CENTRE FOR
CYBERSECURITY
BELGIUM 10Y

ZEHN JAHRE ZENTRUM FÜR CYBERSICHERHEIT BELGIEN

Centre for Cybersecurity Belgium
Unter der Autorität des Premierministers

.be

Verantwortlicher Herausgeber
Zentrum für Cybersicherheit Belgien
M. De Bruycker, Generaldirektor
Wetstraat 18
1000 Brüssel

Recherche, Interviews und Redaktion
the content company

Endredaktion
Katrien Eggers
Michele Rignanese

Fotografie
AdobeStock, Eigenes Archiv ZCB, Karakters, Cookiecutter & Ron Lach for Pexels

Formatierung
Karakters.be

Druck
Druckerei Belgische Kammer der Volksvertreter

Gesetzliche Hinterlegung
D/2025/14828/008

INHALT

Sehr geehrte Leserinnen und Leser,

vor zehn Jahren wurde mit der Gründung des Zentrums für Cybersicherheit Belgien (ZCB) eine zentrale Anlaufstelle für Cybersicherheit in unserem Land geschaffen. Was mit einem Königlichen Erlass auf dem Papier und der Einstellung von zwei engagierten Vordenkern begann, hat sich zu einer angesehenen nationalen Behörde entwickelt, die von einem vielfältigen Team von fast 140 Fachleuten getragen wird. Gemeinsam mit zahlreichen Partnern wachen wir Tag und Nacht über die digitale Sicherheit von Bürgerinnen und Bürgern, Unternehmen und Behörden.

Unsere Wirtschaft und Gesellschaft verlassen sich immer mehr auf digitale Netzwerke. Aber auch die Cyberangriffe werden immer raffinierter und gezielter. Cybersicherheit ist daher ein wesentlicher Baustein unserer Gesellschaft. Die Europäische Union hat in den letzten Jahren den Rechtsrahmen gestärkt, unter anderem durch die NIS1- und NIS2-Richtlinien, den Cybersecurity Act und den Cyber Resilience Act. Jede dieser Initiativen bringt zusätzliche Aufgaben und Verantwortlichkeiten mit sich, aber vor allem auch die Möglichkeit, die Messlatte für die Cybersicherheit noch höher zu legen.

Von unserer zentralen Rolle aus koordinieren wir die Nachverfolgung von Sicherheitsvorfällen, unterstützen wichtige Sektoren und konzentrieren uns auf die Prävention. Vom ersten Tag an haben wir daher nicht nur in Technologie, Know-how und Verfahren investiert, sondern vor allem in die Sensibilisierung und Einbeziehung der Bürgerinnen und Bürger. Denn es ist vor allem das kollektive Handeln aller Bürgerinnen und Bürger und Unternehmen, das zur Erhöhung unserer Cyberresilienz führt. Einfache grundlegende Maßnahmen wie die Überprüfung in zwei Schritten und die rechtzeitige Aktualisierung der Software sind nach wie vor die wirksamsten Mittel zur Verhinderung von Schäden.

Wir sind daher stolz darauf, dass Safeonweb zu einer vertrauenswürdigen Anlaufstelle für die breite Öffentlichkeit geworden ist, mit klaren Tipps und der Möglichkeit, verdächtige Nachrichten einfach zu melden. Jede Meldung hilft uns, schneller zu reagieren, gezieltere Informationen zu liefern und gemeinsam stärker zu sein. Und mit Safeonweb@Work, einschließlich seiner praktischen Leitlinien

und Scans, helfen wir Unternehmen, sich Schritt für Schritt besser zu wappnen.

Inzwischen hat sich auch unser Ökosystem professionalisiert. Durch die enge und vertrauensvolle Zusammenarbeit zwischen öffentlichen Diensten, dem Privatsektor und der Wissenschaft konnte Belgien unter der Koordination des ZCB zu einem europäischen Vorbild für Cybersicherheit werden.

Diese Broschüre blickt auf ein Jahrzehnt des Lernens, Experimentierens und der Einführung von Best Practices zurück. Aber sie blickt auch in die Zukunft, da der Aufstieg der KI und die geopolitische Bedrohungsdynamik neue Herausforderungen mit sich bringen. Unser Engagement und unser Einsatz bleiben jedoch unverändert: Wir werden proaktiv Maßnahmen ergreifen, um unser Land bestmöglich zu schützen.

Gemeinsam können wir Belgien zu einem der sichersten digitalen Umgebungen in Europa machen. Das ist unser Ziel. Und dieser Verantwortung können wir nur gerecht werden, wenn wir uns gemeinsam mit Ihnen dafür einsetzen.

Miguel De Bruycker
Generaldirektor

Phédra Clouner
Stellvertretende Generaldirektorin

WAS BEREITS GESCHAH

Das Zentrum für Cybersicherheit Belgien (ZCB) wurde am 10. Oktober 2014 durch einen Königlichen Erlass gegründet und Anfang 2015 in Betrieb genommen. Doch es wurden bereits zuvor Schritte unternommen, um den Internetverkehr in unserem Land zu sichern.

Im Jahr 1993 wurde Belnet ins Leben gerufen, ein föderales Forschungsprogramm zur Entwicklung eines Netzwerks, über das Forschende per Fernzugriff auf Supercomputer zugreifen konnten. Belnet entwickelte sich zu einem Internet-Knotenpunkt und unternahm Anstrengungen, um die Qualität der Verbindungen zu gewährleisten und sie zu sichern.

Im Rahmen von Belnet wurde im Jahr 2004 das Computer Emergency Response Team (Belnet CERT) ins Leben gerufen. Dieses Team beantwortet Anfragen von Mitgliedern des Untersuchungsnetzwerks zu Sicherheitsfragen und -vorfällen.

Darüber hinaus wurde innerhalb der Behörde die Belgian Network & Information Security Platform (BELNIS) ins Leben gerufen. Dabei handelt es sich um ein beratendes Gremium, in dem alle mit digitaler Sicherheit befassten Abteilungen vertreten sind und das sich mit Fragen der Netz- und Informationssicherheit befassen soll. Da das Gremium weder über Entscheidungsbefugnisse noch über finanzielle Mittel verfügte, führte diese Plattform nicht unmittelbar zu konkreten Maßnahmen.

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.

Königlicher Erlass zur Schaffung des Zentrums für Cybersicherheit Belgien

2012: Die erste Cyberstrategie

Die zunehmenden Sicherheitsvorfälle im Bereich der Cybersicherheit haben das Bewusstsein für die Notwendigkeit einer umfassenden nationalen Strategie geschärft. Diese wurde im Jahr 2012 von Luc Beirens von der föderalen Computer Crime Unit der föderalen Polizei und Miguel De Bruycker, der beim ADIV/SGRS, dem Nachrichtendienst für Cybersicherheit des Verteidigungsministeriums, arbeitete, ausgearbeitet. Mit dieser ersten Cybersicherheitsstrategie wurden drei Ziele verfolgt:

- Belgien wird sich für einen sicheren und geschützten Cyberspace einsetzen, der die Grundrechte und Werte der modernen Gesellschaft respektiert.
- Belgien wird sich bemühen, eine optimale Sicherheit und einen optimalen Schutz kritischer Infrastrukturen und staatlicher Systeme vor Cyberbedrohungen zu gewährleisten.
- Belgien will seine eigenen Fähigkeiten im Bereich der Cybersicherheit entwickeln.

Unter den konkreten Maßnahmen zur Umsetzung der Strategie wird in diesem Papier ausdrücklich die Notwendigkeit genannt, die Cybersicherheit zentral und integriert anzugehen, und zwar durch eine zentrale Leitung und die Entwicklung enger öffentlich-privater Partnerschaften. Im Entwurf des Papiers von Beirens und De Bruycker wurde erstmals die Idee geäußert, in Belgien ein unabhängiges Koordinierungszentrum für Cybersicherheit einzurichten.

Zunächst gab es wenig politische Begeisterung für eine solches zentrales Koordinierungszentrum. Eine Reihe von Cybervorfällen im Jahr 2013 und der Amtsantritt einer neuen Föderalregierung Ende 2014 führten jedoch dazu, dass die Cybersicherheit auf der politischen Agenda an Bedeutung gewann.

2013: Der Belgacom-Hack

Einer der bekanntesten Sicherheitsvorfälle aus dieser Zeit war der Belgacom-Hack. Im Sommer 2013 entdeckten niederländische Cyber-Fachleute Spuren eines digitalen Einbruchs beim Telekommunikationsbetreiber Belgacom. In den IT-Systemen wurde eine äußerst raffinierte Spionagesoftware gefunden, die es wahrscheinlich seit 2011 ermöglicht hat, die Kommunikation und Daten von Belgacom und seiner internationalen Tochtergesellschaft BICS abzufangen. Belgacom hat nach dem Vorfall erheblich in die Cybersicherheit investiert. Dutzende Millionen werden in die Erneuerung der IT-Infrastruktur und einen besseren Schutz vor Cyberangriffen investiert.

2013: Eine europäische Cybersicherheitsstrategie

Auch kann die Einrichtung des ZCB nicht losgelöst von den Entwicklungen in der europäischen Cybersicherheitspolitik betrachtet werden. Im Jahr 2004 wurde die European Network and Information Security Agency (ENISA) gegründet. Doch erst im Februar 2013 legte die Europäische Kommission ihre erste Cybersicherheitsstrategie mit dem Titel „An Open, Safe and Secure Cyberspace“ vor. In dieser Strategie wurden Gesetzesinitiativen zur Förderung der Cybersicherheit skizziert, die Bedeutung der Sensibilisierung des öffentlichen und privaten Sektors hervorgehoben und auf die Notwendigkeit hingewiesen, mehr in Forschung und Entwicklung im Bereich der Cybersicherheit zu investieren.

Gleichzeitig ermutigte die Kommission die Mitgliedstaaten, die notwendigen Strukturen für die Cyberresilienz, -kriminalität und -verteidigung einzurichten, um im Falle von Cybervorfällen besser gewappnet zu sein. Die Strategie empfahl, „die Koordinierung zwischen den Ministerien auf nationaler Ebene zu optimieren und in den nationalen Cybersicherheitsstrategien die Rollen und Zuständigkeiten der verschiedenen nationalen Stellen zu definieren“.

“Auch kann die Einrichtung des ZCB nicht losgelöst von den Entwicklungen in der europäischen Cybersicherheitspolitik betrachtet werden. Im Jahr 2004 wurde die European Network and Information Security Agency (ENISA) gegründet.”

2014-2016

DIE GRÜNDUNG

Die rechtliche Grundlage für die Gründung des Zentrums für Cybersicherheit Belgien wurde im Herbst 2014 geschaffen. Das ZCB hat von der Regierung einen klaren Auftrag erhalten: die Überwachung, Koordinierung und Stärkung der Cybersicherheit in Belgien.

So koordiniert das Zentrum beispielsweise die belgische Cybersicherheitspolitik. Es überwacht dessen Umsetzung, schlägt Initiativen vor und arbeitet an neuen Regelungen mit. Eine seiner Hauptaufgaben ist die Sensibilisierung: Es informiert Bürgerinnen und Bürger, Unternehmen und öffentliche Einrichtungen über Online-Risiken und stellt konkrete Instrumente zur Verfügung, um etwas dagegen zu unternehmen. Auf internationaler Ebene vertritt das Zentrum Belgien in europäischen Konzertierungsorganen. Da es sich um einen Auftrag handelt, der Zuständigkeiten und Ministerien überschreitet, wurde das ZCB in die Zuständigkeit des Premierministers gelegt, der die politische Verantwortung trägt.

Das Interesse an der Besetzung der Schlüsselpositionen war groß. Für die Stelle des Direktors gab es 16 niederländischsprachige und 19 französischsprachige Bewerbungen. Für den Posten des stellvertretenden Direktors gab es 27 niederländischsprachige und 29 französischsprachige Bewerbungen. Im Anschluss an die Auswahlrunde wurden Miguel De Bruycker (bis dahin im Verteidigungsministerium beschäftigt) und Phédra Clouner (im Justizministerium tätig) im August 2015 für fünf Jahre zum Direktor bzw. zur stellvertretenden Direktorin ernannt. Bis heute steht dieses Duo an der Spitze der Organisation. Das übrige Team wurde systematisch erweitert: von zwei Mitarbeitenden im August 2015 auf heute mehr als 140.

Erster Strategieplan des ZCB

Um der Erweiterung der Organisation eine Richtung zu geben, erarbeitete das ZCB einen Strategieplan, der am 26. Oktober 2015 der Öffentlichkeit vorgestellt wurde. Der Plan sah einen Zeitplan in drei Phasen vor: eine sechsmonatige Anlaufphase, gefolgt von einer dreijährigen Aufbauphase und einer fünfjährigen Reifephase. Für jede dieser Phasen wurden gesonderte operative Ziele festgelegt, die sich an einem integrierten, koordinierenden und handlungsorientierten Ansatz orientieren.

Von Anfang an wurde die Entscheidung getroffen, die strategische Vision auf nationaler Ebene mit sehr konkreten Maßnahmen und Dienstleistungen des ZCB zu verbinden. Im Vorfeld des Strategieplans wurden vier Zielgruppen definiert: Bürgerinnen und Bürger, Unternehmen, Organisationen von vitalem Interesse (diese Gruppe wurde in späteren Phasen unter dem Einfluss der europäischen NIS-Richtlinie systematisch erweitert) und öffentliche Dienste.

Damit wurde der Grundstein für den dienstleistungsorientierten Ansatz gelegt, der die Organisation bis heute kennzeichnet. In den Aktionsplänen wurde ausdrücklich darauf hingewiesen, dass sich das ZCB vorrangig auf Dienste für die Bevölkerung konzentriert, wie z. B. Sensibilisierungskampagnen. Der Grund dafür war, dass der Bekanntheitsgrad in der breiten Öffentlichkeit sofort auch zu einer größeren Bekanntheit bei den anderen Zielgruppen führen würde.

Parallel dazu wurde die Ausarbeitung eines Cybernotfallplans als dringende Priorität hervorgehoben. Der Plan würde festlegen, wer im Falle eines Vorfalls die Verantwortung übernehmen kann, um die Auswirkungen von Cyberangriffen einzudämmen. Dies sollte zu einer einheitlichen Führung und einer effizienten Bekämpfung von Cyberangriffen auf wichtige belgische Ziele führen.

In der Anfangsphase wuchs das ZCB von zwei auf fünf Mitarbeitende.

