standpunt

Cyberveilige gemeenten

vvsg

Er gebeuren vandaag reeds een heel aantal waardevolle acties die voornamelijk sensibiliserend werken rond de thematiek van cyberveiligheid bij de lokale besturen of die de problematiek in kaart brengen. We zijn inmiddels op een punt gekomen dat de problemen gekend zijn. Er is nu nood aan een actieplan om deze problemen aan te pakken. De lokale besturen hebben hier zelf een belangrijke verantwoordelijkheid maar ook van de centrale overheid verwachten we de nodige impulsen en ondersteuning om de lokale besturen hierbij te ondersteunen.

Inhoud

1. Het belang van cyberveiligheid voor de lokale besturen

De VVSG visienota ‘naar een volwaardige digitale transformatie van het lokaal bestuur’ definieert veilige digitale infrastructuur en open toepassingen als één van de belangrijke deelaspecten of bouwstenen. Veilige digitale infrastructuur en informatiebeveiliging zijn immers cruciale elementen in deze digitale wereld, ook voor de lokale besturen.

De voorbije maanden hebben lokale besturen omwille van de aanhoudende coronacrisis een digitale versnelling hoger geschakeld. Er wordt massaal van thuis uit gewerkt, vergaderd, digitale dienstverlening aangeboden,… Een cyberveilige infrastructuur is hierbij meer dan ooit een noodzaak gebleken. Gedurende de coronaperiode werd immers een duidelijke toename opgemerkt in cybercriminaliteit, met diverse dreigingen zoals phishing, social engineering, ransomware en datalekken.

De Vlaamse lokale besturen zijn, net zoals andere publieke en private instanties, hiertegen niet immuun. Uit een bevraging die wij deden bij een beperkte steekproef van 42 lokale besturen in het najaar van 2021 is gebleken dat 14 lokale besturen reeds in aanraking kwamen met een vorm van cybercriminaliteit. Sommige cyberaanvallen haalden het nieuws in de afgelopen jaren, denk maar aan de cyberaanvallen in 2020 in de gemeenten Willebroek en Dilbeek en het recente cyberincident in de gemeente Hoeilaart. Maar er zijn evengoed cyberincidenten die onder de radar blijven, zij het door gevoelens van schaamte of angst voor juridische of andere implicaties.

Om de continuïteit van de dienstverlening aan de burger te verzekeren en om de veiligheid van de dossiers en persoonsgegevens die de lokale besturen verwerken te garanderen, is het essentieel dat er blijvend werk gemaakt wordt van een cyberveilige omgeving. De inspanningen voor cyberveilige gemeenten zijn ook nodig om het vertrouwen van de burger in de (lokale) overheid te behouden. Bovendien zijn cyberveilige gemeenten ook van belang voor de nationale veiligheid. In de huidige geopolitieke situatie wordt dit steeds belangrijker.

Ons volledig beschermen tegen cybercriminaliteit is onmogelijk. De toenemende risico’s op vlak van cyberveiligheid zijn inherent aan de digitale transformatie van onze samenleving. Hackers zijn steeds talrijker en worden vernuftiger. We kunnen niet vermijden dat hackers pogingen ondernemen om binnen te breken bij de lokale overheden. We moeten er wel alles aan doen om het risico zoveel als mogelijk te beperken en ook zorgen dat we klaar staan zodat, wanneer we in aanraking komen met cybercriminaliteit, we snel en adequaat hierop reageren.

2. Wat gebeurt er vandaag?

Project cyberveilige gemeenten van de VVSG

In april 2020 is de VVSG gestart met het project ‘Cyberveilige gemeenten’ in samenwerking met het Agentschap Binnenlands Bestuur, Audit Vlaanderen en Digitaal Vlaanderen. Dit project, dat op financiële ondersteuning kon rekenen van Bart Somers, de Vlaams minister van Binnenlands bestuur, Bestuurszaken, Inburgering en gelijke kansen omvat drie afgelijnde sporen:

- De ontwikkeling van een digitale toolkit cyberveiligheid op maat van lokale besturen
- De opstart van een traject met hogeschoolstudenten die als ethische hackers ingeschakeld kunnen worden voor een audit bij lokale besturen
- Het informeren en sensibiliseren van lokale besturen over cyberveiligheid door de organisatie van een sessie op de Trefdag, studiedag en een jaarlijkse inspiratiesessie

De drie verschillende sporen trachten elk bij te dragen aan de cybermaturiteit van steden en gemeentenen spelen in op concrete ondersteuningsnoden.

