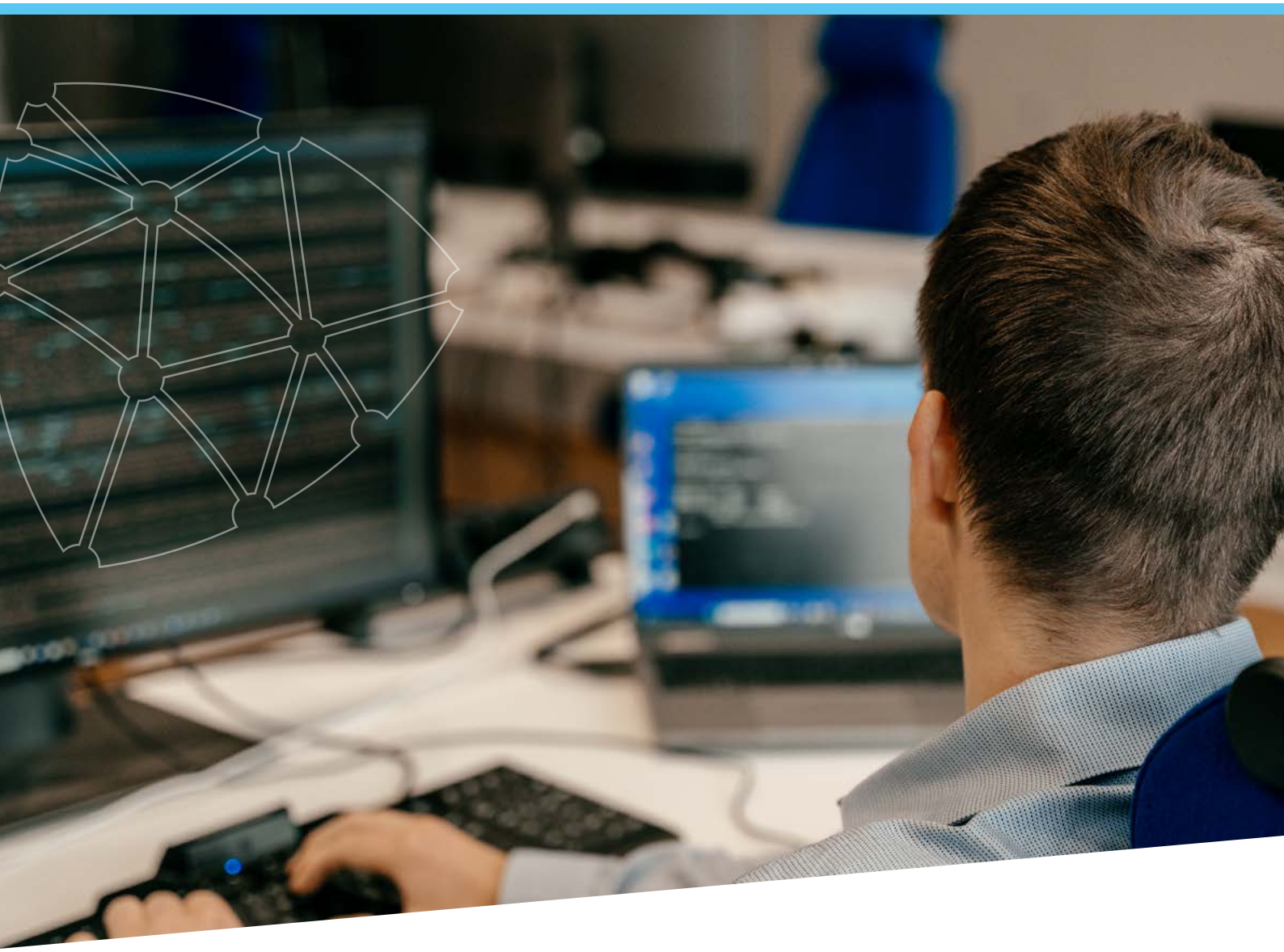
CENTRE FOR
CYBERSECURITY
BELGIUM



EMPOWERING CYBERSECURITY

CCB RAPPORT 1/1/2023 - 30/9/2023

Centre for Cybersecurity Belgium
Onder de autoriteit van de Eerste Minister

Inhoudsopgave

Voorwoord van de directeur

Het verbeteren van de nationale cyberveiligheid en het verminderen van de kwetsbaarheid van een land is een zeer uitdagende opdracht. De cyberruimte is bijna volledig een privéomgeving. Daardoor is het voor de overheid moeilijk om ze te beschermen tegen dreigingen en incidenten, ze op te sporen en erop te reageren.

Zoals in de meeste landen wil het Centrum voor Cybersecurity België (CCB) de veerkracht versterken door middel van nationale en internationale samenwerking, publiek-private partnerschappen, informatiedeling, capaciteitsopbouw en opleiding, bewustmaking, onderzoek, AI-gebaseerde detectie en respons, Quantum ready-cryptografie, nationale cybersecurityoefeningen etc. Hoewel al deze acties essentieel en nuttig zijn, volstaan ze niet. Ondanks al deze maatregelen blijven cybercriminaliteit en online fraude immers toenemen.

Deze maatregelen lijken te algemeen en leiden vaak niet tot concrete acties of resultaten, noch worden ze omgezet in meer kleinschalige, concrete en gerichte projecten en diensten. Je hebt geen marathon gelopen tot je aan de finish bent! Dat is onze ambitie bij het CCB: tot de finish gaan voor al deze essentiële concepten en initiatieven. Elke keer willen we ons afvragen:

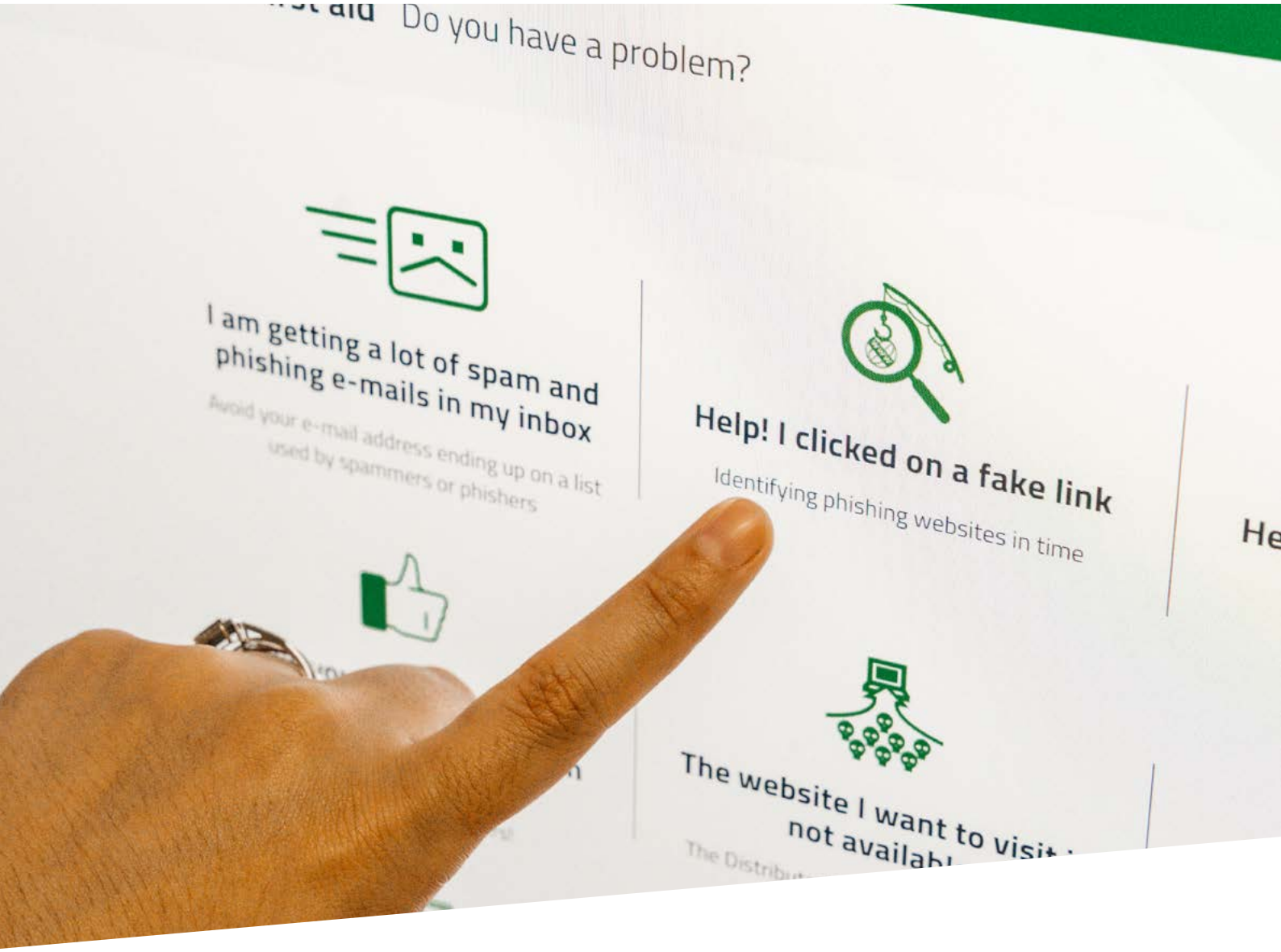
> Wat is de werkelijke impact voor burgers,
> bedrijven, overheden en kritieke infrastructuur?

Om de finish in zicht te krijgen, hebben we een nieuw initiatief op touw gezet: Active Cyber Protection (ACP), onderverdeeld in vijf subthema's. We willen de eigenaars van bedreigde systemen of accounts erbij betrekken, communicatie met 100% kwaadaardige infrastructuren op nationaal niveau filteren, van cybersecurity een standaarddomein maken dat toegankelijk is voor alle bedrijven, kwetsbare systemen in België identificeren en de eigenaars ervan rechtstreeks waarschuwen (Spear Warning). Tot slot willen we ook de ontwikkeling van gevalideerde diensten aanmoedigen, zodat iedereen die via het internet informatie ontvangt, kan controleren of de identiteit van de afzender al dan niet gevalideerd is.

De kernactiviteit van het CCB is het steeds veranderende landschap van cyberdreigingen te evalueren en erop te reageren met concrete projecten in samenwerking met onze partners. We moeten ervoor zorgen dat onze partners zien dat we de finish in zicht hebben.

Miguel De Bruycker
Directeur-generaal,
Centrum voor Cybersecurity België

Brussel, december 2023


Do you have a problem?
I am getting a lot of spam and phishing e-mails in my inbox
Avoid your e-mail address ending up on a list used by spammers or phishers
Help! I clicked on a fake link
Identifying phishing websites in time
The website I want to visit
not availab

NATIONALE PROJECTEN EN INTERNATIONALE PRIORITEITEN

Via projecten en initiatieven gericht op betere cyberbeveiliging en veerkracht van overheidsdiensten, bedrijven, de academische wereld en eindgebruikers, wil het Centrum voor Cybersecurity België, als nationale autoriteit voor cybersecurity, van België tegen 2025 één van de minst kwetsbare Europese landen maken op het vlak van cybersecurity.

Het roulerend voorzitterschap van de Raad van de Europese Unie

Van 1 januari tot 30 juni 2024 neemt België het roulerend voorzitterschap van de Raad van de EU waar.

Tijdens deze periode zal het CCB internationale verantwoordelijkheden opnemen en een leidende rol spelen om de Belgische prioriteiten in de kijker te zetten, alsook het programma van het voorzitterschap op het vlak van cybersecurity, bij de andere landen, met als doel het promoten van doelstelling 6 van onze Nationale Cybersecuritystrategie: het duidelijke internationaal engagement van België op het vlak van cybersecurity.

HET VOORZITTERSCHAP SCHEPT VERPLICHTINGEN EN KANSEN

Het CCB zal het roulerend voorzitterschap waarnemen van verschillende officiële Europese cybersecurity-netwerken waarin het de officieel aangewezen vertegenwoordiger van België is (zoals de NIS-samenwerkingsgroep, het EU Cybercrisis Liaison Network – EU-CyCLONe, en het EU-CSIRTs-netwerk). Het CCB zal de wettelijke verantwoordelijkheden van deze netwerken opvolgen en zal de vergaderingen van al deze groepen op verschillende locaties in België voorzitten, de agenda opstellen en als gastheer optreden, eveneens om ons land in de kijker te zetten.

