CENTRE FOR
CYBERSECURITY
BELGIUM 10Y

10 JAAR CENTRUM VOOR CYBERSECURITY BELGIË

Centre for Cybersecurity Belgium
Onder de autoriteit van de Eerste Minister

.be

Verantwoordelijke uitgever
Centrum voor Cybersecurity België
M. De Bruycker, Directeur Generaal
Wetstraat 18
1000 Brussel

Research, interviews en redactie
the content company

Eindredactie
Katrien Eggers
Michele Rignanese

Fotografie
AdobeStock, eigen archief CCB, Karakters, Cookiecutter & Ron Lach for Pexels

Ontwerp
Karakters.be

Druk
Drukkerij Belgische Kamer van volksvertegenwoordigers

Wettelijk depot
D/2025/14828/005

Publicatiedatum:
31 oktober 2025

INHOUD

Beste lezer,

Tien jaar geleden kreeg ons land met de oprichting van het Centrum voor Cybersecurity België (CCB) één aanspreekpunt voor cyberveiligheid. Wat begon met een Koninklijk Besluit op papier en de aanwerving van 2 gedreven pioniers, is uitgegroeid tot een gerespecteerde nationale autoriteit, gedragen door een divers team van bijna 140 experts. Samen met tal van partners waken wij dag en nacht over de digitale veiligheid van burgers, bedrijven en overheden.

Onze economie en maatschappij vertrouwen hoe langer, hoe meer op digitale netwerken. Maar intussen worden ook cyberaanvallen steeds gesofisticeerder en doelgerichter. Cyberveiligheid is dan ook een essentiële bouwsteen van onze samenleving. De Europese Unie versterkte de voorbije jaren het regelgevend kader, met onder meer de NIS1- en NIS2-richtlijn, de Cybersecurity Act en de Cyber Resilience Act. Elk van die initiatieven brengt bijkomende opdrachten en verantwoordelijkheden met zich mee, maar vooral ook kansen om de lat voor cyberveiligheid nog hoger te leggen.

Vanuit onze centrale rol coördineren we de opvolging van incidenten, ondersteunen we vitale sectoren en richten we ons op preventie. Vanaf de eerste dag hebben we daarom niet alleen geïnvesteerd in technologie, expertise en procedures, maar vooral in bewustmaking en betrokkenheid van de burgers. Want bovenal is het de collectieve actie van alle burgers en bedrijven samen die ertoe leidt dat we onze cyberweerbaarheid verhogen. Simpele basismaatregelen zoals tweestapsverificatie en tijdig updaten van software blijven het meest effectieve middel om schade te voorkomen.

We zijn dan ook trots dat Safeonweb is uitgegroeid tot een vertrouwd baken voor het brede publiek, met heldere tips en de mogelijkheid om eenvoudig verdachte berichten te signaleren. Elke melding helpt ons om sneller te reageren, gerichter te informeren en collectief sterker te staan. En met Safeonweb @Work, inclusief zijn praktische richtlijnen en scans, helpen we bedrijven om zich stap voor stap beter te wapenen.

Intussen professionaliseerde ook ons ecosysteem. Nauwe samenwerking, in volle vertrouwen, tussen overheidsdiensten, de private sector en de academische wereld heeft ertoe geleid dat België onder de coördinatie van het CCB kon uitgroeien tot een Europees rolmodel voor cybersecurity.

Deze brochure blikt terug op een decennium van leren, experimenteren en best practices verankeren. Maar ze blikt ook vooruit, want de opmars van AI en de geopolitieke dreigingsdynamiek stellen ons voor nieuwe uitdagingen. Ons engagement en onze inzet blijven evenwel verzekerd: proactief actie ondernemen om ons land maximaal te beschermen.

Samen kunnen we van België een van de veiligste digitale omgevingen in Europa maken. Dat is onze ambitie. En die verantwoordelijkheid kunnen we alleen waarmaken als we ze samen met u kunnen opnemen.

Miguel De Bruycker
Directeur-generaal

Phédra Clouner
Adjunct-Directeur-generaal

WAT VOORAFGING

Het Centrum voor Cybersecurity België (CCB) werd opgericht bij Koninklijk Besluit op 10 oktober 2014 en ging begin 2015 van start. Maar al eerder waren er stappen gezet om het internetverkeer in ons land te beveiligen.

In 1993 werd Belnet opgestart, een federaal onderzoeksprogramma met als doel om een netwerk te ontwikkelen waarmee onderzoekers vanop afstand verbinding konden maken met supercomputers. Belnet groeide uit tot een internetknooppunt en leverde inspanningen om de kwaliteit van de verbindingen te garanderen en ze te beveiligen.

In de schoot van Belnet zag in 2004 het Computer Emergency Response Team (Belnet CERT) het licht. Dit team antwoordt op vragen over veiligheidsproblemen en -incidenten van leden uit het onderzoeksnetwerk.

Daarnaast werd binnen de overheid het Belgian Network & Information Security Platform (BELNIS) opgestart. Dit was een overlegorgaan waarin alle departementen die betrokken waren bij digitale veiligheid vertegenwoordigd waren, met als doel om netwerk- en informatiebeveiligingsproblemen te bespreken. Omdat het orgaan niet beschikte over beslissingsmacht of financiële middelen, leidde dit platform niet meteen tot concrete acties.

FEDERALE OVERHEIDSDIENST
KANSELARIJ VAN DE EERSTE MINISTER

[2014/207006]

10 OKTOBER 2014. — Koninklijk besluit tot oprichting van het Centrum voor Cybersecurity België

FILIP, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Gelet op de Grondwet, de artikelen 37 en 107, tweede lid;

Gelet op het koninklijk besluit van 11 mei 2001 houdende oprichting van de Federale Overheidsdienst Informatie- en Communicatietechnologie;

Gelet op het advies van de inspecteur van Financiën, gegeven op 9 december 2013;

Gelet op het advies van de inspecteur van Financiën, gegeven op 13 december 2013;

Gelet op de akkoordbevinding van de Staatssecretaris voor Ambtenarenzaken, gegeven op 17 december 2013;

Gelet op de akkoordbevinding van de Minister van Begroting, gegeven op 17 december 2013;

Gelet op het protocol nr. 155/1 van 24 februari 2014 van het Sectorcomité I - Algemeen Bestuur;

Gelet op de vrijstelling van een impactanalyse op basis van artikel 8, § 1, 4°, van de wet van 15 december 2013 houdende diverse bepalingen inzake administratieve vereenvoudiging;

Gelet op het advies nr. 56.335/2 van de Raad van State, gegeven op 4 juni 2014, met toepassing van artikel 84, § 1, eerste lid, 2°, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973;

Op de voordracht van de Eerste Minister, de Minister van Begroting, de Minister van Financiën, belast met Ambtenarenzaken, de Staatssecretaris voor Modernisering van de Openbare Diensten en op het advies van de in Raad vergaderde Ministers,

Hebben Wij besloten en besluiten Wij :

Artikel 1. Bij de Federale Overheidsdienst Kanselarij van de Eerste Minister wordt het Centrum voor Cybersecurity België, hierna "CCB" genoemd, opgericht.

Het CCB staat onder het gezag van de Eerste Minister.

SERVICE PUBLIC FEDERAL
CHANCELLERIE DU PREMIER MINISTRE

[2014/207006]

10 OCTOBRE 2014. — Arrêté royal portant création du Centre pour la Cybersécurité Belgique

PHILIPPE, Roi des Belges,

A tous, présents et à venir, Salut.

Vu la Constitution, les articles 37 et 107, alinéa 2;

Vu l'arrêté royal du 11 mai 2001 portant création du Service public fédéral Technologie de l'Information et de la Communication;

Vu l'avis de l'inspecteur des Finances, donné le 9 décembre 2013;

Vu l'avis de l'inspecteur des Finances, donné le 13 décembre 2013;

Vu l'accord du Secrétaire d'Etat à la Fonction publique, donné le 17 décembre 2013;

Vu l'accord du Ministre du Budget, donné le 17 décembre 2013;

Vu le protocole n° 155/1 du 24 février 2014 du Comité de Secteur I - Administration générale;

Vu la dispense d'analyse d'impact sur la base de l'article 8, § 1er, 4°, de la loi du 15 décembre 2013 portant des dispositions diverses concernant la simplification administrative;

Vu l'avis n° 56.335/2 du Conseil d'Etat, donné le 4 juin 2014, en application de l'article 84, § 1er, alinéa 1er, 2°, des lois sur le Conseil d'Etat, coordonnées le 12 janvier 1973;

Sur la proposition du Premier Ministre, du Ministre du Budget, du Ministre des Finances, chargé de la Fonction publique, du Secrétaire d'Etat à la Modernisation des Services publics et de l'avis des Ministres qui en ont délibéré en Conseil,

Nous avons arrêté et arrêtons :

Article 1er. Auprès du Service public fédéral Chancellerie du Premier Ministre est créé le Centre pour la Cybersécurité Belgique, ci-après dénommé « CCB ».

Le CCB est placé sous l'autorité du Premier Ministre.

Koninklijk besluit tot oprichting van het Centrum voor Cybersecurity België.

2012: De eerste cyberstrategie

De toenemende incidenten rond cyberveiligheid deden het besef rijzen dat er nood was aan een omvattende nationale strategie. Die werd in 2012 uitgewerkt door Luc Beirens van de Federale Computer Crime Unit bij de Federale Politie en Miguel De Bruycker, die bij ADIV, de inlichtingendienst van Defensie rond cybersecurity, werkte. Deze eerste Cybersecurity Strategie schoof drie objectieven naar voren:

- België zal streven naar een veilige en betrouwbare cyberspace met respect voor de fundamentele rechten en waarden van de moderne samenleving.
- België zal streven naar een optimale beveiliging en bescherming van kritieke infrastructuren en overheidssystemen tegen de cyberdreiging.
- België wil eigen cybersecurity capaciteiten ontwikkelen.

Bij de concrete acties om de strategie uit te rollen, vermeldde deze nota uitdrukkelijk de nood om cybersecurity gecentraliseerd en geïntegreerd aan te pakken, door centrale aansturing en het ontwikkelen van nauwe publiek-private samenwerkingen. In de ontwerpnota werd voor het eerst het idee geopperd om een onafhankelijk coördinatiecentrum voor cybersecurity op te richten in België.

Eerst was er weinig politiek enthousiasme voor zo'n centraal coördinatiecentrum. Een aantal cyberincidenten in de loop van 2013 en het aantreden van een nieuwe federale regering eind 2014 leidden er echter toe dat cyberveiligheid hoger op de beleidsagenda kwam te staan.

2013: De Belgacom-hack

Een van de meest bekende incidenten uit die periode was de Belgacom-hack. In de zomer van 2013 ontdekten Nederlandse cyberexperts sporen van een digitale inbraak bij telecomoperator Belgacom. In de IT-systemen werd uiterst ingenieuze spyware gevonden die allicht al sinds 2011 toeliet om communicatie en data te onderscheppen van Belgacom en zijn internationale dochter BICS. Belgacom investeerde na het incident fors in cybersecurity. Er gaan tientallen miljoenen naar de vernieuwing van de IT-infrastructuur en een betere beveiliging tegen cyberaanvallen.

2013: Een Europese cybersecuritystrategie

De oprichting van het CCB kan ook niet los worden gezien van de evoluties in het Europese cyberveiligheidsbeleid. In 2004 al werd het European Network and Information Security Agency ENISA opgericht. Maar pas in februari 2013 presenteerde de Europese Commissie haar eerste cybersecuritystrategie, getiteld "An Open, Safe and Secure Cyberspace". Die strategie stelde wetgevende initiatieven in het vooruitzicht om de cyberveiligheid te bevorderen, wees op het belang van awareness in de publieke en private sector en op de noden om meer te investeren in R&D rond cyberbeveiliging.

Tegelijk moedigde de Commissie de lidstaten aan om de nodige structuren op te zetten die cyberweerbaarheid, -criminaliteit en -verdediging aanpakken, om beter gewapend te zijn bij cyberincidenten. De strategie beval aan om "de coördinatie op nationaal niveau tussen ministeries te optimaliseren en in nationale cyberbeveiligingsstrategieën de rollen en verantwoordelijkheden van de verschillende nationale entiteiten vast te leggen."

"De oprichting van het CCB kan ook niet los worden gezien van de evoluties in het Europese cyberveiligheidsbeleid. In februari 2013 presenteerde de Europese Commissie haar eerste cybersecuritystrategie."

2014-2016

DE OPRICHTING

De wettelijke basis voor de oprichting van het Centrum voor Cybersecurity werd in het najaar van 2014 gelegd. Het CCB kreeg van de overheid een duidelijke opdracht mee: het bewaken, coördineren en versterken van de cyberveiligheid in België.

Zo coördineert het centrum het Belgische beleid rond cyberveiligheid. Het volgt de uitvoering op, stelt initiatieven voor en werkt mee aan nieuwe regelgeving. Sensibilisering is één van de hoofdopdrachten: burgers, bedrijven en publieke instellingen informeren over online risico's en concrete handvaten aanreiken om er iets aan te doen. Internationaal vertegenwoordigt het centrum België in Europese overlegorganen. Omdat het om een opdracht gaat die bevoegdheden en departementen overschrijdt, werd het CCB toegewezen aan de bevoegdheid van de Eerste Minister, die de politieke verantwoordelijkheid draagt.

