als iets om mee uit te pakken.
- ✓ Ook bij nieuwe aankopen staat veiligheid niet altijd centraal tijdens initiële gesprekken.

Realiteit

Actualiseren systemen en toepassingen:

- ✓ Tijdens de interne pentesten door Howest-studenten werden in een meerderheid van de lokale besturen verouderde systemen en toepassingen teruggevonden.
- ✓ Ook uit de ICT-veiligheidsaudits en de thema-audits informatieveiligheid blijkt dat het actualiseren van systemen in de praktijk niet altijd nauwgezet gebeurt.
- ✓ Binnen het Traject Ethisch Hacken werd een geformaliseerd proces om veiligheidsupdates door te voeren bij 1 op 3 lokale besturen teruggevonden.

Realiteit

Zwakke wachtwoorden:

- ✓ Uit de eerste resultaten voor de ICT-veiligheidsaudits blijkt dat 65% van de lokale besturen niet beschikt over een voldoende sterk wachtwoordenbeleid.
- ✓ In 2 op 3 gemeenten wordt bovendien geen beperking op inlogpogingen voorzien.
- ✓ In een kwart van de deelnemende lokale besturen slaagden de studenten erin om wachtwoorden te kraken tijdens de pentesten.
- ✓ De studenten troffen standaardwachtwoorden op systemen en toepassingen aan in meer dan 60% van de gemeenten.

Realiteit

Andere (technische) beschermingsmaatregelen:

- ✓ Bij de eerste ICT-veiligheidsaudits bleek 95% van de lokale besturen niet te beschikken over de nodige netwerksegmentatie of -segregatie om verdere verspreiding te voorkomen bij besmetting.
- ✓ Uit de thema-audit informatieveiligheid 2020 blijkt dat het merendeel van de lokale besturen geen beleid heeft voor de versleuteling van gegevens (cryptografie).
- ✓ De Howest-studenten rapporteren dat gevoelige informatie maar in 1 op 5 besturen opgeslagen of verzonden wordt met de nodige encryptie om deze extra te beveiligen.
- ✓ Zowel uit de thema-audits als het Traject Ethisch Hacken blijkt bovendien dat de aanwezige versleuteling vaak gebaseerd is op verouderde mechanismes.

Mythe: “Toegangen en rechten zijn moeilijk te beheren en bemoeilijken vaak de werking”

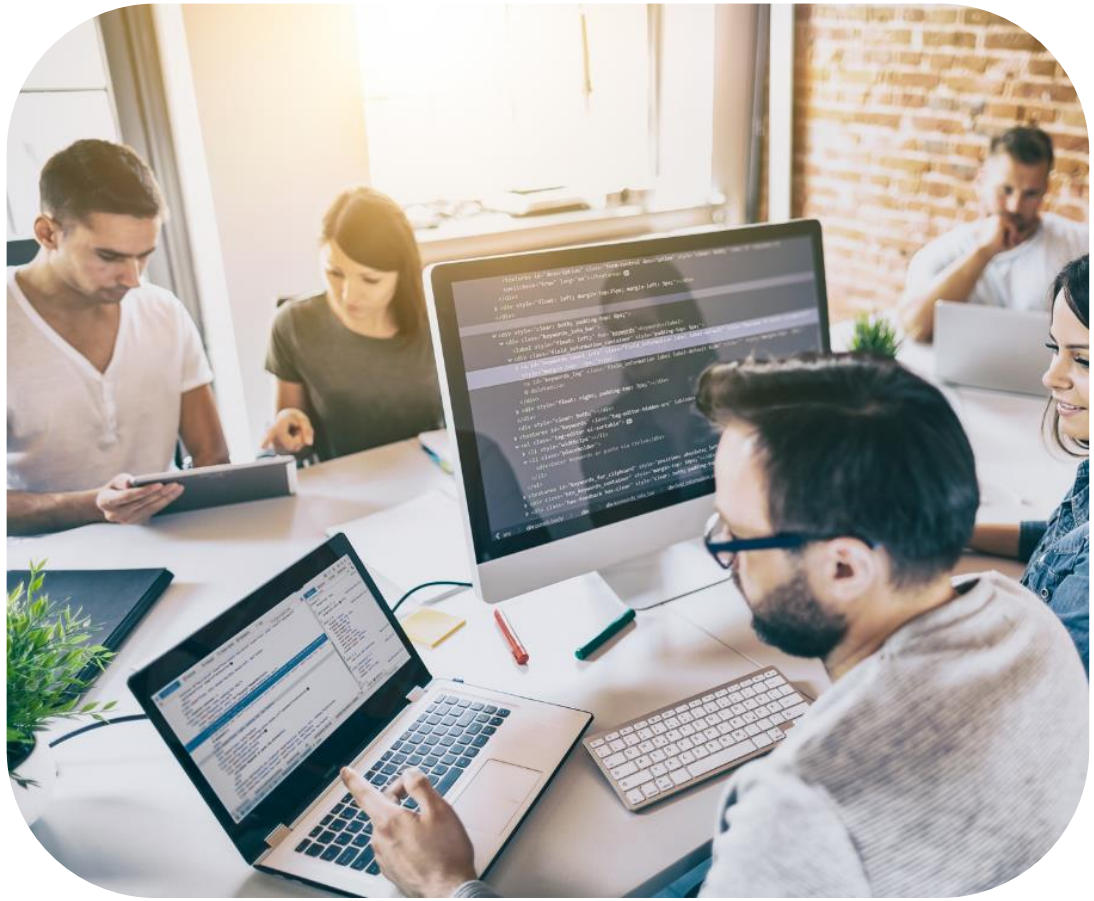
- ✓ Toegangen en rechten beheren voor alle systemen met werknemers die erbij komen, van functie veranderen of vertrekken, is geen sinecure.
- ✓ Rollen en verantwoordelijkheden afspreken is men al jaren gewend, maar dat vertalen naar toegangen en rechten lijkt vaak te gevaarlijk.