Zo tracht de digitale toolkit cyberveiligheid lokale besturen te helpen om de nodige voorbereidingen te treffen om cybercriminaliteit te voorkomen en bestrijden door hen relevante sjablonen, leidraden en materialen aan te reiken, waarmee ze eigenhandig aan de slag kunnen gaan. Het gaat hierbij over plannen als een business continuïteitsplan en crisiscommunicatieplan, handvatten zoals de richtlijnen voor veilige softwareontwikkeling en een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden en hands-on instrumenten als een incidentenregister. Door zelf op voorhand na te denken over de aanpak rond cyberveiligheid en de nodige instrumenten te voorzien om stappen vooruit te zetten, kunnen lokale besturen het werk van cybercriminelen immers aanzienlijk bemoeilijken. De digitale toolkit cyberveiligheid speelt in op deze nood en tracht zo de zelfredzaamheid van lokale besturen te verhogen.

Het tweede spoor omvat een samenwerking tussen de VVSG en HOWEST, waarbij studenten Cyber Security Professional van de hogeschool hun theorie uit de leslokalen toepassen op een concrete setting: de IT-omgeving van lokale besturen. Gedurende enkele dagen gaan de studenten fysiek en virtueel langs bij lokale besturen, om via diverse cyberveiligheidstesten te kijken welke zwakke plekken mogelijk misbruikt kunnen worden door particulieren en organisaties met een kwaadwillig oogmerk. De deelnemende besturen ontvangen op het einde van de rit een rapport met gevonden kwetsbaarheden en aanbevelingen om deze aan te pakken. Via deze weg krijgen lokale besturen kosteloos inzage in mogelijke werkpunten en kunnen ze hun beleid verder scherpstellen.

Tenslotte tracht het Project Cyberveilige Gemeenten ook in te spelen op de nood aan algemene bewustmaking met betrekking tot het thema cyberveiligheid. Via fysieke en online sessies kunnen lokale besturen bijleren over preventieve maatregelen, maar komen ze ook in aanraking met de risico's die cyberveiligheid met zich meebrengt voor lokale overheden. Vaak is de mens nog steeds de zwakste schakel wanneer het aankomt op cybercriminaliteit, bewustmaking is dan ook onontbeerlijk om lokale besturen weerbaar te maken tegen de groeiende dreiging van malware, ransomeware en andere relevante cyberdreigingen.

De VVSG is verheugd dat dit project inmiddels met twee jaar werd verlengd. Het vervolgtraject zal verder bouwen op het werk dat reeds gebeurde en zal concreet volgende luiken bevatten:

- Verspreiding, actualisatie en uitbreiding van de digitale toolkit cyberveilige gemeenten: In het vervolgtraject zal de bovenvermelde toolkit verder bekendgemaakt worden via interactieve webinars, artikels en een heuse communicatie- en sensibiliseringscampagne. Daarnaast zullen de tools ook bijgewerkt en actueel gehouden worden, door nieuwe ontwikkelingen en ervaringen te capteren. Tenslotte zal de toolkit ook uitgebreid worden, onder andere via inspirerende testimonials.
- Verderzetting van het Traject Ethisch Hacken: Gezien de grote interesse bij lokale besturen, werd besloten om het Traject Ethisch Hacken in samenwerking met Howest verder te zetten in 2022 en 2023. Elk jaar zal een oproep gelanceerd worden via de verschillende VVSG-kanalen waarop lokale besturen kunnen ingaan.
- Kennisopbouw en bewustmaking: Aangezien sensibilisering een blijvend aandachtspunt blijft voor lokale besturen, zowel naar eindgebruikers als naar management, zullen sensibiliseringssessies uitgewerkt worden die ingaan op het belang van een goede cyberhygiëne, alsook op strategische keuzes. Naast deze bewustmakingssessies bouwen we ook een denktank uit die zich zal buigen over relevante beleidsvraagstukken, zoals de overgang naar cloudomgevingen.