“Vom ersten Tag an wurde die Messlatte hoch gelegt, und der Zeitraum 2014 bis 2016 hat den Bedarf an Cybersicherheit und einem koordinierten Ansatz in unserem Land sofort in den Vordergrund gerückt. Cyberbedrohungen traten nämlich immer häufiger auf, und die Notwendigkeit eines koordinierten Vorgehens war dringender denn je. In diesem Zusammenhang war eine Zusammenarbeit von Anfang an unerlässlich.”

Das ZCB wuchs von zwei auf fünf Mitarbeitende
Oben von links nach rechts: Miguel De Bruycker, Phédra Clouner. Unten von links nach rechts: Andries Bomans, Valéry Vander Geeten, Jo De Muynck

Vom ersten Tag an wurde die Messlatte hoch gelegt, und der Zeitraum 2014 bis 2016 hat den Bedarf an Cybersicherheit und einem koordinierten Ansatz in unserem Land sofort in den Vordergrund gerückt. Cyberbedrohungen traten nämlich immer häufiger auf, und die Notwendigkeit eines koordinierten Vorgehens war dringender denn je. In diesem Zusammenhang war eine Zusammenarbeit von Anfang an unerlässlich. Die Gründung der Cyber Security Coalition als private Vereinigung ohne Gewinnerzielungsabsicht (VoG) am 26. Januar 2015 war ein wichtiger Schritt in die richtige Richtung.

Die Organisation brachte Behörden, Unternehmen und Wissenseinrichtungen an einen Tisch, um Erfahrungen auszutauschen, Risiken zu analysieren und Lösungen zu entwickeln. Unter anderem dank dieses Netzwerks konnte das ZCB sowohl strategisch als auch operativ schneller vorankommen und den Grundstein für das legen, was heute das Rückgrat der belgischen Cybersicherheitspolitik ist.

November 2015: erster Stresstest

Die Feuertaufe für das junge ZCB ließ nicht lange auf sich warten. Im November 2015 tauchten auf YouTube Beiträge auf, in denen Hacker damit drohten, die Websites der belgischen Behörden lahmzulegen. Für das Zentrum war dies der erste echte Stresstest, der einmal mehr die Notwendigkeit eines ausgeklügelten Cybernotfallplans deutlich machte.

Das Team machte sich sofort an die Arbeit, um den Notfallplan und die notwendige Koordinierung schneller fertigzustellen. Der Notfallplan sieht eine abgestufte Eskalation entsprechend der Schwere des Vorfalls vor und legt fest, welche Dienststellen welche Verantwortung übernehmen sollen. Im Mittelpunkt stehen dabei Schnelligkeit, Zusammenarbeit und klare Kommunikation.

Der Plan, der schließlich auf dem Tisch lag, berücksichtigte viele Empfindlichkeiten aus der Praxis und trug schließlich auch dazu bei, dass das ZCB seinen Platz im größeren Ökosystem behaupten konnte. Der Cybernotfallplan führte zu einer klaren Struktur mit eindeutigen Regelungen für groß angelegte Cybervorfälle, die ein nationales, koordiniertes Vorgehen erfordern. Er wurde im Laufe der Zeit erweitert und aktualisiert.

2016: Aufbau eines Early Warning Systems

Im Jahr 2016 hat das ZCB seine Rolle als Koordinator der belgischen Cybersicherheitsstrategie gestärkt. So arbeitete das Zentrum beispielsweise an der Stärkung der grenzüberschreitenden Cyberresilienz in Vorbereitung auf die europäische NIS-Richtlinie mit. Gleichzeitig wurde in unserem Land eine erste, rudimentäre Version des Early Warning Systems (EWS) entwickelt, mit dem kritische Sektoren schnell vor neuen Bedrohungen gewarnt werden konnten.

Das EWS überwacht die digitalen Netzwerke der belgischen Infrastruktur und analysiert technische Indikatoren, die auf bösartige Aktivitäten hinweisen können (z. B. Botnets, bösgläubige IPs oder verdächtige Domains). Das System basiert auf einer Kombination aus automatischer Datenerfassung, Threat Intelligence und Echtzeit-Warnmeldungen. Die Signale werden in Warnungen für bestimmte Organisationen umgesetzt.

Sektoren wie das Gesundheitswesen, das Finanzwesen und der Energiesektor wurden als vorrangig eingestuft. Die Warnungen reichen von einer Benachrichtigung über ein Leck in einer bestimmten Softwareversion bis hin zu einer konkreten Warnung vor gezielten Phishing-Kampagnen.

2017–2020

DIE OPERATIONALISIERUNG

Seit 2017 ist das ZCB stark gewachsen. Cyberbedrohungen und ihre verschiedenen Erscheinungsformen wurden zu einem gesellschaftlich bekannten Phänomen. Der Entwicklungsprozess innerhalb des ZCB war nicht nur mit einem zahlenmäßigen Wachstum verbunden, sondern auch strategisch und inhaltlich wurden große Fortschritte erzielt.

CERT.be: weiterer Ausbau einer leistungsfähigen Reaktion auf Sicherheitsvorfälle

Am 1. Januar 2017 wurde das föderale Cyber Emergency Response Team (CERT.be) offiziell in das ZCB integriert. Es handelte sich um mehr als eine administrative Umstrukturierung, bei der das CERT von Belnet auf eine andere Dienststelle übertragen wurde. Es war der Beginn einer grundlegenden Einbettung der Reaktion auf Sicherheitsvorfälle in die breitere nationale Cybersicherheitsstrategie.

Für das ZCB bedeutete dies einen ersten großen Schub. Diese Integration ermöglichte es der Organisation, sich weiter zu entwickeln. Ein großer Vorteil war die Tatsache, dass die Arbeitsweise des CERT völlig neu überdacht und in die Strategie, die das Zentrum einführte, integriert werden konnte.

Das Ziel war klar: Die Arbeit von CERT.be sollte ausgeweitet, besser strukturiert und stärker auf die zunehmenden Bedrohungen in der belgischen und internationalen Cyberlandschaft abgestimmt werden. CERT.be fungierte bereits als nationales Computer Security Incident Response Team (CSIRT), aber seine Verankerung in der Struktur des ZCB bot die einmalige Gelegenheit, die Dienststelle weiter zu professionalisieren und mit allen anderen Maßnahmen zur Stärkung der Cybersicherheit in Einklang zu bringen. CERT.be erhielt Zugang zu mehr Ressourcen, spezialisierter Personalbeschaffung und politischer Unterstützung.

Eine der ersten Prioritäten nach der Integration war der Aufbau eines neuen Teams. Durch eine multidisziplinäre Zusammensetzung sollte sichergestellt werden, dass das Team nicht nur auf Sicherheitsvorfälle reagieren, sondern auch Bedrohungen präventiv erkennen, Empfehlungen ausarbeiten und die nationale Koordinierung bei Sicherheitsvorfällen erleichtern kann.

Cyber Europe Cyber-Krisenübungen 2018 und 2024

Ende 2018 wurde ein wichtiger Meilenstein erreicht: Das ZCB war fortan rund um die Uhr für Anbieter von wesentlichen Diensten und kritischen Infrastrukturen einsatzbereit. Diese ständige Verfügbarkeit entsprach dem Bedarf der Wirtschaft und bot gleichzeitig die Möglichkeit, die nationale Vorbereitung auf Cyberkrisen erheblich zu verbessern. Diese operative Ausweitung erfolgte in enger Zusammenarbeit mit dem Nationalen Krisenzentrum (NCCN). Dank dieses Partners konnte ein ständiger Bereitschaftsdienst rund um die Uhr gewährleistet werden.

In der Zwischenzeit arbeitete die Dienststelle am Aufbau von strukturellem Wissen. Die Rekrutierung und Bindung von Cybersicherheitsspezialisten stellte aufgrund des Arbeitskräftemangels und der Konkurrenz durch internationale Akteure eine ständige Herausforderung dar. Dennoch gelang es dem Team, sein Fachwissen zu vertiefen, indem es in gezielte Schulungen investierte und an internationalen Übungen wie Cyber Europe teilnahm, einer groß angelegten europäischen Cyber-Krisenübung, die von der ENISA organisiert wird und bei der Behörden, Unternehmen und andere Organisationen zusammenarbeiten, um ihre Resilienz gegenüber groß angelegten Cybervorfällen zu testen.

Der gute Ruf und die Professionalität wurden auch von anderen öffentlichen Diensten anerkannt. Bei Evaluierungen und Kooperationen wurde deutlich, dass die Integration von CERT.be in das ZCB zu einem effizienteren Vorfallmanagement und einer besseren Zusammenarbeit zwischen verschiedenen föderalen und sektoralen Akteuren führte. Die gestärkte Position von CERT.be wurde zum Katalysator für umfassendere Initiativen wie die Umsetzung der NIS-Richtlinie und den Ausbau der nationalen Meldeplattform.

Nach den Terroranschlägen von 2016 wurde ein Teil der Rückstellung Terror für die Cybersicherheit verwendet

2016: Rückstellung Terror als wirksames Mittel

Da terroristische Netzwerke ebenfalls eifrig Gebrauch vom digitalen Bereich machen, war der Zusammenhang mit Cybersicherheit schnell unübersehbar. In diesem Zusammenhang hat das ZCB Vorschläge unterbreitet, einen Teil der Rückstellung Terror zur Stärkung der digitalen Resilienz Belgiens zu verwenden.

So ermöglichten diese Mittel eine verstärkte Zusammenarbeit zwischen den öffentlichen Diensten. Die Bekämpfung cyberbezogener Formen des Terrorismus erfordert die Zusammenarbeit zwischen dem ZCB, der Staatssicherheit, der föderalen Polizei, dem Ministerium der Landesverteidigung, dem Ministerium der Justiz und ausländischen Partnern. Diese Budgets boten den nötigen Spielraum für die gemeinsame Schulung von Mitarbeitenden, den Aufbau einer gemeinsamen Infrastruktur und die Durchführung von Pilotprojekten, die ansonsten nur schwer zu finanzieren gewesen wären.

Threat Intelligence

Der Wissensstand innerhalb des ZCB wurde weiter ausgebaut, was im Jahr 2020 zur Aufteilung des Dienstes CERT.be in ein Team für Cyber Threat Research and Intelligence Sharing (CyTRIS) und ein CERT-Team führte, das sich weiter auf die Reaktion auf Cybernotfälle konzentrieren würde. Beide Facetten der Cybersicherheit sind heute unverzichtbar und gehören zum Kerngeschäft des ZCB: das Erfassen und Analysieren von Bedrohungsinformationen einerseits und der Umgang mit Sicherheitsvorfällen andererseits.

Das Team für Cyber Threat Research and Intelligence Sharing bietet seit 2018 verschiedene Dienste an. Es überwacht täglich verschiedene Quellen, sammelt und stellt Informationen zusammen, die für die Warnung potenzieller Opfer nützlich sein könnten, und führt eingehende Analysen von Cyber Threat & Intelligence durch, über die es dann berichtet.

Das CyTRIS sendet auch Spear Warnings (individuelle Warnungen) an Organisationen, bei denen eine bestimmte Schwachstelle in der IT-Infrastruktur entdeckt oder Malware oder gestohlene Anmeldedaten gefunden wurden. Es ist auch für den Erstkontakt mit Organisationen zuständig, die dem ZCB einen Sicherheitsvorfall melden, um den Vorfall untersuchen zu können.

BePhish und der Belgian Anti-Phishing Shield (BAPS)

Phishing war von Anfang an ein Schwerpunktthema und ist auch heute noch eine der häufigsten Formen der Internetkriminalität mit großen Auswirkungen. Im Laufe der Jahre haben sich plumpe, einfach gestaltete E-Mails zu sehr realistischen Nachrichten über alle möglichen Kommunikationskanäle entwickelt: E-Mail, SMS, WhatsApp und soziale Medien.

Es wurde schnell klar, dass das traditionelle reaktive Modell (Einschreiten nach der Meldung eines Opfers) nicht ausreicht. Aus diesem Grund hat das ZCB das Projekt BePhish entwickelt. Seit 2019 können Bürgerinnen und Bürger verdächtige Nachrichten rund um die Uhr unter verdacht@safeonweb.be melden. Hinter dieser Mailbox verbirgt sich ein automatisiertes Analyse- und Blockierungssystem. Es verarbeitet durchschnittlich 25.000 E-Mails pro Tag.

Als Ergebnis dieser Initiative verfügte das Zentrum über eine große Menge an Informationen über bösgläubige Websites. Um diese Kriminellen auch aktiv zu bekämpfen, wurde eine zweite Initiative ins Leben gerufen: der Belgian Anti-Phising Shield (BAPS), ein zusätzlicher Schutzwall gegen diese bösgläubigen Seiten im Internet. Besucherinnen und Besucher, die auf einen solchen Link klicken, werden auf eine Warnseite des ZCB umgeleitet und weitergeleitet.

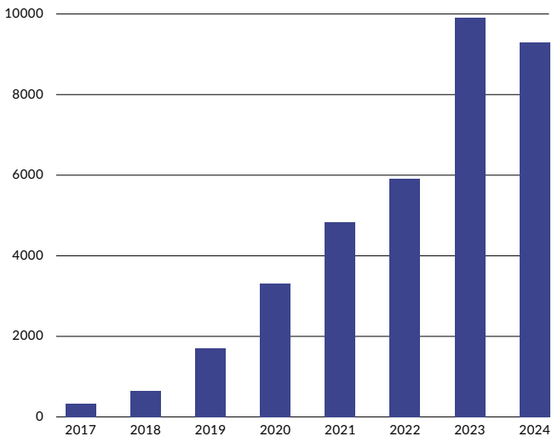
BAPS-Warnseite

Die technische Umsetzung dieser Idee erforderte eine intensive Zusammenarbeit mit den Internetdienstanbietern. Dies ist jedoch heikel, da die Umleitung einer URL rechtlich anfechtbar ist. Proximus war der erste Provider, der sich mit diesem Thema befasste, gefolgt von Telenet. Inzwischen beteiligen sich mehr als 100 Anbieter an BAPS. Die Weiterleitungsseite wurde im Jahr 2024 bis zu 240 Millionen Mal aufgerufen.