Nu de laatste fase van de omzetting van de NIS2-richtlijn in nationale wetgeving ingaat, is een goede coördinatie binnen al deze netwerken van essentieel belang. Binnen het EU-CyCLONe netwerk finaliseren België en het CCB het eerste verslag aan de Raad en het Europees Parlement.

Bij grote cybersecurityincidenten zal het CCB een leidende rol spelen bij het coördineren van de Europese respons, zowel binnen het CyCLONe-netwerk als binnen het EU-CSIRTs-netwerk.

Het CCB zal ook een leidende rol spelen in het wetgevende en beleidswerk van de Werkgroep Cybersecuritykwesties van de Raad. We zullen de Belgische attachés bij de Raad ondersteunen bij het bereiken van de Belgische doelstellingen en bij het vooruit- of afwerken van belangrijke dossiers zoals de cyberweerbaarheidswet, de cybersolidariteitswet of amendementen op de cyberveiligheidswet. of amendementen op de cyberveiligheidswet. We zullen hen ook ondersteunen bij het organiseren van een Europese Cyber Security Review over de staat van het EU-beleid inzake cyberveiligheid, die zal leiden tot conclusies van de Raad over de toekomst van cyberveiligheid.

EN DE VERKIEZINGEN

Het Belgische voorzitterschap staat bovendien niet alleen in het teken van nationale en regionale verkiezingen, maar ook van de Europese verkiezingen, die van 6 tot 9 juni 2024 worden gehouden. Gezien de geopolitieke context kunnen deze verkiezingen aanleiding zijn tot cybersecuritygebeurtenissen of verhoogde dreigingen met gevolgen voor de EU, die versterkte samenwerking op het niveau van crisisbeheer en op technisch niveau vereisen.

NIS2: Gevolgen voor Belgische sectoren en entiteiten

Om het groeiende cyberdreigingslandschap en de nieuwe uitdagingen aan te pakken, heeft de Europese Unie een nieuw wetgevingsbesluit vastgesteld over maatregelen voor een gemeenschappelijk hoog niveau van cybersecurity in de Unie (Richtlijn 2022/2555 van 14 december 2022 – de "NIS2-richtlijn"), die de "NIS1-richtlijn" vervangt (Richtlijn 2016/1148 van 6 juli 2016 inzake maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie).

De NIS2-richtlijn heeft een aantal belangrijke wijzigingen geïntroduceerd ten opzichte van de NIS1-richtlijn: meer sectoren en entiteiten die onder de richtlijn vallen, nieuwe selectie- en registratiemethoden, meer eisen op het gebied van cybersecurity, nieuwe termijnen voor het melden van incidenten, versterking van de controlemechanismen.

De NIS2-richtlijn heeft ook tot doel de nationale capaciteiten en het cybersecuritybeleid te verbeteren. Wat het nationale beleid betreft, gaat het om de nationale cybersecuritystrategie, nationale kaders voor cybercrisisbeheer, de rol van de bevoegde autoriteiten en nationale of internationale samenwerking.

COÖRDINATIE EN IMPLEMENTATIE VAN DE NIS2-RICHTLIJN

Als nationale autoriteit inzake cybersecurity speelt het CCB een sleutelrol bij de coördinatie en uitvoering van deze richtlijn. Het CCB is de bevoegde autoriteit voor alle sectoren (in samenwerking met eventuele sectorale autoriteiten), het nationale CSIRT, het nationale centrale contactpunt, de vertegenwoordiger in de samenwerkingsgroep, het CSIRT-netwerk en het CyCLONe-netwerk.

Essentiële en belangrijke entiteiten moeten voor de risicobeheersmaatregelen inzake cybersecurity passende en evenredige technische, operationele en organisatorische maatregelen nemen om de beveiligingsrisico's te beheren van de netwerk- en informatiesystemen. Die laatste systemen gebruiken ze voor hun activiteiten of voor hun dienstverlening en om de impact van incidenten op de gebruikers van hun diensten te voorkomen of tot een minimum te beperken. Deze maatregelen zijn gebaseerd op een alomvattende aanpak van de risico's, waarvoor het CCB duidelijke richtlijnen heeft opgesteld via de aanname van het CyberFundamentals Framework. Daartoe zullen organisaties die een CyberFundamentals- of ISO/IEC 27001-certificering of -label krijgen, een vermoeden van conformiteit genieten.

Als nationaal CSIRT ontvangt het CCB meldingen van belangrijke incidenten van NIS-entiteiten om de mogelijke verspreiding van incidenten te beperken, entiteiten in staat te stellen bijstand te vragen, crisissituaties zo goed mogelijk te beheren en relevante technische informatie te delen met andere entiteiten.

Tot slot zal het CCB via zijn inspectiedienst (in samenwerking met eventuele sectorale autoriteiten) ook een rol spelen bij het toezicht op de betrokken entiteiten.

Het CyberFundamentals framework

Op het vlak van cybersecurity bestaan er internationale kaders en verschillende internationale normen. Belgische organisaties zijn op de hoogte van deze kaders, maar ze zijn over het algemeen weinig aangepast aan de specifieke Belgische situatie en blijven erg algemeen. Dit betekent dat de maatregelen die organisaties kunnen nemen, op basis van de risico's moeten worden bepaald, wat specifieke problemen oplevert voor organisaties die niet noodzakelijk cyberspecialisten ter beschikking hebben.

In het kader van de opdracht van de Belgische Nationale Cyber Security Strategie 2.0, die ook onder de bevoegdheid van het CCB valt – namelijk om van België tegen 2025 een van de minst cyberkwetsbare landen van Europa te maken – heeft de CCB-Certificeringsautoriteit het CyberFundamentals Framework ontwikkeld.

HET RISICO OP CYBERAANVALLEN VERMINDEREN

Dit kader heeft als doel onze gegevens te beschermen, het risico op cyberaanvallen aanzienlijk te verminderen en de veerkracht van Belgische organisaties te vergroten.

Met deze alomvattende op risico gebaseerde aanpak willen we het vertrouwen in de digitalisering van de samenleving versterken door onze kennis te delen en inzicht te geven in de verschillende cyberbedreigingen. Dit doen we door reële gegevens die we ontvangen van het Belgische Cyber Emergency Response Team (CERT) op te nemen in het raamkader en deze gegevens, samen met andere methodologieën, te gebruiken om het raamwerk te valideren.

Het kader is gebaseerd op het wereldwijd erkende NIST-CSF-framework en bevat verschillende elementen van de ISO 27001- en ISO 62443-normen, die veel gebruikt worden in België, evenals elementen van het CIS Security Framework. De functies Identify, Protect, Detect, Respond en Recover vormen de rode draad van het kader, dat is uitgewerkt in de vorm van een conformiteitsbeoordelingssysteem om compliance of non-compliance met de maatregelen in het raamwerk aan te geven.

VEILIGHEIDSNIVEAUS

Daarnaast volgt het kader de drie veiligheidsniveaus van de Cyber Security Act: 'Basic', 'Important' en 'Essential', en een beginnersniveau 'Small'. Op deze manier, en deels door een maturiteitsbenadering op te nemen, wil het kader een proportioneel antwoord bieden op de behoeften van zowel kleine als grote organisaties, zodat zij hun niveau van cybersecurity geleidelijk kunnen verbeteren.

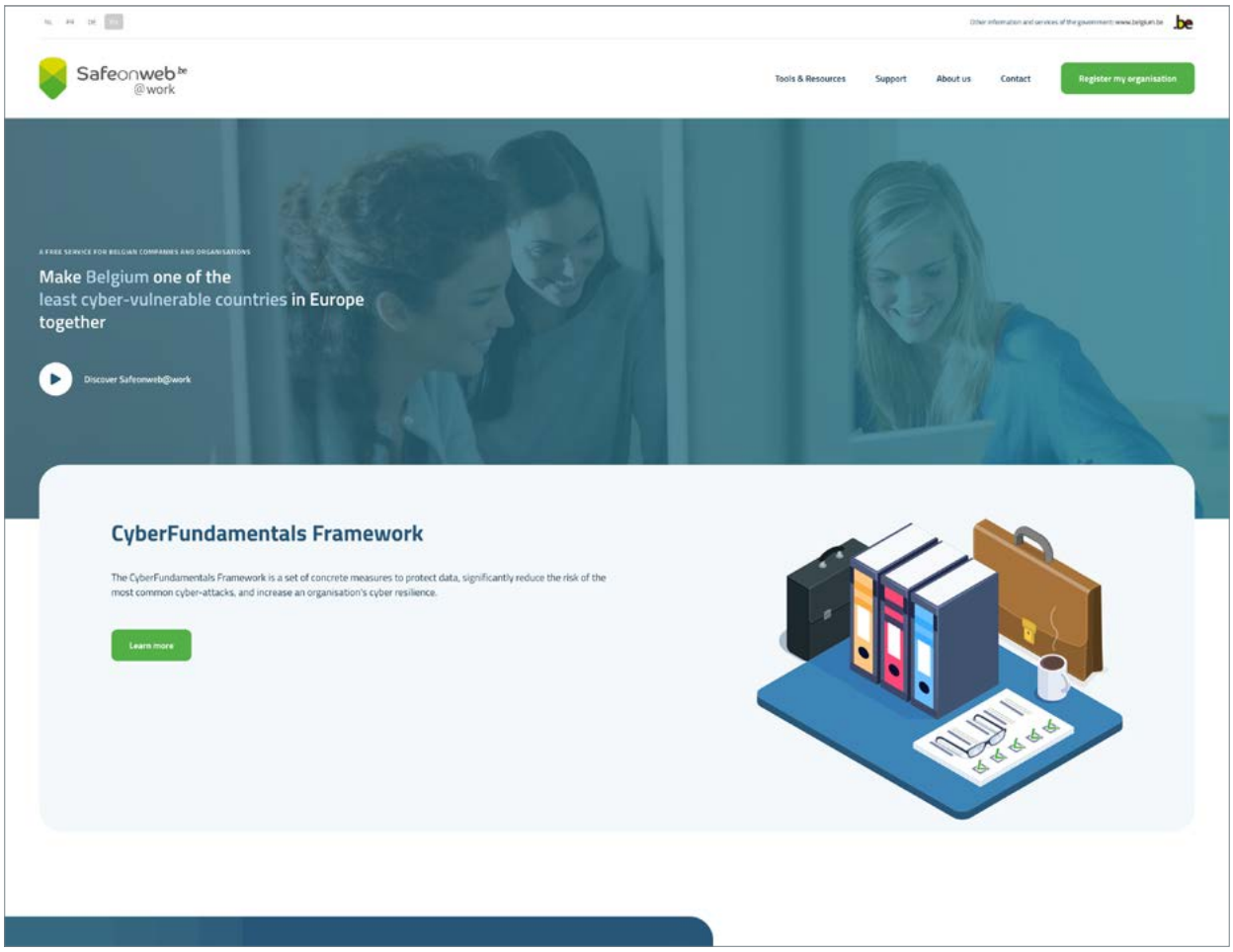
Tot slot biedt het CCB ter ondersteuning van de implementatie van dit raamkader een aantal instrumenten, gaande van een risicoanalyse om het door NIS2 vereiste veiligheidsniveau te bepalen, tot een zelfbeoordelingstool en het in kaart brengen van de verschillende raamkaders en normen waarop die zijn gebaseerd.

Het kader en de tools zijn gratis beschikbaar.

www.cyfun.be

Safeonweb @work

Safeonweb@work is een initiatief dat gericht is op Belgische organisaties en bedrijven. Het doel is om hun niveau van cyberveiligheid te verhogen door advies, aanbevelingen en tools aan te bieden om hen te helpen de kwetsbaarheden van hun systemen te identificeren en te verminderen en hen bewust te maken van cyberbedreigingen. Dankzij deze verschillende diensten kunnen organisaties proactief de gepaste maatregelen nemen om het risico op cyberaanvallen aanzienlijk te verminderen en zo bij te dragen tot onze doelstelling om van België tegen 2025 een van de minst cyberkwetsbare landen in Europa te maken.