Door lokale besturen handvatten aan te reiken om zelf aan de slag te gaan, hen te mogelijkheid te bieden om laagdrempelig zwakke plekken te identificeren en verder te sensibiliseren komt het project cyberveilige gemeenten tegemoet aan enkele belangrijke noden die leven bij lokale besturen.

Audits Audit Vlaanderen met cofinanciering

Audit Vlaanderen evalueerde tussen eind 2016 en midden 2018 de maturiteit rond informatiebeveiliging bij een reeks lokale besturen. De audit werd in 2020 herhaald bij een beperktere groep lokale besturen. De resultaten waren allesbehalve rooskleurig. Lokale besturen struikelen nog vaak over gekende pijnpunten, zoals een gebrek aan afspraken en duidelijke rollen voor informatie- en cyberveiligheid, nalatigheid bij het uitvoeren van veiligheidsupdates en een ontoereikend beheer van toegangen en rechten. De resultaten bij de geauditeerde besturen in 2020 geven aan dat er nog geen sprake is van een fundamentele verbetering. Audit Vlaanderen stelde bovendien vast dat de uitdagingen op vlak van informatiebeveiliging en cyberveiligheid zo groot zijn dat geen enkel lokaal bestuur alle risico's daaromtrent zelfstandig kan beheersen.

In kader van het programma cyberveilige gemeenten besloot de Vlaamse overheid om naast het project met de digitale toolkit cyberveiligheid, samenwerking met ethische hackers en bewustmakingssessies, ook budget ter beschikking te stellen voor de cofinanciering van ICT-veiligheidsaudits via Audit Vlaanderen. Concreet kunnen lokale besturen ervoor kiezen om een basisaudit te laten uitvoeren in hun lokaal bestuur om op professionele wijze risico's en kwetsbaarheden te identificeren, met een dag consultancy om de gedetecteerde risico's te verhelpen. Daarnaast kunnen lokale besturen ook beroep doen op aanvullende auditwerkzaamheden, op maat van de noden die zij zelf zien. Het kan hierbij gaan over een cybercriminaliteitsoefening om de theorie over incident response in de praktijk te brengen, maar bijvoorbeeld ook over ondersteuning bij het opstellen van een degelijk business continuïteitsplan.

Bij de bestelling van een basisaudit is 2/3e cofinanciering voorzien door de Vlaamse overheid. Wanneer een lokaal bestuur ook beroep wil doen op een aanvullende audit na het laten uitvoeren van een basisaudit, kan men rekenen op 50% cofinanciering van de kostprijs. Ook in 2022 geldt dit aanbod voor de lokale besturen. Samen met het traject ethisch hacken in samenwerking met Howest helpen de ICT-veiligheidsaudits via Audit Vlaanderen om de huidige situatie in kaart te brengen en mogelijke verbeterpunten aan te duiden.

Lokale initiatieven – wat doen de lokale besturen?

Naast de initiatieven in kader van het Project Cyberveilige Gemeenten, nemen lokale besturen ook zelf een actieve rol op om hun cybermaturiteit op te krikken en het thema hoger op de lokale agenda te krijgen.

Eerst en vooral geven recente cijfers aan dat lokale besturen gretig gebruik maken van de ondersteuning waarop zij beroep kunnen doen. Zo hebben ondertussen al 125 gemeenten een basisaudit laten uitvoeren via Audit Vlaanderen en zullen tegen eind 2021 103 lokale besturen samengewerkt hebben met de ethische hackers van HOWEST. In totaal werden al ruimschoots de helft van de 300 lokale besturen bereikt met beide initiatieven. Er kan dus geen twijfel over bestaan dat lokale besturen hun verbeterpunten willen kennen, om zo de nodige stappen richting verbetering te zetten.

