CENTRE FOR
CYBER SECURITY
BELGIUM

Adviezen voor antivirus-, EDR- en XDR-beveiligingsoplossingen

Augustus 2022

Inhoudsopgave

Samenvatting

Gezien de huidige context is een "defence in depth"-strategie belangrijk en moeten organisaties zich adequaat voorbereiden. Dit omvat vele aspecten zoals geschikt beleid en procedures, training (bewustwording) van eindgebruikers, processen voor het beheer van kwetsbaarheden, goed configuratiebeheer, (lokale) firewalls, bescherming van webtoepassingen, SIEM-systemen (Security Information and Event Management), IDS-systemen (Intrusion Detection Systems), goede netwerksegmentatie, beheer van mobiele apparaten, ... Dit alles moet worden afgestemd op uw organisatie en rekening houden met de architecturale opzet, zoals cloudgebruik, "Bring your own device"-strategie, enzovoort.

De inzet en het beheer van antivirus, EDR (endpoint detect and respond) en zelfs XDR (extended end-point detection and response) maken deel uit van de oplossing die nodig is om dit doel te bereiken.

Dit document bevat adviezen voor algemene, pragmatische en generieke technische criteria en een aantal relevante referenties voor antivirus-, EDR- en XDR-beveiligingsoplossingen.

Binnen deze aanpak hebben wij drie niveaus gedefinieerd: Niveau 1 (Basic) verwijst naar antivirusbescherming, niveau 2 (substantial) naar EDR en niveau 3 (advanced) naar XDR.

Als uw organisatie al over een basisbeveiligingsoplossing beschikt, kunt u met extra licenties wellicht upgraden naar de geadviseerde mogelijkheden van een EDR-oplossing (zie niveau 2).

Enkele definities

Antivirus (niveau 1, basisbescherming): Toepassingen die (real-time/bij toegang of gepland met een interval) bestanden scannen, op basis van handtekeningen of heuristiek. Ze zijn ideaal voor het detecteren van bekende malware.

EDR - Endpoint Detection and Response (niveau 2, “substantial” bescherming): Dit is de oplossing van de volgende generatie die meestal antivirusscanners omvat, maar extra functies toevoegt gebaseerd op gecentraliseerd beheer, correlatie, en interpretatie van gebeurtenissen.

XDR - eXtended Detection and Response (niveau 3, “advanced” bescherming): Het vergroot de mogelijkheden van een EDR-oplossing(en) in een domein overstijgende omgeving door extra correlatiebronnen maar ook extra functionaliteiten toe te voegen.

Level1, basisbescherming: Antivirus (ook Anti-malware genoemd)

Probleem dat ze oplossen:

De traditionele aanpak was altijd het gebruik van een antivirus als oplossing voor eindpuntbescherming. Scanners waren de meest efficiënte hulpmiddelen, die hoofdzakelijk op handtekeningen en heuristieken steunden. Vandaag de dag zijn antivirusscanners nog steeds de meest gebruikte technische controle voor de beperking van malwarebedreigingen. Zie ook de uitstekende publicatie van NIST.gov over malwaretools (1)

Belangrijke minimale mogelijkheden voor antivirussoftware (1):

- Scant kritische hostonderdelen zoals opstartbestanden en bootrecords;

- Voert real-time scans uit van elk bestand wanneer het wordt gedownload, geopend, of wordt uitgevoerd (on-access scannen);
- Bewaakt het gedrag van veelgebruikte toepassingen, zoals e-mailclients, webbrowsers en instant messaging software;
- Identificeert veel voorkomende soorten malware en hulpmiddelen van aanvallers;
- Desinfecteert, waarbij malware uit een bestand wordt verwijderd, en bestanden in quarantaine geplaatst worden, wat betekent dat bestanden die malware bevatten in een geïsoleerde opslagplaats worden opgeslagen om later te worden gedesinfecteerd of onderzocht;
- Antivirussoftware op systemen moet zo worden geconfigureerd dat alle harde schijven regelmatig worden gescand om eventuele besmettingen van het bestandssysteem op te sporen. Ook wordt aanbevolen verwijderbare media die in de host worden geplaatst te scannen voordat het gebruik ervan wordt toegestaan;
- Gebruikers moeten ook handmatig een scan kunnen starten als dat nodig is, wat bekend staat als scannen op verzoek ("on demand scanning").