De belangstelling tijdens de rekrutering voor de sleutelposities was groot. Voor de functie van directeur stelden zich 16 Nederlandstaligen en 19 Franstaligen kandidaat. Voor adjunct-directeur waren er 27 Nederlandstalige en 29 Franstalige kandidaten. Na de selectieronde werden Miguel De Bruycker (tot dan tewerkgesteld bij Defensie) en Phédra Clouner (die binnen Justitie werkte) in augustus 2015 aangesteld als respectievelijk directeur en adjunct-directeur, met een mandaat van vijf jaar. Tot op vandaag staat dit duo aan het roer van de organisatie. De rest van het team werd stelselmatig uitgebouwd: van twee medewerkers in augustus 2015 tot meer dan 140 vandaag.

Van bij de start werd de keuze gemaakt om de strategische visie op nationaal niveau te laten sporen met zeer concrete acties en dienstverlening van het CCB. Voorafgaand aan het strategisch plan werden vier doelgroepen gedefinieerd: burgers, bedrijven, organisaties van vitaal belang (deze groep werd in latere fases, onder invloed van de Europese NIS-regelgeving, stelselmatig verder uitgebreid) en overheidsdiensten.

Hiermee werd de basis gelegd voor de servicegerichte aanpak die de organisatie tot vandaag kenmerkt. In de actieplannen werd expliciet aangegeven dat het CCB prioritair inzet op diensten aan de bevolking, zoals bewustmakingscampagnes. De redenering hierbij was dat naamsbekendheid bij het brede publiek meteen ook zou leiden tot een grotere ruchtbaarheid bij de andere doelgroepen.

Parallel werd het opstellen van een cybernoodplan als dringende prioriteit naar voren geschoven. Het plan zou bepalen wie in geval van een incident de leiding kan nemen om zo de impact van cyberaanvallen in te perken. Dit moest leiden tot een eenheid van commando en efficiënte bestrijding van cyberaanvallen op belangrijke Belgische doelwitten.

Eerste strategisch plan CCB

Om richting te geven aan de uitbouw van de organisatie, maakte het CCB werk van een strategisch plan dat op 26 oktober 2015 werd voorgesteld aan de buitenwereld. Het plan schetste een tijdslijn in drie fasen: een start-upfase van zes maanden, gevolgd door een build-upfase van drie jaar en een maturiteitsfase over vijf jaar. Voor elk van deze fases werden afzonderlijke operationele doelstellingen gedefinieerd, met als leidraad het opzetten van een geïntegreerde, coördinerende en actiegerichte aanpak.

In januari 2015 werd de Cyber Security Coalition opgericht

“Vanaf dag één lag de lat hoog en de periode 2014-2016 zette de noden rond cyberbeveiliging en een gecoördineerde aanpak in ons land meteen op scherp. Cyberdreigingen werden immers steeds frequenter, en de nood aan een gecoördineerde aanpak urgenter dan ooit. In dat kader was samenwerking van bij de start essentieel.”

In de aanvangsfase groeide het CCB van twee naar vijf medewerkers.
Boven v.l.n.r.: Miguel De Bruycker, Phédra Clouner. Onder v.l.n.r.: Andries Bomans, Valéry Vander Geeten, Jo De Muynck.

Vanaf dag één lag de lat hoog en de periode 2014-2016 zette de noden rond cyberbeveiliging en een gecoördineerde aanpak in ons land meteen op scherp. Cyberdreigingen werden immers steeds frequenter, en de nood aan een gecoördineerde aanpak urgenter dan ooit. In dat kader was samenwerking van bij de start essentieel. De oprichting van de Cyber Security Coalition als een private vzw, op 26 januari 2015, was een belangrijke stap in de goede richting.

De organisatie bracht overheden, bedrijven en kennisinstellingen rond de tafel om ervaringen uit te wisselen, risico’s te analyseren en oplossingen te ontwikkelen. Mede dankzij dat netwerk kon het CCB sneller schakelen, zowel strategisch als operationeel, en het fundament leggen voor wat vandaag de ruggengraat vormt van het Belgische cyberveiligheidsbeleid.

November 2015: eerste stresstest

De vuurdoop voor het jonge CCB liet niet lang op zich wachten. In november 2015 doken op YouTube berichten op met een bedreiging van hackers om Belgische overheidswebsites plat te leggen. Voor het centrum was dit de eerste echte stresstest, die de nood aan een uitgewerkt cybernoodplan nogmaals duidelijk maakte.

Het team ging meteen aan de slag om het noodplan en de nodige afstemming sneller te finaliseren. Het noodplan voorziet in een trapsgewijze escalatie, afgestemd op de ernst van het incident, en legt vast welke diensten welke verantwoordelijkheid moet opnemen. Centraal daarin staan snelheid, samenwerking en heldere communicatie.

Het plan dat uiteindelijk op tafel kwam te liggen, hield rekening met heel wat gevoeligheden uit de praktijk, en hielp het CCB finaal ook om zijn plaats op te eisen in het bredere ecosysteem. Het cybernoodplan leidde tot een heldere structuur met duidelijke afspraken bij grootschalige cyberincidenten die een nationale, gecoördineerde aanpak vereisen. Het werd mettertijd verder uitgebouwd en geüpdatet.

2016: uitbouw van een Early Warning Systeem

In 2016 versterkte het CCB zijn rol als coördinator van de Belgische cyberveiligheidsstrategie. Zo werkte het centrum mee aan de versterking van grensoverschrijdende cyberweerbaarheid, in voorbereiding van de Europese NIS-richtlijn. Tegelijk werd in ons land een eerste, rudimentaire versie van het Early Warning-Systeem (EWS) uitgewerkt, waarmee kritieke sectoren snel konden gewaarschuwd worden bij nieuwe dreigingen.

Het EWS-systeem monitort digitale netwerken van Belgische infrastructuur en analyseert technische indicatoren die kunnen wijzen op kwaadaardige activiteit (zoals botnets, malafide IP’s of verdachte domeinen). Het systeem is gebaseerd op een combinatie van geautomatiseerde datacollectie, threat intelligence en real-time signalering. De signalen worden vertaald naar waarschuwingen voor specifieke organisaties.

Sectoren zoals gezondheidszorg, financiën en energie werden prioritair aangesloten. De waarschuwingen variëren van een melding over een lek in een bepaalde softwareversie tot een concrete waarschuwing voor gerichte phishing-campagnes.

2017–2020

DE OPERATIONALISERING

Vanaf 2017 groeide het CCB sterk. Cyberdreiging en de diverse uitingen ervan werden een maatschappelijk bekend fenomeen. De maturiteitsopbouw binnen het CCB stond niet enkel gelijk aan een numerieke groei, maar ook strategisch en inhoudelijk werden grote stappen vooruitgezet.

CERT.be: verdere uitbouw van performante incident response

Op 1 januari 2017 werd het federale Cyber Emergency Response Team (CERT.be) officieel geïntegreerd in het CCB. Het betekende meer dan een administratieve herschikking, waarbij het CERT werd overgeheveld van Belnet naar een andere dienst. Het was het begin van een fundamentele verankering van incident response in de bredere nationale cybersecuritystrategie.

Voor het CCB vormde dit een eerste grote boost. Dankzij deze integratie kon de organisatie zich verder ontwikkelen. Een belangrijke troef was het feit dat de werking van het CERT volledig kon worden herdacht en geïntegreerd in de strategie die het centrum aan het uitrollen was.

De bedoeling was duidelijk: de werking van CERT.be opschalen, beter structureren en meer afstemmen op de toegenomen dreigingen in het Belgische en internationale cyberlandschap. CERT.be fungeerde al als nationaal CSIRT (Computer Security Incident Response Team), maar de verankering binnen de structuur van het CCB bood een unieke kans om de dienst verder te professionaliseren en te laten aansluiten op alle andere acties die werden genomen om de cyberveiligheid te versterken. CERT.be kreeg toegang tot meer middelen, gespecialiseerde rekrutering en beleidsmatige ondersteuning.

Een van de eerste prioriteiten na de integratie was de uitbouw van een nieuw team. Een meer multidisciplinaire samenstelling moest ertoe leiden dat het team niet alleen op incidenten kon reageren, maar ook preventief dreigingen in kaart kon brengen, aanbevelingen kon uitwerken en de nationale coördinatie bij incidenten zou faciliteren.

Cyber Europe cybercrisis oefeningen 2018 en 2024.

Eind 2018 werd een belangrijke mijlpaal bereikt: het CCB was voortaan 24/7 operationeel voor aanbieders van essentiële diensten en kritieke infrastructuren. Die permanente beschikbaarheid bood een antwoord op noden uit de economie en vormde tegelijk een hefboom om de nationale paraatheid bij cybercrisissen fors te verbeteren. Deze operationele opschaling kwam tot stand in nauwe samenwerking met het Nationaal Crisiscentrum (NCCN). Dankzij deze partner kon de 24/7-permanentie worden gegarandeerd.

De dienst maakte inmiddels werk van structurele kennisopbouw. De aanwerving en retentie van cybersecurityspecialisten vormde daarbij een constante uitdaging door de krapte op de arbeidsmarkt en de concurrentie van internationale spelers. Toch slaagde het team erin om zijn expertise te verdiepen door gericht te investeren in opleidingen en deel te nemen aan internationale oefeningen zoals Cyber Europe, een grootschalige, door ENISA georganiseerde Europese cybercrisisoefening waarbij overheden, bedrijven en andere organisaties samenwerken om hun weerbaarheid tegen grootschalige cyberincidenten te testen.

De opgebouwde reputatie en professionalisering werden ook erkend door andere overheidsdiensten. In evaluaties en samenwerkingen werd duidelijk dat de integratie van CERT.be binnen het CCB leidde tot efficiënter incidentbeheer en een betere samenwerking tussen verschillende federale en sectorale spelers. De versterkte positie van CERT.be werd een katalysator voor bredere initiatieven zoals de implementatie van de NIS-richtlijn en de uitbouw van het nationale meldingsplatform.

Na de terreuraanslagen van 2016 werd een deel van de provisie Terro aangewend voor cybersecurity.

2016: Provisie Terro als hefboom

Na de terreuraanslagen van maart 2016 op Brussels Airport (Zaventem) en op de Brusselse metro, besliste de federale regering om bijkomende structurele en niet-structurele financiering vrij te maken voor projecten die radicalisering, terrorisme en gewelddadig extremisme wilden tegengaan. Hoewel deze zogenaamde 'Provisie Terro' niet expliciet over cybersecurity ging, speelde dit bijzondere budgettair kader toch een belangrijke rol voor het CCB.

Omdat terroristische netwerken ook gretig gebruik maken van het digitale domein, was de link met cybersecurity al gauw onmiskenbaar. In die context diende het CCB voorstellen in om een deel van de Provisie Terro aan te wenden voor het versterken van de Belgische digitale weerbaarheid.

Zo lieten deze middelen toe om de samenwerking tussen overheidsdiensten op te drijven. De bestrijding van cybergerelateerde terrorismevormen vereist immers samenwerking tussen het CCB, de Staatsveiligheid, de Federale Politie, Defensie, Justitie en buitenlandse partners. Deze budgetten boden de nodige ruimte om gezamenlijk personeel op te leiden, gedeelde infrastructuur te bouwen en pilootprojecten te lanceren die anders moeilijk gefinancierd zouden raken.

Threat intelligence

Het kennisniveau binnen het CCB werd verder uitgebouwd, wat in 2020 leidde tot de opsplitsing van de dienst CERT.be in een team voor Cyber Threat Research and Intelligence (CyTRIS) en een CERT-team, dat zich verder zou focussen op cyber emergency response. Beide facetten van cyberveiligheid zijn tot vandaag essentieel en behoren tot de core business van het CCB: het capteren en analyseren van de dreigingsinformatie enerzijds en het afhandelen van incidenten anderzijds.

Het Cyber Threat Research & Intelligence Sharing-team levert sinds 2018 verschillende diensten. Het controleert dagelijks uiteenlopende bronnen, verzamelt en ordent informatie die nuttig kan zijn om potentiële slachtoffers te waarschuwen en voert diepgaande cyber threat & intelligence analyses uit, waarover het rapporteert.

CyTRIS stuurt ook spear warnings (individuele waarschuwingen) naar organisaties waarbij een bepaalde kwetsbaarheid is ontdekt op de IT-infrastructuur, waar malware is aangetroffen of van wie gestolen inloggegevens zijn gevonden. Het is ook verantwoordelijk voor het eerste contact met organisaties die een incident melden bij het CCB, om het incident te kunnen onderzoeken.

BePhish en het Belgian Anti-Phishing Shield

Phishing was van bij de start een belangrijk aandachtspunt en blijft tot vandaag een van de meest voorkomende vormen van cybercriminaliteit, met grote impact. De klunzige, eenvoudig uitgewerkte e-mails zijn door de jaren heen uitgegroeid tot zeer realistische berichten via alle mogelijke communicatiekanalen: e-mail, sms, WhatsApp en sociale media.