Der Anti-Phishing Shield hat die Reaktionszeit gegen bösgläubige Websites von Tagen auf Minuten verkürzt. Die Wirksamkeit des Systems liegt nicht so sehr in seinem technischen Erfindungsreichtum, sondern vielmehr in der Tatsache, dass sich die Bürgerinnen und Bürger von Anfang an engagiert haben und weiterhin massenhaft Nachrichten mit verdächtigen URLs melden. Durch einen gründlichen Spam-Filter, der aus dieser Philosophie entstanden ist, verhindert das ZCB zusammen mit den Anbietern auch, dass bösgläubige Mails in die Posteingänge von Bürgerinnen und Bürgern und Unternehmen gelangen.

Die Kombination aus BePhish und BAPS leistet einen einzigartigen Beitrag zur kollektiven Sicherheit: Dank aller Meldungen kann das ZCB schnell Trends erkennen und über Safeonweb Warnungen verbreiten. Die umstrittene Idee eines aktiven staatlichen Eingriffs in den Internetverkehr wurde zu einem der Steckenpferde des ZCB. Die Einschränkung der Freizügigkeit im Cyberspace führte zu mehreren Beschwerden, die jedoch jedes Mal erfolgreich zurückgewiesen wurden.

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



op de Y-as: Aantal mails x1000

Der „NotPetya“-Vorfall und Spear Warnings

Am 27. Juni 2017 erhielt das ZCB Berichte aus mehreren europäischen Ländern über eine Welle von Cybervorfällen. Die Angriffe sehen aus wie Ransomware, aber in Wirklichkeit handelt es sich um die Malware NotPetya-wiper. Mit anderen Worten, das Ziel war nicht, ein Lösegeld für die Freigabe der Daten zu verlangen, sondern vielmehr die Systeme aus der Ferne dauerhaft unbrauchbar zu machen. Es handelte sich um einen globalen Cyberangriff, der vermutlich von Russland ausging und sich hauptsächlich auf Unternehmen mit Aktivitäten in der Ukraine richtete.

Die Angreifer hatten ein System entwickelt, das sich blitzschnell über verschiedene Netzwerke weiter verbreiten konnte. Eines der Unternehmen, das am stärksten betroffen war, war der dänische Logistikkonzern Maersk. Er musste seine gesamte IT-Infrastruktur abschalten, um den Angriff zu stoppen. Die Mitarbeitenden waren gezwungen, auf Stift und Papier zurückzugreifen.

In unserem Land musste das ZCB besonders schnell handeln, um den Vorfall zu verfolgen. „NotPetya“ war der Auslöser für die Entwicklung der sogenannten Spear Warnings: Wenn in einem IT-Netzwerk Schwachstellen festgestellt werden, ist das ZCB befugt, die IP-Adresse der betreffenden Organisation zu ermitteln. Hier kann es dann Unternehmen und andere Organisationen auf diese Schwachstellen hinweisen. Diese proaktive Haltung trägt dazu bei, Cybervorfälle zu verhindern.

NotPetya-wiper markiert den Beginn der Spear Warnings

Schrittweiser Ausbau des Early Warning Systems

Um schneller und gezielter auf digitale Bedrohungen reagieren zu können, hat sich das Zentrum verpflichtet, sein Early Warning System (EWS) ab 2018 weiterzuentwickeln. Dieses Warnsystem ist seither das technologische Radar Belgiens im Bereich der Cybersicherheit.

Während dieses Zeitraums wurde das System schrittweise sowohl im Umfang als auch in der Tiefe erweitert. Das ZCB entwickelte auch eine Methodik zur Einstufung von Meldungen nach Risiko und Dringlichkeit, was die Wirksamkeit und das Vertrauen in das System stärkte. Das Early Warning System ist inzwischen zu einem wichtigen Instrument im belgischen Cybersicherheitsarsenal geworden.

Quarterly Cyber Threat Report

Zusätzlich zu den Echtzeit-Bedrohungsinformationen benötigte das ZCB ein strukturelles Berichtsmodell, das Einblicke in Trends, Schwachstellen und aufkommende Risiken bietet. So entstand der Quarterly Cyber Threat Report (QCTR), ein vierteljährlicher Bericht, mit dem das Zentrum seit 2019 wichtige Interessengruppen in kritischen Sektoren, politische Entscheidungsträger und andere relevante Stellen transparent über die Cyberbedrohungslage in Belgien informiert. Indem es sie über die breitere Bedrohungslandschaft aufklärt, hilft das ZCB ihnen, ihr eigenes Risikomanagement zu verbessern.

Jeder QCTR enthält Erkenntnisse über vorherrschende Angriffsvektoren, neu auftretende Schwachstellen und sektorale Trends (z. B. verstärkte Aktivitäten im Gesundheitswesen oder bei Kommunalverwaltungen) sowie Interpretationen zu größeren Sicherheitsvorfällen. Das Ziel ist der Informationsaustausch. Zu diesem Zweck sammelt das ZCB Daten aus Vorfallsmeldungen, internationalen Bedrohungsmeldungen und Beiträgen von Partnern innerhalb des Ökosystems, einschließlich kommerzieller Partner und CSIRTs.

NIS1-Richtlinie

Zwischen 2017 und 2020 spielte das ZCB eine Schlüsselrolle bei der Umsetzung der ersten europäischen Richtlinie zur Netz- und Informationssicherheit (NIS1). Diese Richtlinie, die im Juli 2016 förmlich angenommen wurde, war ein wichtiger Schritt zur Verbesserung der Cybersicherheit in der Europäischen Union. Ziel war es, die digitale Resilienz kritischer Infrastrukturen und grundlegender Dienste zu stärken, die grenzüberschreitende Zusammenarbeit zu fördern und die Stabilität des digitalen Binnenmarktes zu gewährleisten.

Bereits in der Vorbereitungsphase hat das ZCB diesen Regulierungsprozess aufmerksam verfolgt. Sobald klar war, dass die NIS-Richtlinie kommen würde, unternahm das Zentrum Schritte, um den belgischen Rechtsrahmen an die kommenden europäischen Anforderungen anzupassen. Um diese komplexe Aufgabe zu bewältigen, hat das ZCB seine rechtlichen und technischen Kapazitäten ausgebaut.

Neben der aktiven Vertretung Belgiens in der Europäischen NIS-Kooperationsgruppe und dem CSIRT-Netzwerk war das ZCB für die Ausarbeitung der nationalen Gesetzgebung zuständig. Dieser Weg führte schließlich zum NIS-Gesetz vom 7. April 2019, das den rechtlichen Rahmen für die Sicherheit von Netz- und Informationssystemen von öffentlichem Sicherheitsinteresse festlegt, sowie zum Königlichen Erlass, der seine Umsetzung regelte.

Die operative Umsetzung der NIS1-Richtlinie lag ebenfalls in den Händen des ZCB. Die Organisation richtete die Cyber Security Sectorale Autoriteiten Platform (CySSAP) ein, eine Struktur, in der die zuständigen öffentlichen Dienste und sektoralen Behörden (wie die FSMA für den Finanzsektor oder das BIPT für Post und Telekommunikation) regelmäßig informiert, beraten und koordiniert werden.

Belgien war jedoch der letzte EU-Mitgliedstaat, der die NIS1-Richtlinie umsetzte. Als besonders problematisch erwies sich die Aufsplitterung der Entscheidungsbefugnisse zwischen den Stakeholdern. In der Tat musste jeder Sektor die Auswirkungen von NIS1 separat bewerten. Da sich die Herausforderungen als neu und schwer zu ergründen erwiesen, traten einige Sektoren auf die Bremse.

Nicht zuletzt hat das ZCB im Einklang mit der NIS-Richtlinie eine Meldestelle für Cybersicherheitsvorfälle ausgearbeitet. Für das Zentrum bedeutete die Einführung von NIS1 nicht nur eine Bestätigung seiner institutionellen Rolle, sondern auch einen neuen Katalysator für einen weiteren Ausbau.

COVID-19 und Cyberrisiken für das Gesundheitssystem

Infolge von NIS1 musste jeder Sektor die Anbieter wesentlicher Dienste auflisten. Im Gesundheitssektor wurde 2019 beschlossen, dass es in diesem Bereich keine solchen Anbieter gibt. Auf diese Weise musste der Gesundheitssektor den Verpflichtungen der NIS-Gesetzgebung nicht nachkommen. Infolgedessen wurde der Sektor auch nicht in die Prioritätenliste des ZCB aufgenommen.

Mit dem Ausbruch der COVID-19-Pandemie im Frühjahr 2020 änderte sich die Situation jedoch völlig. Krankenhäuser gehörten plötzlich zu den bevorzugten Zielen von Cyberkriminellen, die das Gesundheitssystem weiter unter Druck setzen wollten und an den Daten interessiert waren.

Das Cybersicherheitsökosystem bot damals kollektive Hilfe an. Das ZCB unterstützte eine „Coalition of the Willing“ aus Anbietern von Cybersicherheits- und IT-Dienstleistungen, Beratungsunternehmen und unabhängigen Fachleute, die bereit waren, Krankenhäusern kostenlose Unterstützung zu leisten. Über die Website wehelpourhospitals.be konnten Gesundheitseinrichtungen mit diesen Partnern in Kontakt treten, um u. a. Beratung, Risikoanalyse und Reaktion auf Sicherheitsvorfälle zu erhalten.

In dieser Zeit wurde schmerzlich deutlich, dass die Beziehungen zwischen der Cyberwelt und den Behörden der einzelnen Sektoren überprüft werden müssen. Eine Neugestaltung, bei der dem ZCB die zentrale Aufsichtsfunktion übertragen wurde, führte zu einem wesentlich leistungsfähigeren Modell. Dies sollte sich später bei der Umsetzung der NIS2-Richtlinie als richtig erweisen: Obwohl die Zahl der betroffenen kritischen Sektoren von 7 auf 18 anstieg, war Belgien der erste EU-Mitgliedstaat, der die Richtlinie in nationales Recht umsetzte.

Da das Zentrum seine Rolle mit einem effizienten Ressourceneinsatz und einem geschätzten Angebot an praktischen Dienstleistungen und Unterstützung voll erfüllte, setzte sich in diesem Zeitraum bei den politischen Entscheidungsträgern zunehmend die Erkenntnis durch, dass das ZCB für das Sicherheitsökosystem in Belgien von wesentlicher Bedeutung ist. Außerdem entwickelte das Zentrum in diesem Zeitraum die Praxis, seine Strategie und Aktionspläne mit klaren Projektbudgets zu verknüpfen. Dieses hohe Maß an Transparenz in Bezug auf ihre Tätigkeit und Finanzierung ist bis heute erhalten geblieben.

“Um schneller und gezielter auf digitale Bedrohungen reagieren zu können, hat sich das Zentrum verpflichtet, sein Early Warning System (EWS) ab 2018 weiterzuentwickeln. Dieses Warnsystem ist seither das technologische Radar Belgiens im Bereich der Cybersicherheit. ”

2020-2024

WACHSTUM

Trotz aller Bemühungen ist die Zahl der dem ZCB gemeldeten Sicherheitsvorfälle weiterhin stark angestiegen. Unter anderem gewann Ransomware an Bedeutung, sowohl im öffentlichen als auch im privaten Sektor. Weltweit gilt die Cyberkriminalität heute als das größte Risiko für schwere finanzielle Verluste. Der Auftrag des ZCB bleibt also brandaktuell.

Im August 2020 lief das Mandat des Direktors Miguel De Bruycker und der stellvertretenden Direktorin Phédra Clouner aus. Die Föderalregierung beschloss, ihr Mandat um fünf Jahre zu verlängern. Dabei wurde das ZCB beauftragt, neben der Fortführung seiner bestehenden Aufgaben seine Vision und Strategie angesichts der zunehmenden Bedrohung in der Cyberlandschaft weiterzuentwickeln.

Nationale Cybersicherheitsstrategie 2.0

Um diese Mission zu erfüllen, wurde im Rahmen des ZCB die Nationale Cybersicherheitsstrategie 2.0 verabschiedet. Dazu gehörten sechs strategische Ziele:

- Stärkung des digitalen Umfelds und Erhöhung des Vertrauens in das digitale Umfeld
- Vorbereitung von Nutzerinnen und Nutzern sowie Administratorinnen und Administratoren von Computern und Netzwerken
- Schutz wichtiger Organisationen vor allen Cyberbedrohungen
- Reaktion auf die Cyberbedrohung
- Verbesserung der öffentlichen, privaten und akademischen Zusammenarbeit
- Einbezug eines klaren internationalen Engagements

Um diese Mission zu erfüllen, wurde im Rahmen des ZCB die Nationale Cybersicherheitsstrategie 2.0 verabschiedet. Dazu gehörten sechs strategische Ziele:

„In jeder Gesellschaft braucht man durchsetzbare Regeln, und im Cyberspace ist das nicht anders. Wir müssen also ein neues Gleichgewicht zwischen einem völlig offenen, freien und anonymen Internet und einem zuverlässigen Internet finden, in dem durchsetzbare Regeln und nationale Gesetze weiterhin gelten. Nichts davon sollte jedoch die Möglichkeit der freien und anonymen Kommunikation beeinträchtigen.

Ein Gleichgewicht zwischen einem völlig offenen und freien Cyberspace und einem Internet, in dem bestimmte rechtliche Regeln dennoch durchgesetzt werden können, ist meiner Meinung nach durchaus möglich. Drei Konzepte können die Cybersicherheit mittel- und langfristig erheblich verbessern: Trusted Sender, Trusted Publisher und Spear Warning.

So kann beispielsweise auf europäischer Ebene sichergestellt werden, dass der Besuch einer Website, die nicht mit einer national registrierten Organisation oder Einrichtung verknüpft ist, mit einer Kennzeichnung versehen wird.

Die Priorität besteht darin, die belgische Umsetzung des Cybersecurity Act der EU zu realisieren, damit unser Land bis Juni 2021 über die obligatorische National Cybersecurity Certification Authority verfügt. Die dafür erforderlichen Mittel wurden berechnet. Vorbehaltlich einer politischen Entscheidung kann der mit dem FÖD Wirtschaft ausgearbeitete Plan umgesetzt werden."

Die neue Strategie wurde von der Regierung im Jahr 2021 genehmigt. Nachdem das ZCB in seinen ersten fünf Jahren durch die Schaffung von Partnerschaften und die Verbesserung der Koordinierung im Bereich der Cybersicherheit in unserem Land den Weg geebnet und den Grundstein für einen stärker integrierten Sicherheitsansatz gelegt hatte, war es das Ziel des ZCB, das Angebot an Dienstleistungen weiter auszubauen und noch besser auf konkrete Bedürfnisse und Bedrohungen zu reagieren.

