vvsg Vereniging van Vlaamse Steden en Gemeenten

datum: 5 december 2023

Q&A Webinar ‘Een crisisoefening cybercrime’

1. Bij wie kunnen we deze cybercrime crisisoefening bestellen?
    - Antwoord: Je vindt het draaiboek terug via deze link: https://www.vvsg.be/kennisitem/vvsg/crisisoefening-cybercrime
2. Naburige overheden? Je zit met NIS codes... hoe kan je dit op andere locaties doen? Ook extern IP is vaak gekoppeld om enkel op uw gedeelte van Cloud (CiPort) te mogen connecteren.
    - Antwoord: Wij hebben bvb cleane laptops besteld en een volledig apart netwerk met PC's opgezet in onze eigen locatie, maar wel met materiaal van andere organisaties Dit zijn kwesties waarover je in gesprek kan gaan met de betrokken leveranciers en de Vlaamse Overheid. Is het mogelijk om naast de hoofdeigenaar van een collectie bevolkingsgegevens ook enkele “subeigenaars” vast te leggen, die bij dringende noodzaak snel geactiveerd kunnen worden om toegang te krijgen tot de gegevens van die inwoners? Dit vereist uiteraard machtigingen op juridisch gebied.
      Een aantal scenario’s kan je op voorhand testen; een EID aanvragen en afleveren bvb kan op een PC van een naburige gemeente door een ambtenaar uit eigen gemeente.
3. U zegt dat de telefonie (zeker bij VOIP) waarschijnlijk zal uitvallen, maar wat met de mobiele nummers, deze blijven toch beschikbaar/operationeel, niet?
    - Antwoord: Die blijven normaal operationeel inderdaad. VOIP heeft betrekking op vaste telefonie. Het kan natuurlijk wel dat er zich een probleem voordoet bij een operator; dan is mobiele telefonie natuurlijk ook getroffen. Dit kan je eventueel meenemen als extra handicap in een vervolgoefening.
4. Zijn er richtlijnen wanneer je best het Cyber Response Team en wanneer best het CERT contacteert?
    - Antwoord: op dit moment bestaan er nog geen formele afspraken. Beide teams zijn nog volop in opbouw (zeker VO-CRT) maar staan wél al in contact met elkaar. Wij zouden momenteel adviseren om beide in te lichten, en in een vrij vroeg stadium (ook als je nog maar een vermoeden, weliswaar gegrond, hebt van een cyberaanval).
5. We beseffen de impact maar hoe moeten we inschatten hoelang dit invloed kan hebben op de organisatie.
    - Antwoord: dit hangt af van organisatie tot organisatie. We vinden deze vraag een prima invalshoek om een continuïteitsplan op te maken. Vertrek hierbij vanuit het scenario waarbij uw volledige digitale dienstverlening platligt (en je dus gedwongen worden om keuzes te maken en prioriteiten te stellen).
6. Naar IT wordt er niet geluisterd in onze organisatie, hoe pakt men dit aan?
    - Antwoord: Op de projectpagina Cyberveilige gemeenten vind je tips en materiaal terug om te sensibiliseren: https://www.vvsg.be/bestuur/innovatie-en-digitale-transformatie/cyberveiligheid#Project. Daarnaast kan je vragen aan je noodplanningscoördinator om deze oefening eens in te plannen, dan zal er misschien een bewustwording ontstaan. Vergeet zeker niet (en wellicht doe je dit het beste als eerste) om uw functionaris gegevensbescherming te mobiliseren; een externe kan soms meer luisterbereidheid ondervinden bij het bestuur. Met het NIS2 framework is er trouwens afdwingbare regelgeving op komst op vrij korte termijn, hetgeen je als breekijzer kan inzetten.
7. Welke applicaties raken bvb moeilijk terug online na een cyberaanval?
    - Antwoord: eerst moet je een rangorde bepalen voor prioriteit van applicaties qua kriticiteit en afhankelijkheden. Vervolgens kan je per applicatie een hersteltraject proberen op te maken en in te oefenen, waarbij je verschillende struikelblokken en uitdagingen goed documenteert. In een ideale wereld is de betrokken leverancier dan ook bereid hiermee aan de slag te gaan en te proberen het herstelproces eenvoudiger te maken.