Naast het engagement van lokale besturen om actief aan de slag te gaan met lopende initiatieven, werken ze ook zelf acties en samenwerkingen uit om de cybermaturiteit op te krikken. De initiatieven zijn veelvuldig en al even veelzijdig. Zo sloegen Welzijnsregio Noord-Limburg, Welzijnszorg Kempen en de Intercommunale ontwikkelingsmaatschappij voor de Kempen bijvoorbeeld een actieplan voor sensibilisering in lokale besturen uit, met diverse campagnematerialen. Samenwerkingen worden ook onderzocht voor andere aspecten van cyberveiligheid, zoals lokale besturen die kijken met lokale politiezones hoe onderlinge hulpverlening bij cyberincidenten bewerkstelligd kan worden. Daarnaast trachten lokale besturen ook om de mogelijkheden van opkomende technologieën te onderzoeken en implementeren, zoals SIEM oplossingen (Security Information and Event Management), cloud technologie en software voor interactie phishing campagnes. De lokale besturen blijven ook bouwen aan een verdere professionalisering op het gebied van cyberveiligheid, door samenwerkingen te zoeken met betrouwbare externe partners, maar evenzeer door gebruik te maken van de Vlaamse Overheid, zoals het Vlaamse - en gebruikersbeheer (ACM-IDM).

Tenslotte zetten lokale besturen ook in op onderlinge kennisdeling, via diverse initiatieven en kanalen. Zo trachten lokale besturen elkaar op weg te helpen via adviesverlening binnen de Werkgroep Informatieveiligheid en het Kennisdelingsplatform Digitale Gemeenten van de VVSG, en andere initiatieven zoals de Quick Responsive Community van V-ICT-OR. De lokale besturen delen ook met plezier hun expertise en ervaringen tijdens digitale infosessies. Dit kan alleen maar aangemoedigd worden, aangezien cybercriminaliteit een te grote problematiek is om elk binnen hokjes te denken en te werken.

3. Wat moet er nog gebeuren?

Tot nu toe ligt de focus van de acties –naast de toolkit en de inspiratiesessiesvoornamelijk op het in kaart brengen van de problemen bij de lokale besturen. We zijn momenteel echter op een punt beland waarbij we moeten nadenken over concrete gezamenlijke acties die de veiligheid van de IT-systemen van de lokale besturen collectief kunnen opkrikken. Daarbij moeten ontzorging van lokale besturen en betere/meer samenwerking telkens de uitgangspunten zijn.

Wat vragen we aan de centrale overheden?

Informatiebeveiligingsdienst voor de lokale besturen

De lokale besturen zijn vandaag te vaak alleen op zichzelf aangewezen als het gaat over de implementatie van de verschillende aspecten van cyberveiligheid. Daarbij stellen we ook vast dat de budgetten die de lokale besturen hiervoor (kunnen) vrijmaken vandaag nog vaak ontoereikend zijn. Ook de aanwezige expertise en kennis binnen de lokale besturen is gemiddeld genomen te beperkt. Er is zeer veel winst te halen door een aantal zaken centraal te coördineren en faciliteren.

Onderzoek onder welke omstandigheden een informatiebeveiligingsdienst kan opgericht worden onder de vleugels van het nieuw op te richten ondersteuningscentrum voor de lokale besturen zoals beschreven in het relanceproject (VV071). Deze dienst moet in de eerste plaats een responsteam bevatten dat meteen in actie kan schieten wanneer er zich een hack voordoet bij een lokaal bestuur. Vergelijk het met het federale Computer Emergency Response Team (CERT) maar dan specifiek voor de lokale besturen. Daarnaast moet de dienst de lokale besturen verder ondersteunen door het opstellen van goede modeldocumenten, standaarden, instrumenten en sjablonen. De dienst faciliteert kennisdeling tussen gemeenten onderling, met andere overheidsniveaus, met cruciale sectoren en dienstenleveranciers van de lokale besturen. De dienst organiseert daarnaast ook vormingen zowel voor de experts binnen als voor het bredere publiek binnen het bestuur. We hoeven hiervoor zeker zelf het warm water niet opnieuw uit te vinden maar kunnen inspiratie halen bij de beveiligingsdienst voor lokale besturen in Nederland.

Verbetertraject – begeleiding op maat cf. aanbod Crevits voor KMO’s

Uit de bevraging die wij deden bij enkele lokale besturen is gebleken dat er veel vraag is naar begeleiding en ondersteuning op maat. Dat is niet verwonderlijk. In een gemiddeld lokaal bestuur is er geen doorgedreven gespecialiseerde expertise aanwezig m.b.t. cyberveiligheid en is externe begeleiding van een gespecialiseerd bureau noodzakelijk.