Das Direktorenduo hat sich ausdrücklich zum Ziel gesetzt, Belgien zu einem der Länder mit der geringsten Anfälligkeit für Cyberangriffe in der EU zu machen. Alle Maßnahmen, die in diesem Zeitraum durchgeführt wurden, dienten diesem Ziel. Darüber hinaus wurden der Organisation eine Reihe von Sonderaufgaben zugewiesen, die es ihr ermöglichten, ihre Koordinierungsfunktion weiter auszubauen.

Mehr Budget und Teamwachstum

Anfang 2020 verfügte das ZCB über rund 50 Mitarbeitende und ein jährliches Betriebsbudget von etwa 15 Millionen Euro. Infolge der Cyberstrategie 2.0 und der europäischen Vorgabe, eine National Cybersecurity Certification Authority (NCCA) einzurichten, wurde eine Aufstockung auf 80 Mitarbeitende und ein Budget von rund 36 Millionen Euro pro Jahr ins Auge gefasst.

National Cybersecurity Certification Authority

Die Europäische Union hat sich auf eine Vielzahl von Rechtsvorschriften zur Verbesserung der Cybersicherheit konzentriert. So wurde im Jahr 2019 der Cybersecurity Act verabschiedet, der die Grundlage für eine gemeinsame Zertifizierung von IKT-Produkten, -Diensten und -Prozessen schafft. Auf diese Weise wollte die EU die Cyberresilienz aller Mitgliedstaaten erhöhen und die Qualität und das Vertrauen in cybersichere Produkte durch gemeinsame Standards stärken.

In jedem Mitgliedstaat musste nun eine National Cybersecurity Certification Authority (NCCA) eingerichtet werden, die die Zertifizierung überwacht und die Unternehmen dabei begleitet. Die Behörde hat auch das Mandat, Richtlinien für die Zertifizierung auf nationaler Ebene zu erlassen. In Belgien wurde diese Aufgabe dem ZCB übertragen, das seine Rolle gestärkt und seine Kompetenzen erweitert hat.

Die NCCA überwacht die Zertifizierung und die Einhaltung der von den Konformitätsbewertungsstellen (CAB) ausgestellten Zertifikate. Sie kann auch bei Beschwerden über oder Missbrauch von Produktzertifizierungen eingeschaltet werden. Die NCCA ist auch befugt, Maßnahmen zu ergreifen, um die Einhaltung der Vorschriften sicherzustellen.

Nationales Koordinierungszentrum für Cybersicherheit für Belgien (NCC-BE) (2021)

Nationales Koordinierungszentrum für Cybersicherheit

Ein weiteres Ergebnis der europäischen Initiativen war die Einrichtung des Nationalen Koordinierungszentrums für Cybersicherheit für Belgien (NCC-BE) im Jahr 2021. Die EU möchte die Mittel, die sie für Forschung und Innovation im Bereich der Cybersicherheit bereitstellt, koordinierter einsetzen. Ziel ist es, nationale Prioritäten und Bedürfnisse in einen übergreifenden europäischen Ansatz zu integrieren. Gleichzeitig möchte die EU Forschende und innovative Unternehmen besser über die verfügbaren Finanzhilfen informieren, damit mehr grenzüberschreitende Projekte entstehen. Das NCC-BE fördert den Dialog zwischen Unternehmen, Wissenschaft, Forschenden und Behörden. Es stimmt die Politik in den Bereichen Forschung, Entwicklung und Innovation ab und arbeitet an der Umsetzung der belgischen Cybersicherheitsstrategie mit. Das NCC-BE verknüpft bestehende und zukünftige Initiativen im Bereich der Cybersicherheit, schafft Synergien und unterstützt Bildungsprogramme. Darüber hinaus sorgt das NCC-BE dafür, dass alle Regionen, Gemeinden und die Föderalregierung ihre Kräfte bündeln, um ein einheitliches Vorgehen gegen Cyberbedrohungen zu erreichen. Darüber hinaus unterstützt das NCC-BE Organisationen beim Zugang zu EU-Fördermitteln und koordiniert strategische Investitionen.

Auf europäischer Ebene vertritt das NCC-BE Belgien und es sorgt dafür, dass die Interessen der belgischen Regierung, der Industrie und der Wissenschaft im Bereich der Cybersicherheit stets Gehör finden.

Unter der Leitung des European Cybersecurity Competence Centre (ECCC) arbeitet das NCC-BE mit einem Netzwerk aus 29 nationalen Koordinierungszentren zusammen. Diese Initiative stärkt die Innovation im Bereich der Cybersicherheit, unterstützt die Industriepolitik und trägt zur technologischen Souveränität Europas bei.

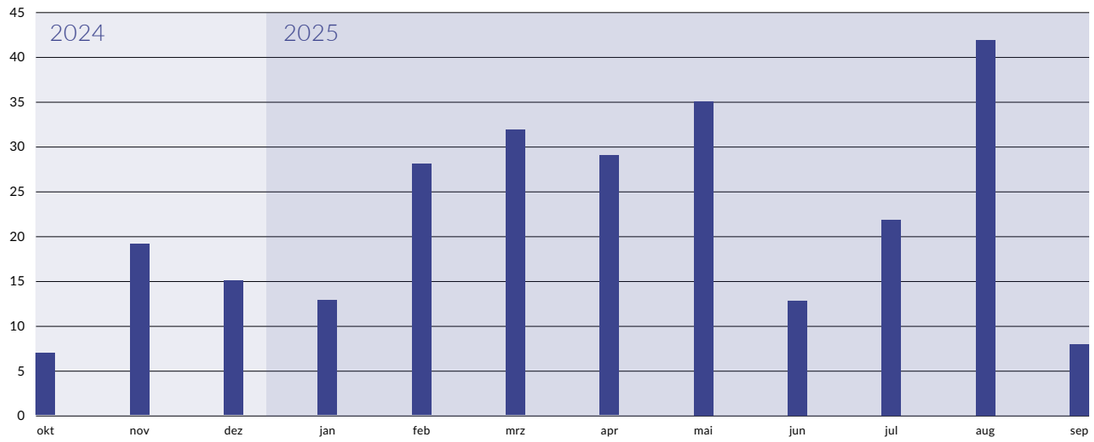
Vorbereitungen NIS2

Im Dezember 2020 kündigte die Europäische Kommission an, dass sie eine NIS2-Richtlinie als Nachfolger und Weiterentwicklung der NIS1-Richtlinie ausarbeiten wird. Ziel war es natürlich, die Cybersicherheit weiter zu erhöhen, aber auch den Ansatz innerhalb der EU weiter zu straffen. NIS1 hatte den Mitgliedstaaten nämlich eine relative Freiheit gelassen, die europäischen Anforderungen konkret auszufüllen. Dies führte jedoch zu unterschiedlichen Auslegungen und Unterschieden bei der Umsetzung in den einzelnen Mitgliedstaaten. Dieses Manko sollte mit NIS2 behoben werden.

Eine der wichtigsten Änderungen gegenüber dem Vorgänger war die Ausweitung der Anzahl der betroffenen Sektoren, die den Verpflichtungen von NIS2 unterliegen würden. In Belgien fielen über 100 Einrichtungen aus sieben Sektoren, darunter Energie, Verkehr, Gesundheitswesen, digitale Infrastruktur und öffentliche Dienste, in den Anwendungsbereich von NIS1. Nach der Umsetzung sollte NIS2 für mehr als 4.000 Einrichtungen aus 18 Sektoren gelten.

Das ZCB nahm auf europäischer Ebene an Konsultationen zur Auslegung der NIS2-Vorschrift teil. Auf nationaler Ebene wurde die parlamentarische Arbeit (die Umsetzung der europäischen Richtlinie in belgisches Recht) zusammen mit den Verwaltungen, dem CySSAP-Forum (in dem die sektoralen Behörden vertreten sind) und der politischen Ebene vorbereitet.

Entwicklung Meldungen NIS2



Das NIS2-Gesetz trat in Belgien im Oktober 2024 in Kraft. Dank der frühzeitigen Diskussionen und Vorbereitungen konnte das ZCB seinen Ansatz für NIS2 reibungslos ausbauen: Es sollte zur zentralen Stelle für die Überwachung und Überprüfung der Einhaltung von NIS2 werden und eng mit den sektoralen Behörden zusammenarbeiten.

Die ZCB schuf ein Registrierungstool für NIS2-Einrichtungen über die bestehende Plattform Safeonweb@work und baute ein pragmatisches System für die Meldung von Sicherheitsvorfällen auf. Nach der neuen Richtlinie sind die Organisationen verpflichtet, einen signifikanten Sicherheitsvorfall sofort nach seiner Entdeckung an das Zentrum zu melden.

Um Organisationen bei der Erfüllung der NIS2-Anforderungen zu unterstützen, wurde das CyberFundamentals Framework (CyFun®) entwickelt, ein praktischer Leitfaden für die Ergreifung von Cybersicherheitsmaßnahmen, der in verschiedene, auf den Reifegrad der Organisation zugeschnittene Stufen unterteilt ist. Auf diese Weise ist der Rahmen auch für Unternehmen und Organisationen außerhalb der NIS2-Sektoren relevant. Die öffentliche Debatte über NIS2 hat das Bewusstsein für Cybersicherheit in der belgischen Geschäftswelt ohnehin stark erhöht.

Koordinierte Offenlegung von Schwachstellen (CVD)

In Belgien gibt es seit 2023 ein gesetzliches Verfahren zur Meldung von Schwachstellen. Dies erfordert, dass das ZCB Meldungen von Forschenden über potenzielle Schwachstellen erhält, die unter das belgische Recht fallen. Die koordinierte Offenlegung von Schwachstellen (CVD) ist ein Verfahren, mit dem Forschende, Unternehmen und Regierungen die Entdeckung und Meldung von Sicherheitsproblemen in IKT-Systemen, -Produkten oder -Diensten auf strukturierte und sichere Weise angehen. Ziel ist es, Schwachstellen rechtzeitig und auf verantwortungsvolle Weise zu beheben, ohne dass sie frühzeitig ausgenutzt werden.

Im November 2024 organisierte das ZCB Hack the Government, die erste Veranstaltung für ethisches Hacken. Damit zeigt es, dass ethische Hackerinnen und Hacker dazu beitragen können, Belgien cybersicherer zu machen. Diese beispiellose Initiative brachte die Gemeinschaft der ethischen Hackerinnen und Hacker zusammen, um Schwachstellen in Websites und Systemen von Behörden zu ermitteln.

Stop Phishing

Die Bemühungen zur Verhinderung von Phishing-Kriminalität im Rahmen des globalen Ansatzes des Belgian Anti-Phishing Shield (BAPS) wurden unvermindert fortgesetzt. Im Jahr 2020 wurde ein neues Projekt „Stop Phishing“ ins Leben gerufen. Damit sollte verhindert werden, dass E-Mails oder Textnachrichten, die einen bösartigen Link enthalten, Bürgerinnen und Bürger und Unternehmen erreichen. Sie wurden abgefangen, noch bevor sie das E-Mail-Postfach oder den SMS-Ordner erreichten.

Dieses Projekt wurde zu einer erfolgreichen öffentlich-privaten Partnerschaft mit den beteiligten Betreibern, die von der Regierung ausdrücklich unterstützt wurde. Dies war ein weiterer Schritt im Rahmen des proaktiven und präventiven Ansatzes des BAPS. Über das ZCB finanzierten die Behörden einen Teil der von den teilnehmenden Dienstanbietern verwendeten Software.

PhishNemo

Eine Erweiterung des BAPS-Projekts ist PhishNemo. Diese Initiative wurde ursprünglich von der Föderalen Gerichtspolizei (FGP) in Limburg entwickelt und hat sich inzwischen zu einer Zusammenarbeit zwischen der FGP und dem ZCB entwickelt. Während sich der Belgian Anti-Phishing Shield hauptsächlich auf Meldungen von Bürgerinnen und Bürgern stützt, sucht PhishNemo seit 2023 proaktiv nach verdächtigen Domainnamen, die in Phishing-Kampagnen verwendet werden könnten.

Zu diesem Zweck werden die neuen Domainnamen gründlich geprüft. Die Initiative sucht nach Spuren bekannter Phishing-Tools – sogenannten „Fingerabdrücken“. Auf diese Weise lassen sich bösgläubige Domains erkennen, noch bevor die erste Phishing-E-Mail versendet wird. Die frühzeitig entdeckten Domains werden sofort in das BAPS-System aufgenommen, sodass sie in Zusammenarbeit mit den Internetanbietern sofort umgeleitet werden können.

Durch die Übernahme dieses Systems von der Limburger FGP konnte das Projekt weiter wachsen. Dazu arbeitet das ZCB mit privaten Partnern zusammen, die die IT-Systeme warten. Dies ermöglicht es PhishNemo, aktiv zum Belgian Anti-Phishing Shield beizutragen.

Hacktivismus erreicht nach dem Einmarsch Russlands in die Ukraine seinen Höhepunkt

Im Februar 2022 marschierte Russland in die Ukraine ein und löste damit einen lang anhaltenden Krieg aus. Obwohl Cyberkriminelle in erster Linie an finanziellem Gewinn interessiert sind, hat sich inzwischen eine enge Verbindung zwischen Geopolitik und Cyberangriffen ergeben. Diese Veränderungen in der geopolitischen Landschaft verschafften dem ZCB einen Platz als ständiges Mitglied des Nationalen Sicherheitsrates.

Diese dauerhafte Aufnahme in die ständige Konsultation der Nachrichten- und Sicherheitsdienste war ein sehr wichtiger Meilenstein für die Organisation. In der Tat war das ZCB von nun an ein integraler Bestandteil der Sicherheitsarchitektur des Landes. Außerdem erhielt die Organisation dadurch Zugang zu zusätzlichen Betriebsmitteln aus der Rückstellung Ukraine.

Dies erwies sich auch in der Praxis als logische Wahl: Je länger, desto mehr Hacktivistengruppen erschienen auf der Bildfläche. Zu ihren bevorzugten Vorgehensweisen gehören DDoS-Angriffe (Distributed Denial of Service), bei denen Websites überlastet werden, sowie Hack-and-Leak-Operationen. Seit dem Ausbruch des Krieges in der Ukraine ist auch in mehreren europäischen Ländern, darunter Belgien, eine Zunahme von Ransomware-Angriffen auf Gemeinden und öffentliche Dienste zu beobachten.