Belangrijke criteria zijn:

- Administratief: Centraal beheerd, gecontroleerd en regelmatig bewaakt door antivirusbeheerders;
    - Bescherming tegen manipulatie: De gebruiker zou niet in staat moeten zijn om antivirus uit te schakelen of te verwijderen,
    - Regelmatige updates van antivirushandtekeningen en -databases,
    - Zichtbaarheid van besmettingen en status van de inzet (rapportage).
- Nauwkeurigheid: Beschrijft het relatieve succespercentage van het instrument en de soorten fouten die het kan maken;
- Systeemoverhead: Invloed op de systeemprestaties.

Implementatiestrategie:

Organisaties moeten antivirussoftware implementeren op alle systemen waarvoor geschikte antivirussoftware beschikbaar is. Antivirussoftware moet zo spoedig mogelijk na de installatie van het besturingssysteem worden geïnstalleerd en vervolgens worden bijgewerkt met de meest recente handtekeningen en antiviruspatches (om bekende kwetsbaarheden in de antivirussoftware zelf te verhelpen) (1).

Productbeoordeling/-vergelijking organisaties

- **AV-Test** https://www.av-test.org/en/: Duitse organisatie die in 2021 is overgenomen door de Zwitserse IT Security Group. Om de maand publiceren de onderzoekers hun testresultaten, waaronder een lijst met producten die een certificering hebben gekregen (2).

  Testmethodologie: AV-Test gebruikt verschillende modules voor elk besturingssysteem, gebaseerd op 3 hoofdcriteria:
    - Bescherming weerspiegelt de resultaten van tests met bescherming tegen malware en andere aanvallen,
    - De prestaties tonen de invloed aan van de geteste producten op de snelheid van de testsystemen,
    - De bruikbaarheid wijst op storende invloeden van de geteste producten als gevolg van valse alarmen en beperkingen bij het gebruik van internet.

- **AV-Comparatives** https://www.av-comparatives.org: Oostenrijkse organisatie die antivirussoftware test en beoordeelt, en regelmatig grafieken en rapporten uitbrengt die vrij beschikbaar zijn. De financiering van AV-Comparatives wordt ondersteund door verschillende universiteiten (3).

  Testmethode: De tests worden jaarlijks uitgevoerd.
  - Real-World Protection Test: online malware-aanvallen waarmee een doorsnee zakelijke gebruiker te maken kan krijgen wanneer hij op internet surft (751 testgevallen in 2021).
  - Malwarebeschermingstest: dit is een scenario waarbij de malware reeds op de schijf aanwezig is of het testsysteem binnenkomt via bv. het lokale netwerk of een verwisselbaar apparaat, in plaats van rechtstreeks van het internet (30 tests in 2021).
  - Prestatietests: Effect op de prestaties van het systeem.

Hoewel antivirussoftware een noodzaak is geworden voor de preventie van malware-incidenten, is het niet mogelijk voor antivirussoftware om alle malware-incidenten tegen te houden. Antivirussoftware blinkt vaak niet uit in het tegenhouden van onbekende bedreigingen. Antivirussoftwareproducten detecteren malware hoofdzakelijk door te zoeken naar bepaalde kenmerken van bekende gevallen van malware, wat zeer effectief is voor het identificeren van bekende malware, maar minder geschikt is voor het detecteren van sterk aangepaste, op maat gemaakte malware (1).

Niveau 2: Aanzienlijke bescherming EDR (Substantial security Endpoint Detection and Response) (4) (5)

Probleem dat ze oplossen:

Correlatie en interpretatie van gebeurtenissen worden steeds belangrijker om meer geavanceerde en aangepaste malware, bijvoorbeeld ransomware, te kunnen opsporen en erop te reageren.

Antivirussoftware is niet erg geschikt om deze taak uit te voeren. Elke afzonderlijke gebeurtenis kan legitiem zijn, maar als er een overvloed aan gebeurtenissen plaatsvindt in een korte periode , kan dit worden veroorzaakt door een kwaadaardig incident.