We verwezen eerder al naar het aanbod van minister Somers voor de cofinanciering van audits (waarbij beperkt ook 1 dag consultancy is voorzien). Naar analogie met de cybersecurity verbetertrajecten voor KMO's van het Agentschap Innoveren en ondernemen, zou een gelijkaardig aanbod met cofinanciering voor de lokale besturen echter ook aangewezen zijn. Tijdens zo'n traject helpt één van de negen erkende dienstverleners de beveiliging van de ondernemers verbeteren. De KMO's kunnen beroep doen op cofinanciering voor het inkopen van extern advies en begeleiding om de uitdagingen rond cyberveiligheid aan te pakken en kiest zelf met welke aanbieder ze hiervoor samenwerken. Interessant aan deze formule is ook dat de beperkte groep van dienstverleners waarop beroep wordt gedaan op die manier ook expertise opbouwen bij de lokale besturen die zij kunnen inzetten bij de andere lokale besturen. We vragen dan ook om de mogelijkheid te onderzoeken om een gelijkaardig aanbod te voorzien voor de Vlaamse lokale besturen.

Strategie implementatie veiligheidsbouwstenen

We vragen om, samen met Digitaal Vlaanderen, werk te maken van een strategie om de veiligheidsbouwstenen van de Vlaamse overheid versneld te implementeren bij de lokale besturen. Zeker de implementatie van bouwstenen zoals het Vlaams toegangs- en gebruikersbeheer kunnen voor snelle toegevoegde waarden zorgen omdat deze de veilige toegang tot systemen garandeert en louter toegang via wachtwoord uitsluit. Een degelijke toegangsbeveiliging is immers cruciaal om onrechtmatige toegang tot (gevoelige) informatie te voorkomen. Zo worden toegangs- en gebruikersrechten telkens best beperkt tot wat nodig is voor het normale functioneren van de gebruiker. Daarnaast vragen we ook om te onderzoeken welke bijkomende veiligheidsbouwstenen de centrale overheden moeten ontwikkelen.

Standaardiseren en centraliseren van de IT-omgeving

Vandaag beheren nog heel wat lokale besturen hun volledige IT-omgeving (of grote delen daarvan) zelf. De complexiteit van de actuele ICT systemen stelt zeer hoge eisen op vlak van kennis en vaardigheden die betrekking hebben op alle domeinen, van ontwikkeling tot operations. Het is voor een gemiddeld bestuur onmogelijk om deze kennis in huis te halen of in te huren. Gezien de zeer beperkte schaal waarop de lokale besturen gemiddeld genomen werken, is het aangewezen om niet-kerntaken af te stoten. Lokale besturen moeten op dat vlak ontzorgd worden door deze taken in te kopen als (cloud)diensten. Door op een doordachte manier over te stappen op (cloud)diensten kunnen we de verantwoordelijkheden rond beveiliging (denk aan back-up's, updaten van (software)systemen, firewalls, …) meer bij derden leggen. Niet alleen op vlak van de hardware, maar ook op vlak software moet de cloud (Software-as-a-Service) de standaard worden. We vragen daarom om, samen met de lokale besturen, te onderzoeken hoe we hun IT-systemen en infrastructuur verder kunnen centraliseren en standaardiseren.

Lokale vertaalslag van minimale vereisten

We vragen om te onderzoeken in welke mate de Vlaamse overheid minimale vereisten kan opleggen aan de lokale besturen en de mate waarin dit wenselijk is. Het gaat hier over minimale vereisten waaraan systemen en processen moeten voldoen om zo een minmale graad van kwaliteit en veiligheid te bereiken. Er zijn op vandaag al aanbevelingen van deze aard, zoals het informatieclassificatieraamwerk. Hier gaat het echter ook over vrijblijvende tips en inspiratie, terwijl de centrale overheid wel verder zou kunnen gaan hierin.

Wat vragen we aan de lokale besturen?

Bijkomende ondersteuning voor lokale besturen om hun cybermaturiteit op te krikken is allesbehalve een overbodige luxe, ook cybercriminelen blijven zich professionaliseren. Zelf kunnen lokale besturen ook reeds merkbare vooruitgang boeken.