DE DIENSTEN VAN SAFEONWEB@WORK OMVATTEN:

Cyber Threat Alerts
Een vroegtijdig-waarschuwings-systeem voor net-werkbedreigingen. Safeonweb@work stuurt een specifieke waarschuwing als er een kwetsbaarheid of infectie is gemeld op het netwerk dat op het platform is geregistreerd.

Quick Scan Report
Een dienst waarmee men een rapport kan ontvangen met een overzicht van de bedrijfsmiddelen van de organisatie, waarin potentiële kwets-baarheden worden geïdentificeerd en aanbevelingen wor-den gedaan om deze te verhelpen.

Policy templates
Een set aanpasbare en bewerkbare beleidsdocumenten voor cybersecurity om de implemen-tatie van informatie-beveiligingsbeheer binnen een organi-satie te vereen-voudigen.

Self-assessment
Een zelfbeoordelings-vragenlijst om het maturiteitsniveau van een organisatie op het gebied van cybersecurity te meten en praktische aanbevelingen te krijgen om eventuele tekortkomingen te verhelpen.

Content
Nieuws, tips, waar-schuwingen, webi-nars, aanbevelingen over de beste prak-tijken op het gebied van cybersecurity en de belangrijkste bedrei-gingen, evenals tools om het niveau van cybersecurity van een organisatie te verbeteren.

atwork.safeonweb.be

Safeonweb Browser extensie

Het CCB heeft de Safeonweb browser extensie ontwikkeld om burgers en organisaties te helpen beoordelen of de identiteit van de eigenaar van een website al dan niet is gevalideerd. Deze informatie wordt gebruikt om de betrouwbaarheid van de website te beoordelen. De extensie is gratis en geeft informatie over de verificatie van de eigenaar van de website, niet over de inhoud.

HOE WERKT DE SAFEONWEB-BROWSEREXTENSIE?

De extensie kent een score toe aan de websites die je bezoekt:

Groen (OK)
score van 4 op 4: de website-eigenaar heeft een Extended Validation Certificaat uitgegeven door een Certificaat Autoriteit of de website-eigenaar is geregistreerd op atwork.safeonweb.be (enkel voor Belgische organisaties).

Daarom:
- Zou het OK moeten zijn om verder te surfen op deze website.
- Zou het OK moeten zijn om gegevens te delen op deze website.

Oranje (!)
scores van 1 tot 3 op 4: de eigenaar van de website heeft een Organisatie Validatie Certificaat, of een Domein Validatie Certificaat uitgegeven door een Certificaat Autoriteit, en de website is niet geregistreerd op atwork.safeonweb.be

Daarom:
- Zou het OK moeten zijn om verder te surfen op deze website.
- Als je twijfelt, onthoud je dan van het delen van gegevens op deze website.

Rood (X)
score van 0 op 4: de website mist basisbeveiligingsfuncties of staat bekend als kwaadaardig. De eige-naar van de website heeft geen certificaat en is daarom niet gevalideerd.

Daarom:
- Raden wij af deze website te bezoeken en gegevens te delen.

Meer informatie over het project en de installatie-instructies zijn te vinden op:

- https://safeonweb.be/en/safeonweb-browser-extension
- https://atwork.safeonweb.be/protect-my-organisation/safeonweb-browser-extension

Innovatie in cybersecurity bevorderen voor Belgische Kmo's: financiële steun voor derden

Financial Support for Third Parties (FSTP) is een project dat wordt uitgevoerd door het **Nationaal Coördinatie-centrum – België** (NCC-BE) binnen het CCB. Dit initiatief heeft als doel EU-investeringen, zoals FSTP, te benutten, zodat startups, kmo's en midcap-bedrijven hun cybersecuritycapaciteiten kunnen versterken en zo de digitale omgeving veiliger te maken.

DE CYBERWEERBAARHEID VAN KMO'S VERSTERKEN

FSTP is niet zomaar een afkorting, het is de poort naar cyberweerbaarheid.

FSTP staat bekend als "cascadefinanciering" en is een belangrijk mechanisme dat door de Europese Commissie wordt gebruikt om startups en kmo's te ondersteunen bij het bevorderen van cybersecurity. Het NCC-BE gebruikt FSTP om baanbrekende cyberbeveiligingsoplossingen te verspreiden en zo de cybersecurity in België te versterken.

DE IMPACT VAN FSTP: STRONGER, SAFER, SMARTER!

Er wordt verwacht dat het FSTP-initiatief belangrijke resultaten zal opleveren die een positieve impact zullen hebben op de Belgische cyberveiligheid in de volgende zin:

- Verbeterde cyberweerbaarheid: kmo's krijgen meer toegang tot innovatieve cyberbeveiligingsoplossingen, waardoor ze beter kunnen omgaan met veranderende cyberbedreigingen.
- Innovatie aanmoedigen: het aanmoedigen van innovatie in de kmo-sector zal het mogelijk maken om geavanceerde cyberbeveiligingstechnologieën te ontwikkelen, wat het vermogen van België om gesofisticeerde cyberbedreigingen te bestrijden, aanzienlijk zal verbeteren.
- Publiek-private samenwerking: samenwerking tussen het NCC-BE en particuliere kmo's zal de uitwisseling van informatie verbeteren en een samenhangende aanpak van cybersecurity bevorderen, wat de algemene cyberweerbaarheid van het land ten goede zal komen.
- Economische groei: door het niveau van cyberveiligheid bij kmo's te verhogen, zal het FSTP-programma bijdragen aan de economische groei door kritieke digitale activa te beschermen en een gunstig klimaat voor bedrijfsactiviteiten te creëren.

FSTP, onder leiding van het NCC-BE, is essentieel om de Belgische cyberveiligheid in lijn te houden met de Europese cyberveiligheidsdoelstellingen. Voor meer informatie en nieuws kunt u de kanalen van het CCB en het NCC-BE volgen.

Financiering en aanbestedingen (europa.eu)

CYBERBEDREIGINGS-LANDSCHAP IN 2023

Het huidige niveau van cyberbedreigingen

HET WERELDWIJDE CYBERBEDREIGINGSLANDSCHAP

In 2023 werd het wereldwijde cyberdreigingslandschap opnieuw gekenmerkt door cyberaanvallen door verschillende actoren, zoals hacktivistische groepen, ransomwaregroepen en door staten gesponsorde hackersgroepen. Hoewel cybercriminelen vooral geïnteresseerd zijn in financieel gewin, is er een nauw verband tussen geopolitiek en cyberaanvallen van hacktivisten en van door staten gesponsorde actoren.

Het conflict tussen Oekraïne en Rusland

Het conflict tussen Oekraïne en Rusland, dat begon in 2022, reactiveerde het hacktivisme en toonde aan dat hacktivistische groepen een belangrijke capaciteit en een effectief middel kunnen zijn om aandacht te trekken ter ondersteuning van fysieke en ideologische activiteiten in tijden van conflict. In 2023 hielden hacktivistische activiteiten voornamelijk verband met het conflict tussen Oekraïne en Rusland. Vanaf het begin van het conflict verschenen er talloze hacktivistische groepen op het online toneel ter ondersteuning van de belangen en politiek van een van de partijen die betrokken waren bij de conflicten. Hun favoriete modus operandi omvat DDoS-aanvallen (Distributed Denial of Service), defacements van websites en hack-and-leak-operaties.

De pro-Russische hacktivistengroepen richtten zich op Oekraïne, maar ook op veel andere Europese landen, waaronder België. Hun doelwitten waren voornamelijk overheids- en militaire entiteiten, maar ook organisaties in de energie-, transport- (havens en luchthavens), logistieke, bank-, telecommunicatie- en zelfs de gezondheidszorgsector. De aanvallen werden uitgevoerd als vergelding voor de militaire, financiële, humanitaire of politieke steun van Europese landen aan Oekraïne en weerspiegelden altijd de strategische doelen van Rusland. Naast hacktivistische activiteiten in verband met het conflict tussen Oekraïne en Rusland, heeft hacktivisme zich ook ontwikkeld in verschillende delen van de wereld, omdat deze groepen voortdurend reageren op veranderende politieke en maatschappelijke kwesties en conflicten over de hele wereld. Politieke kwesties en sociale spanningen, evenals aanhoudende conflicten in verschillende delen van de wereld, hebben de hacktivistische activiteit in 2023 beïnvloed.

Cybercriminele activiteiten worden beïnvloed door macro-economische veranderingen en hebben aanzienlijke transformaties en ontwikkelingen ondergaan. Zo zijn er nu meer mogelijkheden en tactieken, maar ook nieuwe soorten doelwitten, zoals overheidsinstanties, openbare instellingen en organisaties in kritieke sectoren.

Ransomware

Ransomwareaanvallen is de belangrijkste cybercriminele activiteit gebleven die invloed had op organisaties, waaronder kritieke infrastructuur, in Europa en de Verenigde Staten. Ransomwareactoren richtten zich voornamelijk op de volgende sectoren: productie, software en informatietechnologie (IT), gezondheidszorg, onderwijs, zakelijke en adviesdiensten, recht, financiën en bankwezen. Sinds het uitbreken van de oorlog in Oekraïne is er een toename van ransomwareaanvallen tegen gemeenten en overheidsdiensten in Europese landen, waaronder België.

APT-campagnes en cyberspionage

Geopolitiek is nog steeds de belangrijkste drijfveer voor de ontwikkeling van APT-campagnes, waarvan het hoofddoel cyberspionage blijft (exfiltratie en verzamelen van gevoelige gegevens). APT-aanvallen worden voornamelijk uitgevoerd door staten gesponsorde hackersgroepen en hebben een aanzienlijke impact gehad op de geviseerde infrastructuren. Gedurende het hele jaar hebben cyberbeveiligingsbedrijven en nationale autoriteiten meerdere cyberspionagecampagnes gemeld die vooral gericht waren op de overheid, maar ook op bepaalde strategische sectoren.

Bekende, door staten gesponsorde hackergroepen zoals APT 28 (Fancy Bear), APT 29 (Cozy Bear), Emissary Panda, APT 33, Charming Kitten en Lazarus Groups, om er maar een paar te noemen, bleven wereldwijd actief. Er zijn ook meldingen van intensieve activiteit tegen verschillende Europese doelwitten door nieuwe groepen zoals Storm-0978, gemeld door Microsoft, die dit jaar een phishingcampagne voerde tegen de top

van de Noord-Atlantische Verdragsorganisatie (NAVO), of Storm-0558, een actor die ook door Microsoft werd gesignaleerd en die zich voornamelijk richt op West-Europese overheidsinstellingen via spionage, gegevensdiefstal en toegang tot referenties. Door staten gesponsorde actoren hebben ook nieuwe tools en mogelijkheden ontwikkeld en ingezet tegen hun doelwitten om de controle te behouden, detectie te vermijden en hun doelen te bereiken.

HET BELGISCHE CYBERBEDREIGINGSLANDSCHAP

Hoewel Belgische organisaties in 2023 vooral het slachtoffer waren van ransomware- en DDoS-aanvallen, werden ze ook getroffen door andere categorieën cyberincidenten, zoals datalekken, CEO-fraude, dreigingsindicaties op het dark web en speciale fora waarop gestolen gegevens worden gepubliceerd, en het compromitteren van Belgische IP-adressen die worden gebruikt bij cyberoperaties.