Het werd snel duidelijk dat het traditionele reactieve model (ingrijpen na een melding van een slachtoffer) niet volstond. Daarom ontwikkelde het CCB het project BePhish. Sinds 2019 kunnen burgers 24/7 melding maken van verdachte communicaties via verdacht@safeonweb.be. Achter die mailbox gaat een geautomatiseerd analyse- en blokkeersysteem schuil. Het verwerkt gemiddeld 25.000 e-mails per dag.

Als gevolg van dit initiatief beschikte het centrum over een grote hoeveelheid info over malafide websites. Om deze criminelen ook actief te bestrijden, ontstond een tweede initiatief: het Belgian Anti-Phising Shield (BAPS), een extra verdedigingsmuur tegen deze malafide pagina's op het internet. Bezoekers die op zo'n link klikken, worden immers omgeleid en doorgestuurd naar een waarschuwingspagina van het CCB.

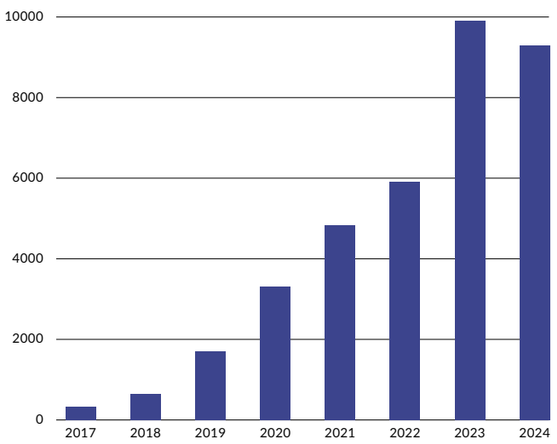
BAPS waarschuwingspagina

Om dit idee technisch te realiseren, was een doorgedreven samenwerking met de internet service-providers nodig. Dat ligt echter gevoelig, omdat het omleiden van een URL juridisch aanvechtbaar is. Proximus stapte als eerste provider in het verhaal, vrij snel gevolgd door Telenet. Intussen nemen meer dan 100 providers deel aan het BAPS. De doorverwijspagina werd in 2024 liefst 240 miljoen keer geactiveerd.

Het Anti-Phishing Shield verhoogde de reactietijd tegen malafide websites van dagen naar minuten. De effectiviteit ligt niet zozeer in zijn technologische inventiviteit, maar wel in het feit dat burgers zich sinds de start betrokken voelen en nog altijd massaal berichten met verdachte URL's melden. Via een doorgedreven spamfilter die uit deze filosofie groeide, voorkomt het CCB samen met de providers ook dat malafide mails in de mailbox van burgers en bedrijven terechtkomen.

De tandem BePhish en BAPS is een unieke bijdrage aan de collectieve veiligheid: dankzij alle meldingen kan het CCB snel trends detecteren en via Safeonweb waarschuwingen verspreiden. Het controversiële idee, namelijk een actief overheidsingrijpen op het internetverkeer, groeide uit tot een van de stokpaardjes van het CCB. Het beperken van de bewegingsvrijheid in cyberspace gaf meerdere malen aanleiding tot een klacht, maar die werd telkens met succes weerlegd.

Evolutie doorheen de jaren van het aantal mails gerapporteerd aan verdacht@safeonweb.be



op de Y-as: Aantal mails x1000

Het 'NotPetya'-incident en de Spear Warnings

Op 27 juni 2017 ontvangt het CCB berichten uit diverse Europese landen over een golf van cyberincidenten. De aanvallen lijken op ransomware, maar betreffen eigenlijk Not Petya-wiper malware. Het doel was met andere woorden niet om losgeld te innen in ruil voor vrijgave van de data, maar wel om vanop afstand systemen permanent onbruikbaar te maken. Het ging om een wereldwijde cyberaanval, voornamelijk gericht op bedrijven met activiteiten in Oekraïne.

De aanvallers hadden een systeem ontwikkeld dat zich razendsnel verder kon verspreiden via diverse netwerken. Een van de bedrijven die de grootste impact hebben ervaren, was het Deense logistieke concern Maersk. Het moest zijn volledige IT-infrastructuur platleggen om de aanval te stoppen. Medewerkers dienden noodgedwongen terug te vallen op pen en papier.

In ons land moest het CCB bijzonder snel schakelen om het incident op te volgen. 'NotPetya' vormde mee de aanleiding om de zogenaamde Spear Warnings te ontwikkelen: wanneer er kwetsbaarheden op een IT-netwerk worden geïdentificeerd, is het CCB gemachtigd om het IP-adres van de organisatie in kwestie te identificeren. Hier kan het bedrijven en andere organisaties vervolgens waarschuwen over die kwetsbaarheden. Deze proactieve houding helpt dus om cyberincidenten te voorkomen.

NotPetya betekende het begin voor de Spear Warnings.

Graduele uitbreiding Early Warning System

Om sneller én gerichter te kunnen reageren op digitale bedreigingen, zette het centrum vanaf 2018 in op de verdere ontwikkeling van zijn Early Warning System (EWS). Dit waarschuwingssysteem vormt sindsdien de technologische radar van België op het vlak van cybersecurity.

In deze periode werd het systeem gradueel uitgebreid, zowel qua reikwijdte als in diepgang. Het CCB ontwikkelde ook een methodiek om meldingen te rangschikken op basis van risico en urgentie, wat de effectiviteit en het vertrouwen in het systeem versterkte. Het Early Warning System is intussen uitgegroeid tot een essentieel instrument voor de Belgische cyberbeveiliging arsenaal.

Quarterly Cyber Threat Report

Naast real-time dreigingsinformatie ervoer het CCB de nood aan een structureel rapportagemodel dat inzicht gaf in trends, kwetsbaarheden en opkomende risico's. Zo ontstond het Quarterly Cyber Threat Report (QCTR) – een kwartaalrapport waarmee het centrum sinds 2019 de cyberdreigingscontext in België transparant deelt met cruciale stakeholders in kritieke sectoren, beleidsmakers en andere betrokken instanties. Door hen te informeren over het bredere dreigingslandschap, helpt het CCB hen om hun eigen risicobeheer te versterken.

Elk QCTR bevat inzichten over dominante aanvalsvectoren, nieuwe kwetsbaarheden en sectorale trends (zoals verhoogde activiteit in de zorgsector of bij gemeentebesturen), en duiding bij grotere incidenten. Het doel is informatiedeling. Het CCB verzamelt hiervoor gegevens uit incidentmeldingen, internationale threat feeds en input van partners binnen het ecosysteem – waaronder commerciële partners en CSIRTs.

NIS1-richtlijn

Tussen 2017 en 2020 speelde het CCB een sleutelrol in de omzetting van de eerste Europese richtlijn inzake netwerk- en informatieveiligheid (NIS1). Deze richtlijn, formeel goedgekeurd in juli 2016, betekende een belangrijke stap vooruit om de cyberveiligheid binnen de Europese Unie te verhogen. Het doel was de digitale weerbaarheid van kritieke infrastructuren en essentiële diensten te versterken, grensoverschrijdende samenwerking te bevorderen en de stabiliteit van de digitale interne markt te waarborgen.

Al vanaf de voorbereidende fase volgde het CCB dit regulerende traject op de voet. Zodra duidelijk werd dat de NIS-richtlijn er zou komen, ondernam het centrum stappen om het Belgische regelgevend kader in overeenstemming te brengen met de aankomende Europese eisen. Om deze complexe opdracht aan te kunnen, versterkte het CCB zijn juridische en technische capaciteit.

Naast de actieve vertegenwoordiging van België in de Europese NIS-samenwerkingsgroep en het CSIRT-netwerk, stond het CCB in voor de voorbereiding van de nationale wetgeving. Dit traject leidde uiteindelijk tot de NIS-wet van 7 april 2019, die het juridische kader vastlegde voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, en het Koninklijk Besluit dat de uitvoering ervan regelde.

Ook de operationele implementatie van NIS1 lag in handen van het CCB. De organisatie zette het Cyber Security Sectorale Autoriteiten Platform (CySSAP) op, een structuur waarin de betrokken overheidsdiensten en sectorale autoriteiten (zoals de FSMA voor de financiële sector of het BIPT voor post en telecommunicatie) op regelmatige basis worden gebrieft, geadviseerd en gecoördineerd.

Toch was België pas de laatste EU-lidstaat die de NIS1-richtlijn implementeerde. Vooral de versnippering van de beslissingsmacht over de verschillende stakeholders bleek problematisch. Elke sector moest immers afzonderlijk inschatten wat de impact van NIS1 zou zijn. Omdat de uitdagingen nieuw en moeilijk te doorgronden bleken, gingen sommige sectoren op de rem staan.

Last but not least werkte het CCB een meldingspunt uit voor cybersecurity-incidenten, conform de NIS-richtlijn. De implementatie van NIS1 betekende voor het centrum niet alleen een bevestiging van zijn institutionele rol, maar ook een nieuwe katalysator voor de verdere uitbouw.

COVID-19 en cyberrisico's voor het zorgsysteem

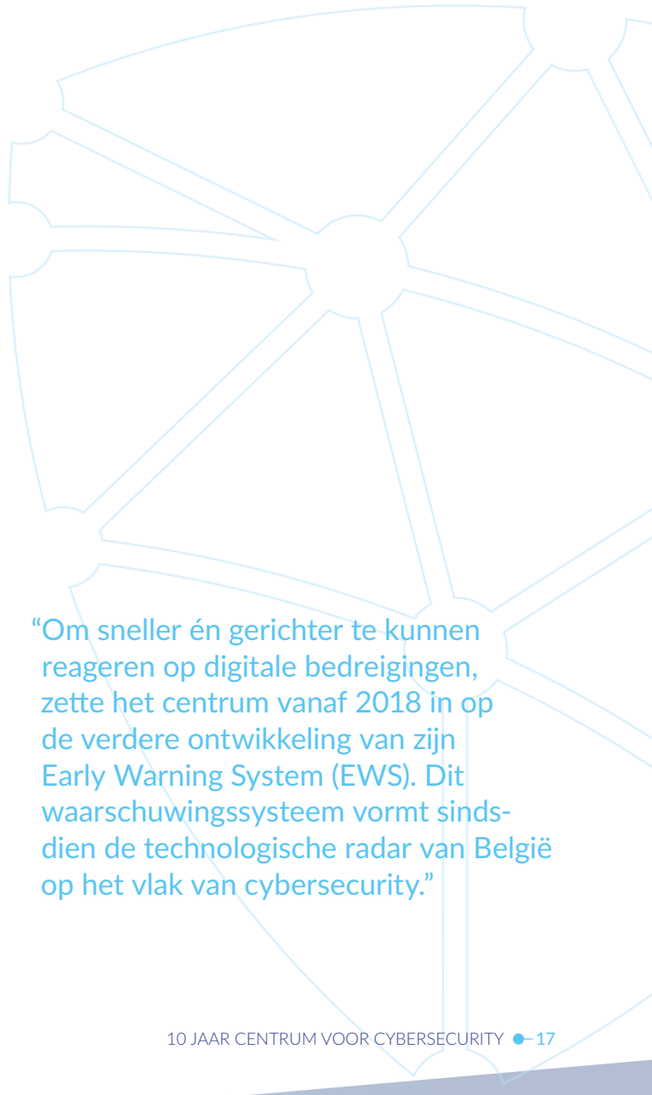
Als gevolg van NIS1 moest elke sector een lijst maken van de aanbieders van essentiële diensten. Binnen de gezondheidssector werd in 2019 besloten dat de sector geen dergelijke aanbieders had. Op die manier hoefde de zorg niet aan de verplichtingen van de NIS-wetgeving te voldoen. Het resultaat was dat de sector ook niet werd opgenomen op de prioritaire lijst van het CCB.

Het uitbreken van de COVID-19-pandemie in het voorjaar van 2020 veranderde de situatie echter compleet. Ziekenhuizen behoorden plots tot de favoriete doelwitten van cybercriminelen, die het zorgsysteem verder onder druk wilden zetten en geïnteresseerd waren in de data.

Het cybersecurity ecosysteem bood op dat moment collectief bijstand. Het CCB steunde een 'coalition of the willing' van cybersecurity en IT-dienstverleners, consultancybedrijven en zelfstandige experts die bereid waren om gratis ondersteuning te geven aan ziekenhuizen. Via de website wehelpourhospitals.be konden zorgvoorzieningen met deze partners in contact komen voor advies, een risicoanalyse, incident response, enzovoort.

Deze periode maakte pijnlijk duidelijk dat de verhouding tussen cyberwereld en sectorale overheden moest worden herzien. Een hertekening, waarin het CCB de centrale rol van toezicht toebedeeld kreeg, leidde tot een veel performanter model. Dat zou later ook blijken bij de implementatie van NIS2: ondanks het feit dat het aantal betrokken kritische sectoren steeg van 7 naar 18, zou België de eerste EU-lidstaat zijn om de richtlijn in nationale wetgeving om te zetten.