In Anbetracht des geopolitischen Kontextes wurde im Vorfeld der Europawahlen sowie der nationalen und regionalen Wahlen im Juni 2024 die Wachsamkeit gegenüber Cybersicherheitsereignissen oder verstärkten Bedrohungen erhöht. Sowohl die föderalen als auch die regionalen und lokalen Behörden konnten sich auf die Beratung und technische Unterstützung des Zentrums verlassen. Während der Wahlwochenenden im Juni und Oktober 2024 wurde eine kontinuierliche Überwachung durchgeführt, und das ZCB hielt auch ein Notfallteam in Bereitschaft.

Im Übrigen führte das Zentrum auch bei früheren Wahlgängen ein Sicherheitsaudit durch. Dies bildete die Grundlage für eine Reihe von Empfehlungen, die zu einer deutlichen Erhöhung der Sicherheit der IT-Systeme für Wahlen führten. Unter anderem aus diesem Grund wurden die Wahlen in Belgien noch nie durch Cyberangriffe gestört.

“Das Direktorenduo hat sich ausdrücklich zum Ziel gesetzt, Belgien zu einem der Länder mit der geringsten Anfälligkeit für Cyberangriffe in der EU zu machen. Alle Maßnahmen, die in diesem Zeitraum durchgeführt wurden, dienten diesem Ziel. Darüber hinaus wurden der Organisation eine Reihe von Sonderaufgaben zugewiesen, die es ihr ermöglichten, ihre Koordinierungsfunktion weiter auszubauen.”

AKTIVER CYBERSCHUTZ, EINE PROAKTIVE VISION

Die Digitalisierung eröffnet ungeahnte Möglichkeiten für Bürgerinnen und Bürger, Unternehmen und Behörden. Aber je mehr wir digitalisieren, desto größer werden die Risiken. Die Cyberkriminalität entwickelt sich in rasantem Tempo, die Angriffe werden immer raffinierter und die Auswirkungen auf unsere Gesellschaft werden immer größer. Um dieser Bedrohung zu begegnen, ist die Sicherung des digitalen Umfelds eine wesentliche Voraussetzung.

Daher hat es sich das ZCB seit seiner Gründung zur Aufgabe gemacht, Schwachstellen (sowohl menschlicher als auch technischer Art) sichtbar zu machen und aktiv dagegen vorzugehen. Anstatt erst nach einem Sicherheitsvorfall zu reagieren, setzt das Zentrum auf Prävention, schnelle Erkennung und gezielte Reaktion.

Im Jahr 2024 erhielt dieser proaktive Ansatz einen neuen Namen: **Active Cyber Protection (ACP)**. Dieses Konzept umfasst eine Reihe laufender und zusätzlicher Projekte, die die Cybersicherheit stärken, noch bevor ein Sicherheitsvorfall eintreten kann.

Auf Drängen des ZCB wurde die ACP in die europäische NIS2-Richtlinie aufgenommen, die in Belgien ab 2024 in Kraft tritt. Diese Vorschrift verpflichtet Unternehmen in einer Reihe von Schlüsselsektoren, zusätzliche Sicherheitsgrundsätze zu übernehmen und Risikomanagementsysteme einzuführen.

Die NIS2-Richtlinie fordert daher von allen Mitgliedstaaten eine aktivere Haltung und schreibt einen aktiven Cyberschutz als gesetzliche Verpflichtung vor. Da Belgien in diesem Bereich eine Vorreiterrolle einnehmen möchte, ist die ACP ein zentraler Pfeiler unserer nationalen Cyberstrategie. Das ZCB macht dieses abstrakte Konzept mit einem proaktiven, maßgeschneiderten, automatisierten und partizipativen Ansatz konkret:

- **Proaktiv:** Nicht warten, bis ein Sicherheitsvorfall eintritt, sondern Bedrohungen erkennen und beseitigen, bevor sie Schaden anrichten.
- **Maßgeschneidert:** Keine Einheitsgröße. Kommunikation und Reaktion sind auf die Bedürfnisse bestimmter Organisationen und Sektoren zugeschnitten.
- **Automatisiert:** Geschwindigkeit ist entscheidend. Die Automatisierung ermöglicht schnellere Reaktionen und gleicht den akuten Mangel an Cybersicherheitsexperten aus.
- **Partizipativ:** Cybersicherheit ist eine gemeinsame Verantwortung. Mitarbeitende, Partner und Bürgerinnen und Bürger sollten aktiv einbezogen werden.

Diese Vision wird durch fünf strategische Säulen konkretisiert. Diese Säulen bilden einen flexiblen Rahmen, der sich entsprechend den sich ständig ändernden Taktiken der Cyberkriminellen kontinuierlich weiterentwickelt.

PIJLER I: BEWUSTZIJN VERGROTEN DOOR MENSEN TE BETREKKEN

Eine starke Cybersicherheitspolitik beginnt bei der breiten Öffentlichkeit und ihrer Sensibilisierung. Dies war von Anfang an der Ausgangspunkt des ZCB. Indem sie verdächtige Nachrichten erkennen, können die Bürgerinnen und Bürger aktiv dazu beitragen, die Cybersicherheit des Landes zu erhöhen. Die Initiativen unter dem Dach von Safeonweb dienen dazu, Bürgerinnen und Bürger und Unternehmen gegen digitale Bedrohungen zu wappnen. Dies bildet unbestreitbar die Grundlage der proaktiven Vision und damit auch der Philosophie des ZCB.

Für Bürgerinnen und Bürger: Safeonweb@home

Safeonweb@home informiert die Bürgerinnen und Bürger über eine Website, Kampagnen und soziale Medien über aktuelle Gefahren. Die Safeonweb-App spielt dabei eine zentrale Rolle: Sie warnt die Nutzer rechtzeitig vor Phishing-Angriffen und gibt leicht verständliche Sicherheitstipps.

Eine weitere Erfolgsgeschichte, die sich an die Bürgerinnen und Bürger richtet, ist suspicious@safeonweb.be, eine E-Mail-Adresse in vier Sprachen, über

Safeonweb is bekend bij 82% van de bevolking.

die die Bürgerinnen und Bürger verdächtige E-Mails melden können. Allein im Jahr 2023 gingen fast 10 Millionen Meldungen ein. Eine beeindruckende Zahl, die zeigt, wie wertvoll ihr Beitrag im Kampf gegen die Cyberkriminalität ist.

Für Unternehmen: Safeonweb@work

Seit 2023 gibt es auch Safeonweb@work, eine auf belgische Unternehmen zugeschnittene Plattform mit klaren, umsetzbaren Empfehlungen zur Integration der Cybersicherheit in die tägliche Unternehmenspolitik – ohne große Investitionen oder komplexe Verfahren.

Über ein Online-Portal können Unternehmen ihre Domains registrieren und erhalten automatisch Warnmeldungen über Schwachstellen in ihrer IT-Infrastruktur. Die Plattform umfasst auch Tools zur Selbsteinschätzung, grundlegende Richtlinien und Best Practices, die es Unternehmen ermöglichen, ihr Sicherheitsniveau in ihrem eigenen Tempo zu verbessern. Das ZCB unterstützt somit die Erhöhung der Cyberreife der Unternehmenslandschaft.

Safeonweb@work 2024

SÄULE II: AUFDECKUNG UND BESEITIGUNG KRIMINELLER INFRASTRUKTUREN

Die zweite Säule konzentriert sich auf den Kern der Cybersicherheit: die Infrastruktur, über die Kriminelle ihre Angriffe ausführen. Beispiele dafür sind Phishing-Websites oder bösgläubige Server. Mit dem Projekt **Belgian Anti-Phishing Shield (BAPS)** bekämpft das ZCB diese Praktiken an der Wurzel.

In Zusammenarbeit mit belgischen Internetanbietern werden bösartige Websites automatisch erkannt und deaktiviert, indem die Nutzerinnen und Nutzer sofort auf eine sichere Zielseite umgeleitet werden. Auf diese Weise werden täglich etwa 100.000 Menschen in Belgien vor potenziell schädlichen Websites geschützt.

Die Geschwindigkeit und Automatisierung sind die Stärken des Systems. Bösgläubige URLs werden ständig aktualisiert und direkt in die DNS-Systeme der Anbieter integriert. Dadurch werden Bedrohungen in Echtzeit abgefangen, oft bevor sie Schaden anrichten können. Der BAPS ist somit ein Paradebeispiel für proaktiven Cyberschutz: unauffällig im Hintergrund, aber mit messbarer Wirkung.

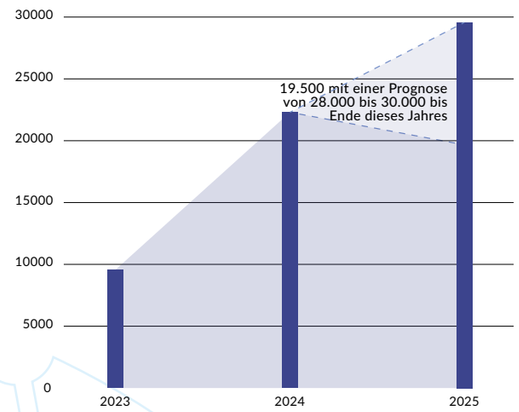
Dieser Ansatz blieb auch bei anderen Behörden, im Finanzsektor und bei den Polizeidiensten nicht unbemerkt. Mehrere Organisationen gaben an, dass sie innerhalb ihrer eigenen Domain über wertvolle Daten verfügen, beispielsweise Informationen über betrügerische Webshops oder Anlagebetrug. Sie sind jedoch nicht in der Lage, Domains auf nationaler Ebene automatisch umzuleiten.

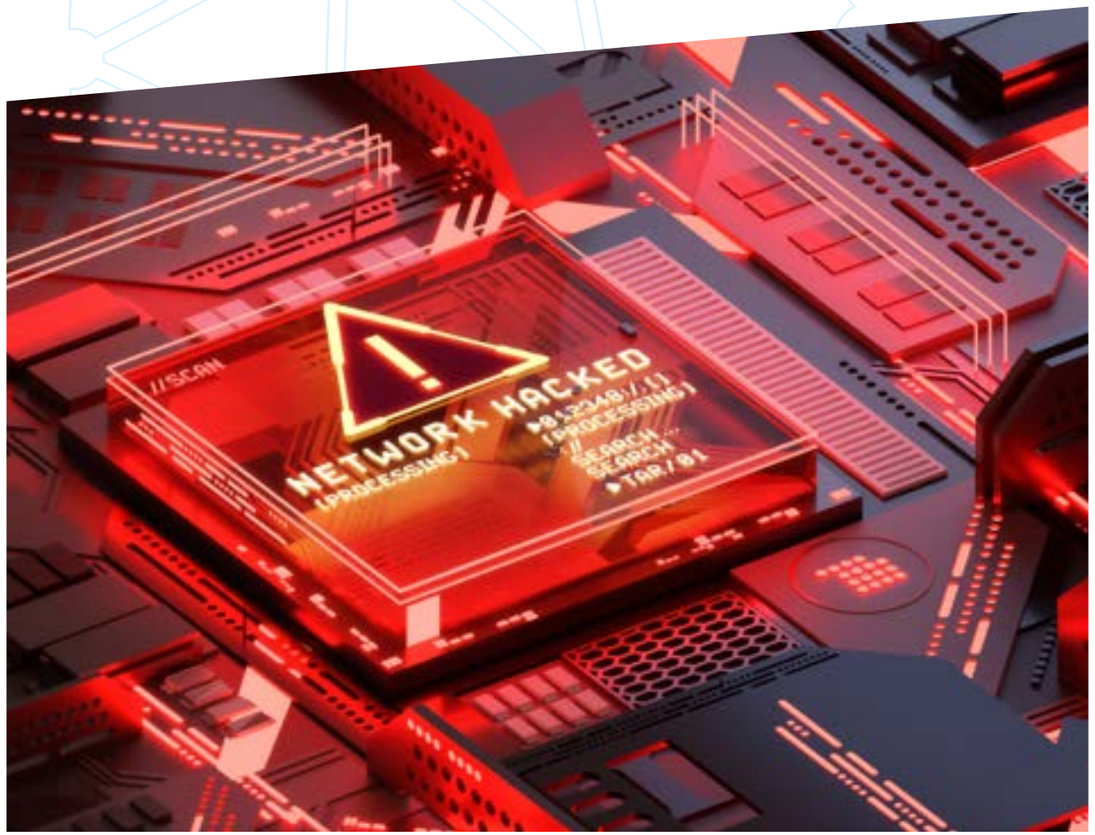
Aus diesem Grund hat das ZCB das Konzept der Trusted Partners entwickelt: ein privilegierter Zugang zum BAPS-System für sorgfältig ausgewählte Partner. Die Partner stellen die Daten zur Verfügung, das ZCB kümmert sich dann in Zusammenarbeit mit den Internetanbietern um die praktische Umsetzung der Umleitung der verdächtigen Domain. Heute sind unter anderem der FÖD Wirtschaft, die FSMA, Itsme und eine Reihe belgischer Banken als Trusted Partner in diesem System tätig.

SÄULE III: GEZIELTES ERKENNEN VON BEDROHUNGEN

Cyberkriminelle nutzen häufig Spear Phishing: gezielte Angriffe auf bestimmte Personen, um an sensible Informationen zu gelangen. Das ZCB verfolgt einen ähnlichen Ansatz, allerdings zum Vorteil des Nutzers. Mit sogenannten Spear Warnings informiert das Zentrum Organisationen direkt über Schwachstellen in ihrer digitalen Umgebung.

