Veiligheidsconferentie 05/10/2021

Cyberveiligheid: uw rol als lokaal bestuur en politie

Slotbeschouwingen – Cathy Berx

Dames en heren,

Wat een dag! Er zijn van die momenten dat een mens overal tegelijk wil zijn en alles wil horen en zien. Dat was vandaag niet anders! We hebben alleszins veel bijgeleerd.

Na de slotbeschouwingen van Miguel De Bruycker, directeur van het Centrum voor Cybersecurity België (CCB) blik ik graag even terug op het rijke programma dat wij vandaag samen beleefden.

Fenomenen als cyberveiligheid en cybercriminaliteit tellen bijzonder veel facetten. Het is schier onmogelijk om ze allemaal te belichten.

Daarom kozen we een aantal hoofdlijnen rekening houdend met u, gewaardeerde deelnemers en partners.

Het **project van Vlaams viceminister-president Bart Somers** voor de **informatiebeveiliging en cyberveiligheid van de lokale besturen** zal zijn meerwaarde bewijzen.

Dit nuttige initiatief geeft de lokale besturen toegang tot een toolkit, tot de inzet van ethische hackers en een audit om het maturiteitsniveau van de organisatie, haar werkprocessen en informatiestromen te bepalen. Het is een voorbeeld van hoe de Vlaamse overheid in samenwerking met de Vereniging van Vlaamse Steden en Gemeenten (VVSG) de lokale besturen daadwerkelijk en op maat kan ondersteunen in deze complexe materie. Het zal de bestaande lokale inspanningen met behulp van de data protection officers of DPO's verder versterken.

Cedric De Vroey schetste in zijn bijdrage hoe **ethische hackers** overheden en bedrijven ondersteunen om zich te beschermen in een steeds complexere digitale wereld. Dankzij het door het Centrum voor Cybersecurity België (CCB) ontwikkelde kader rond 'ethical disclosure' kan men de kwetsbaarheden in de controlesystemen, zoals firewalls en toegangscontrole opsporen. Het laat toe om de eerste verdedigingslinie tegen hackers met minder fraaie bedoelingen te testen en zo nodig te verbeteren.

De informatiebeveiliging en cyberveiligheid is een belangrijke uitdaging voor de lokale besturen. Burgers vertrouwen er immers op dat overheden informatie op een professionele wijze beschermen, ook al schrikken ze er niet voor terug om zelf hun intiemste zielenroerselen te delen via de sociale media…

Lokale besturen moeten trouwens niet enkel hun data, informatie en reputatie beschermen…Ook de **continuïteit van hun dienstverlening** en **andere kritieke infrastructuur** vereist hun continue aandacht.

De getuigenissen van burgemeester Eddy Bevers en noodplanningscoördinator Steven Vermeeren verruimden onze kennis over deze opdracht. Ze stonden stil bij de oorzaak van een cyberincident, de impact ervan op de gemeentelijke dienstverlening, de aanpak binnen de diverse diensten, de crisisbeheersstructuur en bij de lessons learned. Bovendien wordt die kennis ook breed gedeeld en is ze eenvoudig opvraagbaar.

Kurt Callewaert ging in zijn bijdrage nog dieper in op de kwetsbaarheden van allerlei kritieke infrastructuur in steden en gemeenten. Want ja, de digitalisering en de genetwerkte informatisering maken onze samenlevingen buitengewoon kwetsbaar voor cyberaanvallen.

En dus is de nood aan effectief **risicomanagement** door alle betrokken actoren erg groot.

Welke waarden moeten wij beschermen?

Welke zijn de ‘kroonjuwelen’ van onze organisatie?

Welke dreigingen kunnen we verwachten en waar bevinden zich onze kwetsbare plekken?

Bovendien moet er ook veel aandacht gaan interne dreigingen, bv. van eigen medewerkers bij conflicten. Laat u vooral niet misleiden door een gevoel van **Not In My Organisation** of NIMO-syndroom!

Na goede risicoanalyse kunnen we gericht aan de slag met maatregelen om zowel de kans op een incident als de mogelijke impact ervan te beperken.

Wordt een al dan niet verwachte dreiging toch bewaarheid, maakt een tijdige en professionele reactie het verschil. Of nog, ook **crisis*beheer*** vergt heel voorbereiding.

Hoe willen wij bv. dat onze medewerkers en IT-systemen op kantoor en thuis reageren op een cyberaanval?

In welke plan B voorzien wij om onze business continuity te vrijwaren?

Net als bij andere noodplannen zijn **oefenmomenten** nuttig om de haalbaarheid en effectiviteit van onze reactie op een incident te kunnen inschatten.

Van elkaars ervaringen leren en vruchtbaar samenwerken, gelden ook hier als kritieke succesfactoren.

