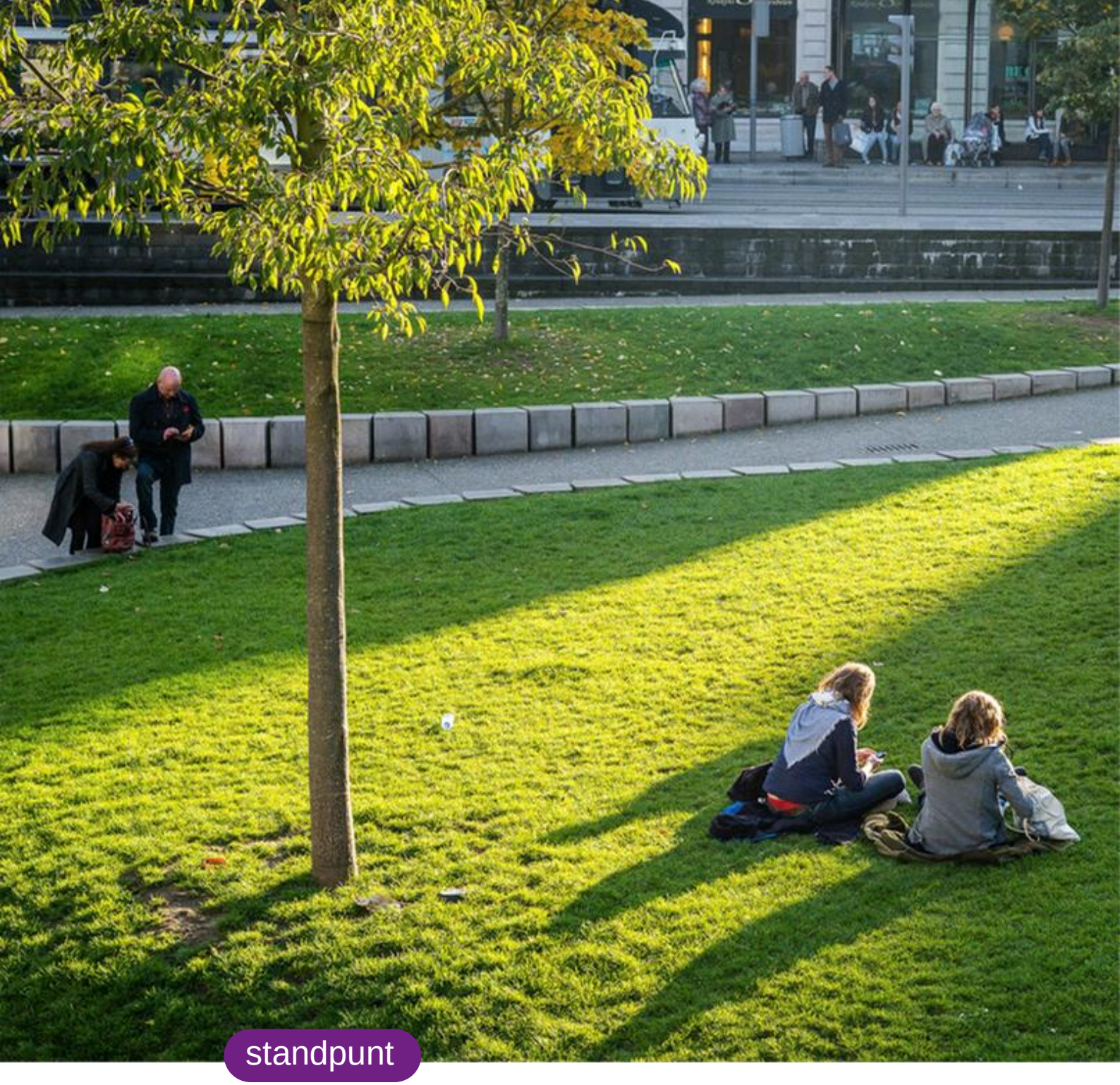
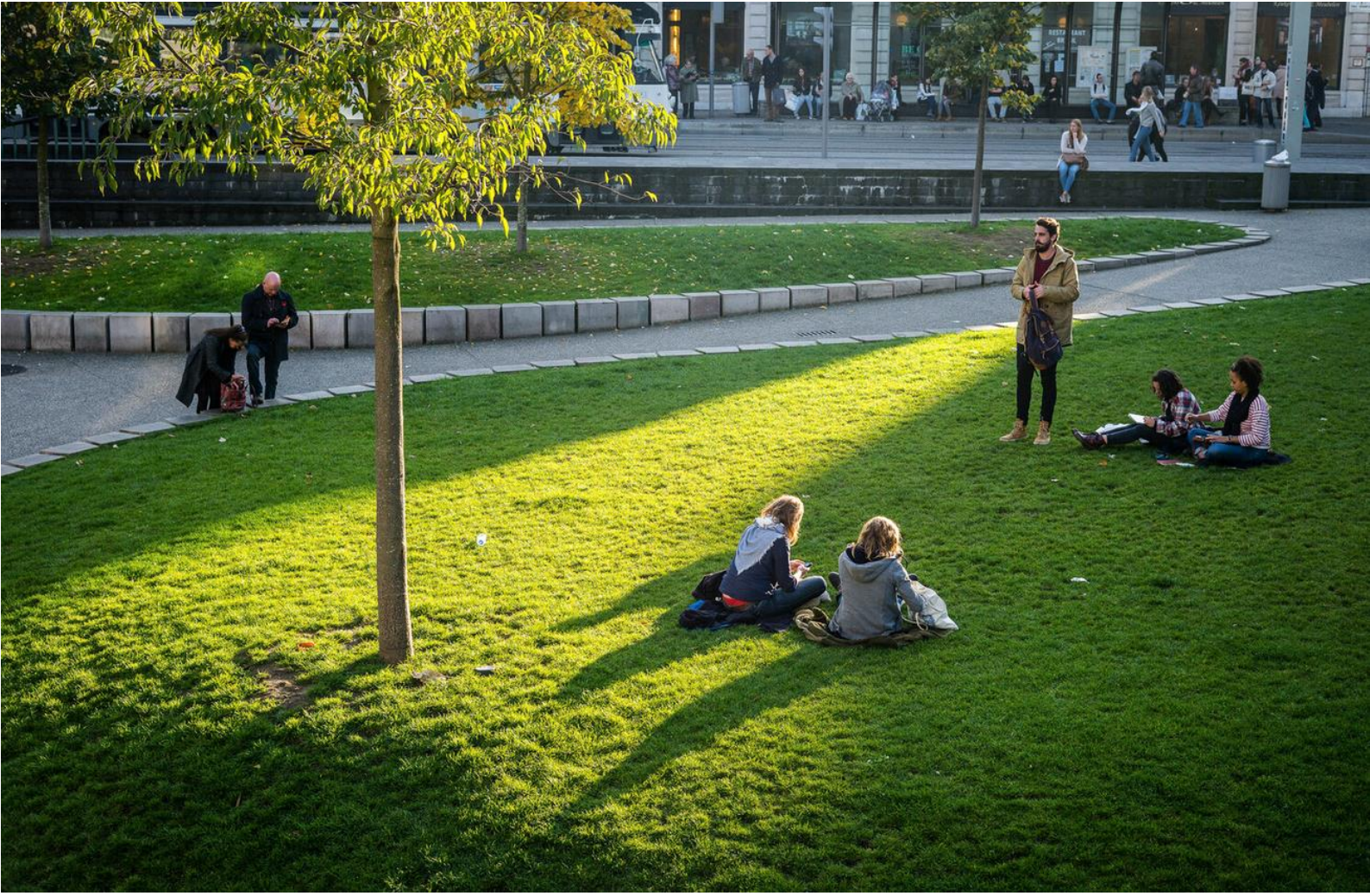