Zahlen Entwicklung der Spear Warnings

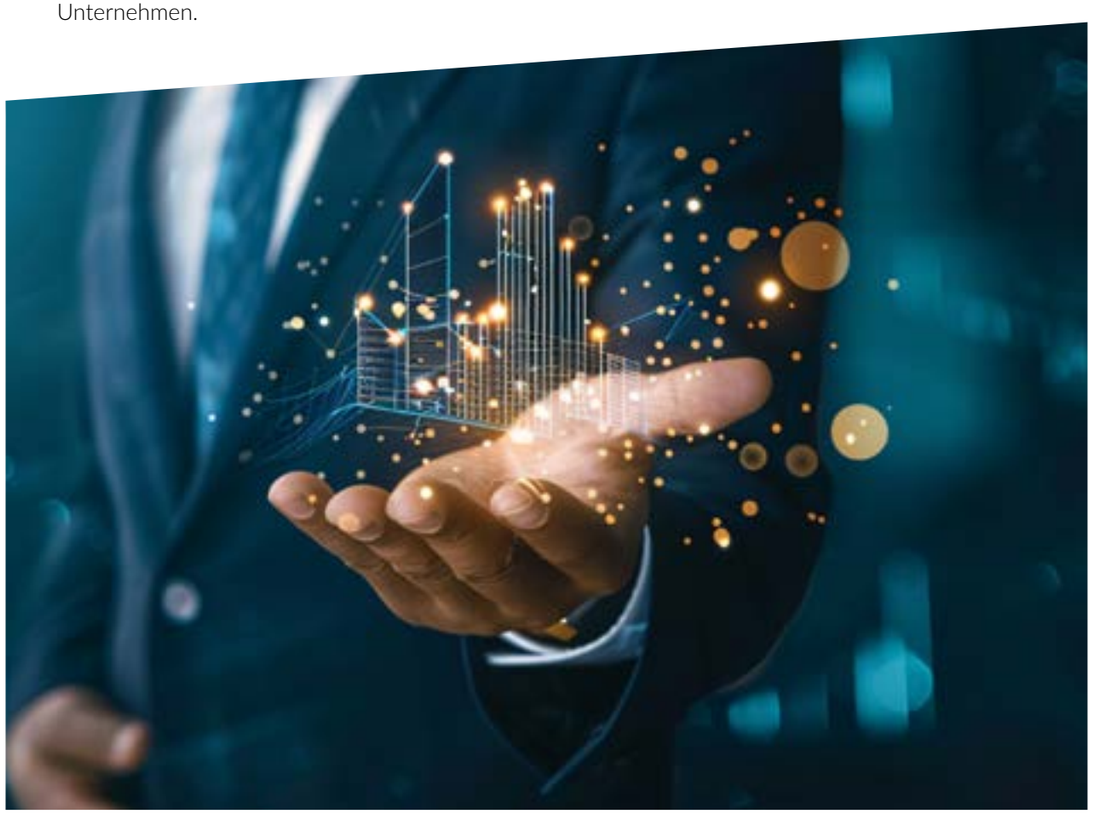




Dieser Ansatz ermöglicht es Unternehmen, schnell und gezielt zu handeln, noch bevor eine Schwachstelle ausgenutzt werden kann. Die bekannteste Initiative ist das Early Warning System (EWS), eine Plattform, die sich speziell an Organisationen mit kritischen oder lebenswichtigen Infrastrukturen richtet, die unter die Verpflichtungen der NIS2-Richtlinie fallen.

Über dieses Portal stehen die Analystinnen und Analysten des ZCB in direktem Kontakt mit diesen wichtigen Organisationen. Für sie ist das EWS wie ein zusätzliches Paar Augen: Es überwacht digitale Signale, erkennt Risiken und sendet proaktiv Warnmeldungen. Darüber hinaus erhalten Unternehmen auch personalisierte Meldungen über Datenschutzverletzungen, durchgesickerte Anmeldedaten und unsichere Systeme innerhalb ihrer Infrastruktur, um nur einige zu nennen.

Dieser proaktive Ansatz trägt nicht nur zur Vermeidung von Sicherheitsvorfällen bei, sondern erhöht auch das Bewusstsein und die Reaktionszeit in den Unternehmen.



SÄULE IV: VERANKERUNG DER CYBERSICHERHEIT IN DER ORGANISATION

Um wirklich resilient und belastbar zu werden, müssen Unternehmen die Cybersicherheit in ihre täglichen Abläufe integrieren. Das ZCB hat daher das CyberFundamentals Framework entwickelt: ein praktisches und skalierbares Modell, das Organisationen hilft, ihren digitalen Schutz Schritt für Schritt zu verbessern. Der Rahmen besteht aus vier Stufen (Small, Basic, Important und Essential), wobei jede Stufe eine Reihe von konkreten Maßnahmen umfasst. Small dient dabei als Leitfaden für sehr kleine Organisationen, die noch keine Erfahrung mit Cybersicherheit haben und die allerersten Schritte unternehmen.

Die Maßnahmen aus dem CyberFundamentals Framework sind auf die häufigsten Cyberangriffe zugeschnitten und wurden anhand von CERT-Angriffsprofilen validiert. Die Wirksamkeit des Modells hat sich inzwischen erwiesen:

- Die Stufe **Basic** deckt etwa 82 % der gängigen Angriffsarten ab.
- Mit der Stufe **Important** erhöht sich dieser Prozentsatz auf 94 %.
- Organisationen, die die Stufe **Essential** erreichen, schützen sich sogar zu 100 % vor diesen Angriffen.

Der Rahmen basiert auf internationalen Normen wie NIST, ISO und IEC und ist für Organisationen jeder Größe zugänglich. Eine Zertifizierung durch eine externe Stelle ist möglich, aber nicht zwingend erforderlich.

Mit CyberFundamentals wird Cybersicherheit konkret, messbar und erreichbar, auch für KMU oder Organisationen ohne IT-Abteilung. Außerdem wächst das Modell mit den Risiken: Es wird ständig weiterentwickelt, um in einer sich schnell verändernden digitalen Welt relevant zu bleiben.

SÄULE V: SCHAFFUNG EINES VERTRAUENSWÜRDIGEN UMFELDS

Das Internet bietet eine gewisse Freiheit, und mit dieser Freiheit kommt die Anonymität. Aber natürlich ist diese Anonymität ein zweischneidiges Schwert. Einerseits schützt sie unsere Privatsphäre und unsere Meinungsfreiheit. Andererseits öffnet sie die Tür für Missbrauch. Genau aus diesem Grund besteht ein wachsender Bedarf an mehr Transparenz und digitaler Validierung: um das Vertrauen wiederherzustellen und die dunkle Seite der Anonymität zu bekämpfen.

Die Suche nach dem neuen Gleichgewicht zwischen Anonymität und Identität ist keine leichte Aufgabe. Im Wesentlichen handelt es sich um eine Verhaltensänderung: Die Bürgerinnen und Bürger müssen sich an den Gedanken gewöhnen, dass die Identifizierung ein natürlicher Bestandteil ihrer digitalen Präsenz ist. Nur so lassen sich Online-Aktivitäten besser zuordnen und damit sicherer machen.

"In Zusammenarbeit mit belgischen Internetanbietern werden bösartige Websites automatisch erkannt und deaktiviert, indem die Nutzerinnen und Nutzer sofort auf eine sichere Zielseite umgeleitet werden. Auf diese Weise werden täglich etwa 100.000 Menschen in Belgien vor potenziell schädlichen Websites geschützt."

Um den Internetnutzerinnen und -nutzern mehr Vertrauen in die Parteien zu geben, mit denen sie online interagieren, hat das ZCB die Browsererweiterung Safeonweb entwickelt. Sie zeigt einen klaren Farbcode für jeden Website-Besuch:

- **Grün** bedeutet, dass der Inhaber der Website validiert und somit vertrauenswürdig ist.
- **Orange (oder gelb)** weist auf einen unbekannten oder nicht bestätigten Eigentümer hin. In diesem Fall ist Vorsicht geboten.
- **Rot** bedeutet, dass es sich um eine bekanntermaßen unsichere oder bösartige Website handelt, die man am besten ganz meidet und mit der man am besten keine Daten austauscht.

Bei der Entwicklung der Erweiterung wurde sowohl auf Sicherheit als auch auf Benutzerfreundlichkeit geachtet. Sie arbeitet automatisch im Hintergrund und zeigt auf einen Blick, ob personenbezogene Daten sicher weitergegeben werden können. Dies gibt den Surferinnen und Surfern bzw. Nutzerinnen und Nutzern mehr Gewissheit über die Sicherheit des Empfängers, mit dem sie Daten austauschen möchten.

Werden dennoch verdächtige Inhalte auf einer validierten Website entdeckt? Dann ändert sich der Status sofort – abhängig von der ersten Meldung – von grün zu orange oder sogar zu rot. So bleibt das System immer aktuell und zuverlässig.

ZCB FÜR ALLE

SENSIBILISIERUNG: HERAUSFORDERUNG NUMMER EINS BEIM START

In den ersten Jahren seines Bestehens stand das ZCB vor strukturellen Herausforderung: Belgien sah sich zunehmend mit Cyberbedrohungen konfrontiert, aber die breite Öffentlichkeit war noch nicht sensibilisiert. Bürgerinnen und Bürger, Unternehmen und sogar einige öffentliche Dienste unterschätzen das Risiko.

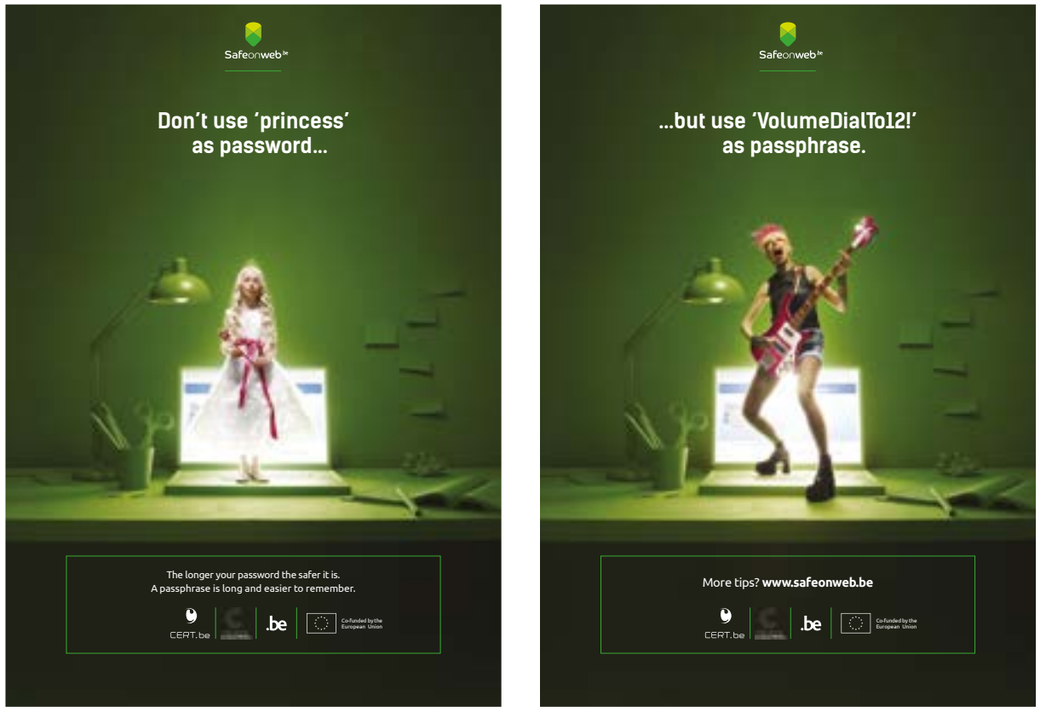
In dem Bewusstsein, dass die Stärke eines jeden Sicherheitssystems letztlich von der menschlichen Komponente abhängt, wurde beschlossen, nicht nur in die Erkennung und Reaktion auf Sicherheitsvorfälle zu investieren, sondern gleichzeitig durch Sensibilisierungskampagnen das Bewusstsein in großem Maßstab zu schärfen.

Die ersten Kampagnen konzentrierten sich auf konkrete Risiken: Phishing-E-Mails, schwache Passwörter, Klicken auf verdächtige Links und die Notwendigkeit, Software regelmäßig zu aktualisieren. Um die Wirkung dieser Maßnahmen zu verstärken, verpflichtete sich das ZCB zur Zusammenarbeit mit Partnern wie Banken und Telekommunikationsunternehmen und der Cyber Security Coalition. Arbeitgeber und Gemeinderäte wurden gezielt angesprochen, um die Informationen weiter zu verbreiten.

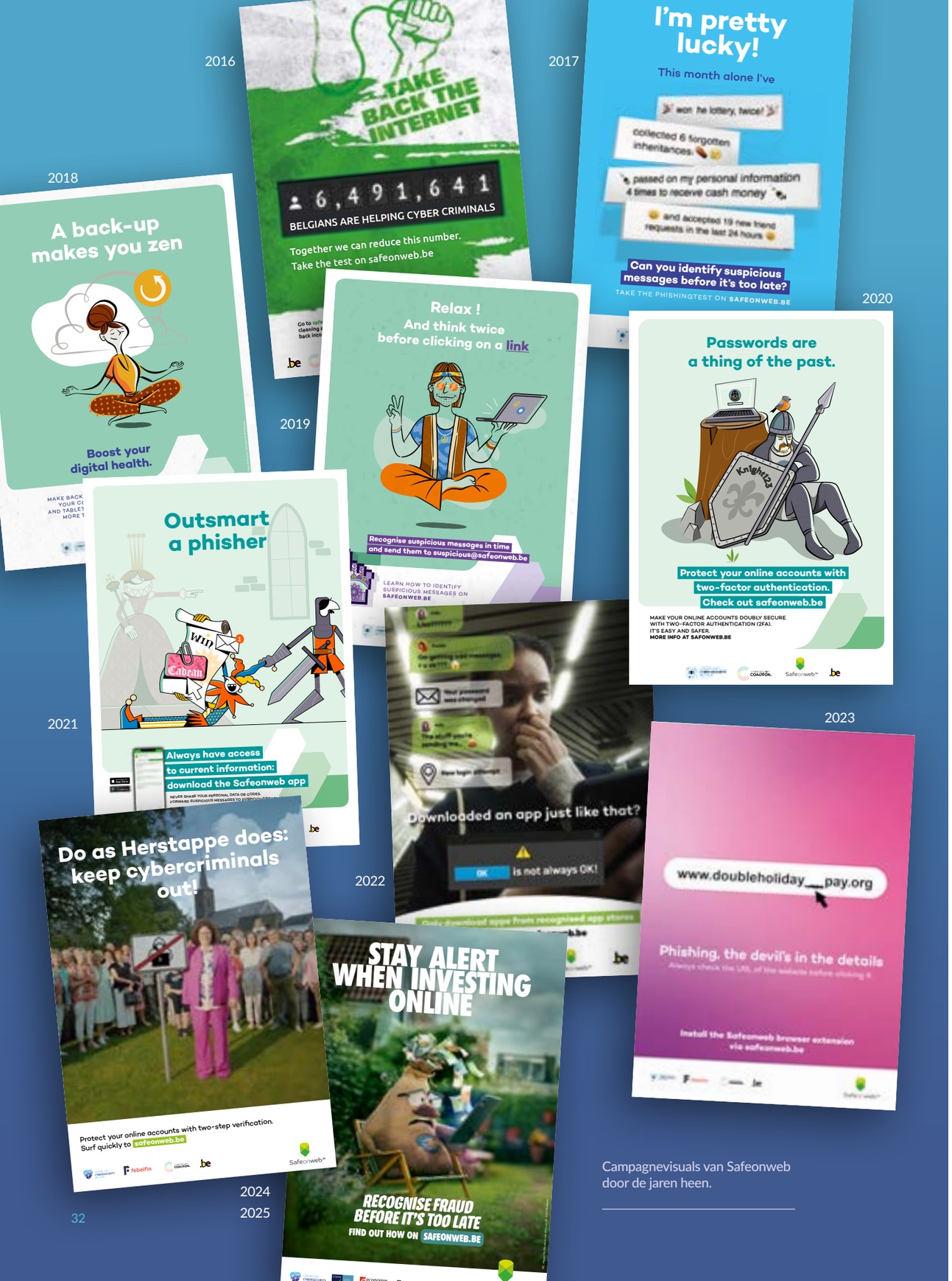
Intern legten diese Kampagnen den Grundstein für eine neue, multidisziplinäre Arbeitsweise im ZCB. Kommunikationsfachleute und technische Teams arbeiteten mit Verhaltenspsychologinnen und -psychologen und Marketingfachleuten zusammen, um die ersten Kampagnen zu entwickeln. Für eine staatliche Organisation war dies ein bahnbrechender, kreativer Weg, um die Sensibilisierung anzugehen.