Doordat het centrum zijn rol ten volle vervulde, met een efficiënte inzet van middelen en een gewaardeerd aanbod van praktische dienstverlening en ondersteuning, groeide in deze periode bij beleidsmakers het besef dat het CCB essentieel was voor het beveiligingsecosysteem in België. Bovendien ontwikkelde het centrum in deze periode ook het gebruik om haar strategie en actieplannen te koppelen aan duidelijke projectbudgetten. Deze grote mate van transparantie over de werking en financiering blijft tot vandaag intact.



"Om sneller én gerichter te kunnen reageren op digitale bedreigingen, zette het centrum vanaf 2018 in op de verdere ontwikkeling van zijn Early Warning System (EWS). Dit waarschuwingssysteem vormt sindsdien de technologische radar van België op het vlak van cybersecurity."

2020-2024

DE GROEI

Ondanks alle geleverde inspanningen bleef het aantal incidenten dat aan het CCB werd gemeld nog steeds sterk toenemen. Onder meer ransomware kreeg een steeds grotere impact, zowel in de publieke als privésector. Wereldwijd wordt cybercriminaliteit tot vandaag beschouwd als het grootste risico op ernstige financiële schade. De opdracht van het CCB blijft dan ook brandend actueel.

In augustus 2020 liep het mandaat van directeur Miguel De Bruycker en adjunct-directeur Phédra Clouner af. De federale regering besliste om hun mandaat te verlengen met vijf jaar. Het CCB kreeg daarbij als opdracht mee om, naast het voortzetten van zijn bestaande opdrachten, zijn visie en strategie te laten evolueren met de toenemende dreiging in het cyberlandschap.

De Nationale Cybersecuritystrategie 2.0

Om de missie waar te maken, werd binnen het CCB de Nationale Cybersecuritystrategie 2.0 uitgeschreven. Die omvatte zes strategische doelstellingen:

- versterken van de digitale omgeving en het vertrouwen in de digitale omgeving vergroten
- gebruikers en beheerders van computers en netwerken wapenen
- organisaties van vitaal belang beschermen tegen alle cyberdreigingen
- reageren op de cyberdreiging
- publieke, private en academische samenwerkingen verbeteren
- een duidelijk internationaal engagement opnemen

Directeur-generaal Miguel De Bruycker gaf volgende toelichting bij de nieuwe strategie:

"In elke samenleving heb je afdwingbare regels nodig en dat is in cyberspace niet anders. We moeten dus een nieuw evenwicht vinden tussen een totaal open, vrij en anoniem internet en een betrouwbaar internet waarin afdwingbare regels en nationale wetten blijven gelden. Dit alles mag echter géén afbreuk doen aan de mogelijkheden om vrij en anoniem te communiceren.

Een evenwicht tussen een totaal open en vrije cyberspace en een internet waarin bepaalde rechtsregels toch kunnen afgedwongen worden, is naar mijn mening zeker mogelijk. 3 concepten kunnen de cybersecurity op middellange en lange termijn significant verbeteren: Trusted Sender, Trusted Publisher & Spear Warning.

Zo is het bijvoorbeeld mogelijk om er op Europees niveau voor te zorgen dat je een markering krijgt als je op een website komt waar geen nationaal geregistreerde organisatie of entiteit mee gelinkt is.

Prioritair moet de Belgische implementatie van de EU CybersecurityAct gerealiseerd worden zodat ons land tegen juni 2021 de verplichte National CybersecurityCertification Authority heeft. De noodzakelijke middelen hiervoor zijn berekend. Mits een politieke beslissing kan het met de FOD Economie uitgewerkte plan worden uitgevoerd."

De nieuwe strategie werd goedgekeurd door de regering in 2021. Nadat het CCB in zijn eerste vijf jaar het pad had geëffend door samenwerkingsverbanden te creëren en door de coördinatie rond cybersecurity in ons land te verbeteren, en nadat het de fundamenten voor een meer geïntegreerde aanpak van de beveiliging had gelegd, was het doel om het aanbod aan diensten verder uit te bouwen en nog meer in te spelen op concrete noden en dreigingen.

Als uitdrukkelijke ambitie schoof het directieduo naar voren om van België één van de minst cyberkwetsbare landen van de EU te maken. Alle acties die in deze periode werden uitgerold, kaderden in deze doelstelling. Bovendien kreeg de organisatie een aantal bijzondere verantwoordelijkheden toegewezen, waardoor het zijn coördinerende rol nog beter kon gaan vervullen.

Budget en team groeien

Het CCB telde begin 2020 ongeveer 50 medewerkers en een jaarlijks werkingsbudget van ongeveer 15 miljoen euro. Als gevolg van de Cyberstrategie

2.0 en de Europese verplichting om een National Cybersecurity Certification Authority (NCCA) op te richten, werd een groei vooropgesteld naar 80 medewerkers en een budget van ongeveer 36 miljoen euro per jaar.

National Cybersecurity Certification Authority

De Europese Unie legde zich toe op heel wat regelgevend werk om de cyberveiligheid te verhogen. Zo werd in 2019 de Cybersecurity Act aangenomen, die de basis legde voor een gemeenschappelijke certificering van ICT-producten, -diensten en -processen. Daarmee wilde de EU de cyberweerbaarheid van alle lidstaten verhogen en via gemeenschappelijke standaarden de kwaliteit van en het vertrouwen in de cyberveilige producten versterken.

In elke lidstaat moest voortaan een Nationale Cybersecurity Certification Authority (NCCA) toezien op de certificering en bedrijven erbij begeleiden. De autoriteit heeft ook het mandaat om richtlijnen voor certificering op nationaal niveau uit te geven. In België werd die taak toegewezen aan het CCB, dat haar rol versterkte en competenties uitbreidde.

De NCCA houdt toezicht op de certificering en controleert de naleving van de certificaten die zijn afgegeven door Conformiteitsbeoordelingsinstanties (CABs). Het kan ook worden ingeschakeld bij klachten over of misbruik van de certificering van producten. De NCCA heeft ook de bevoegdheid om op te treden om de naleving van de regelgeving te garanderen.

Nationaal cybersecurity Coördinatiecentrum voor België (NCC-BE) (2021).

Nationaal Coördinatie-centrum voor Cybersecurity

Een ander uitvloeisel van Europese initiatieven was de oprichting van het Nationaal cybersecurity Coördinatiecentrum voor België (NCC-BE) in 2021. De EU wil de middelen die ze ter beschikking stelt voor onderzoek en innovatie in het domein van cybersecurity, op een meer gecoördineerde manier besteden. De bedoeling is om de nationale prioriteiten en noden te integreren in een overkoepelende Europese aanpak. Tegelijkertijd wil de EU onderzoekers en innovatieve bedrijven beter informeren over de beschikbare financiële ondersteuning zodat dit leidt tot meer grensoverschrijdende projecten. Het NCC-BE stimuleert dialoog tussen bedrijven, academici, onderzoekers en de overheid. Het stemt het beleid in onderzoek, ontwikkeling en innovatie op elkaar af en werkt mee aan de realisatie van de Belgische Cybersecurity Strategie. Het NCC-BE koppelt bestaande en toekomstige initiatieven in cybersecurity, creëert synergieën en ondersteunt educatieve programma's. Daarenboven waakt het NCC-BE erover dat alle regio's, gemeenschappen en de federale overheid de krachten bundelen voor een uniforme aanpak van cyberdreigingen. Bovendien ondersteunt het NCC-BE organisaties bij het verkrijgen van toegang tot EU-financiering en coördineert het strategische investeringen.

Op Europees niveau vertegenwoordigt het NCC-BE België en zorgt ervoor dat de cybersecurity-belangen van de Belgische overheid, industrie en academici altijd worden gehoord.

Onder leiding van het European Cybersecurity Competence Centre (ECCC) werkt het NCC-BE samen met een netwerk van 29 nationale coördinatiecentra. Dit initiatief versterkt de innovatie op het gebied van cybersecurity, ondersteunt het industriebeleid en draagt bij tot de technologische soevereiniteit van Europa.

Voorbereidingen NIS2

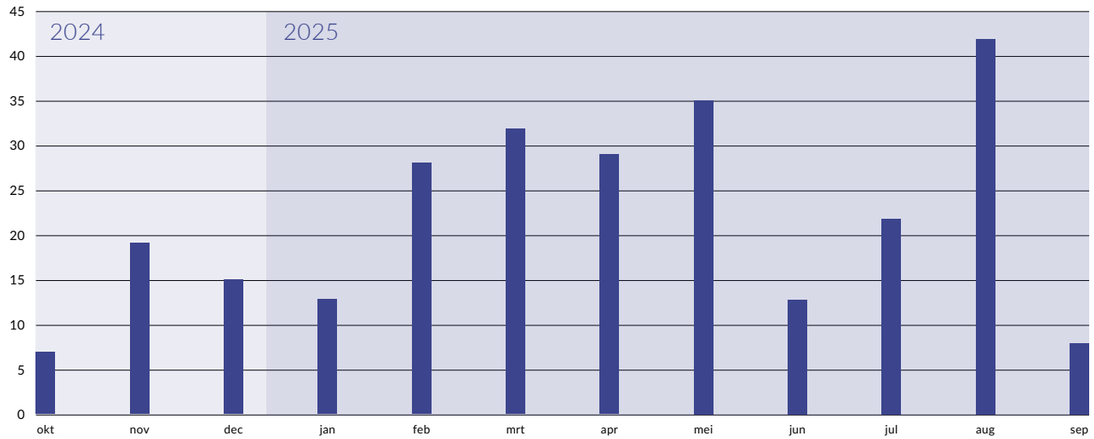
In december 2020 kondigde de Europese Commissie aan dat ze een NIS2-richtlijn zou voorbereiden, als opvolger en verdere verfijning van NIS1. De bedoeling was uiteraard om de cyberveiligheid verder te verhogen, maar ook om de aanpak binnen de EU nog meer te stroomlijnen. NIS1 had de lidstaten immers een relatieve vrijheid gelaten om de Europese vereisten concreet invulling te geven. Dat leidde echter tot uiteenlopende interpretaties en verschillen in de implementatie tussen lidstaten. Dat euvel zou met NIS2 verholpen worden.

Een van de belangrijkste wijzigingen ten opzichte van zijn voorganger, was de uitbreiding van het aantal betrokken sectoren die onderhevig zouden zijn aan de verplichtingen van NIS2. In België vielen ruim 100 entiteiten uit 7 sectoren waaronder energie, transport, gezondheidzorg, digitale infrastructuur en publieke diensten binnen het toepassingsgebied van NIS1. Na de implementatie zou NIS2 van toepassing zijn op meer dan 4.000 entiteiten uit 18 sectoren.

Het CCB nam op Europees niveau deel aan het overleg over de invulling van de NIS2 regelgeving. In eigen land werd het parlementaire werk (de omzetting van de Europese directieve in Belgische wetgeving) voorbereid samen met zowel de administraties, het CySSAP-forum (waarin de sectorale overheden vertegenwoordigd zijn) en het politieke niveau.

De NIS2-wet werd in België van kracht in oktober 2024. Dankzij de vroegtijdig opgestarte besprekingen en voorbereidingen, kon het CCB vlot zijn aanpak voor NIS2 opschalen: het zou uitgroeien tot het centrale orgaan voor de opvolging en controle op de naleving van NIS2, in nauwe samenwerking met de sectorale autoriteiten.

NIS2 meldingen van oktober 2024 tot september 2025



Hack the Government, het allereerste ethische hackingevenement (2024).

Het CCB realiseerde een registratietool voor NIS2-entiteiten via het bestaande platform Safeonweb@work en bouwde een pragmatisch systeem uit voor incidentnotificatie. De nieuwe richtlijn legde organisaties immers op om een significant incident te melden bij het centrum meteen nadat het werd ontdekt.

Om organisaties te ondersteunen om te voldoen aan de NIS2-vereisten, werd het CyberFundamentals framework (CyFun®) uitgewerkt, een praktische leidraad voor het nemen van de cybersecurity-maatregelen, gestructureerd in verschillende niveaus, afgestemd op de maturiteit van de organisatie. Op die manier is het framework ook relevant voor ondernemingen en organisaties die buiten de NIS2-sectoren vallen. Het publieke debat over NIS2 leidde bij het Belgische bedrijfsleven sowieso tot een sterk verhoogd bewustzijn over cyberveiligheid.

"Als uitdrukkelijke ambitie schoof het directieduo naar voren om van België één van de minst cyberkwetsbare landen van de EU te maken. Alle acties die in deze periode werden uitgerold, kaderden in deze doelstelling. Bovendien kreeg de organisatie een aantal bijzondere verantwoordelijkheden toegewezen, waardoor het zijn coördinerende rol nog beter kon gaan vervullen."

Gecoördineerde bekendmaking van kwetsbaarheden

In België is sinds 2023 een wettelijke procedure voor de melding van kwetsbaarheden van kracht. Hierdoor moet het CCB meldingen ontvangen van onderzoekers over potentiële kwetsbaarheden die onder Belgisch recht vallen. De gecoördineerde bekendmaking van kwetsbaarheden (CVD) is een proces waarbij onderzoekers, bedrijven en overheden op een gestructureerde en veilige manier omgaan met de ontdekking en de rapportering van beveiligingsproblemen in ICT-systemen, -producten of -diensten. Het doel is om kwetsbaarheden tijdig en verantwoord te verhelpen, zonder dat ze vroegtijdig worden misbruikt.