Om deze situatie te verhelpen, is door verschillende leveranciers een nieuwe generatie van tools ontwikkeld. Er is geen unieke definitie of standaard voor EDR, wat betekent dat de mogelijkheden tussen leveranciers sterk kunnen verschillen. Verschillende leveranciers verpakken de EDR functies met andere functionaliteiten zoals antivirus of netwerkbeveiliging. Dit alles maakt het moeilijk om te vergelijken.

Belangrijke minimumcapaciteiten voor EDR (4):

1) Beveiligingsincidenten detecteren;
2) Incidenten beperken tot en bewaren op het eindpunt (ter verdere analyse);
3) Onderzoeken van beveiligingsincidenten ;
4) Zorgen voor herstelbegeleiding.

De CCB beveelt aan dat een EDR-oplossing ten minste over de volgende mogelijkheden moet beschikken:

- Bewaking van eindpunten en registratie van gebeurtenissen;

- Zoeken onderzoeken en opsporen van bedreigingen;
- Detectie van verdachte activiteiten;
- Bruikbare inlichtingen om de reactie te ondersteunen;
- Ondersteuning voor meerdere OS;
- Geautomatiseerde sanering;
- Centrale beheers component.

Het CCB adviseert dat het geselecteerde instrument ook over de volgende aanvullende mogelijkheden beschikt:

- Detectie en rapportage van kwetsbaarheden;
- Forensische capaciteiten / verzamelen van gegevens uit systemen;
- API voor het koppelen van externe systemen.

Mogelijkheden meer in detail:

- Bewaking van eindpunten en registratie van gebeurtenissen

  Wij raden aan dat het gekozen gereedschap de mogelijkheid heeft om gebeurtenissen te registreren, zoals actieve processen, actieve gebruikers op het systeem, actieve netwerkverbindingen, diensten die bestaan op de machine, enz.

  Wij bevelen aan dat het instrument waarschuwingen/gebeurtenissen kan doorsturen naar een extern systeem zoals een SIEM of een logboek/opslagoplossing.

- Zoeken, onderzoeken en opsporen van bedreigingen

  Wij bevelen aan dat het gekozen instrument aangepaste query's kan uitvoeren. Bij voorkeur kan het ook aangepaste scripts uitvoeren naar een gespecificeerde reeks eindpunten.

  Idealiter ondersteunt het instrument live interactie met het eindpunt systeem, zodat het beveiligingsteam bedreigingen op het specifieke eindpunt kan onderzoeken en monsters kan exfiltreren voor verdere analyse in een afzonderlijke (sandboxed) omgeving.

- Detectie van verdachte activiteiten

  Wij bevelen aan dat het gekozen instrument de creatie van aangepaste detectieregels door de organisatie zelf ondersteunt. Detectie op basis van handtekeningen en detectie op basis van regels (gedragsdetectie) worden aanbevolen.

- Bruikbare inlichtingen om de reactie te ondersteunen

  Wij bevelen aan dat het gekozen instrument de mogelijkheid biedt om indicators of compromise (IOC) op te nemen. Hierbij kan het gaan om netwerkadressen (IP), hashes van bestanden, bestandsnamen, domeinnamen, e-mails, enz. Hoe meer indicatoren op een geautomatiseerde manier kunnen worden opgenomen, hoe beter.

- Ondersteuning voor meerdere OS

  Wij bevelen aan dat het gekozen instrument agents heeft die beschikbaar zijn voor meerdere besturingssystemen. Systemen op basis van Windows, Windows Server, Mac OS, en Linux-distributies op basis van Debian of Redhat moeten minimaal worden ondersteund indien aanwezig in uw infrastructuur.

- Geautomatiseerde sanering

  Wij bevelen aan dat het gekozen instrument de mogelijkheid heeft om automatisch te reageren op gedetecteerde incidenten en dat het instrument een eindpunt in quarantaine kan plaatsen.

- Centrale beheerscomponent

  Wij bevelen aan dat het gekozen instrument voortdurend verbinding kan maken met zijn centrale beheerplatform. Elke (internet)netwerkverbinding moet worden ondersteund (ook als dit betekent dat er geen directe VPN-verbinding naar de organisatie is).