Teil der europäischen Bewusstseinsbildung

Das ZCB plant seine jährliche Kampagne in dem Monat Oktober. Dies ist kein Zufall. Der Oktober wurde nämlich zum European Cybersecurity Month erklärt, eine jährliche Initiative der Europäischen Kommission und der ENISA. Diese Kampagne zielt



Erste Safeonweb-Kampagne



Campagnevisuals van Safeonweb door de jaren heen.

auch darauf ab, das Bewusstsein für Cybersicherheit zu schärfen und die Bürgerinnen und Bürger und Organisationen umfassend darüber zu informieren, wie sie sich online besser schützen können.

Um zusätzliche Wirkung zu erzielen, führt das ZCB auch zwischenzeitliche Informationskampagnen durch, und zwar zu Zeiten, in denen Betrüger besonders aktiv sind: rund um die Feiertage, zu Schlussverkaufszeiten oder aus aktuellem Anlass.

Das Zentrum beteiligt sich auch am Safer Internet Day, einer weltweiten Sensibilisierungskampagne, die jährlich im Februar stattfindet und sich speziell an Schulen und Jugendorganisationen richtet.

Darüber hinaus teilt und unterstützt die Organisation gerne Kampagnen von Partnerorganisationen zum Thema Cyberprävention.

Partner reichen sich die Hände

Das Thema der jährlichen belgischen Kampagne wird auf der Grundlage aktueller Themen und wichtiger Trends ausgewählt. Die Aktion wird in den drei Landessprachen durchgeführt und bezieht Akteure aus allen Bereichen ein.

Diese Einbindung ist eine der Stärken der Sensibilisierungskampagnen: Einerseits verfügt das ZCB über eine Reihe von privilegierten Partnern wie den FÖD Wirtschaft, die FSMA, die föderale Polizei, den Bankenverband Febelfin und die Cyber Security Coalition. Sie fungieren als Resonanzboden, sitzen in allen Phasen der Kampagnenentwicklung mit am Steuer und geben Feedback: von der Wahl des Themas über die Übersetzung und Darstellung in der Kampagne bis hin zur Überzeugungskraft und der Aufforderung an die Bevölkerung, ihr Verhalten zu ändern. Jeder Partner bringt sein Know-how und seine Fachkenntnisse mit ein.

Andererseits kann das Zentrum auch auf mehr als 600 Organisationen zählen, die sich für die Verbreitung der Materialien einsetzen. Die Tatsache, dass alle diese Partner die Kampagne mittragen, bedeutet, dass sie eine viel weitreichendere und nachhaltigere Wirkung hat als der jährlich bereitgestellte bezahlte Medienplan.

Eine weitere Stärke liegt in der Philosophie der Kampagnen. Der Ton ist unbeschwert, einfach und klar. Ziel ist es, so viele Menschen wie möglich (auch solche, die sich mit IT schwer tun oder Angst vor der Online-Szene haben) davon zu überzeugen, dass sie etwas bewirken können. Diese positive Verstärkung ist mit einer lösungsorientierten Botschaft gekoppelt, sodass die Sensibilisierung von einer konkreten Lösung begleitet wird, die das Leben erleichtert, wie z. B. das E-Mail-Postfach verdacht@safeonweb.be. Und schließlich werden erkennbare Situationen gewählt – wie die Frustration über lange, komplizierte Passwörter – und in ein humorvolles Konzept umgesetzt.

Konkrete Ergebnisse

Eines der wichtigsten Ergebnisse der letzten zehn Jahre ist, dass sich die übergreifende Plattform Safeonweb.be zu einer erkennbaren Marke für digitale Sicherheit in Belgien entwickelt hat, mit klaren, leicht zugänglichen Informationen und Erfahrungsberichten. Untersuchungen haben ergeben, dass 82 % der Bevölkerung safeonweb.be als Referenz für Cybersicherheit kennen. Der Bekanntheitsgrad dieser Marke ist also größer als der des ZCB.

44 % der Menschen in Belgien geben an, dass sie schon einmal eine verdächtige E-Mail oder SMS an verdacht@safeonweb.be gemeldet haben. Das System empfängt mehr als neun Millionen Meldungen pro Jahr. Damit wird das Ziel des Zentrums erreicht: Die Öffentlichkeit als erste und wichtigste Zielgruppe für die Verbesserung der Cyberresilienz zu gewinnen.

DIE KRÖNUNG

VORSITZ IM RAT DER EU 2024

In der ersten Hälfte des Jahres 2024 hatte Belgien den rotierenden Vorsitz im Rat der Europäischen Union inne. In dieser Zeit übernahm das ZCB internationale Verantwortung und spielte es eine führende Rolle bei der Förderung belgischer Prioritäten. Während des Vorsitzes lag ein starker Schwerpunkt auf der Cybersicherheit. Es war eine einmalige Gelegenheit, Belgien als internationalen Vorreiter auf diesem Gebiet bekannt zu machen.

Eine der wichtigsten Prioritäten waren die Verhandlungen zwischen dem Rat der Europäischen Union (dem Treffen der zuständigen Ministerinnen und Minister), dem Europäischen Parlament und der Europäischen Kommission über zwei Gesetzesinitiativen: den Cyber Solidarity Act und eine Änderung des Cybersecurity Act (der auf das Jahr 2019 zurückgeht). Der belgischen Delegation, die sich aus der Ständigen Vertretung bei der EU sowie Expertinnen und Experten des ZCB zusammensetzte, gelang es, in Rekordzeit eine politische Einigung über beide Gesetze zu erzielen, sogar noch vor den Europawahlen im Juni 2024.

Mit dem **EU Cybersecurity Act** wurde im Jahr 2019 der Grundstein für ein europäisches Zertifizierungssystem für cybersichere Produkte, Prozesse und Dienstleistungen gelegt. Auf diese Weise war eine Zertifizierung für die gesamte Union gültig. Während des belgischen Vorsitzes wurde über eine Änderung dieses Acts abgestimmt. Dazu gehörte die Aufnahme von Anbietern von „Managed Security Services“ (wie Sicherheitsaudits, Penetrationstests oder Incident Response) in das Zertifizierungssystem. Durch diese Zertifizierung erhalten die Kundinnen und Kunden dieser Dienstleister mehr Garantien für Qualität und Zuverlässigkeit. Außerdem können sie damit ihre Lieferkette verifizieren.

Der **Cyber Solidarity** Act trat Anfang 2025 in Kraft. Dazu gehört auch die Einrichtung eines europäischen Warnsystems für groß angelegte Cyberbedrohungen. Dieses System bündelt die Kompetenzen nationaler und grenzüberschreitender Cybersicherheitszentren mit dem Ziel, Angriffe zu erkennen, zu analysieren und darauf zu reagieren. Dieser grenzüberschreitende Informationsaustausch ist von grundlegender Bedeutung für die erfolgreiche Bekämpfung groß angelegter Cyberkriminalitätsoperationen mit einem kohärenten Ansatz.

Die EU hat in diesem Act auch beschlossen, einen gemeinsamen Notfallmechanismus einzurichten. Er umfasst Maßnahmen in drei Bereichen:

- Verstärkte Abwehrbereitschaft zur Reaktion in Schlüsselsektoren wie Finanzen, Energie und Gesundheitswesen. Organisationen aus diesen Bereichen sollten auf Schwachstellen geprüft werden, die für Cyberangriffe anfällig sein könnten.
- Schaffung einer EU-Cybersicherheitsreserve, die sich aus einer Reihe ausgewählter Anbieter aus dem Privatsektor zusammensetzen wird. Diese Reserve kann dann von den EU-Mitgliedstaaten oder -Institutionen (und sogar von Nicht-EU-Ländern) in Anspruch genommen werden, um bei größeren Sicherheitsvorfällen zu helfen. Die ENISA erhielt im Sommer 2025 den Auftrag, dies auf europäischer Ebene umzusetzen.
- Einführung von Amtshilfe: Ein Mitgliedstaat, der von einem Cybersicherheitsvorfall betroffen ist, kann dabei auf die Unterstützung anderer Mitgliedstaaten zurückgreifen.

Um die Zusammenarbeit zwischen den verschiedenen Akteuren in den 27 Mitgliedstaaten zu stärken, organisierte das ZCB im Januar 2024 den **Brussels Cybersecurity Summit**. Dabei wurde das Ökosystem unseres Landes mit Vertreterinnen und Vertretern von Cybersicherheitsökosystemen aus der übrigen EU zusammengebracht – und zwar in verschiedenen Handlungsfeldern: technische, strategische und Finanzierungsfachleute. Neu war auch, dass sich die Direktorinnen und Direktoren der nationalen und regionalen Cybersicherheitsbehörden zu einem informellen Gipfel trafen.

Bildunterschrift 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.

Eine weitere Errungenschaft betraf EU-CyCLONe, die Organisation, die als Bindeglied zwischen den nationalen Behörden der Mitgliedstaaten bei der Bewältigung einer Cyberkrise fungiert. Die Einrichtung dieser Stelle war eine Folge der NIS2-Richtlinie. Während des belgischen Vorsitzes wurden im Rahmen von EU-CyCLONe die ersten Verfahren und Regeln für den Informationsaustausch und die Koordinierung von Einsätzen vereinbart. Diese Verfahren und die Führung des ZCB konnten bei den Europawahlen 2024 und bei „Cyber Europe“, einer der größten internationalen Übungen zum Management von Cybervorfällen, sofort getestet werden.

Neben EU-CyCLONe hatte das ZCB auch den Vorsitz in zwei weiteren europäischen Netzwerken inne. Erstens die NIS Cooperation Group, in der die Mitgliedstaaten zusammenkommen, um die Umsetzung der NIS2-Richtlinie zu gestalten und wesentliche Dienste in der EU sicherzustellen. Das ZCB hat dabei unter anderem den Ton angegeben, indem es als erster europäischer Mitgliedstaat die Richtlinie umgesetzt hat. Darüber hinaus führte das Zentrum 18 Monate lang den Vorsitz im europäischen Netzwerk Computer Security Incident Response Teams (CSIRT), in dem sich die technischen „Feuerwehrteams“ von Cybervorfällen gegenseitig beraten.

Unter der Leitung des ZCB wurde auch eine umfassende Bewertung und Aufstellung der Cybersicherheitslandschaft in der EU vorgenommen. Die daraus resultierenden **Schlussfolgerungen des Rates über die Zukunft der Cybersicherheit**, die in einem Text mit dem Titel „Implement and Protect Together“ zusammengefasst sind, wurden nach Verhandlungen von allen europäischen Ministerinnen und Ministern für Telekommunikation formell angenommen. In dem Dokument fordern die 27 Mitgliedstaaten unter anderem eine geringere Rechtszersplitterung, klarere Rollen und Zuständigkeiten, eine engere Zusammenarbeit mit den Vollzugsbehörden und eine stärkere Konzentration auf den Active Cyber Protection. Dadurch verlagerte sich der Schwerpunkt der europäischen Politik de facto auf die Umsetzung und nicht auf neue Rechtsvorschriften. Auf diese Weise wurden einige der Kernpunkte des ZCB auch auf europäischer Ebene bestätigt.

Internationale Anerkennung

Belgien wurde zum Ende seines europäischen Vorsitzes Ende Juni 2024 einhellig gelobt. Zu diesem Erfolg haben auch Realisierungen im Cyberbereich beigetragen. Der bereichsübergreifende Ansatz und die transparente Art und Weise, in der die Vertretung des ZCB die Dossiers gemeinsam mit der Ständigen Vertretung bei der EU vorbereitet hatten, wurde sehr geschätzt. Ihr Enthusiasmus und ihre Bemühungen, Fachleute und politische Entscheidungsträger um konkrete Ergebnisse zu vereinen, führten zu Ergebnissen.

Infolgedessen entwickelte sich das Zentrum zu einer angesehenen und maßgeblichen Stimme auf europäischer Ebene. Dies weckte ein großes Interesse an der belgischen Cybersicherheitsstrategie und den verschiedenen Projekten im Rahmen des Konzepts der Active Cyber Protection. Der vom ZCB entwickelte Ansatz findet daher auch andernorts Anklang:

- Das Konzept des Aktiven Cyberschutzes wird von der EU als Best Practice anerkannt, die sich in die NIS2-Richtlinie einfügt (erhöhte Resilienz gegenüber Cyberangriffen in kritischen und wesentlichen Sektoren).
- Der CyberFundamentals Framework wurde seither von mehreren Ländern sowie von Privatunternehmen umgesetzt.
- Spear Warnings: Verschiedene Cybersicherheitsbehörden erwägen die Einrichtung eines ähnlichen Warnsystems in ihren eigenen Ländern.
- Belgian Anti-Phishing Shield: Das Vereinigte Königreich hat ein solches System für öffentliche Dienste eingeführt, die französische Datenschutzbehörde und das Cybersicherheitszentrum ANSSI prüfen die Entwicklung einer französischen Version und auf europäischer Ebene besteht Interesse an einer breiteren Einführung.