In november 2024 organiseerde het CCB *Hack the Government*, het allereerste ethische hackingevenement. Hiermee toont het aan dat ethische hackers kunnen helpen om België cyberveiliger te maken. Dit nooit eerder geziene initiatief bracht de gemeenschap van ethische hackers samen om kwetsbaarheden in overheidswebsites en -systemen te identificeren.

Stop Phishing

De inspanningen om criminaliteit via phishing te voorkomen, binnen de globale aanpak van het Belgian Anti-Phishing Shield (BAPS), werden onverminderd voortgezet. In 2020 werd een nieuw project "Stop Phishing" boven de doopvont gehouden. Het doel was om te voorkomen dat e-mails of sms'en met een kwaadaardige link bij burgers en bedrijven zouden terechtkomen. Ze werden onderschept nog voor ze in de e-mailbox of sms-map terechtkwamen.

Dit project werd een succesvol publiek-privaat partnership met de betrokken operatoren, dat expliciete steun kreeg van de regering. Het vormde een nieuwe stap in de proactieve en preventieve aanpak van het BAPS. De overheid financierde via het CCB een deel van de software die gebruikt wordt door de deelnemende serviceproviders.

PhishNemo

Een uitbreiding op het BAPS-project is PhishNemo. Dit initiatief werd oorspronkelijk uitgewerkt door de Federale Gerechtelijke Politie (FGP) van Limburg, en is intussen uitgegroeid tot een samenwerking tussen de FGP en het CCB. Terwijl het Belgian Anti-Phishing Shield zich vooral baseert op meldingen van burgers, gaat PhishNemo sinds 2023 proactief op zoek naar verdachte domeinnamen die mogelijk in phishingcampagnes zullen worden gebruikt.

Dat doet het systeem door de nieuwe domeinnamen grondig te screenen. Er wordt gezocht naar sporen van gekende phishingtools – zogenaamde "vingerafdrukken". Dankzij deze aanpak kunnen malafide domeinen worden opgespoord nog voor de eerste phishingmail verzonden wordt. De vroegtijdig opgespoorde domeinen worden meteen opgenomen in het BAPS-systeem, zodat ze via de samenwerking met internetproviders direct omgeleid kunnen worden.

Door dit systeem over te nemen van de Limburgse FGP kon het project verder doorgroeien. Het CCB werkt hiervoor samen met privé-partners, die de IT-systemen onderhouden. Daardoor kan PhishNemo een actieve bijdrage leveren aan het Belgian Anti-Phishing Shield.

Hacktivisme piekt na inval Rusland in Oekraïne

In februari 2022 viel Rusland Oekraïne binnen, het begin van een lang aanslepende oorlog. Hoewel cybercriminelen vooral geïnteresseerd zijn in financieel gewin, bleek er sindsdien een nauw verband tussen geopolitiek en cyberaanvallen. Het CCB kreeg door deze verschuivingen in het geopolitieke landschap een plaats als permanent lid van de Nationale Veiligheidsraad.

Deze permanente toetreding tot het vaste overleg van inlichtingen- en veiligheidsdiensten was voor de organisatie een zeer belangrijke mijlpaal. Voortaan was het CCB immers niet meer weg te denken uit de beveiligingsarchitectuur van het land. Het gaf de organisatie ook toegang tot extra werkingsmiddelen uit de provisie Oekraïne.

Ook in de praktijk bleek het de logische keuze: er verschenen hoe langer, hoe meer hacktivistische groepen op het toneel. Hun favoriete modus operandi omvat DDoS-aanvallen (Distributed Denial of Service), waarbij websites overbelast geraken en hack-and-leak-operaties. Sinds het uitbreken van de oorlog in Oekraïne wordt ook een toename van ransomware-aanvallen tegen gemeenten en overheidsdiensten vastgesteld in diverse Europese landen, waaronder België.

Gezien de geopolitieke context werd in de aanloop naar de Europese, nationale en regionale verkiezingen van juni 2024 een verhoogde waakzaamheid aan de dag gelegd voor cybersecurity gebeurtenissen of verhoogde dreigingen. Zowel de federale, regionale als lokale overheden konden rekenen op advies en technische ondersteuning van het centrum. Tijdens de verkiezingsweekends van juni en oktober 2024 werd voorzien in een continue monitoring en hield het CCB ook een emergency team paraat.

Ook bij voorgaande verkiezingsrondes voerde het centrum overigens al een veiligheidsaudit uit. Die vormde de basis voor een reeks aanbevelingen, wat leidde tot een significante verhoging van de beveiliging van de IT-systemen voor de verkiezingen. Mede daardoor werden verkiezingen in België nog nooit verstoord door cyberaanvallen.

ACTIEVE CYBERBESCHERMING, EEN PROACTIEVE VISIE

Digitalisering opent ongeziene mogelijkheden voor burgers, bedrijven en overheden. Maar hoe meer we digitaliseren, hoe groter de risico's. Cybercriminaliteit evolueert razendsnel, aanvallen worden geraffineerder en de impact op onze samenleving neemt almaar toe. Om die dreiging het hoofd te bieden, is het beveiligen van de digitale omgeving een essentiële voorwaarde.

Sinds zijn oprichting ziet het CCB het als zijn opdracht om kwetsbaarheden (zowel menselijke als technische) zichtbaar te maken en er actief op in te grijpen. In plaats van pas te reageren na een incident, zet het centrum in op preventie, snelle detectie en doelgerichte respons.

In 2024 kreeg die proactieve aanpak een overkoepelende naam: **Active Cyber Protection (ACP)**. Dit concept omvat een reeks lopende en bijkomende projecten die de cyberveiligheid versterken nog voor een incident kan plaatsvinden.

Op aandringen van het CCB werd ACP opgenomen in de Europese NIS2-richtlijn, die vanaf 2024 van kracht werd in België. Die regelgeving verplicht ondernemingen in een hele reeks essentiële sectoren om bijkomende beveiligingsprincipes te hanteren en systemen voor risicomanagement te implementeren.

De NIS2-richtlijn vraagt dus een actievere houding van alle lidstaten en legt Actieve Cyberbescherming ook op als wettelijke vereiste. Aangezien België op dat vlak een voortrekkersrol wil spelen, vormt ACP een centrale pijler van onze nationale cyberstrategie. Het CCB maakt dit abstracte begrip concreet met een aanpak die proactief, op maat, geautomatiseerd én participatief is:

- **Proactief**: niet wachten tot een incident zich voordoet, maar dreigingen detecteren en aanpakken voor ze schade veroorzaken.
- **Op maat**: geen one-size-fits-all. Communicatie en respons worden afgestemd op de noden van specifieke organisaties en sectoren.
- **Geautomatiseerd**: snelheid is cruciaal. Automatisatie laat toe om sneller te reageren én compenseert het nijpende tekort aan cybersecurity-experten.
- **Participatief**: cyberveiligheid is een gedeelde verantwoordelijkheid. Medewerkers, partners en burgers moeten actief worden betrokken.

Deze visie krijgt vorm via vijf strategische pijlers. Deze pijlers vormen een flexibel kader dat voortdurend evolueert, in functie van de steeds veranderende tactieken van cybercriminelen.

PIJLER I: BEWUSTZIJN VERGROTEN DOOR MENSEN TE BETREKKEN

Een sterk cybersecuritybeleid begint bij het grote publiek en het vergroten van zijn bewustzijn. Dit is van bij het begin het uitgangspunt geweest van het CCB. Door verdachte berichten te signaleren, kunnen burgers actief bijdragen aan het verhogen van het cyberveiligheidsniveau van het land. De initiatieven onder de noemer Safeonweb dienen om burgers én bedrijven te wapenen tegen digitale dreigingen. Dit vormt onmiskenbaar de basis van de proactieve visie, en bij uitbreiding de filosofie van het CCB.

Voor burgers: Safeonweb@home

Safeonweb@home informeert burgers via een website, campagnes en sociale media over actuele gevaren. De Safeonweb-app speelt hierin een centrale rol: ze waarschuwt gebruikers tijdig voor phishingaanvallen en geeft toegankelijke beveiligingstips.

Een ander succesverhaal dat zich toespitst op burgers is suspicious@safeonweb.be, een e-mailadres in vier talen, waar burgers verdachte mails kunnen melden. In 2023 alleen al kwamen er bijna 10 miljoen meldingen binnen. Een indrukwekkend cijfer dat aantoont hoe waardevol hun bijdrage is in de strijd tegen cybercriminaliteit.

Safeonweb is bekend bij 82% van de bevolking.

Voor bedrijven: Safeonweb@work

Sinds 2023 is er ook Safeonweb@work, een platform op maat van Belgische ondernemingen met duidelijke, bruikbare aanbevelingen om cyberveiligheid in het dagelijkse beleid te integreren – zonder zware investeringen of complexe procedures.

Via een online portaal kunnen bedrijven hun domeinen registreren en automatisch waarschuwingen ontvangen over kwetsbaarheden in hun IT-infrastructuur. Het platform bevat daarnaast tools voor zelfevaluatie, basisrichtlijnen en best practices, zodat organisaties op eigen tempo hun beveiligingsniveau kunnen versterken. Het CCB ondersteunt zo het verhogen van de cybermaturiteit van het professionele landschap.

Safeonweb@work 2024

PIJLER II: CRIMINELE INFRASTRUCTUUR OPSPOREN EN UITSCHAKELEN

De tweede pijler richt op de kern van cyberveiligheid: de infrastructuur waarmee criminelen aanvallen uitvoeren. Denk aan phishingwebsites of malafide servers. Met het project **Belgian Anti-Phishing Shield (BAPS)** pakt het CCB deze praktijken aan bij de bron.

Samen met de Belgische internetproviders worden schadelijke websites automatisch gedetecteerd en uitgeschakeld, door de gebruiker onmiddellijk om te leiden naar een veilige landingspagina. Op die manier worden per dag zo'n 100.000 Belgen beschermd tegen potentieel schadelijke websites.

De snelheid en automatisatie vormen de kracht van het systeem. Malafide URL's worden continu bijgewerkt en rechtstreeks geïntegreerd in de DNS-systemen van providers. Zo worden bedreigingen in real time onderschept, vaak nog voor ze schade kunnen aanrichten. BAPS is daarmee een schoolvoorbeeld van proactieve cyberbescherming: geruisloos op de achtergrond, maar met meetbare impact.

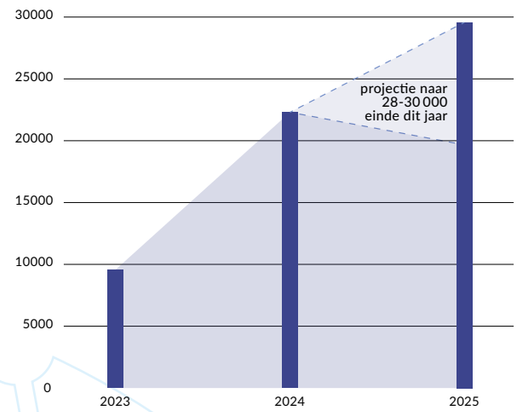
Deze aanpak is ook elders binnen de overheid, de financiële sector en bij politiediensten niet onopgemerkt gebleven. Verschillende organisaties gaven aan dat zij over waardevolle gegevens beschikken binnen hun eigen domein, zoals informatie over frauduleuze webshops of beleggingsfraude. Zij hebben echter niet de mogelijkheid om op een geautomatiseerde manier domeinen op nationaal niveau om te leiden.