Ransomware

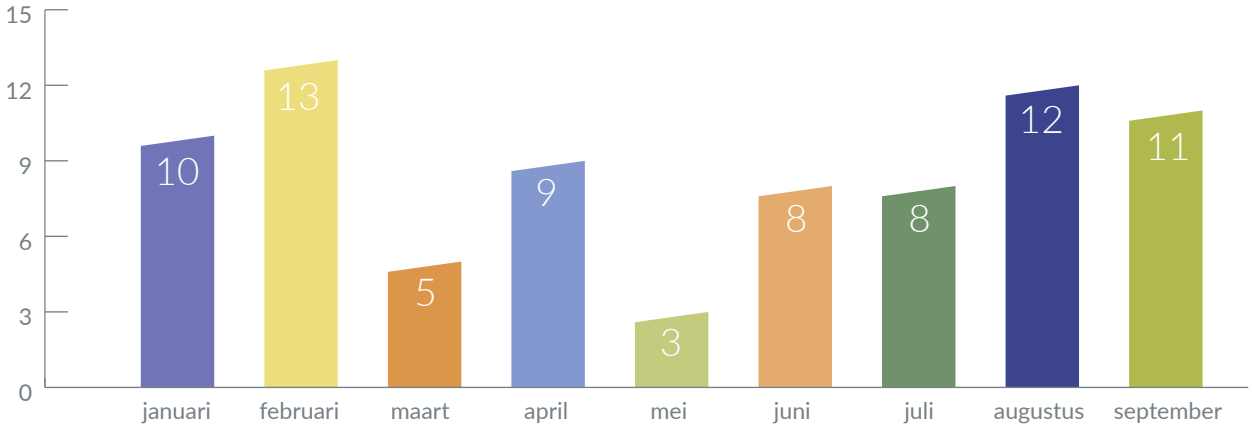
Net als in andere Europese landen is ransomware nog steeds de grootste en meest constante cyberbedreiging, zowel in aantal als in impact. Verschillende ransomware groepen, waarvan LockBit, Play en Cl0p de bekendste zijn vielen Belgische organisaties aan.

Volgens onze gegevens maakte LockBit de meeste slachtoffers in België, wat overeenstemt is met de wereldwijde activiteiten van de groep.

Door de massale uitbuiting van de kritieke MOVEit-kwetsbaarheid is de Cl0p-ransomwarebende gestegen naar de top van de ransomwaredreiging.

De doelwitten waren private en publieke entiteiten in verschillende sectoren, waaronder overheden, lokale besturen, gezondheidszorg, industrie, IT en voedsel en drank. De impact varieerde van klein tot groot, afhankelijk van de doelorganisatie, de cyberbeveiligingsinfrastructuur en de bestaande praktijken en beleidsregels. In sommige gevallen deden cybercriminelen aan dubbele afpersing en werden ransomwareaanvallen gevolgd door datalekken en blootstelling aan Data Leak Site van ransomwaregroepen. In deze gevallen is de impact altijd groter, omdat de aanvallen niet alleen de beschikbaarheid van infrastructuren aantasten, maar ook het publieke imago van de bedrijven die het doelwit zijn. In de eerste drie kwartalen van het jaar hebben publieke en private entiteiten in België 79 gevallen van ransomware aan het CCB gemeld.

Ransomwareaanvallen: Januari – september 2023



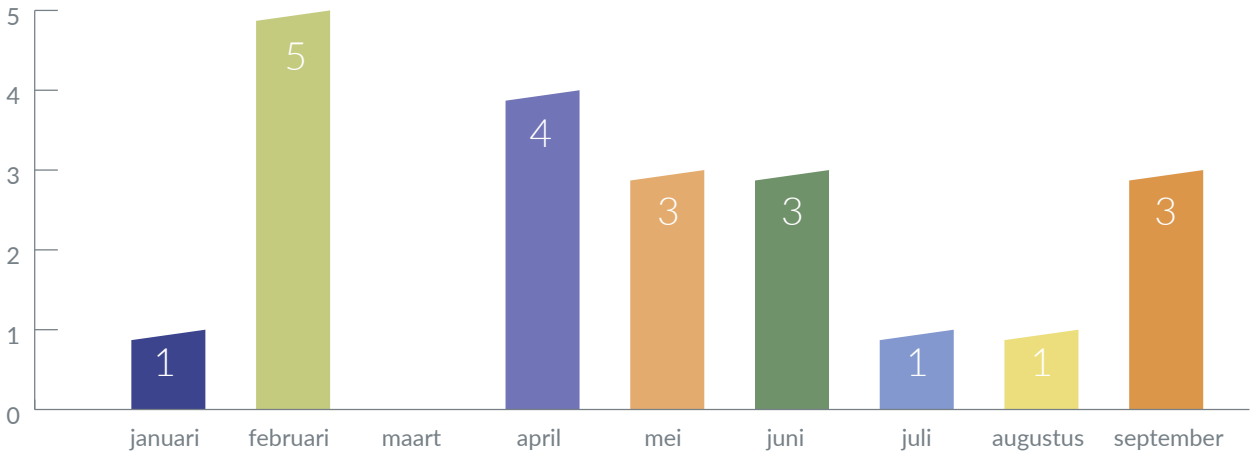
DDoS

DDoS-aanvallen tegen Belgische entiteiten vormden een permanente dreiging, maar met een lage impact. De aanvallen belemmerden tijdelijk de beschikbaarheid van bepaalde middelen of diensten van de geviseerde organisaties. Over het algemeen werden de situaties correct beheerd en werden de diensten opnieuw beschikbaar en functioneel. Sommige aanvallen werden opgeëist door de pro-Russische hacktivistengroepen KillNet, NoName057(16) en NET-WORKER ALLIANCE en werden gelinkt aan de officiële standpunten van de Belgische staat met betrekking tot de ontwikkelingen in het conflict tussen Oekraïne en Rusland of de militaire steun die ons land bood aan Oekraïne.

Het is belangrijk om erop te wijzen dat DDoS-aanvallen die worden uitgevoerd door pro-Russische hacktivisten over het algemeen gecombineerd worden met informatieoperaties, om gemakkelijk de aandacht van de media te trekken. De zichtbare onbeschikbaarheid van diensten of de disproportionele impact van de aanval kan dus de reputatie van een bedrijf schaden en op lange termijn een veel ernstiger effect hebben.

Andere DDoS-aanvallen, die niet werden opgeëist door pro-Russische hacktivistengroepen, werden voornamelijk uitgevoerd tegen overheidsinstanties, waarmee het totale aantal gemelde aanvallen tussen januari en september 2023 op 21 komt.

DDos-aanvallen: januari – september 2023



En in 2024?

Ransomwareaanvallen zullen een van de meest voorkomende en schadelijke cyberbedreigingen voor België blijven.

Afhankelijk van de ontwikkelingen in de lopende conflicten en de geopolitieke situatie, alsook van beslissingen en maatregelen die België neemt, zal het risico op DDoS-aanvallen door hacktivistische groeperingen tegen Belgische doelen blijven bestaan.

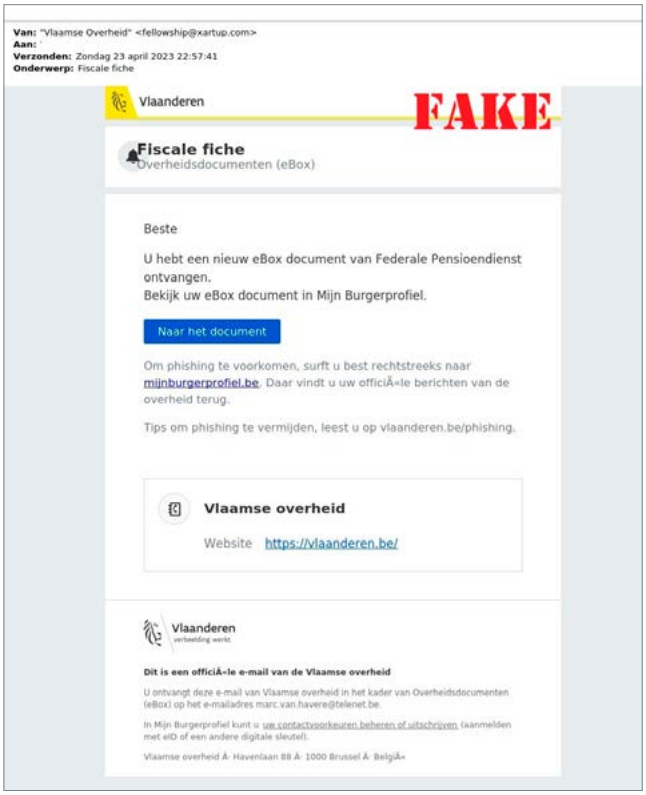
België zal een doelwit blijven voor cyberspionage, met Brussel als hoofdstad en als thuisbasis van veel internationale bedrijven, organisaties en EU-instellingen.

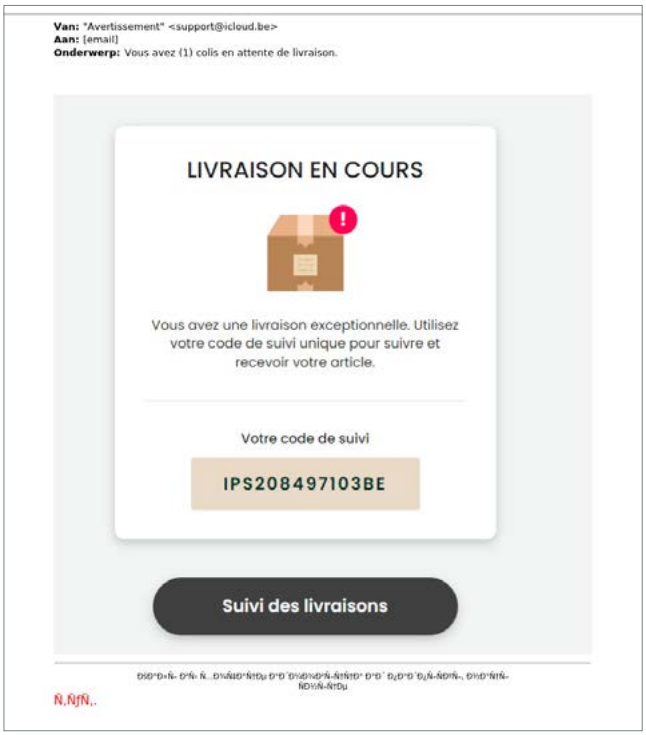
Voorbeelden van aanvallen op Belgische organisaties: januari – oktober 2023

	Type	Beschrijving of activiteit
12/03/2023	Ransomware	Een bedrijf in de gezondheidszorg is getroffen door ransomware.
11/05/2023	Ransomware	Een bedrijf in de gezondheidszorg is het slachtoffer geworden van ransomware.
20/06/2023	DDoS	Pro-Russische DDoS-aanval tegen Belgische entiteiten in de maritieme sector. NoName057(16) zat achter de aanval.
27/06/2023	DDoS	De Belgische federale overheid is het doelwit van een DDoS-aanval.
14/07/2023	Ransomware	Een Belgische gemeente is het slachtoffer geworden van een cyberaanval.
2/08/2023	Ransomware	Een Belgische vereniging is het slachtoffer geworden van een ransomwareaanval.
22/08/2023	Ransomware	Een infrastructuur van een Belgische gemeente was het doelwit van een cyberaanval.
24/08/2023	Cyberaanval	De overheid is getroffen door een DDoS-aanval.
12/10/2023	DDoS	NoName057(16) richtte zich op Belgische overheidsinstanties als vergelding voor de belofte van militaire en financiële steun aan Oekraïne.

Het anti-phishingproject

Phishing is nog steeds een van de belangrijkste **aanvalsmethoden** waarmee actoren malware installeren op een geviseerd systeem, maar ook een van de **meest voorkomende aanvalsvormen om gegevens te stelen**, zoals persoonsgegevens en identificatiegegevens, en om cyberfraude te plegen. Phishing-aanvallen zijn sterk afhankelijk van ***social engineering*-technieken** die meer gebruikmaken van menselijke fouten dan van technische kwetsbaarheden en vormen **een risico voor zowel Belgische organisaties als individuen**.





Van: Proximus <r[redacted]...@lureldkq.yangtaie.com>
Datum: 3 november 2023 om 15:03:16 CET
Aan: _
Onderwerp: Procédez à la conversion de vos points de fidélité avant le 10/11/2023.

Le service clients Proximus

Cher(e) Client(e) ,

Nous tenons à vous informer que depuis votre souscription, vous avez cumulé un total de 61 890 crédits de fidélité. Veuillez noter que ces crédits expireront après le 10 Novembre 2023.