8. Hoe gaat men om met het vingerwijzen naar de IT wanneer zoiets gebeurt wanneer duidelijk is dat de eindgebruiker de zwakke schakel is...?
    - Antwoord: in vele gevallen zal men wel twee keer nadenken vooraleer IT zomaar de schuld te geven. Omdat men ook wel beseft dat de organisatie hiervoor zowel tijd als budget moet voorzien (en andere zaken dus moeten wachten).
      Het is aan de ICT dienst om op voorhand het MT in te lichten van de genomen acties door ICT om het risico te beperken en er tegelijk voor te waarschuwen welke risico's niet afgedekt zijn. Op dat moment kan ook een actieplan voorgesteld worden om bvb medewerkers te sensibiliseren.
9. Welke lessen trekken jullie op vlak van architectuur en netwerksegmentatie om de impact te verkleinen?
    - Antwoord: trek segmentatie niet alleen door op vlak van netwerktopologie maar ook in de gebruikte databanken. Uw architectuur moet toestaan dat je bij cyberaanvallen bepaalde domeinen (of functionaliteiten) volledig moet kunnen isoleren van andere. Draag er als IT-administrator absoluut zorg voor dat beheerdersdashboarden (bv. van een VSphere console, van een Veeam paneel, ...) niet toegankelijk zijn voor niet-systeembeheerders!
10. Ik hoor dat pc's kunnen worden gecleand en gewiped, maar ik hoorde eerder dat deze moesten worden vernieuwd? PC's vernieuwen lijkt me toch wat drastisch?
    - Antwoord: via CERT krijgt men detectie tool om te kijken of pc besmet is - om te kijken of er info naar de hacking te vinden is op het toestel - nadien kan je toestel formateren. Je kan een tweesporenbeleid voeren. Enerzijds proberen we tijd te kopen door met name de leden van het crisisteam, bestuur en diensthoofden van nieuwe laptops te voorzien. Anderzijds gaan we voor andere functies besmette toestellen grondig wissen, opnieuw installeren van nul en deze vervolgens veilig verklaren voor gebruik.
11. Is er een aanbod bekend om dergelijke crisisoefeningen extern te laten begeleiden?
    - Antwoord: er lopen nu reeds contacten met VO-CRT om te kijken hoe we dit verder kunnen (laten) begeleiden vanuit de overheid. Privébedrijven raden we af omdat we het niet opportuun vinden om te betalen voor kennis die we per slot van rekening volledig zelf hebben ontwikkeld en gestructureerd. Er zal begin volgend jaar een bevraging uitgaan om te kijken welke besturen plannen hebben om te oefenen in 2024; vervolgens kan gekeken worden hoe we ons hierop het beste organiseren.
12. Welke lessen trekken jullie op vlak van interne/externe crisiscommunicatie?
    - Antwoord: https://www.vvsg.be/kennisitem/vvsg/crisiscommunicatieplan. Zie ook opmerkingen hierover in presentatie bij deze webinar.
13. Virussen kunnen zich tevens nestelen in bootloaders en firmware van randapparatuur, printers, bluetooth apparatuur, enz..., zijn jullie daar van bewust?
    - Antwoord: Ja, dat beseffen we zeer goed. Alles waar een computerchip inzit is kwetsbaar (en dat zijn tegenwoordig een heleboel apparaten). In een gebeurteniskaart van het draaiboek staat bv. een event waarbij printers willekeurig afdrukken beginnen te maken.
14. Hebben jullie nog extra voorbeelden van BCP 's ?
    - Antwoord: Deze zijn vrij specifiek op maat van de organisatie gemaakt. Het is zeker mogelijk om samen met enkele naburige besturen een BCP op te stellen, waarin je bvb ook aangeeft op elkaar beroep te kunnen doen. Dit staat of valt natuurlijk met de bereidheid om kwetsbaarheden en werkpunten in een sfeer van vertrouwen met elkaar te delen en daarvan te leren. Een BCP moet ook regelmatig getest en geactualiseerd worden.
15. Zijn er voorbeelden van efficiënte sensibiliseringscampagnes binnen lokale besturen?
    - Antwoord: https://www.vvsg.be/kennisitem/vvsg/training-en-sensibiliseringsmateriaal