standpunt

Richtlijnen NIS2

vvsg



De Europese richtlijn NIS2 stelt strenge eisen op het gebied van cybersecurity aan specifieke entiteiten en sectoren. Lidstaten kunnen beslissen of ook de lokale overheidsentiteiten onder het toepassingsgebied vallen. De VVSG is geen voorstander om de lokale besturen mee te nemen als entiteiten die onder de NIS2-verplichtingen omdat er vandaag nog geen duidelijke strategie en doordacht plan van aanpak voor hen op tafel ligt. De VVSG roept de Vlaamse overheid dan ook op om van dit momentum gebruik te maken om werk te maken van zo'n strategie en bijhorend plan van aanpak en niet te wachten tot een volgende herziening van de richtlijn.

Inhoud

1. Context

De Europese Unie is al jaren bezig met het ontwikkelen van een cyberdefensiebeleid. In 2016 introduceerde de EU de Directive on Security of Network and Information Systems (NIS). Deze NIS stelt op het gebied van cybersecurity strenge eisen aan “essentiële bedrijven” in bijvoorbeeld de energie- en telecomsector. Om de cybersecurity verder aan te scherpen, heeft het Europees Parlement op 28 november 2022 ingestemd met een herziening van de richtlijn. NIS2 is bedoeld om de uitvoering van het bestaande cybersecurity kader uit te breiden, te versterken en te harmoniseren. In de nieuwe NIS2-richtlijn worden de beveiligingseisen verder aangescherpt, de beveiliging van toeleveringsketens aangepakt, de rapportageverplichtingen gestroomlijnd en strengere toezichtmaatregelen en handhavingsvereisten ingevoerd, waaronder geharmoniseerde sancties in de hele EU. De NIS2-richtlijn heeft ook haar toepassingsgebied uitgebreid, waardoor er meer entiteiten en sectoren worden verplicht maatregelen te nemen. Zo is de richtlijn automatisch van toepassing op overheidsdiensten van centraal en regionaal niveau. De lidstaten kunnen zelf beslissen of ook de lokale overheidsinstanties gevat worden.