Realiteit

- ✓ Uit de eerste ICT-veiligheidsaudits blijkt dat gemiddeld ongeveer een kwart van de accounts niet toe te wijzen zijn aan actieve personeelsleden.
- ✓ De thema-audits Informatieveiligheid leren dat lokale besturen vaak (nog) geen gedefinieerde aanpak hebben voor de toekenning, wijziging en intrekking van toegangs- en gebruikersrechten.
- ✓ Tijdens het traject ethisch hacken werden in een kwart van de besturen te ruime toegangen en gebruikersrechten aangetroffen voor interne gebruikers.
- ✓ Ook bij lokale besturen valt er nog een weg af te leggen om multi-factorauthenticatie op te zetten voor alle belangrijke systemen.

Mythe: “Cyberveiligheid is een puur IT-verhaal”

- ✓ Wanneer het woord cyberveiligheid valt, wordt al snel doorverwezen naar IT. Het gaat tenslotte over IT-systemen en toepassingen.
- ✓ Gezien de rol van DPO’s en CISO’s inzake informatieveiligheid worden zij sneller betrokken, maar andere diensten komen zelden aan bod in relevante discussies.
- ✓ Vaak wordt de link tussen IT en andere diensten pas gelegd wanneer er sprake is van een hoog risico of een incident heeft plaatsgevonden.



Realiteit

- ✓ Rollen en verantwoordelijkheden rond cyber- of informatieveiligheid worden vaak uitsluitend toegekend aan medewerkers van de dienst ICT of de lokale DPO, terwijl diensten als HR, communicatie, noodplanning en technische dienst ook een rol te spelen hebben.
  - ✓ **Communicatie:** Uit een vragenlijst in kader van het Traject Ethisch Hacken naar 1495 lokale medewerkers blijkt dat zij in zekere mate bewust zijn van goede praktijken, maar dat de concrete toepassing varieert en bijkomende sensibilisering aangewezen is. Dit geldt ook voor phishing, aangezien 16% klikt op een phishing mail.
  - ✓ **HR:** Ex-medewerkers hebben vaak nog toegang tot accounts binnen het lokaal bestuur.
  - ✓ **Facility management:** Is een uitwijklocatie voorzien voor crisissituaties zoals een cyberaanval? Dan is het belangrijk dat deze locatie ook voorzien is op de noden die daarbij horen, zoals routers en stopcontacten in noodruimtes.
- ✓ Verantwoordelijkheden of verwachtingen voor medewerkers zijn bovendien vaak weinig of niet gedefinieerd. Ook de vertaalslag van verwachtingen of verantwoordelijkheden naar concrete taken wordt onvoldoende gemaakt.

Mythe: “Ons bestuur is een open, maar veilig huis.”

- ✓ In heel wat lokale besturen gaat men uit van het ‘open huis’ principe, waar drempels voor toegang tot een minimum beperkt worden en bezoekers soms vrij kunnen rondzwerven.
- ✓ Dat heeft zo z’n voordelen, maar doordacht omgaan met de bijhorende veiligheidsrisico’s vergt aangepaste beheersmaatregelen.