  Indien een cloud-oplossing wordt gebruikt, raden wij aan dat deze oplossing zich fysiek in een Europees datacentrum bevindt en dat een gegevensbeschermingseffectbeoordeling (DPIA) wordt uitgevoerd.

  Sommige geïntegreerde cloud-oplossingen kunnen een aantal voordelen bieden, zoals geautomatiseerde setup, onderhoud van de beheers componenten, voor gedefinieerde geïntegreerde rapportering, ...

Implementatiestrategie:

Wij raden aan om zoveel mogelijk apparaten te onboarden (op alle ondersteunde besturingssystemen).
Software moet zo snel mogelijk na de installatie van het besturingssysteem worden geïnstalleerd en vervolgens worden bijgewerkt met de meest recente softwarepatches. Updates zijn normaal gesproken niet zo frequent als voor antivirussoftware, maar organisaties moeten in staat zijn om updates zo snel mogelijk uit te rollen nadat een patch is uitgebracht.

Productbeoordeling/-vergelijking Organisaties

Wij bevelen aan om altijd de minimale capaciteiten van elke oplossing te beoordelen met de aanbevelingen uit de MITRE ATT&CK™ kennisdatabank (6).

De ATT&CK™ kennisdatabank biedt een gemeenschappelijke basis voor het beschrijven van zowel testcriteria als resultaten. ATT&CK is een door MITRE ontwikkelde, wereldwijd toegankelijke kennisdatabank van tactieken en technieken van tegenstanders, gebaseerd op waarnemingen uit de praktijk van operaties van tegenstanders (6).

MITRE heeft op een interessante manier een evaluatietest van specifieke EDR-tools uitgevoerd. Volgens sommige leveranciers is MITRE de eerste in de branche die EDR-leveranciers beoordeelt. MITRE koos 2 specifieke dreigingsactoren (APT3 & APT29) en voerde vervolgens de bijbehorende ATT&CK-technieken uit in een cyberoefening.

De meest recente evaluatie werd uitgevoerd op basis van de tactieken, technieken en procedures (TTP's) van 2 groepen:

- Wizard Spider (7) is een financieel gemotiveerde criminele groepering die sinds augustus 2018 ransomware-campagnes uitvoert tegen uiteenlopende organisaties, variërend van grote bedrijven tot ziekenhuizen.
- Sandworm Team (8) is een destructieve Russische *threat group* die door het Amerikaanse ministerie van Justitie en het Britse National Cyber Security Centre (NCSC_UK) wordt toegeschreven aan de Russische GRU-eenheid 74455. Tot de meest opvallende aanvallen van Sandworm Team behoren de aanvallen van 2015 en 2016 op Oekraïense

elektriciteitsbedrijven en de NotPetya-aanvallen van 2017. Sandworm Team is ten minste sinds 2009 actief.

De gedetailleerde resultaten per leverancier zijn te vinden op de Att&ck Evaluations (9) website.

Het is belangrijk op te merken dat MITRE de deelnemers niet rangschikt, maar op het internet, vindt u aanvullende info en (vrijblijvende) vergelijkingen.

Level3: Geavanceerde bescherming XDR – (Advanced protection eXtended Endpoint Detection and Response

Probleem dat ze oplossen (10) (5)

De meeste organisaties beschikken niet over een uniforme, standaard en geconsolideerde (eindpunt)infrastructuur. Beveiligingsteams moeten een overzicht kunnen krijgen van alle systemen en waarschuwingen van de complete infrastructuur. XDR stroomlijnt de opname, analyse en workflows van beveiligingsgegevens in de gehele beveiligingsstack van een organisatie, waardoor het zicht op verborgen en geavanceerde beveiligingsbedreigingen wordt verbeterd en de respons wordt geüniformeerd.

XDR is de evolutie van EDR. Terwijl EDR activiteiten op meerdere eindpunten verzamelt en correleert, verbreedt XDR de reikwijdte van detectie verder dan eindpunten en biedt detectie, analyse en reactie op eindpunten, netwerken, servers, cloud-workloads, SIEM en nog veel meer.

Dit zorgt voor een eenduidig overzicht over meerdere tools en aanvalsvectoren. Dit verbeterde overzicht biedt context over deze bedreigingen om te helpen bij triage, onderzoek en snelle herstelinspanningen.

