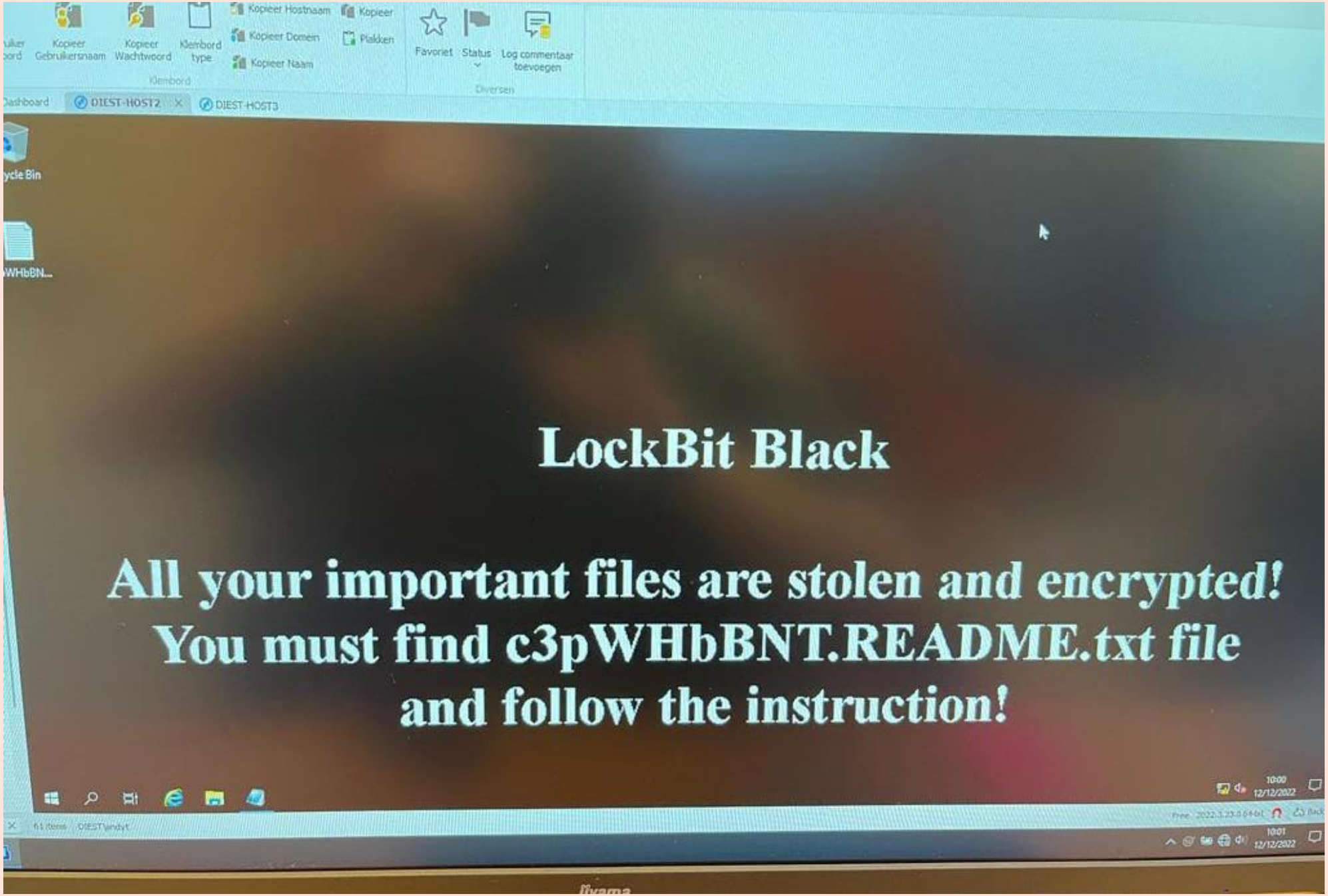
Vlaamse Ombudsdienst

Hacking bij Stad Diest

Myriam Parys