Realiteit

- ✓ Uit de thema-audit informatieveiligheid 2017-2018 blijkt dat ongeveer 1 op 3 besturen archiefruimtes niet consequent afsluiten. In 2 op 5 besturen hanteert men geen clean desk beleid.
- ✓ Ook blijkt dat circa de helft van de besturen nog bijkomende maatregelen kan treffen om serverruimtes beter te beveiligen.
- ✓ Als je fysiek aan ICT-apparatuur kan, is het nog veel makkelijker om problemen te veroorzaken.
- ✓ Uit een vragenlijst naar 1495 lokale medewerkers in kader van het Traject Ethisch Hacken geeft 38% aan dat ze gevoelige informatie al eens in de papiermand gooien zonder te versnipperen.

Mythe: “Je kan je niet voorbereiden op een cyberaanval”

- ✓ Heel wat lokale besturen beseffen dat ze ooit het slachtoffer kunnen worden van een cyberaanval, maar het is niet altijd duidelijk welke voorbereidingen getroffen kunnen worden om het schip recht te houden.
- ✓ Plannen die een aanpak en richtlijnen vooropstellen vragen tijd en werk en op het eerste zicht lijkt het nut soms beperkt.

Realiteit

- ✓ Preventieve maatregelen zijn van belang om cybercrime zoveel mogelijk te voorkomen, maar er zijn ook stappen die je als lokaal bestuur kan zetten om snel actie te ondernemen in crisissituaties.
- ✓ De opmaak van een crisiscommunicatieplan kan helpen om tijdig en correct te communiceren over een mogelijk incident. Kant-en-klare instructiefiches kunnen interne communicatie faciliteren.
- ✓ Een overzicht van relevante interne en externe contactpersonen bij IT-gerelateerde incidenten met bijhorende contactgegevens kan een waardevol instrument zijn.
- ✓ Over logistieke aspecten is vaak onvoldoende nagedacht, denk hierbij aan de uitwijklocatie, oprichting van loketten, benodigdheden, …

Mythe: “Bedrijfscontinuïteit? We hebben al een rampenplan en back-ups.”

- ✓ Soms gaat men er te snel van uit dat men de nodige voorbereidingen heeft genomen om de dienstverlening te kunnen garanderen in tijden van nood.
- ✓ In rampenplannen wordt echter vaak geen luik IT voorzien en ook voor de inzet van back-ups dienen de nodige voorzorgen genomen te worden.

Realiteit

- ✓ Uit het Traject Ethisch Hacken en de recente ICT-veiligheidsaudits blijkt dat slechts een beperkt aantal lokale besturen beschikt over een business continuïteitstrategie en -plan om de dienstverlening snel en efficiënt opnieuw op te starten na een cyberaanval.
- ✓ De back-ups of de toestellen waarop deze opgeslagen staan, zijn soms onvoldoende beschermd. Het testen van back-ups blijkt eerder de uitzondering dan de regel.
- ✓ Een volledig uitgewerkt back-up of herstelplan om zo snel mogelijk beroep te kunnen doen op data en systemen ontbreekt bij 1 op 4 gemeenten.

Poll: Denk je dat je kan terugvallen op je leverancier wanneer een cyberaanval zich voordoet?

- ✓ Ja
- ✓ Nee
- ✓ Deels
- ✓ Geen leverancier voor cyberincidenten

Mythe: “Bij problemen hebben we onze toeleveranciers.”

- ✓ Veel lokale besturen doen beroep op de expertise van externe partners voor cyberveiligheid en IT-infrastructuur. Het gros van de verantwoordelijkheden wordt dan ook vaak bij hen gelegd.
- ✓ Wanneer de samenwerking met de toeleverancier vlot en gemoedelijk loopt, lijkt het niet altijd nodig om na te kijken of zij hun beloftes waarmaken en hun verantwoordelijkheden opnemen.

Realiteit

- ✓ Een goede samenwerking met externe partners kan een waardevolle meerwaarde zijn, maar dit vraagt om **duidelijke afspraken** en **voldoende monitoring**:
- ✓ De thema-audit Informatieveiligheid 2020 leert dat bepaalde formele contracten niet aanwezig zijn bij diverse lokale besturen. Wanneer dit wel het geval is, zijn ze vaak niet actueel.
- ✓ Ook blijkt dat concrete afspraken vaak ontbreken voor de samenwerking rond beheer en opvolging van zaken als licenties, configuraties, storingen, logging, …
- ✓ Uit het Traject Ethisch Hacken blijkt dat slechts een kwart van de lokale besturen toeziet op de naleving van Service Level Agreements.
- ✓ In welke mate is je lokaal bestuur prioritair wanneer er meerdere slachtoffers zijn? Beschikken leveranciers de nodige informatie om optimaal bijstand te kunnen verlenen?