Implementatiestrategie:

Wij raden aan om zoveel mogelijk platformen te onboarden. Een gefaseerde uitrol is echter aan te bevelen. Een XDR-platform moet voldoende tijd hebben om het gedrag van de gegevensstroom te baseren en zo nauwkeurig anomalieën in de beveiliging te detecteren (11).

Belangrijke mogelijkheden voor XDR (12)

- Controls-agnostisch

  XDR-oplossing moet integreren met meerdere technologieën en vendor lock-in vermijden.

- Machinegebaseerde correlatie- en detectiecapaciteiten

  Maakt een snellere analyse van veel grotere data sets mogelijk en vermindert het aantal valse positieven.

- Vooraf gebouwde gegevensmodellen

  Integreert informatie over bedreigingen en automatiseert detectie en reactie zonder dat software-engineers al het programmeerwerk hoeven te doen of alle regels hoeven te maken. Wij bevelen wel aan dat de XDR-oplossing de mogelijkheid biedt om extra aangepaste regels te maken.

- Integratie met SIEM's, SOAR's en hulpmiddelen voor dossierbeheer

In plaats van dergelijke producten te moeten vervangen, stelt XDR bedrijven in staat de waarde van hun investeringen te maximaliseren

Opmerking: Het is belangrijk te kwantificeren hoeveel log- en telemetriegegevens zullen worden verzameld en hoe lang gegevens moeten worden opgeslagen. Dit zal helpen bepalen hoeveel opslagruimte het XDR-platform nodig heeft, evenals de bandbreedte die zal worden verbruikt via LAN's, WAN's, en cloud-verbindingen om gegevens naar een XDR-gegevensverzamelingsagent te verzenden.

Productbeoordeling/-vergelijking Organisaties (11)

Het CCB beveelt aan eerst de infrastructuur en de hulpmiddelen van uw organisatie te beoordelen voordat u op beslist over de aanschaf van een XDR-oplossing. Er zijn enkele kleine verschillen tussen XDR-platforms.

- Opsporingsniveau
  Sommige XDR-toepassingen zullen meer vertrouwen op de gegevens van de eindpuntdetectie, andere meer op netwerk gegevens. De aanwezigheid van thuiswerkers in uw organisatie, een groot, divers, en complex netwerk, ... kunnen belangrijke factoren zijn in het beslissingsproces.

- Informatie over bedreigingen
  Het is belangrijk om na te gaan hoe de leverancier omgaat met bedreigingsinformatie of ze proactief genoeg zijn. De meeste XDR-platforms maken gebruik van hun eigen interne teams voor het opsporen of om nieuwe of opkomende bedreigingen te identificeren.
  Informatie over bedreigingen die door deze teams wordt verzameld, kan worden gebruikt om automatisch beveiligingsbeleidslijnen op te stellen die vervolgens naar de beveiligingshulpmiddelen van de -organisatie worden gepusht. Het vermogen van deze teams om bedreigingen snel te identificeren en een beleid op te stellen is een kritieke factor voor zero-day-exploits.

Windows eco systeem

Elk recent Windows-besturingssysteem wordt geleverd met een gratis Windows Defender (antivirus) client geïnstalleerd, out of the box. Organisaties zijn natuurlijk vrij om het antivirusproduct te installeren. Als u een ander antivirusproduct installeert, wordt de antiviruscomponent in de Defender client gewoon vervangen. Alle andere componenten in de Defender client zullen blijven werken (Windows Defender Firewall,...).

Aan de andere kant kan de gratis Windows Defender client worden geconfigureerd en geüpgraded naar een EDR client. (13) (14)

De Windows Defender client kan ook worden ingezet op Windows-servers (15) of op uw cloudinfrastructuur (16).

Als toegevoegde waarde voor het defender eco-systeem, kan Defender for Identity een belangrijke functie zijn. Na installatie van een sensor op alle Active Directory domeincontrollers (on premise) zijn extra opties voor identiteitsbeheer beschikbaar in het cloudplatform. (17)

Zoals bij alle in de cloud geïntegreerde producten kunnen er standaard enkele wijzigingen in de cloud omgeving optreden, waardoor uw beveiligingsrisico's veranderen. Dit vereist een voortdurende follow-up en evaluatie van deze wijzigingen die door de leverancier worden toegepast.