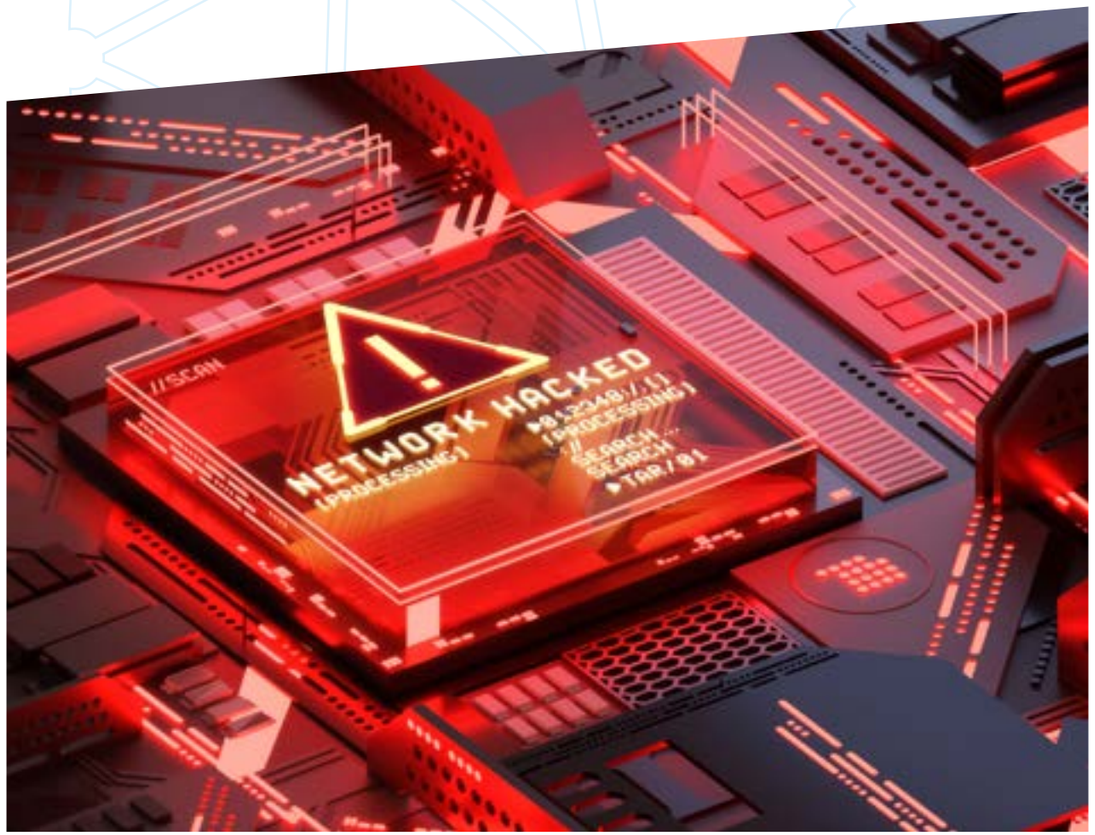
Daarom heeft het CCB het concept van trusted partners uitgewerkt: een bevoorrechte toegang tot het BAPS-systeem voor zorgvuldig geselecteerde partners. De partners leveren de data aan, het CCB neemt vervolgens de praktische afhandeling op zich om de verdachte domeinen om te leiden via de samenwerking met de internetproviders. Vandaag zijn onder andere de FOD Economie, de FSMA, Itsme en een aantal Belgische banken actief als trusted partner binnen dit systeem.

PIJLER III: HET GERICHT SIGNALEREN VAN DREIGINGEN

Cybercriminelen maken vaak gebruik van spear phishing: gerichte aanvallen op specifieke personen om gevoelige informatie te bemachtigen. Het CCB hanteert eenzelfde aanpak, maar dan in het voordeel van de gebruiker. Met zogenaamde spear warnings informeert het centrum organisaties rechtstreeks over kwetsbaarheden in hun digitale omgeving.

Cijfers evolutie Spear Warnings





Deze aanpak stelt organisaties in staat om snel en gericht actie te ondernemen, nog voor een kwetsbaarheid kan worden uitgebuit. Het bekendste initiatief is het Early Warning System (EWS), een platform dat specifiek gericht is op organisaties met kritische of vitale infrastructuur die onder de verplichtingen van de NIS2-richtlijn vallen.

Via dit portaal staan CCB-analisten in direct contact met deze vitale organisaties. Voor hen is het EWS een extra paar ogen: het monitort digitale signalen, detecteert risico's en stuurt proactief waarschuwingen. Daarnaast krijgen de organisaties ook gepersonaliseerde meldingen over onder meer datalekken, gelekte inloggegevens en onveilige systemen binnen hun infrastructuur.

Deze proactieve werkwijze helpt niet alleen om incidenten te vermijden, maar verhoogt ook het bewustzijn en de reactietijd binnen organisaties.

PIJLER IV: CYBERVEILIGHEID VERANKEREN IN DE ORGANISATIE

Om écht weerbaar en veerkrachtig te worden, moeten organisaties cyberveiligheid opnemen in hun dagelijkse werking. Het CCB ontwikkelde daarom het CyberFundamentals Framework: een praktisch en schaalbaar model dat organisaties helpt om hun digitale bescherming stapsgewijs te versterken. Het raamwerk bestaat uit vier niveaus (Small, Basic, Important en Essential) waarbij elk niveau een set concrete maatregelen omvat. Small geldt daarbij als leidraad voor zeer kleine organisaties die nog geen ervaring hebben met cybersecurity en de allereerste stappen zetten.

De maatregelen uit het CyberFundamentals Framework zijn afgestemd op de meest voorkomende cyberaanvallen en werden gevalideerd aan de hand van CERT-aanvalsprofielen. De effectiviteit van het model is intussen bewezen:

- Het **Basic**-niveau dekt zo'n 82% van de gangbare aanvalstypes.
- Met het **Important**-niveau stijgt dat percentage naar 94%.
- Organisaties die het **Essential**-niveau behalen, beschermen zich zelfs tegen 100% van deze aanvallen.

Het raamwerk is gebaseerd op internationale normen zoals NIST, ISO en IEC, en is toegankelijk voor organisaties van alle groottes. Certificering door een externe instantie is mogelijk, maar geen vereiste.

Met CyberFundamentals wordt cyberveiligheid concreet, meetbaar en haalbaar, zelfs voor kmo's of organisaties zonder IT-afdeling. Het model groeit bovendien mee met de risico's: het is in voortdurende ontwikkeling om relevant te blijven in een snel veranderende digitale wereld.

PIJLER V: HET CREËREN VAN EEN BETROUWBARE OMGEVING

Het internet geeft een zekere vrijheid en met die vrijheid komt ook anonimiteit. Maar uiteraard is die anonimiteit een tweesnijdend zwaard. Enerzijds beschermt ze onze privacy en meningsuiting. Anderzijds opent ze de deur voor misbruik. Net daarom groeit de nood aan meer transparantie en digitale validatie: om het vertrouwen te herstellen en de schaduwzijde van anonimiteit tegen te gaan.

De zoektocht naar dat nieuwe evenwicht tussen anonimiteit en identiteit is geen eenvoudige oefening. In essentie gaat het om een gedragsverandering: burgers moeten wennen aan het idee dat identificatie een vanzelfsprekend onderdeel wordt van hun digitale aanwezigheid. Alleen zo kunnen online activiteiten beter worden toegewezen en dus veiliger worden gemaakt.

"Samen met de Belgische internetproviders worden schadelijke websites automatisch gedetecteerd en uitgeschakeld, door de gebruiker onmiddellijk om te leiden naar een veilige landingspagina. Op die manier worden per dag zo'n 100.000 Belgen beschermd tegen potentieel schadelijke websites."

Om internetgebruikers meer vertrouwen te geven in de partijen met wie ze online in contact komen, ontwikkelde het CCB de Safeonweb-browserextensie. Die toont bij elk websitebezoek een duidelijke kleurcode:

- **Groen** betekent dat de eigenaar van de website gevalideerd en dus betrouwbaar is.
- **Oranje (of amber)** wijst op een onbekende of niet-gevalideerde eigenaar. In dit geval is voorzichtigheid geboden.
- **Rood** duidt op een gekende onveilige of kwaadaardige website die je beter volledig vermijdt en waarmee je best geen gegevens deelt.

De extensie is ontworpen met veiligheid én gebruiksgemak in het achterhoofd. Ze werkt automatisch op de achtergrond en laat in één oogopslag zien of persoonlijke gegevens veilig gedeeld kunnen worden. De surfer/gebruiker krijgt zo meer zekerheid over de veiligheid van de ontvanger met wie hij of zij gegevens wil delen.

Wordt er toch verdachte inhoud op een gevalideerde website ontdekt? Dan verandert de status onmiddellijk, op basis van de eerste melding: van groen naar oranje of zelfs rood. Zo blijft het systeem te allen tijde actueel en betrouwbaar.

CCB VOOR IEDEREEN

SENSIBILISERING: UITDAGING NUMMER 1 BIJ DE START

In de eerste jaren van zijn bestaan botste het Centrum voor CCB op een structurele uitdaging: België kreeg steeds vaker met cyberdreigingen te maken, maar er was bij het brede publiek nog geen bewustzijn. Burgers, bedrijven en zelfs sommige overheidsdiensten onderschatten het risico.

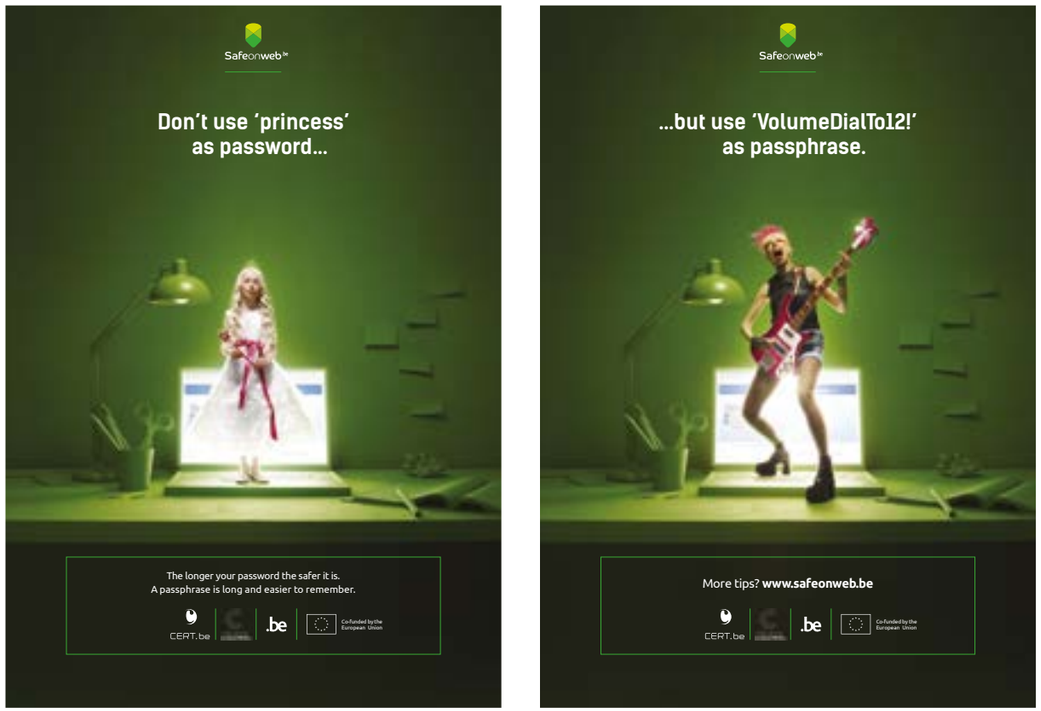
Vanuit het besef dat de sterkte van elke beveiliging finaal bepaald wordt door de menselijke schakel, werd er beslist om niet alleen te investeren in detectie en incident response, maar tegelijk werk te maken van bewustmaking op grote schaal via sensibiliseringscampagnes.

De eerste campagnes richtten zich op concrete risico's: phishingmails, zwakke wachtwoorden, het klikken op verdachte links en de nood om regelmatig software te updaten. Om de impact van deze acties te versterken, zette het CCB in op samenwerking met partners zoals banken en telecombedrijven en de Cyber Security Coalition. Werkgevers en lokale besturen werden specifiek benaderd om de info verder te verspreiden.

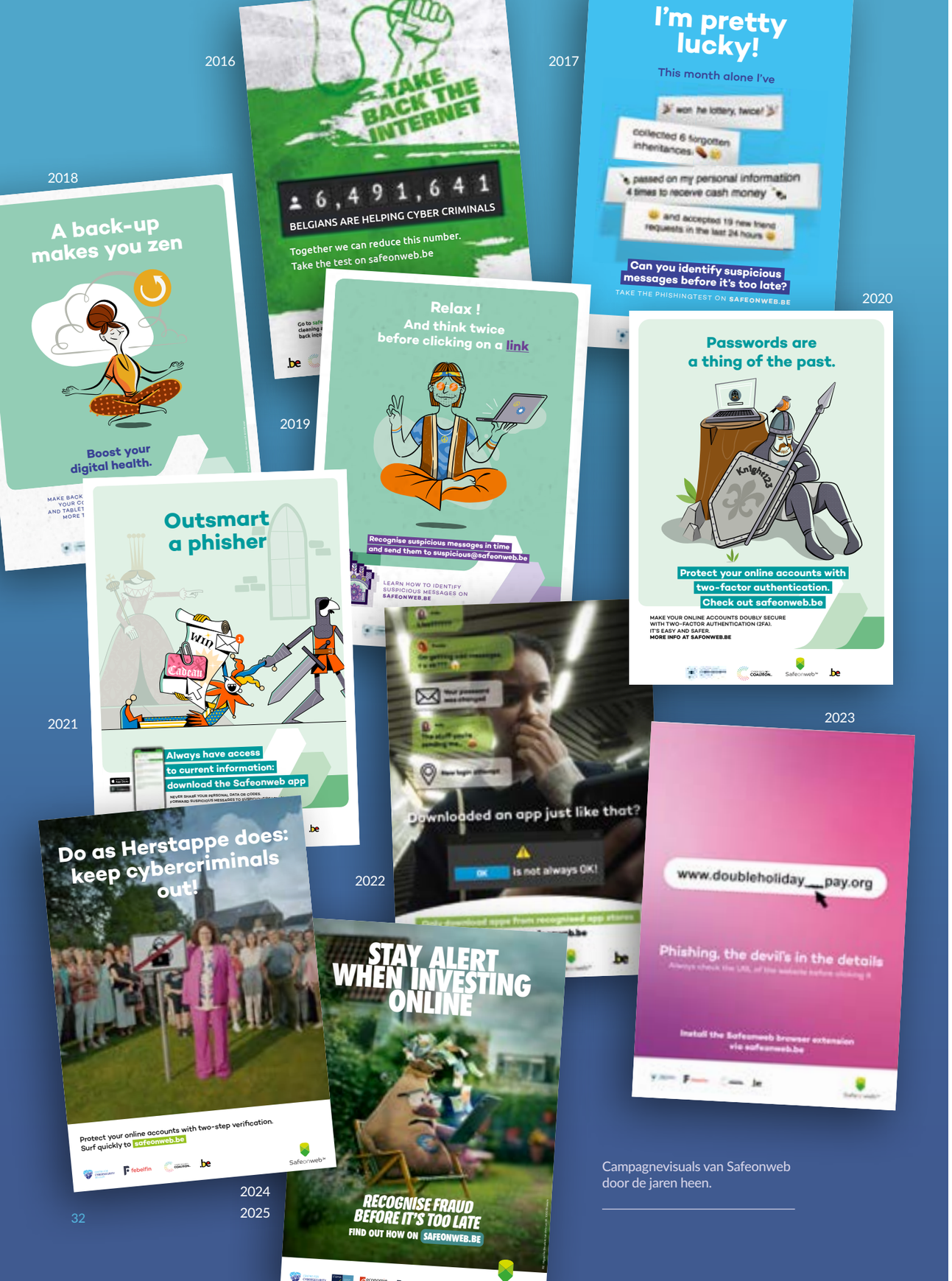
Intern legden deze campagnes de basis voor een nieuwe, multidisciplinaire manier van werken bij het CCB. Communicatiespecialisten en technische teams werkten samen met gedragspsychologen en marketeers om de eerste campagnes te ontwikkelen. Voor een overheidsorganisatie was het een baanbrekende, creatieve manier om sensibilisatie aan te pakken.