Project cyberveilige gemeenten

Als lokaal bestuur kan je beroep doen op enkele interessante diensten en tools.

Project Cyberveilige Gemeenten

Naar aanleiding van de cyberaanval in Willebroek besloot de Vlaamse Overheid om 2,18 miljoen euro te investeren in de cyberveiligheid van lokale besturen op voorstel van **minister Bart Somers**.

Samen met het **Agentschap Binnenlands Bestuur**, **Audit Vlaanderen**, **het Facilitair Bedrijf** en VVSG werd een aanbod uitgewerkt voor lokale besturen:

1. ICT-veiligheidsaudits met cofinanciering via Audit Vlaanderen
2. De ontwikkeling van een Cyber Security Toolkit
3. Een Traject Ethisch Hacken in samenwerking met Howest

Poll: Heeft je bestuur de afgelopen 2 jaar inspanningen geleverd om de informatiebeveiliging te verbeteren?

- ✓ Informatie- of ICT-veiligheidsaudit
- ✓ Traject Ethisch Hacken
- ✓ Audit in combinatie met Ethisch Hacken
- ✓ Andere testen of maatregelen
- ✓ Geen concrete inspanningen

ICT-veiligheidsaudits met cofinanciering

Wat zit in het aanbod?

- ✓ **Basisaudit:** 6 auditdagen waarvan 1 dag consultancy, 2/3e cofinanciering voor elk lokaal bestuur.
- ✓ **Optionele aanvullende audit:** auditdagen en controleprogramma vrij te bepalen, 50% cofinanciering.

Waar uit bestaat de basisaudit?

- ✓ Interne en externe penetratietesten op min. 3 systemen
- ✓ Controle op het gebruik van zwakke wachtwoorden
- ✓ Controle op toegangen en rechten
- ✓ Nazicht op basis van documenten
- ✓ Consultancy op maat in functie van de noden/vragen van het bestuur

ICT-veiligheidsaudits met cofinanciering

Optionele aanvullende auditwerkzaamheden

- ✓ Technische ondersteuning bij oplossen kwetsbaarheden
- ✓ Advies over het oplossen van kwetsbaarheden
- ✓ Advies over verdere ontwikkeling/uitbouw van de ICT-systemen en ICT-omgeving
- ✓ Begeleiding bij de opmaak van een bedrijfscontinuïteitsplan
- ✓ Workshop simulatie van een cyberaanval :
  - ✓ Simulatie-oefening cyber aanval en de gevolgen daarvan op de organisatie
  - ✓ Te ondernemen stappen tot herneming normale werking, prioritering processen, …
  - ✓ Betrokkenheid : ICT-medewerkers, management, politieke niveau, veiligheidscoördinator, DPO, …
- ✓ …

Toolkit cyber security

In 2021 werkt VVSG samen met een taskforce van lokale besturen aan sjablonen, checklists en plannen voor steden en gemeenten:

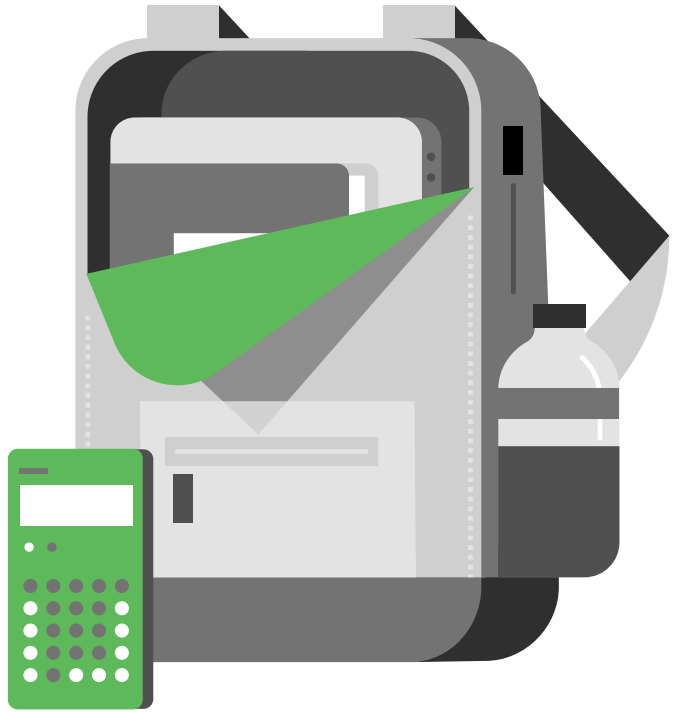
- ✓ **Business Continuïteitsplan**
- ✓ **Crisiscommunicatieplan**
- ✓ Informatieveiligheidsplan
- ✓ Richtlijnen voor secure software development
- ✓ Sjabloon voor gecoördineerde bekendmaking
- ✓ Nieuw sensibiliseringsmateriaal
- ✓ …