Benutten van de ontwikkelde tools

Eerst en vooral roepen we de lokale besturen op om aan de slag te gaan met de materialen die ontwikkeld werden binnen de digitale toolkit cyberveiligheidom hun aanpak voor cyberpreventie en incidentbestrijding scherp te stellen. De thema-audits door Audit Vlaanderen wezen bijvoorbeeld al meermaals uit dat slechts een beperkt aantal lokale besturen beschikt over een uitgewerkt business continuïteitsplan om de kritieke dienstverlening terug op te starten na een cyberaanval. Het sjabloon in de digitale toolkit cyberveiligheid kan hen hierbij op weg helpen. De richtlijnen voor secure software development kunnen dan weer gebruikt worden om software veilige te (laten) ontwikkelen, volgens een logisch en behapbaar proces. De toolkit cyberveiligheid bevat ook een aantal instrumenten die meteen inzetbaar zijn, zoals het register voor cyberincidenten en de checklist crisisbeheer. Door de aanpak vast te leggen in plannen en instrumenten zijn lokale besturen beter voorbereid op de diverse vraagstukken en processen die cyberveiligheid met zich meebrengt.

Testen in de praktijk

Het uitwerken van concrete plannen en instrumenten is een belangrijke eerste stap, maar nog te weinig worden deze ook getest en ingeoefend. Zo werd zowel tijdens de themaaudits door Audit Vlaanderen en het Traject Ethisch Hacken vastgesteld dat lokale besturen wel over back-ups beschikken om de digitale dienstverlening herop te starten in de nasleep van een incident, maar dat slechts een beperkt aantal lokale besturen de back-upstrategie ook in de praktijk brengt met een simulatie of test. Dit brengt menig risico met zich mee, aangezien een plan maar kan uitgroeien tot een gecontroleerd proces door er ook actief mee aan de slag te gaan. Enkele besturen hebben reeds een business continuïteitsoefening uitgevoerd, of plannen dit te doen, maar dit aantal is beperkt en er is dus nog ruimte voor verbetering.

Detecteren van kwetsbaarheden

Daarnaast is het ook aangewezen dat lokale besturen op reguliere basis kwetsbaarheden binnen de IT-omgeving in kaart brengen. De ICT-veiligheidsaudits via Audit Vlaanderen en het Traject Ethisch Hacken bieden de mogelijkheid om dit aan een betaalbare prijs of zelfs kosteloos te doen. Door deel te nemen aan een van deze ondersteunende initiatieven gaat de cybermaturiteit niet vanaf dag 1 naar omhoog, maar door de pijnpunten te leren kennen,

kunnen lokale besturen efficiënter en gerichter bouwen aan een cyberveilige IT-omgeving en werking. Het staat lokale besturen natuurlijk ook vrij om buiten deze initiatieven om scans en testen te laten uitvoeren, zolang de nodige stappen maar gezet worden om de huidige situatie zichtbaar te maken en hierrond oplossingen te formuleren.

Erkennen van belang en blijvend investeren

Verder is het ook aangewezen dat lokale besturen zelf blijvend investeren in cyberveiligheid. Het gaat hierbij zowel over het investeren van de nodige middelen in technische maatregelen die de cyberveiligheid verhogen, als het hoger op de agenda krijgen van deze snelgroeiende thematiek en investeren in vormingen. Wat investeringen in technische oplossingen betreft moeten lokale besturen overigens het warm water niet heruitvinden. Een voorbeeld van zo'n technische maatregel is de multifactorauthentifcatie. Auditorganisaties en expertisecentra zoals het Centre for Cyber Security Belgium (CCB) hameren al langer op de positieve impact die multifactorauthenticatie kan hebben en er zijn reeds diverse programma's voor versleuteling die het mogelijk maken om documenten veilig te delen met externen.