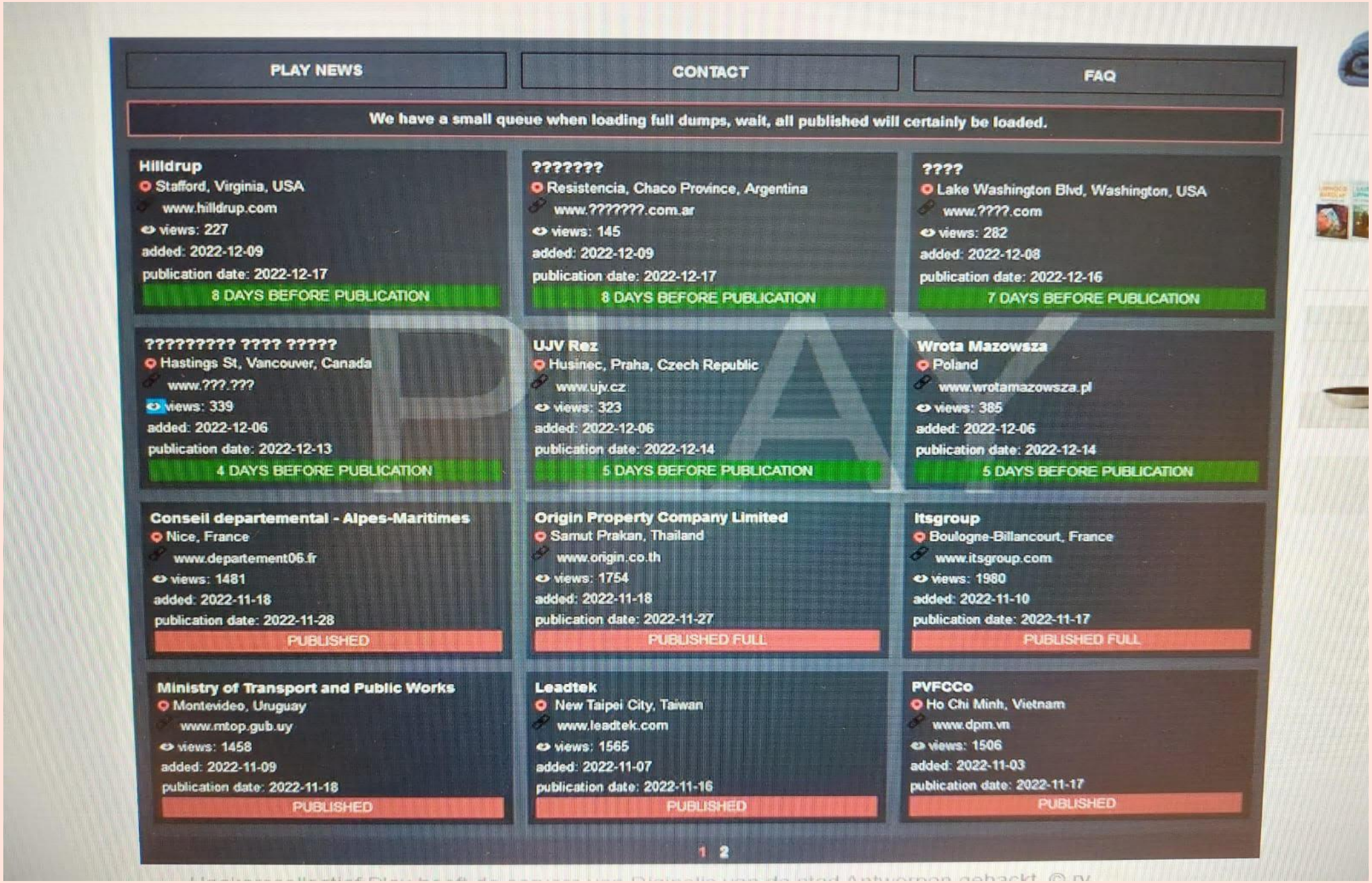
diest mijn stad

Onbekenden hebben onze computers gehackt. Daardoor ligt de dienstverlening plat.