Nous vous invitons donc à **échanger vos points de fidélité** pour vous offrir un **samsung Galaxy S23 gratuit**. Une fois que vous aurez confirmé votre **adresse et payé les frais d'expédition, votre samsung Galaxy S23 sera expédiée.**

En acceptant cette offre, votre compte sera **débité de 55 365 points**. Aucun abonnement ne sera souscrit sans votre accord préalable .

CONFIRMER & CONTINUER

*** Aucun abonnement ne sera souscrit sans votre accord préalable.**

De **onderwerpen** en **lokmiddelen** die hackers gebruikten in phishingberichten en e-mails om gegevens van Belgische slachtoffers te stelen, hadden voornamelijk betrekking op onderwerpen die van belang zijn voor burgers (communicatie met de bank, pakjes en postdiensten) en waren geïnspireerd op de sociaaleconomische context, de tijd van het jaar of de geopolitieke omstandigheden.

Actoren deden zich vaak voor als officiële autoriteiten of overheidsinstellingen. Hoewel sommige phishing-pogingen zeer professioneel overkomen, zijn veel phishing-e-mails en -berichten nog steeds gemakkelijk te herkennen. Naast de 'traditionele' onderwerpen met betrekking tot pakjes, laatste aanmaningen voor verplichte betalingen etc., verschenen er in 2023 bijvoorbeeld berichten over **energiesubsidies** en **belastingen**. Vroegere onderwerpen met betrekking tot COVID-19 zijn intussen in onbruik geraakt.

Aangezien het hoofddoel van phishingcampagnes het verzamelen van gegevens van slachtoffers is, waren de **vijf meest gebruikte malware-informatiestelers** Agent Tesla, xloader, remcos, snake keylogger, Loki password stealer.

TOP 10 Malware-families

Malware-familie	Totaal
agent tesla	545
xloader	124
remcos	68
snake keylogger	57
loki password stealer (pws)	46
cloudeye	41
blustealer	40
dbatloader	29
upatre	25
ave maria	22

Bron: CCB, 2023

Agent Tesla[1], de meest actieve malware in 2023, is een geavanceerde remote access trojan (RAT) die gespecialiseerd is in het stelen van gevoelige informatie van geïnfecteerde machines ("**Infostealer**"). Het dook voor het eerst op in 2014 en werd vanaf 2020 veel gebruikt in phishingcampagnes met COVID-19-thema's.

Agent Tesla verstuurt e-mails met *.zip-*, *.gz-*, *.cab-*, *.msi-* en *.img*-bestanden en Microsoft Office-documenten met schadelijke VBA-macro's (Visual Basic Application) om systemen van slachtoffers te compromitteren. Van de phishing-campagnes is bekend dat ze nauwkeurig de communicatietoon en visuele identiteit van een legitiem bedrijf reproduceren, inclusief logo's en lettertypen.

De malware kan verschillende soorten gegevens verzamelen, waaronder toetsaanslagen, inloggegevens die worden gebruikt in browsers, e-mailsoftware, draadloze profielen en andere waardevolle informatie.

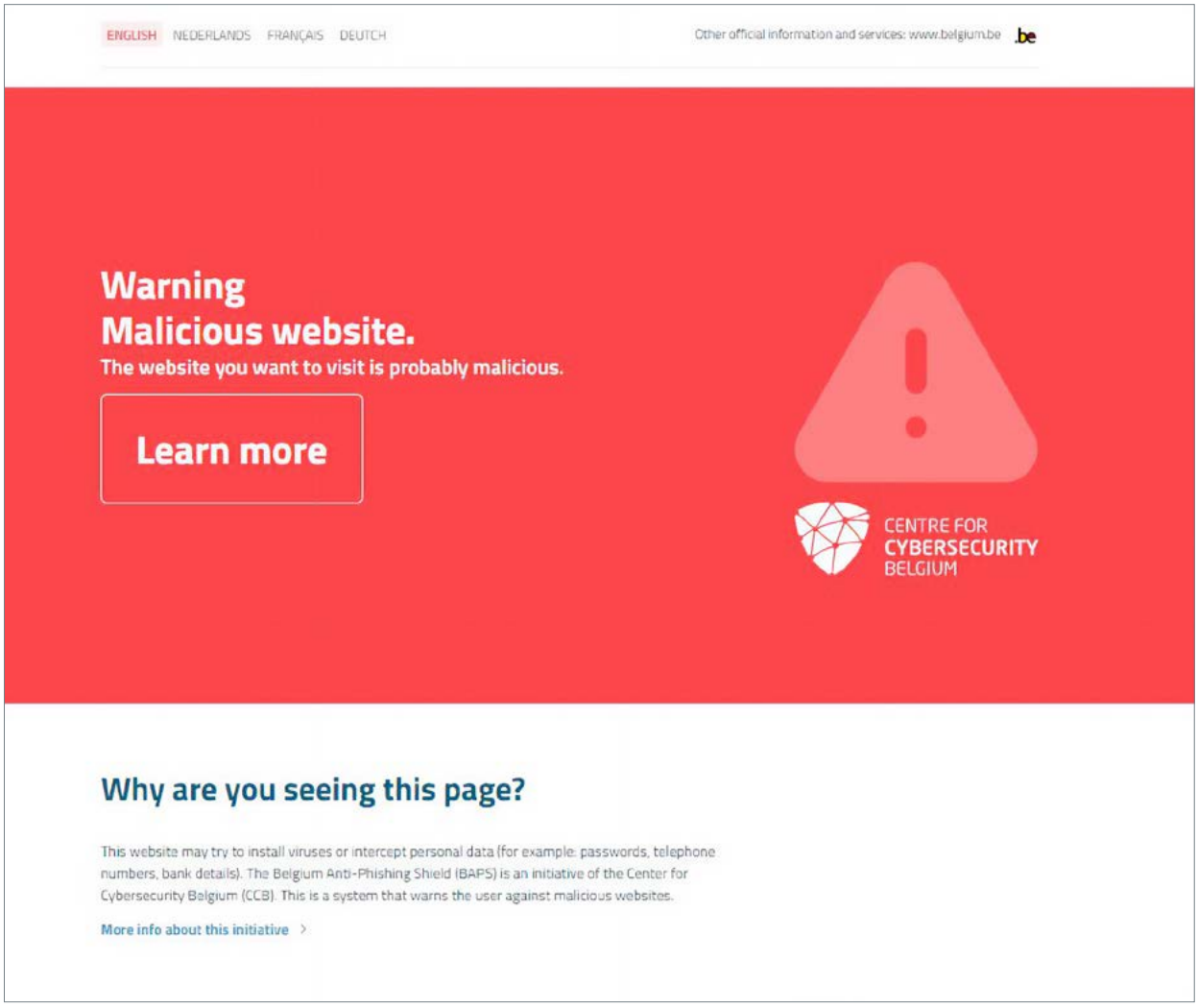
1 https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/agent-tesla
https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/agent-tesla-malware

SAFEONWEB EN HET BELGISCH ANTI-PHISHING SHIELD

Om het Belgische publiek te helpen veilig te surfen en zich beter te beschermen tegen cyberbedreigingen en kwetsbaarheden, biedt het CCB de dienst Safeonweb aan, die de nodige actuele informatie en speciale campagnes over een specifiek onderwerp biedt. De Belgische Cybersecurity 2.0-strategie stelt: "Het internet is van en voor iedereen. Ook de veiligheid ervan is een gezamenlijke inspanning. Daarom wordt de bevolking aangespoord om deel te nemen aan de beveiliging."

Safeonweb is een zeer goed voorbeeld van constructieve samenwerking tussen overheidsinstellingen, burgers en de privésector, aangezien het de mogelijkheid biedt om phishingactiviteiten te bestrijden door verdachte links en berichten te melden aan verdacht@safeonweb.be. Op basis van deze dienst heeft het CCB het Belgian Anti-Phishing Shield-initiatief (BAPS) gecreëerd als onderdeel van de Active Cyber Protection-aanpak, dat internetgebruikers in België waarschuwt voor gevaarlijke websites (zoals de websites die gebruikt worden bij phishingpogingen) en gemelde verdachte links doorstuurt naar onze waarschuwingspagina.

In de eerste drie kwartalen van 2023 werden meer dan 7 miljoen berichten (7 207 167) verstuurd naar verdacht@safeonweb.be, tegenover bijna 4 miljoen berichten in dezelfde periode vorig jaar (3 954 641 in 2022), wat duidelijk het bereik en de burgerbetrokkenheid aantoont. Als gevolg van deze berichten kon het CCB 633 361 unieke URL's en 163 736 unieke domeinen die als kwaadaardig werden beschouwd, omleiden. Tussen januari en september 2023 waarschuwde het BAPS-systeem Belgische burgers 5 736 374 keer dat ze een kwaadaardige website of server probeerden te raadplegen.

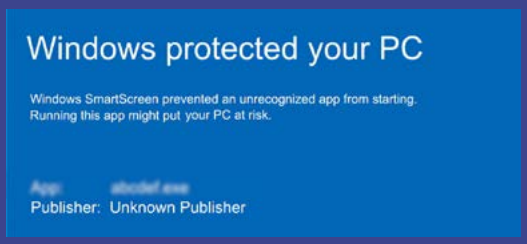


Bron: https://baps.safeonweb.be/

Belgisch Anti-Phishing Shield (BAPS)

Hoe werkt het?

1. Het CCB ontvangt informatie over mogelijk schadelijke websites wanneer internet-gebruikers verdachte berichten doorsturen naar verdacht@safeonweb.be.
2. De bijlagen en andere links worden vervolgens uit de verdachte berichten gehaald. De URL's worden ook uit schermafbeeldingen en QR-codes gehaald.
3. Het analyseert de URL/link/bijlage. Als het een schadelijke site blijkt te zijn, wordt er een lijst met schadelijke sites naar onze partners gestuurd (zoals ISP's, Google Safe Browsing en Microsoft SmartScreen).



4. Wanneer een internetgebruiker op een link klikt die naar een kwaadaardige site leidt, vergelijkt de ISP in kwestie het DNS-verzoek met de lijst van kwaadaardige sites.
5. De gebruiker wordt omgeleid naar een waarschuwingspagina en kan de kwaadaardige site niet bezoeken.

Actieve cyberbeveiliging – spear warnings

Het Centrum voor Cybersecurity België (CCB) introduceerde het Spear Warning-concept begin 2021. Het belangrijkste doel van spear warnings is om bedrijven en particulieren tijdig op de hoogte te brengen van een cyberdreiging, zodat ze op tijd actie kunnen ondernemen om een cyberaanval te voorkomen. De term "Spear Warning" (SW) is een woordspeling op "Spear Phishing", een modus operandi gebruikt door cybercriminelen die bestaat uit het verzenden van zeer gerichte phishing-e-mails naar potentiële slachtoffers, meestal met de bedoeling om hen te overhalen hun persoonsgegevens te delen. Spear warnings vallen ook onder het concept van Active Cyber Protection (ACP), dat nu is opgenomen in de Europese NIS2-richtlijn.

Het spear warning-concept is erop gericht om internetgebruikers (bedrijven of eindgebruikers) "actief" te benaderen, per e-mail, brief of zelfs telefonisch (de snelste en meest effectieve manier in het geval van een acute dreiging). Op deze manier kunnen ze proactief en tijdig worden geïnformeerd over cyberdreigingen of kwetsbaarheden. Het feit dat deze persoonlijke boodschap rechtstreeks van het CCB komt, zou in principe nog meer aandacht moeten trekken.

VOORKOMEN DAT CYBERCRIMINELEN TOT ACTIE OVERGAAN

Het CCB verzendt spear warnings om te vermijden dat de dreigingsactor zijn doelen bereikt, zoals het compromitteren van systemen, deze onbeschikbaar maken of het exfiltreren van gegevens.

De spear warnings van het CCB maken vaak deel uit van langlopende campagnes en hebben voornamelijk betrekking op:

- kwetsbare IT-systemen die verbonden zijn met het internet en die cybercriminelen gemakkelijk kunnen compromitteren/aanvallen/uitbuiten;
- kritieke kwetsbaarheden die een impact kunnen hebben op Belgische organisaties;
- lekken van identificatiegegevens en ongeoorloofde toegang tot de gegevens van Belgische bedrijven voor verkoop op cybercriminele fora, die gebruikt kunnen worden voor andere spear phishing-campagnes;
- systemen die geïnfecteerd zijn met malware die gebruikt kan worden voor een grotere cyberaanval, zoals het geval is wanneer Belgische infrastructuren gecompromitteerd zijn door malware die gebruikt wordt als voorloper van ransomwareaanvallen;
- verdachte certificaten en domeinregistraties;
- meldingen van aangetaste bedrijfsmiddelen.