Onderdeel van de Europese bewustmaking

Het CCB plant zijn jaarlijkse campagne in de maand oktober. Dat is geen toeval. Oktober werd namelijk uitgeroepen tot European Cybersecurity Month, een jaarlijks terugkerend initiatief van de Europese Commissie en het agentschap ENISA. Die campagne



Safeonweb campagne 2015.



Campagnevisuals van Safeonweb door de jaren heen.

richt zich eveneens op het verhogen van het bewustzijn over cyberveiligheid en het breed informeren van burgers en organisaties over hoe ze zich online beter kunnen beschermen.

Om bijkomend effect te genereren, houdt het CCB ook tussentijdse informatiecampagnes, op momenten dat ook oplichters extra actief zijn: rond de feestdagen, de koopjesperioden of in functie van de actualiteit.

Het centrum haakt ook in op de Safer Internet Day, een globale sensibiliseringsactie die jaarlijks in februari plaatsvindt en specifiek mikt op scholen en jongerenorganisaties.

Ten slotte deelt en versterkt de organisatie graag campagnes van partnerorganisatie rond het thema cyberpreventie.

Partners reiken de hand

Het onderwerp van de jaarlijkse Belgische campagne wordt gekozen op basis van de actualiteit en de belangrijkste trends. De actie verloopt in de drie nationale talen en er worden actoren uit alle sectoren bij betrokken.

Die betrokkenheid vormt één van de sterktes van de sensibiliseringscampagnes: enerzijds heeft het CCB een reeks geprivilegieerde partners zoals de FOD Economie, de FSMA, de Federale Politie, bankenfederatie Febelfin, en de Cyber Security Coalition. Zij fungeren als een klankbord dat in alle stadia van de ontwikkeling van de campagne mee aan het stuur zit en feedback geeft: van de keuze van het onderwerp, over de vertaling en de beeldvorming in de campagne, tot de kracht om de bevolking te overtuigen en te stimuleren om haar gedrag aan te passen. Elke partner brengt zijn knowhow en terreinkennis aan de tafel.

Anderzijds kan het centrum ook rekenen op meer dan 600 organisaties die zich engageren om de materialen te verspreiden. Door het feit dat al die partners de campagne mee uitdragen, geniet ze een impact die veel verder reikt en duurzamer is dan het betalende mediaplan dat jaarlijks wordt voorzien.

Een andere sterkte ligt in de filosofie van de campagnes. De toon is luchtig, eenvoudig en duidelijk. Het opzet is zoveel mogelijk mensen (ook zij die moeite ondervinden met IT of schrik hebben van het online gebeuren) te overtuigen dat ze een verschil kunnen maken. Die positieve bekrachtiging wordt gekoppeld aan een oplossingsgerichte boodschap, waardoor de sensibilisering gepaard gaat met een concrete oplossing die het leven makkelijker maakt, zoals de mailbox verdacht@safeonweb.be. En tot slot wordt gekozen voor herkenbare situaties – zoals de frustratie over lange, ingewikkelde wachtwoorden – die vertaald worden in een humoristisch concept.

Tastbare resultaten

Eén van de belangrijkste resultaten van de afgelopen 10 jaar is dat het overkoepelende platform Safeonweb.be werd uitgebouwd tot herkenbaar merk voor digitale veiligheid in België, met heldere, laagdrempelige informatie en getuigenissen. Uit onderzoek is gebleken dat 82 procent van de bevolking inmiddels safeonweb.be kent als referentie voor cyberveiligheid. De naamsbekendheid van dit merk is het CCB dus ontgroeid.

44% van de Belgen geeft aan dat ze al een verdachte mail of SMS gemeld hebben bij verdacht@safeonweb.be. Het systeem krijgt jaarlijks meer dan 9 miljoen berichten te verwerken. Daarmee is het opzet van het centrum bereikt: de bevolking maximaal betrekken als eerste en belangrijkste doelpubliek om de cyberweerbaarheid te verhogen.

DE BEKRONING

HET EUROPEES VOORZITTERSCHAP 2024

In de eerste helft van 2024 nam België het roterend voorzitterschap van de Raad van de Europese Unie waar. In die periode nam het CCB internationale verantwoordelijkheden op en vervulde het een leidende rol om de Belgische prioriteiten te behartigen. Er werd tijdens het voorzitterschap sterk ingezet op cybersecurity. Het was een unieke kans om België als internationale voortrekker in dit domein op de kaart te zetten.

Eén van de topprioriteiten waren de onderhandelingen tussen de Raad van de Europese Unie (de vergadering van de bevoegde ministers), het Europees Parlement en de Europese Commissie over twee wetgevende initiatieven: de Cyber Solidarity Act en een aanpassing van de Cybersecurity Act (die dateerde uit 2019). De Belgische delegatie, die bestond uit de Permanente Vertegenwoordiging bij de EU en experten van het CCB, slaagde erin om in recordtijd een politiek akkoord te bereiken over beide wetten, nog voor de deadline van de Europese verkiezingen van juni 2024.

De **EU Cybersecurity Act** legde in 2019 de basis voor een Europees certificatiesysteem voor cyberveilige producten, processen en diensten. Op die manier was één certificatie geldig voor de hele unie. Tijdens het Belgische voorzitterschap werd een aanpassing van deze act gestemd. Die betrof onder meer het toevoegen van aanbieders van 'managed security services' (zoals beveiligingsaudits, penetratietests of incident response) aan het certificatiesysteem. Via deze certificatie krijgen klanten van deze dienstverleners meer garanties over de kwaliteit en betrouwbaarheid. Ze kunnen zo ook hun supply chain verifiëren.

De **Cyber Solidarity Act** trad begin 2025 in werking. Ze omvat de oprichting van een Europees waarschuwingssysteem voor grootschalige cyberbedreigingen. Dit systeem brengt de competenties van nationale en grensoverschrijdende centra voor cyberbeveiliging samen met als doel om aanvallen op te sporen, te analyseren en ertegen te reageren. Die uitwisseling van informatie over de grenzen is fundamenteel om met succes grootschalige cybercriminele operaties te kunnen bestrijden met een coherente aanpak.

De EU besliste in deze act eveneens om een gezamenlijk mechanisme voor noodsituaties uit te bouwen. Het gaat om acties in drie domeinen:

- een verhoogde paraatheid om te reageren in essentiële sectoren zoals financiën, energie en gezondheidszorg. Organisaties uit die sectoren moeten getest worden op zwakke punten die kwetsbaar kunnen zijn voor cyberaanvallen.

- de oprichting van een EU Cyberbeveiligingsreserve, die zal bestaan uit een reeks geselecteerde aanbieders uit de privésector. Deze reserve kan vervolgens worden opgeroepen door lidstaten of instellingen van de EU (en zelfs door niet-EU-landen) om grootschalige incidenten mee aan te pakken. Het agentschap ENISA kreeg in de zomer van 2025 een mandaat om dit operationeel waar te maken op Europees niveau.

- het instellen van wederzijdse bijstand: een lidstaat die getroffen wordt door een cyberbeveiligingsincident kan daardoor rekenen op ondersteuning van de andere lidstaten.

Om de samenwerking tussen de diverse actoren in de 27 lidstaten te versterken, organiseerde het CCB in januari 2024 de **Brussels Cybersecurity Summit**. Die bracht het ecosysteem uit ons land samen met vertegenwoordigers van cybersecurity ecosystemen uit de rest van de EU – over verschillende actiedomeinen heen: technische, strategische en financieringsexperten. Nieuw was ook dat de directeurs van de nationale en regionale cybersecurity autoriteiten elkaar ontmoetten op een informele topontmoeting.

Brussels Cybersecurity Summit (2024).

Een andere verwezenlijking had betrekking op **EU-CyCLONe**, de organisatie die als liaison fungeert tussen de nationale autoriteiten van de lidstaten voor het beheren van een cybercrisis.

De oprichting van dit orgaan was een gevolg van de NIS2-richtlijn. Tijdens het Belgische voorzitterschap werden de eerste procedures en regels afgesproken binnen EU-CyCLONe, rond het uitwisselen van informatie en het coördineren van interventies. Deze procedures, en het CCB leiderschap, konden meteen getest worden tijdens de Europese verkiezingen van 2024 en ook tijdens de 'Cyber Europe' oefening, een van de grootste internationale oefeningen in cyberincident management.

Naast EU-CyCLONe was het CCB ook voorzitter van twee andere Europese netwerken. Ten eerste de NIS Cooperation Group, waar lidstaten samenkomen om de implementatie van de NIS2-richtlijn vorm te geven en zo essentiële dienstverlening in de EU te verzekeren. Hierin zette het CCB onder meer de toon door als eerste Europese lidstaat de richtlijn om te zetten. Daarnaast was het centrum ook 18 maanden lang voorzitter van het Europese Computer Security Incident Response Team (CSIRT) Netwerk, waar de technische 'brandweerploegen' van cyberincidenten met elkaar overleggen.

Onder leiding van het CCB werd ook een uitgebreide evaluatie en inventarisatie gemaakt van het cybersecurity landschap in de EU. De hieruit volgende **Raadsconclusies over de toekomst van cyberveiligheid**, samengevat in een tekst getiteld "Implement and Protect Together", werden na onderhandeling formeel aangenomen door alle Europese ministers van telecommunicatie. In het document pleitten de 27 lidstaten onder andere voor minder versnippering van de wetgeving, duidelijkere rollen en verantwoordelijkheden, nauwere samenwerking met handhavingsinstanties en meer aandacht voor Active Cyber Protection. Hiermee werd de focus van het Europese beleid de facto verlegd naar implementatie in plaats van nieuwe wetgeving. Op deze manier werden enkele van de speerpunten van het CCB ook Europees bekrachtigd.

Internationale erkenning

België ontving unanieme lof aan het einde van zijn Europees voorzitterschap eind juni 2024. Ook de realisaties in het cyberdomein hadden bijgedragen tot dat succes. De transversale aanpak en de transparante manier waarop de vertegenwoordigers van het CCB samen met de Permanente Vertegenwoordiging bij de EU dossiers hadden voorbereid, werd sterk geapprecieerd. Hun enthousiasme en inspanningen om experts en beleidsmakers te verenigen rond concrete verwezenlijkingen, leverden resultaat op.

Het centrum groeide hierdoor uit tot een gerespecteerde en gezaghebbende stem op het Europese niveau. Dit wekte veel belangstelling op voor de Belgische cybersecuritystrategie en de diverse projecten binnen het concept Active cyber Protection. De aanpak die het CCB heeft bedacht, vindt dan ook elders ingang:

- Het concept Actieve Cyberbescherming wordt door de EU erkend als een best practice, die past binnen de NIS2 regelgeving (verhoogde cyberweerbaarheid in kritieke en essentiële sectoren).
- Het CyberFundamentals framework werd intussen door diverse landen, maar ook door privébedrijven, geïmplementeerd.
- Spear Warnings: verscheidene cybersecurity agentschappen bekijken hoe ze een soortgelijk waarschuwingssysteem kunnen opzetten in hun eigen land.
- Belgian Anti-Phishing Shield: het Verenigd Koninkrijk heeft zo'n systeem geïmplementeerd voor de overheidsdiensten, de Franse gegevensbeschermingsautoriteit en het cybersecurity centrum ANSSI onderzoeken de uitbouw van een Franse versie, en op Europees niveau is er interesse in een bredere uitrol.