Ein weiterer Beleg für den guten Ruf des ZCB ist die weltweite Community, die das Zentrum durch seine Online-Veranstaltungen Connect and Share erreicht. Seit 2020 haben mehr als 8.000 IT- und Cyber-Fachleute aus 70 Ländern an diesen Sitzungen teilgenommen. Sie behandeln sowohl technische als auch strategische Themen. Internationale Keynotes tragen gerne dazu bei.

Auszeichnungen

Belgien hat sich innerhalb eines Jahrzehnts unbestreitbar zu einem Vorreiter im Bereich des Cyberschutzes entwickelt. Das Ziel, unser Land zu einem der am wenigsten durch Cyberangriffe gefährdeten Länder in der EU zu machen, wurde erreicht. Vergleichende Studien und internationale Rankings bestätigen dies.

Dank der Arbeit und der Koordination des ZCB mit nationalen Partnern gehört Belgien zu den Top 10 in renommierten Cybersicherheitsindizes, darunter der **National Cyber Security Index** (NCSI) und der EU Cybersecurity Index. Im **BitSight EU Ranking** ist Belgien unter den ersten drei.

Die International Telecommunication Union (ITU) ist die Agentur der Vereinten Nationen für Informations- und Kommunikationstechnologie. In ihrem **Global Cybersecurity Index 2024** wird Belgien als Tier-1-Rolmodel für Europa aufgeführt. In dieser Studie werden fünf Bereiche untersucht (Regulierung, technische Maßnahmen, Organisation, Niveau der Zusammenarbeit und Aufbau von Kapazitäten). Belgien erreicht eine Gesamtbewertung von 96,81 von 100 Punkten und übertrifft damit den europäischen und weltweiten Durchschnitt in allen Bereichen.

Dies ist eine internationale Anerkennung für die Bemühungen des Zentrums und des gesamten belgischen Ökosystems für Cybersicherheit.

Die jährlichen belgischen Awareness-Kampagnen finden auch international Beachtung: 2022 und 2024 wurde das Video der jährlichen Sensibilisierungskampagne mit dem European Cybersecurity Award für das beste Awareness-Video ausgezeichnet.

2023 erhielt das Projekt Spear Warning einen Publica Award

“Belgien hat sich innerhalb eines Jahrzehnts unbestreitbar zu einem Vorreiter im Bereich des Cyberschutzes entwickelt. Das Ziel, unser Land zu einem der am wenigsten durch Cyberangriffe gefährdeten Länder in der EU zu machen, wurde erreicht. Vergleichende Studien und internationale Rankings bestätigen dies.”

CB IN DER WELT: AKTUELLE BE-DROHUNGEN VERSUS „ALTE“ BEDROHUNGEN

Die Gewährleistung der Cybersicherheit unseres Landes, seiner Bürger, Unternehmen und öffentlichen Einrichtungen bleibt auch zehn Jahre nach der Gründung des ZCB eine Herausforderung. Die technologische Entwicklung, die Professionalisierung im Umfeld der Cyberkriminellen und geopolitische Entwicklungen haben zur Folge, dass die Zahl der Cyberangriffe weiterhin stark ansteigt und immer neue Formen des Betrugs auftauchen. Als nationales Koordinationszentrum verfolgt das ZCB die Situation aufmerksam.

HUIDIGE DREIGINGEN VERSUS ‘OUDE’ DREIGINGEN

Die Bedrohungslandschaft hat sich in den letzten Jahren ständig weiterentwickelt. Vor allem hat sich die Arbeitsweise von Kriminellen und staatlichen Akteuren verändert. Im Großen und Ganzen lassen sich drei große Gruppen unterscheiden, von denen jede ihre eigenen Methoden hat.

Welche Bedrohungen treten auf?

ORGANISIERTE CYBERKRIMINELLE

Während Cyberkriminalität früher hauptsächlich das Werk einzelner Hackerinnen und Hacker war, sehen wir heute international organisierte Gruppen, die nach einem ausgeklügelten Geschäftsmodell arbeiten. Ransomware-Angriffe, bei denen Daten verschlüsselt und erst nach Zahlung freigegeben werden, haben sich zu einer milliardenschweren Industrie entwickelt. Auch die Angriffe sind heute viel gezielter.

Ein groß angelegter Angriff wie WannaCry, bei dem weltweit Hunderttausende von Computern für kurze Zeit als Geiseln genommen wurden, ist heute seltener. Ransomware-Angriffe sind heute besser vorbereitet und genau auf ein bestimmtes Opfer oder eine Gruppe von Opfern zugeschnitten.

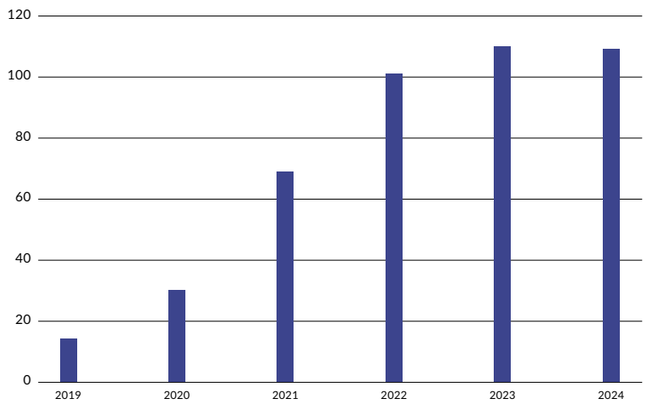
Gleichzeitig hat die technologische Entwicklung auch die Durchführung von Ransomware-Angriffen erleichtert. Ransomware-as-a-Service (RaaS) ist ein Dienst, bei dem Cyberkriminelle ein komplettes Ransomware-Paket für andere Kriminelle anbieten. Auf diese Weise muss die böswillige Person nicht mehr über einen IT-Hintergrund verfügen, um ein Unternehmen erfolgreich anzugreifen, was zu einer viel größeren Verbreitung und Häufigkeit von Angriffen führt.

HACKTIVISTEN

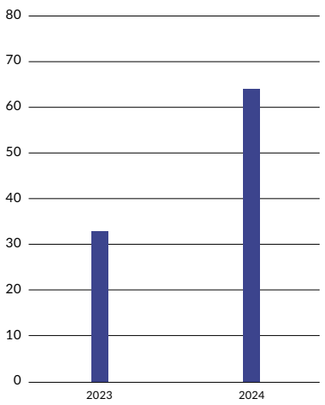
Hacktivisten führen Angriffe aus ideologischen oder politischen Motiven durch. Ihr Hauptziel ist nicht der finanzielle Gewinn, sondern die Störung der demokratischen Prozesse einer Gesellschaft oder die Verbreitung einer Botschaft.

In den meisten Fällen nutzen sie dazu DDoS-Angriffe, bei denen Websites oder Online-Dienste durch Überlastung vorübergehend unzugänglich gemacht werden. Kurzfristig sind die Auswirkungen in der Regel begrenzt, aber der symbolische Wert kann groß sein. Vieles hängt von der geopolitischen Lage und den Spannungen ab, die zu einer Häufung solcher Angriffe führen. Der Modus Operandi ist im Laufe der Jahre weitgehend gleich geblieben.

Entwicklung von Ransomware



Entwicklung DDOS



STAATLICHE AKTEURE

Staatliche Akteure handeln im Namen eines Staates oder verhalten sich im Namen eines Staates. Ihr Ziel unterscheidet sich von dem der Hacktivisten und kriminellen Gruppen. Sie verfügen über mehr Ressourcen, hochentwickelte Technologie und arbeiten mit äußerster Diskretion. Ihr Ziel ist in der Regel strategisch: Sie wollen sensible Informationen oder Technologien erbeuten und in kritische Infrastrukturen eindringen.

Auch wenn die Zahl der sichtbaren Sicherheitsvorfälle heute eher gering zu sein scheint, heißt das nicht, dass sie nicht vorkommen. Im Gegenteil, gerade weil solche Angriffe oft unter dem Radar bleiben, sind ihre tatsächlichen Auswirkungen schwer zu beurteilen. Außerdem nutzen staatliche Akteure manchmal kriminelle Gruppen als Deckung, sodass nicht immer klar ist, wer genau hinter dem Angriff steckt.

Häufigkeit: von sporadisch bis täglich

Die Zahl der Cybervorfälle hat in den letzten Jahren unbestreitbar zugenommen. Während Ransomware und Phishing vor 20 Jahren regelmäßig auftraten, sind sie heute eine alltägliche Realität. Der Grund dafür ist, dass die Schwelle für einen Angriff niedriger ist. Die Folge ist ein explosionsartiger Anstieg der Zahl der Akteure.

Darüber hinaus beobachten wir, dass die Angriffe immer schneller aufeinander folgen. Infolgedessen ist der Bedrohungsdruck strukturell höher als noch vor einigen Jahren. Cyberangriffe sind daher nicht mehr die Ausnahme, sondern eine Tatsache, mit der jedes Unternehmen rechnen muss.

Wo Kriminelle heute zuschlagen

Viele Cyberangriffe im Jahr 2025 sind opportunistischer Natur: Kriminelle suchen nach dem schwächsten Glied und schlagen zu, wenn sie ihre Chance sehen. Es zeichnen sich jedoch klare Muster ab. Regierungsbehörden, Netzbetreiber und Finanzinstitute sind nach wie vor besonders gefährdet, nicht nur, weil sie über wertvolle Daten verfügen, sondern auch, weil sie symbolische Ziele sind.

Auch Wissenseinrichtungen und Technologieunternehmen sind häufiger Zielscheibe für den Diebstahl von geistigem Eigentum, sensiblen Forschungsergebnissen oder technologischem Know-how. Die Industrie und der Logistiksektor sind ebenfalls einem höheren Risiko ausgesetzt. Angriffe in diesen Sektoren können Produktionsprozesse stören, Lieferketten unterbrechen und erhebliche wirtschaftliche Schäden verursachen.

Cyber als geopolitische Waffe

Geopolitische Spannungen haben sich auf den digitalen Bereich übertragen, und die wachsende Rivalität zwischen internationalen Machtblöcken hat die Zahl der Cyberangriffe mit (geo-)politischen Motiven spürbar erhöht. Dabei setzen die Staaten selbst zunehmend auf Cybersabotage und Cyberspionage als Teil ihrer Außenpolitik. Cyber ist somit zu einer eigenständigen Waffe geworden: Sie kann ein Land stören, Druck auf kritische Infrastrukturen ausüben und vertrauliche Informationen preisgeben.

Interessanterweise verschwimmen die Grenzen zwischen kriminellen Gruppen und staatlichen Akteuren immer mehr. Manchmal agieren Kriminelle auf Geheiß eines Regimes, manchmal nutzen Staaten bestehende Netzwerke, um ihre Spuren zu verwischen. Das Ergebnis ist eine Bedrohungslandschaft, in der Geopolitik und Cyberkriminalität zunehmend miteinander verwoben sind.

Die Auswirkungen der neuen Technologien: KI und Quanten

Neue Technologien stellen eine Bedrohung dar, bieten aber gleichzeitig auch Chancen. Die künstliche Intelligenz (KI) ist ein treffendes Beispiel dafür. So setzen Kriminelle beispielsweise zunehmend KI ein, um Phishing-E-Mails überzeugender zu gestalten, gefälschte Bilder oder Videos (Deepfakes) zu generieren und Angriffe zu automatisieren. Das Ausmaß und die Geschwindigkeit, mit der dies geschieht, erschweren die Aufdeckung. Gleichzeitig kann die KI aber auch ein Verbündeter sein: eine Technologie, die hilft, Angriffe schneller zu erkennen, Muster zu verstehen und Abwehrsysteme intelligenter und effizienter zu machen.

Während die KI vor allem einen Durchbruch bei der Software darstellt, wird die Quantentechnologie die Hardware revolutionieren. Wenn Quantencomputer einsatzbereit sind, wird ihre beispiellose Rechenleistung in der Lage sein, klassische Verschlüsselungen und Kodierungen in kurzer Zeit zu knacken. Forschende arbeiten daher bereits intensiv an quantenresistenten Lösungen wie der Post-Quanten-Kryptografie. Wann diese Technologie ausgereift sein wird und wie weitreichend die Folgen sein werden, lässt sich derzeit noch schwer vorhersagen.

Es ist daher notwendig, ständig nach neuen Durchbrüchen Ausschau zu halten und gleichzeitig weiter in Forschung und Know-how zu investieren. Diejenigen, denen es gelingt, die Möglichkeiten von KI und Quanten rechtzeitig zu nutzen, werden sich in einer immer schneller werdenden digitalen Welt einen Vorteil verschaffen.

Belgien als Vorreiter in Sachen digitale Sicherheit in Europa

Als relativ kleines Land kann sich Belgien heute getrost als Vorreiter im Bereich der Cybersicherheit bezeichnen und es gehört zu den führenden europäischen Ländern. Und das ist kein Zufall: Unsere Stärke liegt in einem pragmatischen und ergebnisorientierten Ansatz, während andere Länder sich manchmal noch in endlosen Verfahren und Bürokratie verzetteln.

> “Die Unterschiede zwischen Vergangenheit und Gegenwart liegen nicht in der Art der Angriffe, sondern vor allem in der Professionalisierung, dem Umfang und der Verflechtung mit geopolitischen, kriminellen und ideologischen Motiven. Während die Welt bei WannaCry und NotPetya gesehen hat, wie zerstörerisch ein Cyberangriff sein kann, sehen wir heute, dass die Angriffe subtiler und gezielter sind.”

Ein anschauliches Beispiel ist die Art und Weise, wie wir die NIS2-Richtlinie in einen nationalen Rahmen umgesetzt haben. Auch das Early Warning System (EWS), das das ZCB entwickelt hat, um Bedrohungen schnell zu erkennen und zu melden, gilt als Erfolgsgeschichte. Und der CyberFundamentals Framework, der Instrumente für einen besseren Cyberschutz bietet, stößt auf internationales Interesse.

Cyberkriminalität ist nach wie vor ein ausgesprochen internationales Phänomen. Ein Angriff auf unsere Infrastruktur könnte weitreichende Folgen für andere Länder haben. Europa bleibt daher der wichtigste Rahmen für die Koordinierung des Kampfes gegen Cyberkriminalität und digitale Bedrohungen. Durch gemeinsame Projekte, Informationsaustausch und Vernetzung verstärken sich die nationalen und regionalen Ökosysteme gegenseitig. Unser Land hat sich bewusst dafür entschieden, eine führende Rolle in dieser europäischen Geschichte zu übernehmen.

CENTRE FOR
CYBERSECURITY
BELGIUM 10Y

ccb.belgium.be