Lokale besturen zijn **niet alleen doelwit van cybercriminelen** die zich willen verrijken. Ze worden ook geconfronteerd met **New Ways Of Protesting** (NWOP) via het internet door allerlei extremisten en activisten.

Waakzaamheid en een actief communicatiebeleid om burgers correct te informeren zijn heilzamer dan in discussie gaan met de verspreiders van haat of fake news.

Ik roep alle lokale besturen graag op om samen met andere actoren bij te dragen aan de **aanpak van cybercrime**. Schade voorkomen door preventie en schade beperken door een gepaste reactie en nazorg lukt immers best, zo niet enkel als we de krachten bundelen. Alleen zo kunnen we wendbaar en kort op de bal inspelen op de steeds wijzigende verschijningsvormen van cybercriminaliteit.

De **lokale besturen en politiekorpsen** kunnen bovendien de alertheid en de weerbaarheid van hun inwoners verhogen. Jullie zijn nabij, kennen de lokale gemeenschap, en beschikken over gekende communicatiekanalen en netwerken. Het zou te gek zijn om die niet te benutten.

Daarom lanceerde ik een aanbod aan de burgemeesters om mee te werken aan een coherente communicatie. We reiken kant-en-klare boodschappen aan. Informeren over preventiecampagnes, en delen goede praktijken. Voorts zullen we ondersteuning aanbieden bij de evaluatie van preventiecampagnes.

Daartoe richten we een **provinciaal knooppunt** op bij de coördinator preventie van mijn federale diensten. Een gezamenlijke en inclusieve communicatie versterkt o.i. de boodschap.

Dat heel wat lokale besturen en politiezones initiatieven nemen om cybercrime te voorkomen, de schade te beperken en de daders te vatten, verheugt me, stelt me enigszins gerust.

Op de **expo** konden jullie al kennismaken met bijvoorbeeld het **cybervrijwilligersproject** van de politiezone Geel-Laakdal-Meerhout, met de preventiecampagne op broodzakken in de politiezone Minos en met de **publiek-private samenwerking** binnen het SHIELD-netwerk van de PZ Antwerpen.

Op het **federale niveau** focust de Algemene Directie Veiligheid en Preventie van de FOD Binnenlandse Zaken doelgroepgericht op personen die al slachtoffer waren van cybercrime en op andere kwetsbare personen.

De aandacht voor criminaliteitspreventie past zich terecht aan, aan de verschuivingen in het criminaliteitsbeeld en de nieuwe modus operandi.

Ik refereerde deze ochtend al aan de forse toename van cybercrime gerelateerde feiten. De tussenkomsten van Procureur-generaal Patrick Vandenbruwaene en andere magistraten evenals de bijdragen van de politiemensen tijdens deze conferentie overtuigen mij ervan dat de sense of urgency in onze provincie groot is. Terecht!

De oprichting van een **provinciale stuurgroep cybercrime** door de Procureur des Konings Franky De Keyzer is belangrijk om de toestroom van phishing- en emo-fraudedossiers te kunnen verwerken. Het is vooral ook een knap initiatief om het fenomeen holistisch te benaderen.

De aanpak in verschillende werven brengt heel wat actoren samen en bundelt de krachten. De **werf Preventie** vormt de brug tussen de verschillende overheden.

Politie en justitie leveren grote inspanningen om hun werkprocessen beter op elkaar af te stemmen. Bovendien versterken ze de samenwerking met de

banken om te vermijden dat de slachtoffers van phishing en internetoplichting hun zuurverdiende spaargeld in luttele seconden in rook zien opgaan.

Toch is er nog veel **ruimte voor verbetering**. Terwijl de daders vanuit hun luie zetel, soms in een ver buitenland, hun argeloze slachtoffers bestoken via het internet, of criminele organisaties **specialisten inhuren voor *crime as a service*** praktijken, strijden onze politiemensen en magistraten met ongelijke wapens.

De **pakkans** verhogen impliceert afstemming tussen de ketenpartners. Dit veronderstelt meer investeringen in mensen en middelen. Het vereist bovendien een aangepast juridisch kader, internationale samenwerking en burgerparticipatie.

De rekrutering van gespecialiseerde onderzoekers bij politie en justitie is een must, net als de bijscholing van de bestaande medewerkers in de eerstelijnsdiensten zoals het onthaal.

Het initiatief om **politiemensen stage** te laten lopen bij de referentiemagistraten op het Parket te Mechelen helpt om elkaars opdrachten, beslissingen en uitdagingen beter te begrijpen.

De ontwikkeling van tools zoals **een Mule Stop Police app** door de politiezones Schoten en Grens laat toe om de interactie met de banken te versnellen en de vaak jonge geldezels te behoeden voor verder misbruik door criminele organisaties.