Een andere illustratie van de reputatie die het CCB geniet, is de wereldwijde community die het centrum intussen bereikt via zijn online Connect and Share-evenementen. Sinds 2020 namen meer dan 8.000 IT- en cyberprofessionals uit 70 landen deel aan deze sessies. Ze behandelen zowel technische als strategische onderwerpen. Internationale keynotes leveren er graag een bijdrage aan.

Onderscheidingen

België is in tien jaar tijd onmiskenbaar uitgegroeid tot voortrekker in cyberbescherming. De ambitie om ons land te laten uitgroeien tot één van de minst cyberkwetsbare landen van de EU, is verwezenlijkt. Dat blijkt ook uit vergelijkende studies en internationale rangschikkingen.

Door het werk en de coördinatie van het CCB met nationale partners, wordt België in gerenommeerde cybersecurity-indexen gerekend tot de top 10 waaronder de **National Cyber Security Index** (NCSI) en de EU Cybersecurity Index. In de **BitSight EU Ranking** behoort België tot de top-3.

De International Telecommunication Union (ITU) is het agentschap van de Verenigde Naties voor informatie- en communicatietechnologie. In zijn **Global Cybersecurity Index 2024** wordt België als Tier 1-rolmodel naar voren geschoven voor Europa. Deze studie onderzoekt 5 domeinen (regelgeving, technische maatregelen, organisatie, niveau van samenwerking en de uitbouw van capaciteit). België haalt een totaalscore van 96,81 op 100 en doet het op alle pijlers beter dan het Europese en globale gemiddelde.

Dit is een internationale erkenning van de geleverde inspanningen door het centrum en het hele Belgische cybersecurity ecosysteem.

Ook de Belgische jaarlijkse awarenesscampagnes lopen internationaal in de kijker: in 2022 en 2024 werd de video van de jaarlijkse sensibiliseringscampagne bekroond met een European Cybersecurity Award voor de beste awareness video.

In 2023 won het Spear Warning project een Publica Award.

"België is in tien jaar tijd onmiskenbaar uitgegroeid tot voortrekker in cyberbescherming. De ambitie om ons land te laten uitgroeien tot één van de minst cyberkwetsbare landen van de EU, is verwezenlijkt. Dat blijkt ook uit vergelijkende studies en internationale rangschikkingen."

CCB EVOLUEERT MEE

De cyberveiligheid van ons land, zijn burgers, bedrijven en publieke instellingen garanderen blijft tien jaar na de start van het CCB een uitdaging. De technologische evolutie, professionalisering in het milieu van de cybercriminelen en geopolitieke ontwikkelingen hebben tot gevolg dat het aantal cyberaanvallen sterk blijft stijgen en dat er nog steeds nieuwe vormen van fraude opduiken. Als nationaal coördinatiecentrum volgt het CCB de situatie op de voet.

HUIDIGE DREIGINGEN VERSUS ‘OUDE’ DREIGINGEN

Het dreigingslandschap is de laatste jaren verder geëvolueerd. Vooral de werkwijze die criminelen en state actors hanteren, is veranderd. Wij onderscheiden grosso modo drie grote groepen, die er elk hun eigen methodes op nahouden.

Welke dreigingen komen voor?

GEORGANISEERDE CYBERCRIMINELEN

Waar cybercriminaliteit vroeger vooral het werk was van individuele hackers, zien we vandaag internationaal georganiseerde groepen die werken volgens een uitgekiend businessmodel. Ransomware-aanvallen, waarbij gegevens worden versleuteld en pas na betaling worden vrijgegeven, zijn uitgegroeid tot een miljardenindustrie. De aanvallen gebeuren vandaag ook veel gerichter.

Een breed verspreide aanval, zoals Wannacry, waarbij honderdduizenden computers wereldwijd korte tijd gegijzeld werden, komt vandaag minder frequent voor. Ransomware-aanvallen worden nu beter voorbereid en zijn nauwkeurig afgestemd op een bepaald slachtoffer of bepaalde groepen slachtoffers.

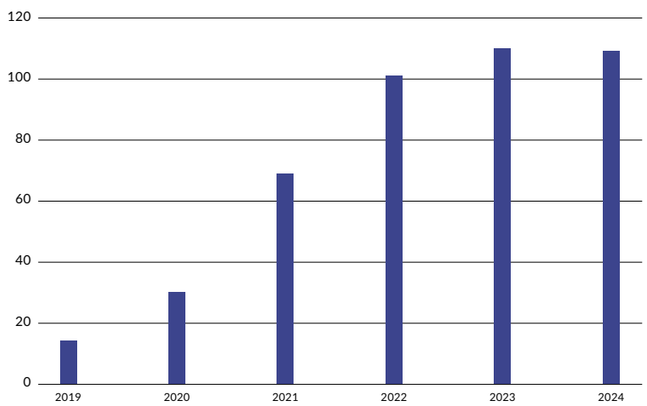
Tegelijk is het door de technologische evolutie ook makkelijker geworden om een ransomware-aanval uit te voeren. Ransomware-as-a-Service (RaaS) is een dienstverlening waarbij cybercriminelen een volledig ransomware-pakket aanbieden aan andere criminelen. Op die manier hoeft de kwaadwillige geen IT-achtergrond meer te hebben om met succes een organisatie te treffen, wat leidt tot een veel grotere spreiding en frequentie van de aanvallen.

HACKTIVISTEN

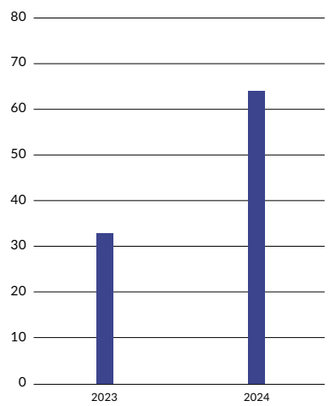
Hacktivisten voeren vanuit ideologische of politieke motieven aanvallen uit. Hun voornaamste doel is niet financieel gewin, maar het ontwrichten van de democratische processen van een maatschappij of het uitdragen van een boodschap.

In de meeste gevallen gebruiken ze hiervoor DDoS-aanvallen, waarbij websites of online diensten tijdelijk onbereikbaar worden gemaakt door ze te overbelasten. Op korte termijn is de impact doorgaans beperkt, maar de symbolische waarde kan groot zijn. Veel hangt af van de geopolitieke situatie en spanningen, die tot pieken in dergelijke aanvallen leiden. De modus operandi is over de jaren heen grotendeels dezelfde gebleven.

Evolutie ransomware



Evolutie DDOS



STATE ACTORS

State actors handelen in opdracht van of gedragen zich namens een staat. Hun doel verschilt van dat van de hacktivisten en criminele groeperingen. Ze beschikken over meer middelen, over zeer geavanceerde technologie en opereren uiterst discreet. Hun doel is meestal strategisch: het buit maken van gevoelige informatie of technologie en het binnendringen bij kritieke infrastructuren.

Hoewel het aantal zichtbare incidenten vandaag eerder beperkt lijkt, betekent het niet dat ze niet plaatsvinden. Integendeel, net omdat zulke aanvallen vaak onder de radar blijven, is hun werkelijke impact moeilijk in te schatten. Bovendien gebruiken state actors soms criminele groepen als dekmantel, waardoor het niet altijd duidelijk is wie er precies achter de aanval zit.

De frequentie: van sporadisch naar dagelijks

Het aantal cyberincidenten is de voorbije jaren onmiskenbaar toegenomen. Waar ransomware en phishing 20 jaar geleden met de regelmaat van de klok opdoken, zijn ze inmiddels een dagelijkse realiteit. Dat komt omdat de drempel om een aanval op te zetten, lager ligt. Het gevolg is een explosieve toename van het aantal actoren.

Bovendien zien we dat de aanvallen zich steeds sneller opvolgen. Daardoor ligt de dreigingsdruk structureel hoger dan enkele jaren geleden. Cyberaanvallen zijn dus niet langer een uitzondering, maar een gegeven waar elke organisatie rekening mee moet houden.

Waar criminelen vandaag toeslaan

Veel cyberaanvallen zijn anno 2025 van opportunistische aard: criminelen zoeken naar de zwakste schakel en slaan toe wanneer ze hun kans zien. Toch tekenen zich duidelijke patronen af. Overheidsdiensten, netbeheerders, en financiële instellingen blijven bijzonder geviseerd, niet alleen omdat ze over waardevolle data beschikken, maar ook omdat ze symbolische doelwitten zijn.

Ook kennisinstellingen en technologiebedrijven zijn vaker het doelwit voor diefstal van intellectueel eigendom, gevoelige onderzoeksresultaten of technologische knowhow. Industrie en de logistieke sector lopen eveneens een hoger risico. Aanvallen in deze sectoren kunnen productieprocessen verstoren, leveringsketens ontwrichten en aanzienlijke economische schade veroorzaken.

Cyber als geopolitiek wapen

Geopolitieke spanningen hebben zich vertaald naar het digitale domein en door de groeiende rivaliteit tussen internationale machtsblokken is het aantal cyberaanvallen met (geo-)politieke motieven merkbaar gestegen. Daarbij zetten staten zelf steeds vaker cybersabotage en cyberspionage in als verlengstuk van hun buitenlandse politiek. Cyber is daarmee een volwaardig wapen geworden: het kan een land ontregelen, kritieke infrastructuur onder druk zetten en vertrouwelijke informatie blootleggen.

Opvallend is dat de grenzen tussen criminele groepen en state actors steeds vager worden. Soms opereren criminelen in opdracht van een regime, soms gebruiken staten bestaande netwerken om hun sporen te verbergen. Het resultaat is een dreigingslandschap waarin geopolitiek en cybercriminaliteit steeds meer met elkaar verweven zijn.

De impact van nieuwe technologie: AI en quantum

Nieuwe technologieën vormen een bedreiging, maar bieden tegelijk kansen. AI is daar een treffend voorbeeld van. Zo gebruiken criminelen AI steeds vaker om phishingmails overtuigender te maken, valse beelden of video's (deepfakes) te genereren en aanvallen te automatiseren. De schaal en snelheid waarmee dit gebeurt, maakt detectie moeilijker. Tegelijkertijd kan AI net zo goed een bondgenoot zijn: technologie die helpt om aanvallen sneller te herkennen, patronen te doorgronden en verdedigingssystemen slimmer en efficiënter te maken.

Terwijl AI vooral een doorbraak betekent in software, zal quantumtechnologie voor een revolutie in hardware zorgen. Wanneer quantumcomputers op punt zullen staan, zal hun ongeziene rekenkracht in staat zijn om klassieke codering en encryptie in korte tijd te kraken. Onderzoekers werken daarom al volop aan quantumbestendige oplossingen zoals post-quantum cryptografie. Het blijft voorlopig moeilijk te voorspellen wanneer deze technologie matuur zal zijn en hoe ingrijpend de gevolgen zullen zijn.

Waakzaam blijven voor nieuwe doorbraken en tegelijk blijven investeren in onderzoek en expertise, is daarom een noodzaak. Wie er tijdig in slaagt om de kracht van AI en quantum te benutten, bouwt een voorsprong op in een digitale wereld die verder accelereert.

België als voortrekker in Europa's digitale veiligheid

België mag zich als relatief klein land gerust vandaag een voortrekker noemen op het vlak van cyberveiligheid en behoort tot de Europese top. En dat is geen toeval: onze kracht ligt in een pragmatische en resultaatgerichte aanpak, waar andere landen soms nog verzanden in eindeloze procedures en bureaucratie.

"De verschillen tussen vroeger en nu liggen niet in het type aanvallen, maar vooral in de professionalisering, de schaal en de verwevenheid met geopolitieke, criminele en ideologische motieven. Waar de wereld tijdens WannaCry en NotPetya zag hoe ontwrichtend een cyberaanval kan zijn, zien we vandaag dat aanvallen subtieler en doelgerichter plaatsvinden."

Een sprekend voorbeeld is de manier waarop we de NIS2-richtlijn hebben vertaald naar een nationaal kader. Ook het Early Warning System (EWS) dat het CCB heeft ontwikkeld om dreigingen snel te detecteren en te delen, geldt als een succesverhaal. En het framework CyberFundamentals dat handvatten aanreikt voor een betere cyberbescherming, kan op internationale belangstelling rekenen.

Cybercriminaliteit blijft bij uitstek een internationaal fenomeen. Een aanval op onze infrastructuur kan ook elders verregaande gevolgen hebben. Europa blijft daarom het primaire kader om de strijd tegen cybercriminaliteit en digitale dreigingen te coördineren. Via gezamenlijke projecten, het delen van informatie en het opbouwen van netwerken versterken de landelijke en regionale ecosystemen elkaar. Ons land kiest er bewust voor om in dat Europese verhaal een leidende rol op te nemen.

CENTRE FOR
CYBERSECURITY
BELGIUM 10Y

https://ccb.belgium.be