HET VERLOOP

Een van de belangrijkste onderdelen van het spear warning-concept is de detectie van cyberdreigingen en -kwetsbaarheden voor de hele Belgische cyberspace, en dit is een van de belangrijkste opdrachten van het CCB. Het CCB gebruikt verschillende technieken en processen voor de "verzamelprocessen": technische oplossingen, informatiebronnen (open en commercieel) en partnerschappen. Wat de kwetsbaarheden betreft, heeft het CCB een nationaal "Vulnerability Management"-project opgestart om prioriteit te geven aan kwetsbaarheden en te bepalen voor welke kwetsbaarheden een spear warning zal worden gegeven. Zodra een kwetsbaarheid is geselecteerd, begint het spear warning-proces, waarbij de betrokken organisaties worden geïnformeerd en voorzien van de volgende informatie:

- een risico- en impactanalyse van de kwetsbaarheid,
- aanbevolen acties,
- actieve uitbuiting door cybercriminelen.

Een andere vorm van het spear warning-concept bestaat uit het versturen van geautomatiseerde berichten over kwetsbaarheden en infecties in de IT-infrastructuur naar organisaties die zich op deze dienst abonneren en het IP-bereik delen met het CCB, aangezien er in dit geval geen IP-identificatie plaatsvindt. Met de lancering van het safeonweb@work-project kan elk bedrijf zich op deze dienst abonneren.

Bij grote incidenten maken spear warnings soms deel uit van een bredere procedure die ook persberichten, het publiceren van berichten op websites, het versturen van waarschuwingen via een systeem voor vroegtijdige waarschuwing en zelfs het organiseren van specifieke webinars omvat. Spear warnings leveren een belangrijke bijdrage aan de officiële opdracht van het CCB om van België een van de minst kwetsbare cyberruimtes in Europa te maken. Door beter geïnformeerd te zijn, kunnen organisaties hun niveau van cyberveiligheid aanzienlijk verhogen. Hierdoor worden hun IT-systemen minder blootgesteld aan aanvallen van cybercriminelen, die steevast de weg van de minste weerstand kiezen.

Het komt vaak voor dat organisaties een spear warning van de CCB ontvangen en toegeven dat ze niet op de hoogte waren van het beveiligingsprobleem, de kwetsbaarheid, het datalek of de infectie van hun IT-systemen. In sommige gevallen was de aanval al in volle gang of in voorbereiding op het moment dat het slachtoffer de spear warning van het CCB ontving en kon die persoon dus op tijd reageren.

Het Centrum voor Cybersecurity van België (CCB) kondigt met trots aan dat het met het baanbrekende project “Spear Warning” de Publica Awards heeft gewonnen in de categorie “Security & Safety”. De Publica Awards erkennen uitmuntendheid in overheidsprojecten en het CCB is verheugd dat het deze prestigieuze wedstrijd heeft gewonnen die plaats vond op 16 november 2023 in Brussel. in Brussels on 16 November 2023.

“We zijn erg blij en dankbaar dat we deze prijs van de Publica Awards hebben ontvangen. Deze prijs bevestigt de impact en innovatie van het Spear Warning-project. Het toont aan dat proactieve maatregelen zoals deze een cruciale rol spelen bij het versterken van de digitale weerbaarheid van onze samenleving. We zullen ons blijven inspannen om de cybersecurity te verbeteren en onze burgers en bedrijven te beschermen tegen steeds veranderende dreigingen.”

Miguel De Bruycker, Directeur-generaal CCB

SPEAR WARNING – HAFNIUM: HET EERSTE BELANGRIJKE PRAKTIJKGEVAL

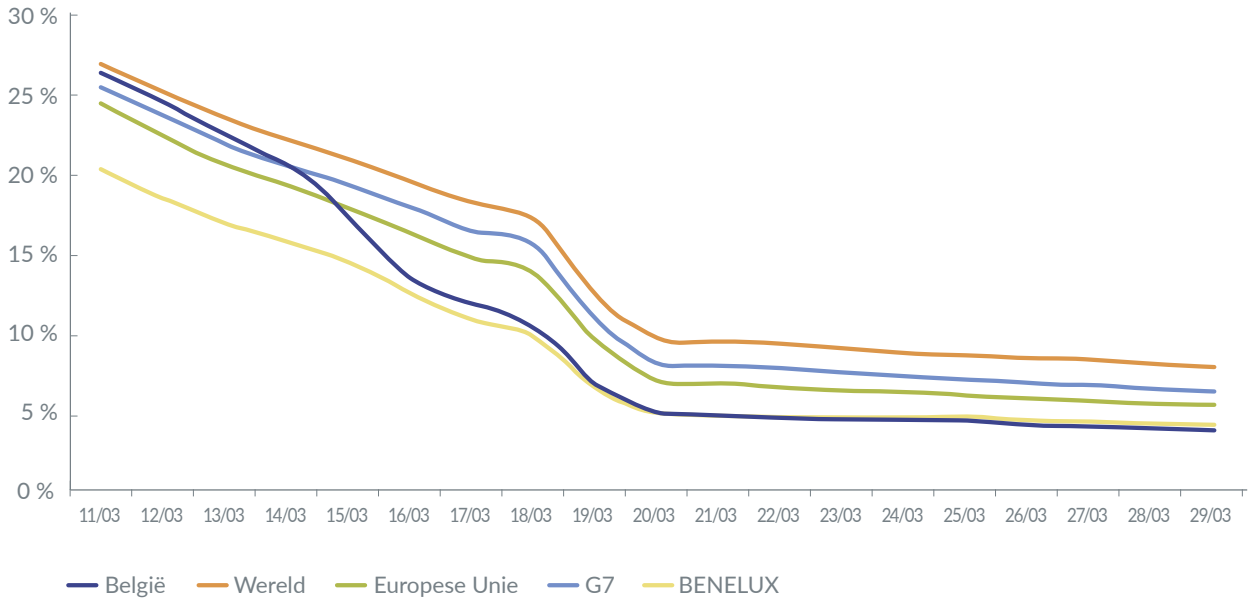
Hafnium maakte gebruik van een fout in Microsoft Exchange en op dat moment waren veel Belgische Exchange-installaties kwetsbaar en blootgesteld aan het internet. België had het hoogste percentage kwetsbare en blootgestelde Microsoft Exchange-systemen. De introductie van het spear warning-systeem markeerde echter het begin van een positieve trend. De eerste spear warning die naar potentiële slachtoffers werd verstuurd, leidde tot een aanzienlijke vermindering van het aantal kwetsbare systemen.

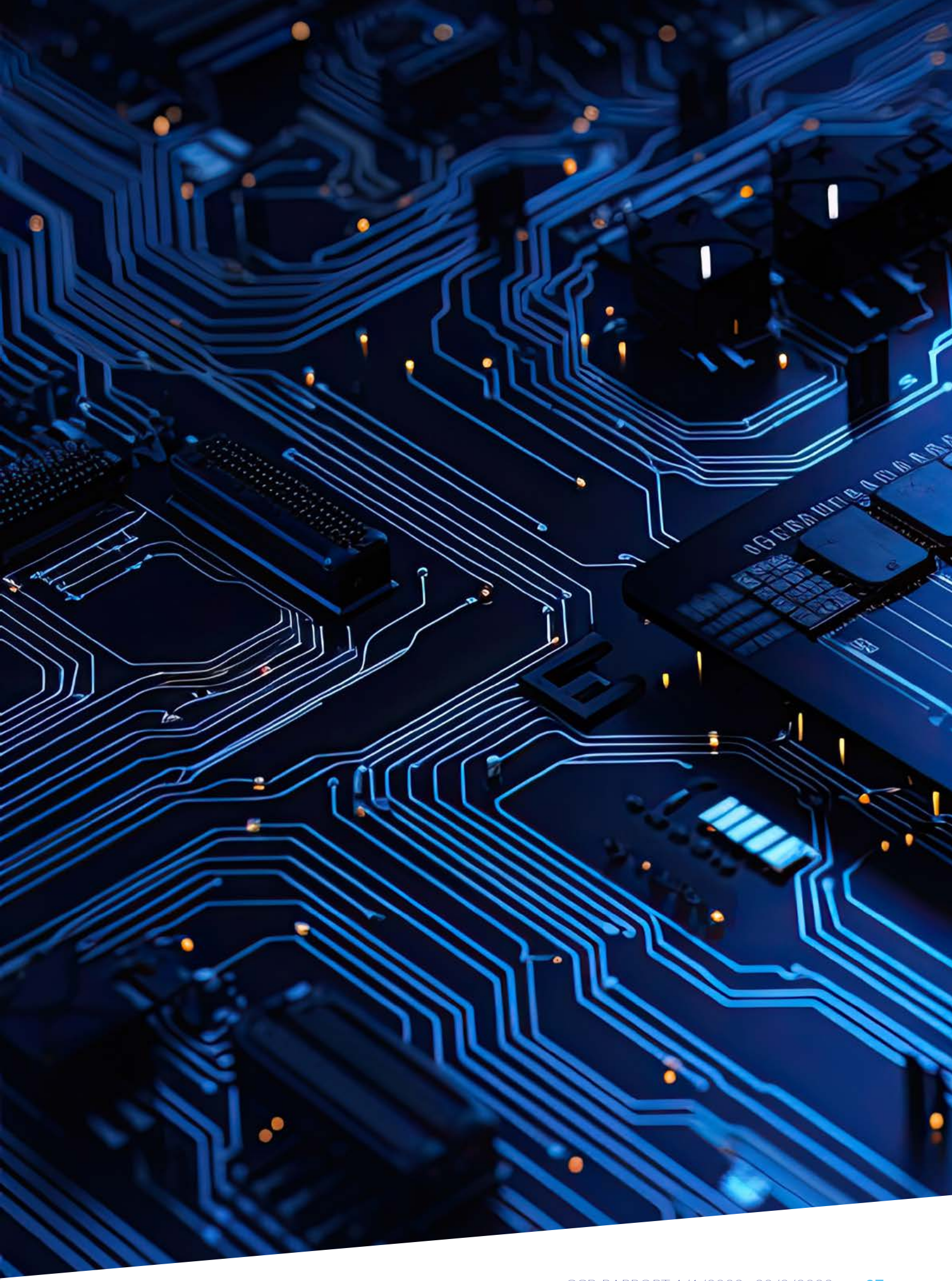
De situatie verbeterde nog verder met de tweede spear warning, wat leidde tot een opmerkelijke ommekeer. België ging van het hoogste aantal kwetsbare systemen naar het laagste aantal, wat de doeltreffendheid van het spear warning-systeem aantoont.

- Planning en beheer: formulering van een strategisch plan en voorbereiding van de identificatie van kwetsbaarheden met de grootste impact op de Belgische cyberruimte.
- Inzameling: uitvoeren van een volledige scan om kwetsbare systemen in België op te sporen.
- Verwerking en exploitatie: identificatie van de eigenaren van deze kwetsbare systemen.
- Analyse en productie: start van een communicatiecampagne om systeemeigenaars te informeren over hun kwetsbaarheden.
- Verspreiding: na een bepaalde periode worden systemen opnieuw beoordeeld om te bepalen of ze nog kwetsbaar zijn.
- Feedback: indien nodig worden herinneringen verstuurd naar systeemeigenaren.

2021

Meldingen verstuurd naar 1259 kwetsbare organisaties
Meldingen verstuurd naar 355 getroffen organisaties
Daarna zijn er meerdere herinneringen verstuurd





KRITIEKE KWETSBAARHEDEN

Kritieke kwetsbaarheden in het cyberdreigingslandschap tussen januari en september 2023

Actoren met verschillende belangen maken bij hun aanvallen gebruik van kritieke kwetsbaarheden. Ze worden steeds sneller in het bewapenen van 'zero-day'-kwetsbaarheden in hun voordeel dan dat ze hun cyberbeveiligingsmaatregelen via organisatie bijwerken. Er is ook vastgesteld dat actoren met succes gebruik maken van reeds bestaande kwetsbaarheden in "ongepatchte" software wanneer organisaties ontoereikende beveiligingsmaatregelen nemen.