We stellen alles in het werk om onze systemen zo snel mogelijk terug operationeel te krijgen. Maar onze loketdiensten werken niet, inwoners een afspraak geven, lukt dus niet en we kunnen ook geen e-mails ontvangen of beantwoorden.

Onze website blijft beschikbaar en ook voor dringende zaken blijven we telefonisch bereikbaar.

Vlaamse Ombudsdienst

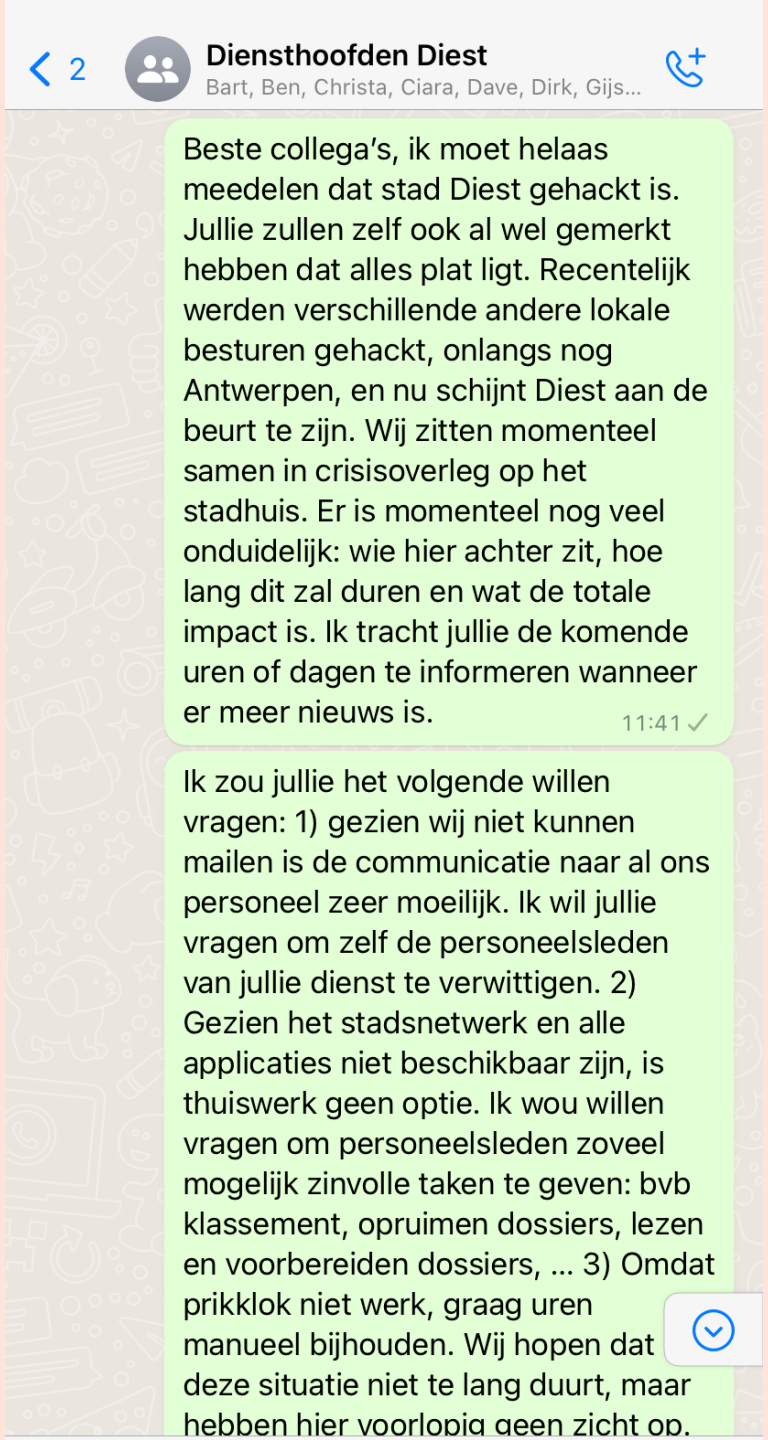


Worst case scenario

- geen e-mail @gemeente.be
- geen laptops
- geen desktops
- geen wifi
- geen bekabeld netwerk
- geen interne telefooncentrale
- geen netwerkprinters
- geen netwerkschijven met data
- geen toepassingen die op de lokale server draaien
- geen prikklok
- geen gebruik van usb sticks