Er kunnen speciale licentievoorwaarden van toepassing zijn, controleer altijd eerst de licentievoorwaarden met uw leverancier.

We raden ook aan om Sysmon te installeren, wat uw logging en diagnostische mogelijkheden zal verrijken. (18)

Andere besturingssystemen (Linux, Mac OS, ...) of apparaten die niet van Microsoft zijn, bieden mogelijk niet altijd hetzelfde niveau van functies en beveiligingsbereik binnen de Defender-suite. Controleer uw niet-Microsoft systemen, de gebruikte versie en/of distro en hoe deze door de leverancier wordt ondersteund (19)

Het gebruik van Yara-regels wordt nog niet ondersteund (juni 2022), maar er is wel Advanced query hunting beschikbaar met een leverancier-specifieke implementatie.

Referenties

1. **NIST 800-83.** Guide to Malware Incident Prevention and Handling for Desktops and Laptops. *Nist.gov.* [Online] https://csrc.nist.gov/publications/detail/sp/800-83/rev-1/final.

2. **Wikipedia AV-test. *nl.wikipedia.org.* [Online] https://nl.wikipedia.org/wiki/AV-test.org.**

3. Wikipedia AV-Comparatives. *en.wikipedia.org.* [Online] https://en.wikipedia.org/wiki/AV-Comparatives.

4. Gartner. endpoint-detection-and-response-solutions. *gartner.com.* [Online] https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions.

5. Crowdstrike. edr vs mdr vs xdr. *crowdstrike.com.* [Online] https://www.crowdstrike.com/cybersecurity-101/endpoint-security/edr-vs-mdr-vs-xdr/.

6. Mittre Attck Product evaluaties. attck gebaseerde product evaluaties. *Mittre.com.* [Online] https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/attck%E2%84%A2-based-product-evaluations.

7. Wizard Spider. [Online] https://attack.mitre.org/groups/G0102/.

8. Sandworm Team. [Online] https://attack.mitre.org/groups/G0034/.

9. mitre-engenuity.org. [Online] https://attackevals.mitre-engenuity.org/.

10. sentinelone.com. [Online] https://www.sentinelone.com/blog/understanding-the-difference-between-edr-siem-soar-and-xdr/.

11. Evalueer XDR. *techtarget.com.* [Online] https://www.techtarget.com/searchsecurity/tip/How-to-evaluate-and-deploy-an-XDR-platform.

12. *XDR volgens Mandiant.* [Online] mandiant.com. https://www.mandiant.com/resources/what-is-xdr.

13. Wat is Defender voor Endpoint. *docs.microsoft.com.* [Online] https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide.

14. Configureer Defender voor Endpoint (client). *docs.microsoft.com.* [Online] https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints?view=o365-worldwide.

15. Configureer Defender voor Endpoint (server). *docs.microsoft.com.* [Online] https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-server-endpoints?view=o365-worldwide.

16. Defender voor Endpoint (cloud) configureren. *docs.microsoft.com.* [Online] https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-servers-introduction.

17. Wat is Defender voor Identiteit. *docs.microsoft.com.* [Online] https://docs.microsoft.com/en-us/defender-for-identity/what-is.

18. Sysmon, Microsoft. [Online] https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon.

19. Defender voor Endpoint configureren (overig). *docs.microsoft.com.* [Online] https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints-non-windows?view=o365-worldwide.

Contact

Centrum voor Cybersecurity België
Wetstraat 18
1000 Brussel
info@ccb.belgium.be

Disclaimer

Deze gids en de bijbehorende documenten zijn opgesteld door het Centrum voor Cybersecurity België (CCB), een federale overheidsdienst opgericht bij koninklijk besluit van 10 oktober 2014 en onder het gezag van de eerste minister.

De verstrekte informatie:

- is uitsluitend van algemene aard en heeft niet tot doel alle specifieke gevallen te behandelen;
- is niet noodzakelijk op alle punten volledig, nauwkeurig of up-to-date.

Verantwoordelijke uitgever

Centrum voor Cybersecurity België

M. De Bruycker, Directeur

Wetstraat 18

1000 Brussel