CVEs staat voor Common Vulnerability Exposures (algemene kwetsbaarheden). Wanneer cybersecurity onderzoekers of organisaties nieuwe kwetsbaarheden ontdekken, voegen ze deze toe aan de CVE-lijst die wordt bijgehouden door de MITRE Corporation. Er wordt een CVE-identificatienummer aan de kwetsbaarheid toegekend, zodat deze gemakkelijker kan worden geïdentificeerd en kan worden beschermd.

De vijf meest kritieke kwetsbaarheden door actoren misbruikt in 2023

CVE-2023-0669

CVE-2023-0669, een zero-day-kwetsbaarheid in Fortra's GoAnywhere Managed File Transfer (MFT)-tool, een platform voor het centraal beheer van interne en externe bestandsoverdracht, werd actief uitgebuit door actoren, waaronder ransomware-groepen. Deze kwetsbaarheid maakt remote code execution (RCE) mogelijk, wat getroffen systemen kan compromitteren of kan leiden tot wijdverspreide datalekken en financiële afpersing. De beheerde software voor bestandsoverdracht van een slacht-offer kan worden gebruikt om andere slachtoffers te infecteren door kwaadaardige bestanden te verzenden. Bovendien kan een succesvolle inbraak leiden tot een massale ketenaanval. De Clop-ransomwaregroep richtte zich specifiek op ongeveer 490 000 mensen en bracht hun persoonsgegevens in gevaar door misbruik te maken van deze kwetsbaarheid.

CVE-2023-2868

De kwetsbaarheid CVE-2023-2868 in Barracuda Email Security Gateway-apparaten maakt het moge-lijk dat gebruikersinvoer wordt uitgevoerd als een systeemopdracht, waardoor cyberaanvallers vanop afstand systeemopdrachten kunnen manipuleren met aanzienlijke rechten. Het lek werd uitgebuit in grootschalige campagnes van oktober 2022 tot mei 2023 door een zeer bekwame dreigingsactor, namelijk Mandiant geïdentificeerd als UNC4841. Bijna een derde van de getroffen organisaties waren overheidsinstellingen in alle gewesten. Mandiant denkt dat er een link is met China en dat het, op basis van het waargenomen doelwitprofiel, om een spionagecampagne zou kunnen gaan.

CVE-2023-34362

CVE-2023-34362 is een kritieke zero-day-kwets-baarheid in MOVEit Transfer, een oplossing voor bestandsoverdracht. Deze kwetsbaarheid, die kan leiden tot een toename van rechten en ongeautori-seerde toegang tot de omgeving. Ze werd op grote schaal misbruikt door de Cl0p-ransomwaregroep om gegevens van organisaties te stelen. De auteurs van de Cl0p-ransomware beweerden toegang te hebben gekregen tot informatie van “honderden” bedrijven die MOVEit-software gebruikten en begonnen met het opstellen van een lijst van slacht-offers op hun Data Leak Site (DLS).

CVE-2023-23397

Een andere kwetsbaarheid die op grote schaal wordt misbruikt door cyberbedreigers is CVE-2023-23397, een kritieke toename van de kwetsbaarheid van rechten in alle ondersteunde versies van de e-mailclient Microsoft Outlook voor Windows. Door deze fout kunnen aanvallers verificatiemaatregelen omzeilen, waardoor onbevoegden toegang krijgen tot vertrouwelijke gegevens en zich kunnen voordoen als gebruikers binnen organisaties.

CVE-2023-38831

CVE-2023-38831 is een beveiligingslek in het archiveringsprogramma WinRAR voor Windows, waardoor cybercriminelen een willekeurige code kunnen uitvoeren wanneer een gebruiker een bestand in een ZIP-archief probeert te bekijken. Deze kwetsbaarheid is op grote schaal uitgebuit door cybercriminele organisaties en door staten gesponsorde actoren, zoals APT 28, Sandworm, DarkPink of APT40, om remote code uit te buiten.

Het CCB publiceert altijd technische adviezen waarin wordt gewaarschuwd voor de mogelijke uitbuiting van kwetsbaarheden en waarin de juiste acties worden aanbevolen om de risico's te beperken, zoals “patches” toepassen.

In het geval van kritieke kwetsbaarheden met een hoog risico op impact in België, stuurt het CCB spear warnings uit, waarmee Belgische organisaties direct op de hoogte worden gebracht van de dreiging en de dringende noodzaak om “patches” toe te passen. Deze proactieve aanpak beschermt Belgische slachtoffers en voorkomt met succes dreigende aanvallen, zoals ransomwareaanvallen waarbij misbruik wordt gemaakt van kwetsbaarheden.

Overzicht van Belgische Cyber Metrics in 2023

2023	Q1	Q2	Q3
PHISHING			
Ontvangen mails	2.695.345	2.381.106	2.130.716
Unieke URL's geclassificeerd als kwaadaardig	186.792	237.740	211.031
Unieke domeinen geclassificeerd als kwaadaardig	12.382	93.481	59.727
BAPS			
Aantal hits op de waarschuwingspagina	2.031.888	2.464.489	1.239.997
WAARSCHUWINGEN			
Technische adviezen gepubliceerd op www.cert.be	35	39	41
Technische tweets	67	67	79
Spear warnings			
Automatisch verwerkt	1.193	863	1.221
Handmatig verwerkt	1.653	946	1.255
Totaal	2.846	1.809	2.476
INCIDENTEN			
Ransomware (gemeld)	28	20	31
Denial of Service	6	10	5
COMMUNICATIE			
Websites			
Sessies www.safeonweb.be	674.243	615.379	450.365
Nieuwsitems op Safeonweb	22	19	16
CCB-evenementen			
Connect & Share events	2	2	0

BELGISCHE CYBER METRICS IN 2023

Bewustmaking en opbouw van een sterke gemeenschap van professionals uit de cybersecuritysector

Het Connect & Share-initiatief van het CCB heeft als doel meer bewustzijn te creëren en een gemeenschap op te bouwen door cyberbeveiligingsprofessionals samen te brengen, zodat ze hun gedachten kunnen delen over de verschillende cyberbedreigingen in België en de rest van de wereld. Als onderdeel daarvan werden er in 2023 verschillende evenementen georganiseerd met een hoge opkomst, zowel face-to-face als in hybride vorm:

12 JANUARI 2023 – QUARTERLY CYBER THREAT REPORT Q4 2022 EVENT

De CCB-professionals onderzochten de cyberbedreiging samen met deskundigen van bedrijven die gespecialiseerd zijn in cyberbeveiliging, met een focus op cloudbeveiliging en de energiesector.

19 JANUARI 2023 – ICS RAPID RESPONSE EVENT

Het evenement, georganiseerd door SANS en het CCB, bood ervaren ICS-specialisten en niet-ICS-specialisten de gelegenheid om presentaties bij te wonen over verschillende onderwerpen, waaronder: Five Critical Controls, Defensible Architecture, OT Visibility, Threat Intelligence en OSINT.

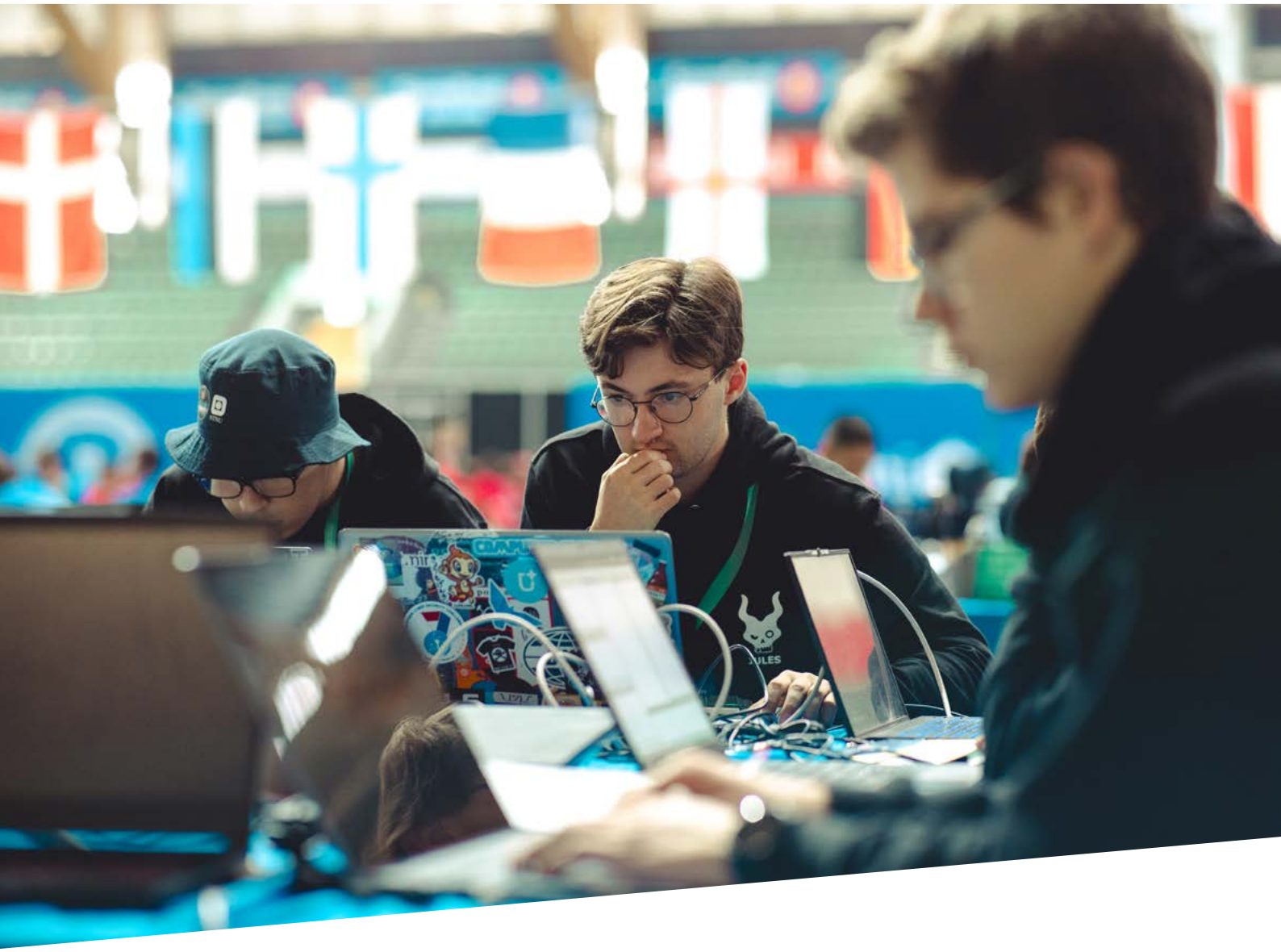
20 APRIL 2023 – QUARTERLY CYBER THREAT REPORT Q1 2023 EVENT

Het CCB organiseerde een nieuw evenement om de bevindingen uit het eerste kwartaal van 2023 te bekijken en onderwerpen te bespreken zoals DDoS-aanvallen, wifi-beveiliging, malware en de laatste waarnemingen over spionage en hacktivisme. Het was ook een gelegenheid voor de deskundigen om hun nieuwste bevindingen te delen.

25 MEI 2023 – 11e EU MITRE ATT&CK® COMMUNITY WORKSHOP

Het CCB organiseerde samen met MITRE Engenuity een hybride evenement om updates voor te stellen over het gebruik van het ATT&CK®-framework voor een betere verdediging tegen dreigingen. Op het evenement kwamen presentaties aan bod van het CCB, MITRE Engenuity en andere ontwikkelaars van systemen en tools die het ATT&CK®-framework ondersteunen.