Impact op dienstverlening

- geen boekhouding (geen betalingen)
- geen registratie geboorte/overlijden
- geen loonadministratie (salarissen)
- geen administratie sociale dienst (leefloon)
- geen omgevingsvergunningen
- geen digitale registratie kinderen in kinderopvang
- geen digitale registratie ontlenen boeken in bib
- geen telefonische bereikbaarheid van een aantal vestigingen
- geen werkopdrachten arbeiders
- geen ticketingsysteem cultureel centrum
- geen registratie post
- geen kassasysteem zwembad
- geen werkend afsprakensysteem
- ….



To do

- Lokale crisiscel samenroepen. Computer crime unit, CERT, DPO en externe ICT-experten inschakelen.
- In lockdown gaan (afsluiten van de netwerkconnecties om de schade te beperken).
- Communicatie zo breed mogelijk (burgers, personeel, leveranciers …).
- Via business impact analyse bepalen welke applicaties zo snel mogelijk terug beschikbaar moesten komen en prioriteiten stellen.
  (Burgerzaken! Boekhouding! Uitbetaling lonen! Uitbetaling leeflonen! e.d.)
- Kijken welke back ups beschikbaar zijn (intern en bij externe leveranciers).
- Opties tot datarecuperatie maximaal bekijken.
- Nieuwe veilige IT-omgeving opbouwen. In veilige IT-omgeving noodloketten bouwen.

Stap 1: Bepaal de RTO (Recovery Time Objective)

Proces	Meer dan 2 uur	Meer dan 2 dagen	Meer dan 2 weken	Meer dan 2 maanden	Gekozen RTO
Vernieuwen E-ID	L	H	H	K	48u

Stap 2: Vul de processenlijst in

Omvang impact	RTO	Prioriteit RTO	RPO	Afhankelijkheden	TKP/EP/ NP	

Stap 3: Definieer de benodigde middelen voor kritieke processen

Vereiste rollen	Vereiste tools en systemen	Vereiste Hardware	Vereiste werkruimte	Benodigde andere diensten of leveranciers	Contactpersonen met -info	

Stap 4: assessment van bedreigingen of risico's

Bedreiging of risicostatement	Kans of reden	Kans: L, M, H	Impact of beschrijving	Impact: L, M, H	Risico: L, M, H	Aanvaarden, verminderen, verwijderen, preventieve maatregelen?	

Lessons learned

- Geoblocking activeren op de firewall
- Buitenlandse IP-adressen blacklisten
- Multi-factor authenticatie
- Offline back-ups
- Service level agreement met softwareleverancier heronderhandelen, vragen sterkere garanties, bijv. inzake aansprakelijkheid.
- Toepassingen die lokaal draaien maximaal in de cloud zetten.
- Dankzij samenwerking met buurgemeente Scherpenheuvel-Zichem, die soortgelijke softwareoplossingen gebruiken, noodloket burgerzaken kunnen installeren. Interessant met buurgemeenten afspraken te maken rond het opzetten van noodloketten.
- **De gebruiker zelf is het grootste risico.** Dus stevig blijven inzetten op sensibiliseren van het personeel door phishing-acties en andere.
- Onze kwetsbaarheid én afhankelijkheid van technologie zijn zeer groot.

Vlaamse
Ombudsdienst

Vlaamse
Ombudsdienst

Leuvenseweg 86, 1000 Brussel I info@vlaamseombudsdienst.be I www.vlaamseombudsdienst.be I 02 552 48 48