2. Standpunt

De VVSG is geen voorstander om de lokale besturen mee te nemen als entiteiten die onder de NIS2-verplichtingen vallen omdat er vandaag nog geen duidelijke strategie en doordacht plan van aanpak op tafel ligt dat de cyberweerbaarheid van de lokale besturen verhoogt. Uiteraard mogen we van de lokale besturen wel verwachten dat ze meer werk maken van het thema en dat het hoger op hun agenda komt. Maar door hen louter een verplichting op te leggen zullen we deze doelstellingen niet halen. Een ondoordachte verplichting zal eerder leiden tot zeer hoge investeringen (vaak dubbel op en zonder alle synergiën te benutten) en verlegt de focus op administratieve lasten en compliance zonder garantie op het effectief verhogen van hun cyberweerbaarheid.

Dit wil allerminst zeggen dat we vandaag al geen actie kunnen of moeten ondernemen. Vanuit de veronderstelling dat de lokale besturen bij een opvolging van de richtlijn wel als belangrijke entiteiten worden beschouwd en vanuit de vaststelling dat lokale besturen vaker slachtoffer worden van cyberaanvallen, is het cruciaal dat we vandaag werk maken van een duidelijke strategie en plan van aanpak. De strategie en bijhorend plan van aanpak moeten een duidelijke richting geven over hoe we de uitdagingen van de lokale besturen rond cyberveiligheid (zie bijlage) structureel en collectief kunnen opnemen. De uitdagingen rond cyberveiligheid zijn immers van die aard dat zo goed als geen enkel lokaal bestuur deze individueel te baas kan.

Rond de uitdaging ‘Technologie’ bijvoorbeeld lijkt het ons niet onlogisch dat we (gegeven de versnippering op vlak van IT-systemen) op termijn meer moeten evolueren naar een standaard IT-omgeving waar de lokale besturen vrijblijvend gebruik van kunnen maken. Allereerst moeten we duidelijk en volledig zicht krijgen op de huidige situatie bij de lokale besturen op vlak van (1) ICT-omgeving, (2) ICT-organisatie en (3) de grote lijnen van het applicatielandschap. Rekening houdend met deze AS IS moeten we verschillende scenario’s van gewenste situaties definiëren met verschillende ambitieniveaus. Elk scenario bevat de kosten en baten en een gefaseerde roadmap om tot de gewenste situatie te bekomen.

Rond elk van de drie hieronder gedefinieerde uitdagingen moeten we zicht krijgen hoe we collectief stappen vooruit kunnen zetten. Eens we over een duidelijk en gedragen plan beschikken kunnen we een (gefaseerde) verplichting voor de lokale besturen overwegen. Een strategie en plan van aanpak laat ons bovendien ook toe om de huidige en toekomstige acties gerichter te kunnen bepalen. De Vlaamse overheid neemt vandaag immers al heel wat acties om de weerbaarheid op vlak van cyberveiligheid bij de lokale besturen te verhogen. Denk aan de cloud landingzone, het Vlaamse cyberresponse team, de cybercase van Lokaal Digitaal (SIEM/SOC as service), het project cyberveilige gemeenten met onder andere toolkit en traject ethisch hacken, cofinanciering audits, …. Al deze projecten hebben hun toegevoegde waarde, maar zijn vooralsnog losse elementen die niet kunnen ondergebracht worden in zo’n ruimere strategie en plan van aanpak.

3. Bijlage

De uitdagingen rond cyberveiligheid voor de lokale besturen situeren zich ruwweg rond 3 domeinen:

Technologie

Met de voortdurende evolutie van technologieën en het groeiende aantal digitale platforms en apparaten, staan lokale besturen voor de uitdaging om bij te blijven met nieuwe bedreigingen en beveiligingsoplossingen. Het implementeren en beheren van beveiligingsmaatregelen voor complexe IT-infrastructuren, cloudomgevingen, endpoints (zoals mobiele apparaten, sensoren, …) vormt een enorme uitdaging.

Menselijke factor

Menselijke fouten en het gebrek aan beveiligingsbewustzijn vormen een grote uitdaging. Zwakke wachtwoorden, onzorgvuldig klikken op phishing-e-mails, onjuist gebruik van gegevens en onbewust delen van vertrouwelijke informatie zijn enkele voorbeelden van risico's die voortkomen uit menselijke gedragingen. Het creëren van een cultuur van beveiligingsbewustzijn en het bieden van effectieve training en educatie aan medewerkers zijn belangrijke aspecten om deze uitdaging aan te pakken.

Beleid en organisatie

Lokale besturen zijn in grote mate afhankelijk van externe partners en leveranciers. Het waarborgen van een effectieve beveiliging over de gehele toeleveringsketen en het beheren van risico's die voortvloeien uit externe relaties en gegevensuitwisseling is complex.

Het opmaken van responsplannen, zoals Business Impact Analyse (BIA), Business Continuïteitsplan (BCP) en een crisiscommunicatieplan vergt veel tijd en expertise.

De implementatie van logisch toegangs- en gebruikersbeheer waardoor onrechtmatige toegang voorkomen wordt, verloopt moeizaam.

…

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.

Een uitgave van de Vereniging van Vlaamse Steden en Gemeenten
VVSG vzw • Bischoffsheimlaan 1-8 • 1000 Brussel
september 2021

vvsg

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