CONNECT & SHARE EVENTS



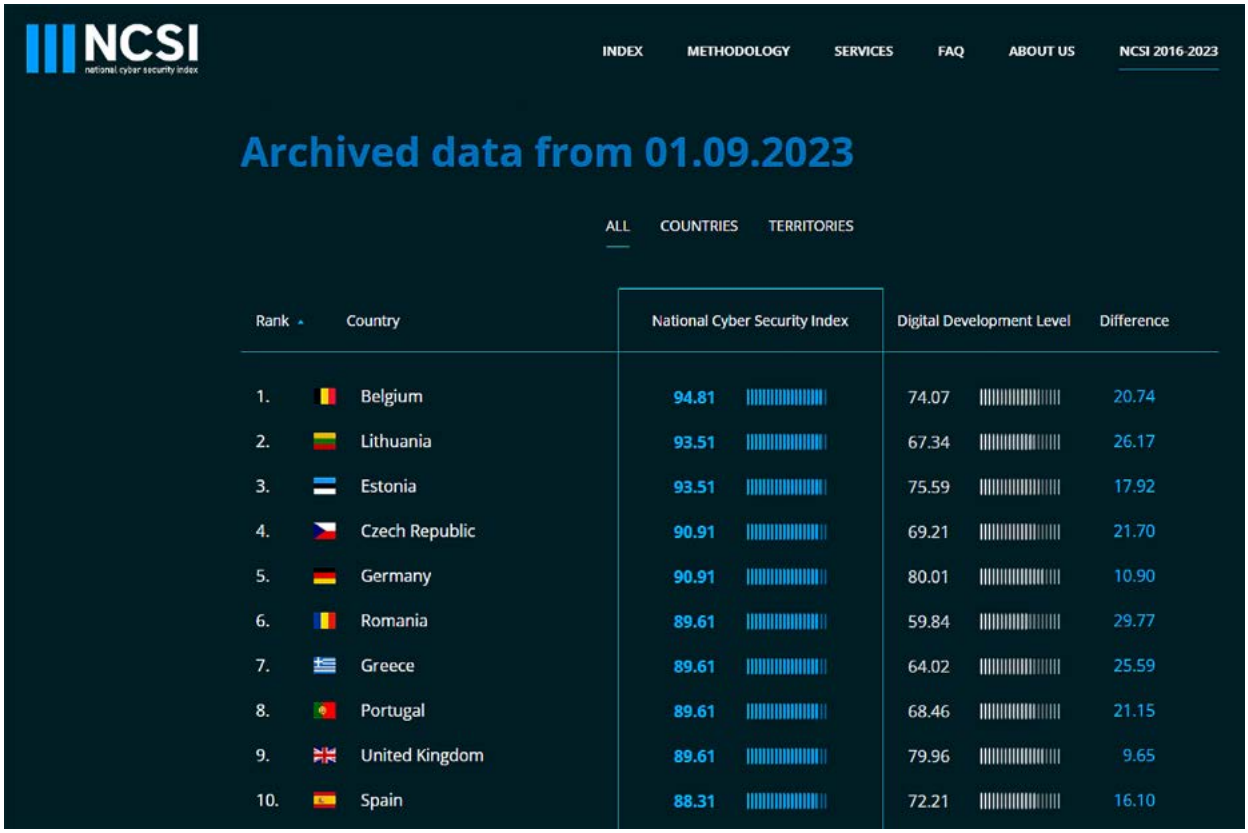
BELGIË IN DE WERELD

Belgische cybersecurity in internationale ranglijsten

België bekleedt vaak een zeer goede algemene positie in internationale ranglijsten op het vlak van cybersecurity en de bereidheid om cyberdreigingen te voorkomen en cyberincidenten die nationale organisaties treffen, te beheren.

In 2023 stond België wereldwijd op de eerste plaats, volgens de National Cyber Security Index, de live wereldwijde index die meet in hoeverre landen voorbereid zijn om cyberbedreigingen te voorkomen en cyberincidenten te beheren.

De NCSI-score geeft aan hoeveel procent het land kreeg ten opzichte van de maximumwaarde van de indicatoren die op basis van de gebruikte methodologie in aanmerking werden genomen.



Rank	Country	National Cyber Security Index	Digital Development Level	Difference
1.	Belgium	94.81	74.07	20.74
2.	Lithuania	93.51	67.34	26.17
3.	Estonia	93.51	75.59	17.92
4.	Czech Republic	90.91	69.21	21.70
5.	Germany	90.91	80.01	10.90
6.	Romania	89.61	59.84	29.77
7.	Greece	89.61	64.02	25.59
8.	Portugal	89.61	68.46	21.15
9.	United Kingdom	89.61	79.96	9.65
10.	Spain	88.31	72.21	16.10

Bron: https://ncsi.ega.ee/ncsi-index/?archive=1

Belgische cyberkampioenen: De Red Daemons op de ECSC 2023

In oktober 2023 reisde het Red Daemons-team af naar Hamar, Noorwegen, om België met trots te vertegenwoordigen op de 8e jaarlijkse European Cyber Security Challenge (ECSC). De Red Daemons namen het op tegen teams uit 29 andere Europese landen en beleefden drie intense dagen, waarbij ze beveiligingsuitdagingen moesten aanpakken om punten te verzamelen. België nam voor de zesde keer deel aan dit prestigieuze internationale evenement.

Zoals gewoonlijk werden er tien cybertalenten geselecteerd uit de winnende teams van de Cyber Security Challenge Belgium (CSCBE), die in maart van hetzelfde jaar werd gehouden. In de afgelopen zeven jaar heeft de Cyber Security Challenge België de interesse gewekt van duizenden Belgische studenten die hun vaardigheden wilden testen, wilden bijleren en betrokken wilden zijn bij de spannende wereld van cybersecurity.

De vraag naar cybersecuritydeskundigen bij bedrijven, organisaties en veiligheids- en politiediensten neemt toe. Dankzij een samenwerking tussen het CCB en NVISO kunnen de Red Daemons deelnemen aan dit evenement. Deze partners staan elk jaar in voor de organisatie van het evenement, de sponsoring en de organisatie van de voorbereidende workshops.

NVISO organiseert jaarlijks de nationale competitie (CSCBE) met de steun van het CCB.

Evenementen zoals de ECSC en de CSCBE spelen een cruciale rol bij het aanmoedigen van jonge mensen om een dynamische carrière in cybersecurity te ambiëren.

Volg de Belgian Red Daemons op sociale media:

- X: @BelRedDaemons
- Instagram: @belgianreddaemons
- Facebook: https://www.facebook.com/BelRedDaemons

CYBER SPOTLIGHT: AI & CYBERSECURITY

Cyber Spotlight: AI & Cybersecurity

Achter de huidige hype rond AI in de technologische wereld schuilt een echte onderliggende trend naar het gebruik van AI in alle sectoren. Cybersecurity vormt hierop geen uitzondering en de innovatie en het multi-disciplinaire karakter van een breed scala aan technologieën maken het een onderwerp bij uitstek voor AI-toepassingen. Om de interacties tussen deze twee onderwerpen beter te begrijpen, kunnen de volgende drie **belangrijke convergentiegebieden** worden gedefinieerd:

- AI 'voor' cybersecurity: hoe kunnen cybersecuritydeskundigen AI gebruiken om de bescherming van hun systemen te verbeteren (bv. malwareanalyse en detectie van aanvallen)?
- AI 'tegen' cybersecurity: hoe kunnen hackers voordeel halen uit AI om hun technieken en tactieken te verbeteren (bv. deepfake en het opsporen van kwetsbaarheden)?
- Beveiliging van AI-toepassingen: zijn er kwetsbaarheden in AI-toepassingen en hoe kunnen ze worden beschermd (bv. tegen datavergiftiging en modelontwijking)?

Deze verschillende benaderingen zijn talrijk en evolueren voortdurend, maar we zullen ons best doen om ze in een reeks artikelen aan te kaarten. Het eerste artikel gaat over chatbots en Large Language Models (LLM's). We hebben beslist om ons te richten op de derde benadering, AI-beveiliging, vanuit het oogpunt van de gemiddelde gebruiker.

ALGEMENE OVERWEGINGEN VOOR EEN VEILIG EN VERANTWOORD GEBRUIK VAN GENERATIEVE AI

Generatieve AI zoals ChatGPT en Bard, die zich baseren LLM's, worden steeds populairder. Veel Belgen hebben ze eveneens geïntegreerd om hun productiviteit te verbeteren. In deze context heeft het CCB gewezen op het belang om de problemen die deze technologieën met zich meebrengen, duidelijk te definiëren.

We willen hier een eerste lijst van “goede reflexen” voorstellen voor een veilig en verantwoord gebruik van deze technologieën.

Ter inleiding: ook al lijkt het een kwestie van gezond verstand, het is essentieel om nooit blindelings te vertrouwen op de antwoorden van chatbots en altijd kritisch te blijven. Aangezien de antwoorden van deze tools onvolmaakt zijn, moeten ze altijd worden herlezen en gecorrigeerd. Bovendien hebben chatbots over het algemeen geen logisch redeneervermogen; ze zijn getraind om woordreeksen met een hoge mate van waarschijnlijkheid te genereren.

Daarnaast moet bijzondere aandacht worden besteed aan de volgende aspecten:

- Bescherm vertrouwelijke gegevens: vermijd het delen van gevoelige informatie, aangezien AI-chatbots deze gegevens kunnen opslaan en hergebruiken. Schakel het opslaan van gespreksgeschiedenis indien mogelijk uit.
- Foutdetectie: AI-chatbots maken fouten, dus vertrouw ze alleen taken toe waarover je voldoende kennis hebt (zodat je de resultaten kunt verifiëren en controleren).
- Factchecking: controleer de feiten (factchecking), omdat chatbots vaak bronnen weglaten.
- Automatisering: door AI-chatbots te vaak te gebruiken, geeft men soms de voorkeur aan de resultaten daarvan en vertrouwt men er te veel op, terwijl mensen op veel gebieden competenter zijn.
- Beperkingen en vooroordelen: AI-chatbots kunnen worden beïnvloed door vooroordelen en worden beperkt in hun kennis door hun trainingsgegevens. Leg ze verschillende bronnen voor om een objectieve en volledige context te verkrijgen.
- Transparantie: gebruik chatbots transparant. Probeer het gebruik ervan niet te verbergen, maar deel het mee. Dat versterkt het vertrouwen en de verantwoordelijkheid.
- Copyright: de antwoorden van chatbots kunnen inbreuk maken op het auteursrecht, dus wees voorzichtig als je ze gebruikt voor academische of commerciële doeleinden.
- Menselijkheid: vergeet niet dat chatbots geen geweten en emotie hebben. Let op voor emotionele manipulatie.

Indien gebruikers met al deze aspecten rekening houden, denken we dat ze effectief gebruik kunnen maken van chatbots als ze de beperkingen begrijpen en verantwoordelijk handelen.

WIE ZIJN WIJ?

Wie zijn wij?

Het Centrum voor Cybersecurity België (CCB) is de nationale autoriteit voor cyberveiligheid in België. Het CCB is opgericht bij koninklijk besluit op 10 oktober 2014 en staat onder het gezag van de eerste minister.

Door optimale informatie-uitwisseling kunnen bedrijven, de overheid, aanbieders van essentiële diensten en de bevolking zich gepast beschermen.

Het CCB superviseert, coördineert en waakt over de toepassing van de Belgische cyberveiligheidsstrategie, die in 2021 werd goedgekeurd door de Nationale Veiligheidsraad. Het is zijn opdracht om van België tegen 2025 een van de minst cyberkwetsbare landen in Europa te maken.

Het CCB speelt een sleutelrol om België te helpen deze doelstelling te bereiken, onder meer door het verstrekken van informatie en meer bewustzijn te creëren over de belangrijkste cyberbedreigingen en hoe men zich ertegen kan beschermen.

Volg het Centrum voor Cybersecurity België op sociale media en op de website:

- X: @CCBbelgium
- X: @CCBAlerts
- LinkedIn
- www.ccb.belgium.be

Verantwoordelijke uitgever
Centrum voor Cybersecurity België
Mr. De Bruycker, Directeur-generaal
Wetstraat 18, 1000 Brussel

Wettelijk depot
D/2024/14828/002