Inmiddels bouwen deze politiezones aan een nieuwe app die zal zorgen voor een versnelling van de registratie en de opsporing van de verdachten en de automatische verwittiging van de banken.

Als de app voldoet aan de verwachtingen zal hij nationaal geïmplementeerd worden.

Dit bewijst dat er heel veel mogelijk is als velen de krachten bundelen.

Het proces van samenwerking en innovatie wordt ook sterk bevorderd door de **werf Cybercrime** van het Provinciaal Overleg van de Korpschefs (POK). Vanuit deze werf is sterk bijgedragen aan het overleg binnen het POK en met het openbaar ministerie.

Wie strijdt tegen cybercrime moet vooral ook oog hebben voor de menselijke en psychologische aspecten.

Waarom doen **slachtoffers** wel of vooral geen aangifte?

Welke gevoelens ervaren zij bij die aangifte?

Hebben ze nood aan bijstand en psychologische begeleiding?

Slachtoffers blijven best zoveel mogelijk gespaard van schaamte en schuldgevoelens. Ook aangepaste nazorg is bijgevolg cruciaal.

Veel is mogelijk. Zeker als we met alle betrokkenen de krachten bundelen en een aantal prioriteiten stellen. Die prioriteiten zijn o.i.:

- De **empowerment van de bevolking** zodat zij beter geïnformeerd, bewuster en weerbaarder zijn in de cyberruimte
- De **uitbreiding van de capaciteit en middelen** van de overheden om cybercrime te bestrijden, o.a. door slimme samenwerking en afspraken over de toewijzing van onderzoeken en gevolgverlening
- De **versterking van de wetgeving** en het cyberstrafrecht over gevoelige kwesties zoals dataretentie en het gebruik van databanken
- De **samenwerking met partners** in binnen- en buitenland

Ook het **Cybercrime Center van Europol** stelt een toename van cybercrime vast. Meer concreet gaat het over cyberaanvallen, ransomware en het online kindermisbruik. In het bijzonder ook tijdens de pandemie, wisten de meeste ouders niet hoe ze hun kinderen hiertegen moesten beschermen.

Daarom gaat ook Europol tools en goede praktijken uitwisselen. Zo zullen burgers gratis **decryption tools** kunnen downloaden. Via het virtueel Expert platform SPACE zal men de beste expert kunnen opzoeken. Via het digitaal platform SIRIUS zullen handleidingen en ondersteuning worden aangeboden over de manier waarop providers e-evidence kunnen bezorgen aan politiediensten.

In **innovatielabs** zal de politie behoeften kunnen doorgeven. Experten zullen dan samen met Europol en andere partners de nodige tools ontwikkelen. Europol bevestigt hiermee ook het belang van **samenwerking met academici en de private sector**, zoals telecomproviders en financiële instellingen. De

hamvraag blijft: **hoe kan men nieuwe technologie gebruiken én misbruiken en adequaat reageren op dat misbruik?**

Ook op Europees vlak wordt de strijd tegen cybercrime duidelijk opgevoerd.

Dames en heren,

Samen met procureur-generaal Patrick Vandenbruwaene dank ik de verschillende sprekers van vandaag meest hartelijk voor hun bijdrage. U allen dank ik voor uw belangstelling, aanwezigheid en actieve deelname. We hopen dat u verder actief aan de slag zal blijven gaan met de opgedane kennis en ervaringen.

Uiteraard staan mijn medewerkers en ik graag blijvend ter beschikking om een verbindende rol op te nemen en een en ander te faciliteren.

De procureur-generaal en ik zijn ook allen die voor of achter de schermen meewerkten aan de voorbereiding en organisatie van deze conferentie zeer erkentelijk voor hun inspanningen.

Heel in het bijzonder dank ik de drie verbindingsofficieren Luc Smeyers, Tina Bruggeman en Marc Vercammen en mijn kabinet. Heel veel dank ook aan Sophie van Ostaeyen, Robbrecht De Keersmacker, Peter Peereboom, Philippe van Ingelgem, Christophe van Bortel, Katrien Goffings, Alain Matteeussen, Johan Vandenberghe en tot slot, maar zeker niet in het minst aan Walter Coenraets, de korpschef van de Balen-Dessel-Mol én voormalig diensthoofd van de Federal Computer Crime Unit. We geven er ons scherp rekenschap van dat het zo mogelijk nog intenser en uitdagender was om ook van deze conferentie een succes te maken.

Tot slot nodig ik u graag uit om na te praten en te netwerken op het digitale platform. Uiteraard krijgt u ook de kans om alle bijdragen en voorgestelde projecten later te bekijken en te delen met uw medewerkers. Informatie daarover volgt later.

Heel veel dank en blijf cyberveilig en gezond!