Traject ethisch hacken

- ✓ In 2020 kregen reeds 60 steden en gemeenten ethische hackers van de Howest-hogeschool over de vloer, die in kader van hun opleiding de lokale IT-systemen en toepassingen onder de loep nemen en aanbevelingen formuleren.
- ✓ Momenteel wordt een herhaling van het traject voorbereid die dit najaar zal doorgaan. Zodra hier meer info over is wordt dit gecommuniceerd via de VVSG-website en nieuwsbrief.
- ✓ Wie interesse heeft kan dit al aangeven via cyberveiligheid@vvsg.be. Bij de lancering van de oproep krijgen deze lokale besturen een direct mail.
- ✓ Op de pagina van het project kan je terecht voor meer informatie bij de Cyber Security Toolkit en het Traject Ethisch Hacken 2021.

Wat leren we hier uit?

Enkele globale inzichten



Nog een weg te gaan

- ✓ In haast alle besturen is nog werk aan de winkel om de organisatie zo goed als mogelijk te beschermen tegen cyberaanvallen en andere IT-gerelateerde incidenten.
- ✓ Uit de gemiddelde resultaten van de Informatieveiligheidsaudits blijkt dat de vooruitgang op twee jaar tijd beperkt is.
- ✓ Vaak gaat het over **haalbare maatregelen** en **reeds gekende pijnpunten**.

		Gem. 2020	Gem. 2017-2018
	Organisatiebeheersing	1,5	1,8
Persoons-gegevens	AVG-basisverplichtingen	2,8	-
Persoons-gegevens	AVG-paraatheid	2	-
Gevoelige en vertrouwelijke gegevens	Informatiebeveiligingbeheersstructuren	1,8	1,9
Gevoelige en vertrouwelijke gegevens	Rollen en verantwoordelijkheden doorheen de organisatie	2	1,9
Gevoelige en vertrouwelijke gegevens	Leveranciersrelaties	1,2	1,0
Gevoelige en vertrouwelijke gegevens	Actualisatie van systemen	1,2	1,6
Gevoelige en vertrouwelijke gegevens	Technische beschermingsmaatregelen	1,2	1,2
Gevoelige en vertrouwelijke gegevens	Toegangen en rechten	1	1,4
	Continuïteit	2	2,2

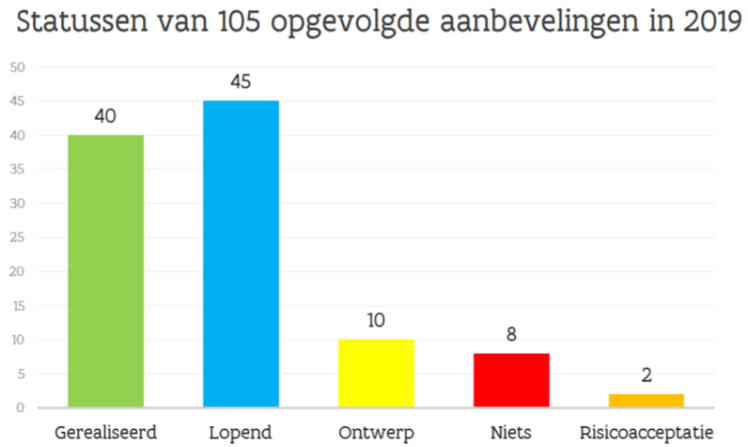
Poll: “Inspanningen rond informatie- en cyberveiligheid renderen.”