Naast de noodzaak om middelen te investeren blijkt uit auditresultaten en gesprekken met medewerkers die lokaal instaan voor cyberveiligheid dat er ook nog werk aan de winkel is om het thema hoger op de bestuurlijke agenda te krijgen. De resultaten van een cyberveilige IT-omgeving en werking zijn minder zichtbaar en lijken hierdoor minder prioritair te zijn prioritair burgers en inwoners maar dat verandert al snel wanneer een lokaal bestuur geconfronteerd wordt met datalekken of het uitvallen van cruciale dienstverlening ten gevolge van cybercriminaliteit. Het is belangrijk dat de lokale mandatarissen en het management het thema actief mee opvolgen en in gesprek gaan met DPO's en IT-medewerkers om quick wins en actiepunten te identificeren. Cyberveiligheid is bij momenten een erg technische en complexe thematiek maar dit mag geen drempel vormen wanneer essentiële dienstverlening en gevoelige gegevens risico lopen. Het moet hier overigens gaan over een aangehouden engagement, aangezien de digitale wereld aan een razendsnel tempo evolueert en elke dag wel nieuwe dreigingen opduiken.

Definiëren van rollen en verantwoordelijkheden

Er zijn hoe dan ook nog verschillende oplossingen binnen het handbereik van steden en gemeenten om zich te wapenen tegen cybercriminelen. Zo kan de werking verder geprofessionaliseerd worden door in te zetten op een duidelijke rolverdeling voor cyberveiligheid en incidentbestrijding. Wie staat in voor het uitvoeren van veiligheidsupdates? Welke profielen moeten aanwezig zijn binnen een incident response team mocht het lokaal bestuur geconfronteerd worden met een omvangrijk cyberincident? Wie kan toegangen en rechten toekennen voor systemen en toepassingen en wie zorgt ervoor dat deze ook weer ingetrokken worden wanneer ze niet langer nodig zijn, bijvoorbeeld door uitdiensttreding? Door keuzes te maken met betrekking tot de invulling van de IT-functie en andere interne rollen, wordt het mogelijk om informatie- en cyberbeveiliging meer structureel in te bedden.

Implementeren van ICT - bouwstenen

Lokale besturen kunnen de IT-omgeving ook eenvoudig versterken door de ICTbouwstenen van de Vlaamse overheid te implementeren. De adaptatie van deze betrouwbare technische oplossingen zorgt er immers voor dat een aantal relevante aanbevelingen met betrekking tot versleuteling, toegang- en rechtenbeheer en veilig gegevensverkeer invulling krijgen.

Samenwerken

Tenslotte is ook een belangrijk rol weggelegd voor samenwerking. In het auditrapport in kader van de thema-audits informatieveiligheid onderstreepte Audit Vlaanderen de nood om samenwerking op te zoeken als lokaal bestuur: “Verschillende van de uitdagingen rond informatiebeveiliging zijn zo groot en complex dat geen enkel geauditeerd lokaal bestuur alle risico’s daaromtrent zelfstandig kan beheersen. Naast de individuele inspanningen is daarom ook meer samenwerking een belangrijk element om als bestuur voldoende garanties te kunnen bieden omtrent informatiebeveiliging.” Door samenwerking op te zoeken met collega-besturen in kader van expertisedeling en het uitwerken van gedeelde oplossingen, kunnen de vele uitdagingen die cybercriminaliteit met zich meebrengt sneller en beter beantwoord worden. Dit geldt zeker voor kleinere besturen, met een beperkte interne IT-capaciteit en sterke afhankelijkheid van toeleveranciers. De lokale besturen kunnen alvast rekenen op de VVSG en haar kanalen om met andere leden over het onderwerp in gesprek te treden en vragen en kennis met elkaar te delen.

vvsg

Over VVSG

De Vereniging van Vlaamse Steden en Gemeenten vzw is het steunpunt, de belangenbehartiger en de beweging van het lokale bestuur. Alle 300 gemeenten en OCMW's in Vlaanderen zijn lid, naast vele politiezones en intergemeentelijke samenwerkingsverbanden. Een huis van vertrouwen dat haar leden advies en begeleiding verleent, informatie geeft op maat, zorgt voor opleiding en vorming, ontmoetingsdagen organiseert en andere ondersteunende diensten biedt. Meer dan 10.000 politici of ambtenaren volgen elk jaar een studiedag of een opleiding bij de VVSG.

VVSG vzw • Bischoffsheimlaan 1-8 • 1000 Brussel • T +32 2 211 55 00
info@vvsg.be • www.vvsg.be