- ✓ Helemaal akkoord
- ✓ Akkoord
- ✓ Neutraal
- ✓ Niet akkoord
- ✓ Helemaal niet akkoord

Inspanning loont

- ✓ Een aantal bevindingen uit de thema-audit informatieveiligheid 2018 werden opnieuw getest en de hoge risico's bleken in 53% van de gevallen al volledig weggewerkt.
- ✓ Eerder geauditeerde lokale besturen die aan de slag gaan, boeken effectief vooruitgang, maar het vergt een volgehouden inspanning.

Hoge veiligheidsrisico's	Volledig geremedieerd	Deels geremedieerd	Niet geremedieerd
Configuraties	20	2	6
Beveiligingsupdates	9	4	8
Wachtwoordbeleid	8	9	4
	37	15	18
	53%	**21%**	**26%**



Poll: Werkt je stad of gemeente samen met andere lokale besturen rond ICT?

- ✓ **Ja:** gezamenlijke projecten
- ✓ **Ja:** kennisdeling
- ✓ **Ja:** gezamenlijke aankopen
- ✓ Ja: wederzijdse uitwisseling van ICT-experten
- ✓ **Neen:** weinig tot geen samenwerking

In hetzelfde schuitje

- ✓ De resultaten uit het traject ethisch hacken 2020 laten duidelijk zien dat alle types besturen, van klein tot middelgroot en groot, vatbaar zijn voor courante kwetsbaarheden.
- ✓ De bevindingen van de Howest-hackers bevestigen ook aangehaalde werkpunten uit de eerdere thema-audits informatiebeveiliging, zoals het actualiseren van systemen en toepassingen, het opmaken van een plan voor business continuïteit en leveranciersrelaties.
- ✓ De winsten zijn gekend en gelden voor het merendeel van lokale besturen: aan **mogelijkheden tot samenwerking** dus geen gebrek.

Wat neem ik mee?

Van resultaten naar concrete acties.

Wat neem ik mee?

1. **Ook jouw lokaal bestuur loopt risico:** bijkomende stappen zijn geen overbodige luxe

2. **Heel wat haalbare beveiligingsmaatregelen worden onderbenut:** sterk wachtwoordbeleid, rollen voor het up-to-date houden van systemen en toepassingen, encryptie, MFA, …

3. **Toegangen en rechten verdienen evenveel aandacht als rollen en verantwoordelijkheden:** doordacht maatwerk bij elke personeelsbeweging kan worden gecombineerd met goede afspraken voor in geval van nood en aangepast monitoring

4. **Cyberveiligheid is een verantwoordelijkheid van iedereen:** betrek alle diensten en definieer duidelijke rollen en verantwoordelijkheden

Wat neem ik mee?

5. **Ook een open huis heeft nood aan fysieke beveiliging:** IT-beveiliging is belangrijk, maar ook een clean desk policy en afgesloten archiefruimtes hebben impact.

6. **Je kan nu al maatregelen nemen om klaar te staan bij een cyberaanval:** maak de nodige plannen op en denk na hoe je organisatie zich zal organiseren in tijden van nood.

7. **Bedrijfscontinuïteit is meer dan back-ups en rampenplannen:** maak werk van een business continuïteitsstrategie en -plan en ga strategisch om met back-ups

8. **Een goede leverancier is waardevol, maar vaak geen garantie voor succes:** maak afspraken, leg deze formeel vast en voorzie in reguliere monitoring

Meer dan IT

- ✓ Cyberveiligheid is te groot en te belangrijk om het alleen bij de IT-dienst te leggen.
- ✓ Op strategisch- en directieniveau worden al heel wat belangrijke keuzes gemaakt met een grote impact op IT, zoals prioriteiten en investeringen.
- ✓ De stappen die je als lokaal bestuur kan zetten gaan verder dan technologie.
- ✓ **Kortom:** zowat elke dienst en medewerker heeft een rol te spelen…

    - ✓ **HR:** Indiensttreding, uittreding, arbeidsreglement, …
    - ✓ **Communicatie:** Sensibilisering, aankoop informatie- en communicatietools
    - ✓ **Baliemedewerkers:** Fysieke beveiliging
    - ✓ **Noodplanning:** Uitwerking draaiboek
    - ✓ **Algemene medewerkers:** Goede cyberhygiëne, problemen signaleren

Vragenronde

- ✓ Stel je vragen via de chat.
- ✓ Vermeld je naam en lokaal bestuur.

Reeks Privacy & Persoonsgegevens

[Bestellen via politeia.be](#)

Ook beschikbaar in extenso

Bekijk de openingssessie

Dank dat je erbij was!

Via e-mail ontvang je deze week een **evaluatiemail** met de **presentatie** van dit webinar.