CENTRE FOR
CYBERSECURITY
BELGIUM

AKTIVER CYBERSCHUTZ (ACP)

Strategiedokument, Juni 2024

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Inhaltsübersicht

Tabelle der Zahlen

Tabelle der Tabellen

1. Vision für die Zukunft

Die Welt steht erst am Anfang des digitalen Wandels. Damit wir die Chancen, die dieser Wandel unserer Gesellschaft und Wirtschaft bietet, in vollem Umfang nutzen können, ist es entscheidend, dass unsere Bürger, Unternehmen und Regierungen das Vertrauen in den digitalen Bereich aufrechterhalten können. Um dieses Vertrauen zu gewährleisten, ist die Cybersicherheit von entscheidender Bedeutung.

In den letzten Jahren wurden auf nationaler und internationaler Ebene viele Anstrengungen unternommen, um die Cybersicherheit von Organisationen und potenziellen Opfern zu verbessern. Diese Bemühungen sind zwar für die Stärkung der Widerstandsfähigkeit eines Landes von entscheidender Bedeutung, doch zeigen die jüngsten Trends, dass diese Bemühungen möglicherweise nicht ausreichen, da Vorfälle im Bereich der Cybersicherheit, der Cyberkriminalität und des Online-Betrugs weiter zunehmen. Laut dem belgischen Zentrum für Cybersicherheit (CCB) liegt die Ursache hierfür in Schwachstellen, und zwar sowohl in menschlichen als auch in technischen Schwachstellen. Als nationale Cybersicherheitsagentur sehen wir es als unsere Aufgabe an, Organisationen und Bürger bei der Überwindung dieser Schwachstellen zu unterstützen.

Im Laufe der letzten Jahre hat das CCB daher mehrere Projekte entwickelt, um diese Schwachstellen durch einen proaktiveren Ansatz zu beheben, den wir unter **dem ursprünglichen Konzept der aktiven Cybersicherheit** zusammenfassen**, das später in aktiver Cyberschutz (ACP) umbenannt wurde**. Ein wichtiger politischer Schritt wurde erreicht, als die NIS2-Richtlinie die Bedeutung eines proaktiven Ansatzes anerkannte und ACP als rechtliche Anforderung in die Definition der nationalen Cybersicherheitsstrategien aufnahm. Folglich ist es für die EU-Mitgliedstaaten nun unerlässlich, in ihre nationalen Cybersicherheitsstrategien Maßnahmen zu integrieren, die die ACP als Teil einer umfassenden Präventions- und Resilienzstrategie umsetzen. Diese Entwicklung unterstreicht die Bedeutung proaktiver Maßnahmen zum Schutz der Cyberinfrastruktur und gewährleistet die Sicherheit der digitalen Kommunikation in der EU.

Das CCB ist fest davon überzeugt, dass es möglich ist, ACP zu fördern und möchte nicht nur die EU-Mitgliedstaaten, sondern auch andere Länder ermutigen, das ACP Konzept zu übernehmen. In diesem Leitfaden möchten wir unser Verständnis des ACP Konzepts darlegen und einige unserer Erfahrungen weitergeben, sofern sie für andere von Nutzen sein können und die Zusammenarbeit fördern.

Cybersicherheit ist kein Projekt, es ist eine Reise.

Generaldirektor des Zentrums für Cybersicherheit Belgien,
Miguel De Bruycker, Juni 2024

2. Einführung

In der EU-Richtlinie 2022/2555 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, der sogenannten NIS 2, wird in Erwägungsgrund 57 und Artikel 7 erstmals rechtlich auf das Konzept des aktiven Cyber-Schutzes (ACP) Bezug genommen.

In der Richtlinie heißt es: "Im *Rahmen ihrer nationalen Cybersicherheitsstrategien sollten die Mitgliedstaaten Maßnahmen zur Förderung des aktiven Cyberschutzes als Teil einer umfassenderen Verteidigungsstrategie ergreifen*."[1] Bereits die vorherige NIS-Richtlinie verpflichtete die Mitgliedstaaten, nationale Cybersicherheitsstrategien zu verabschieden und darin strategische Ziele und Prioritäten festzulegen. Nun **verspricht die ACP, sich zu einer zentralen Anlaufstelle für nationale Behörden und politische Entscheidungsträger zu entwickeln, die** im Rahmen ihrer NIS2-Umsetzungsverpflichtungen **mit der Überarbeitung, Aktualisierung und Verabschiedung nationaler Cybersicherheitsstrategien beauftragt sind.**

Da die EU-Mitgliedstaaten jedoch noch dabei sind, die NIS 2 in nationales Recht umzusetzen, gibt es noch kein gemeinsames Verständnis oder besser eine gemeinsame Definition dessen, was ACP genau bedeutet, und wie das ACP-Konzept auf nationaler Ebene umgesetzt werden könnte. **In diesem Grundsatzpapier möchte das CCB sein Verständnis des Konzepts darlegen und bewährte Praktiken für dessen Umsetzung vorstellen**.

In Erwägungsgrund 57 der NIS 2 wird ACP beschrieben als:

> *"Anstatt reaktiv zu reagieren, ist aktiver Cyberschutz die Verhinderung, Erkennung, Überwachung, Analyse und Abschwächung von Verletzungen der Netzsicherheit auf aktive Weise, kombiniert mit dem Einsatz von Fähigkeiten innerhalb und außerhalb des Opfernetzes. Dazu könnte gehören, dass die Mitgliedstaaten bestimmten Einrichtungen kostenlose Dienste oder Instrumente anbieten, darunter Selbstbedienungsprüfungen, Erkennungsinstrumente und Dienste zur Beseitigung von Angriffen. Die Fähigkeit, Bedrohungsinformationen und -analysen, Warnmeldungen zu Cyberaktivitäten und Reaktionsmaßnahmen schnell und automatisch auszutauschen und zu verstehen, ist von entscheidender Bedeutung, um Angriffe auf Netz- und Informationssysteme mit vereinten Kräften erfolgreich zu verhindern, zu erkennen, zu bekämpfen und abzuwehren. Aktiver Cyberschutz basiert auf einer defensiven Strategie, die offensive Maßnahmen ausschließt.*

Das CCB, die nationale Behörde für Cybersicherheit in Belgien, die für die Koordinierung der europäischen Verpflichtungen und die Vertretung zuständig ist, betrachtet ACP als einen proaktiven, maßgeschneiderten, automatisierten und partizipativen Ansatz für die Cybersicherheit.

[1] Wie in Erwägungsgrund 57 der Richtlinie (EU) 2022/2555 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union erwähnt.

Tabelle 1 Merkmale des CCB-Ansatzes für ACP

Proaktiv	Anstatt nur auf Angriffe zu reagieren, beinhaltet ACP eine proaktive Suche nach potenziellen Bedrohungen, Schwachstellen und anfälligen Systemen, bevor diese in großem Umfang ausgenutzt werden können. Auf diese Weise unterstützt ACP die Verhinderung größerer Verletzungen der Cybersicherheit in Organisationen.
Maßgeschneidert	Da es keine "Einheitslösung" gibt, fördert ACP maßgeschneiderte Lösungen, die den unterschiedlichen Bedürfnissen und der Cyberlage der Beteiligten - von Einzelpersonen und kleinen Organisationen bis hin zu Großunternehmen und öffentlichen Verwaltungen - Rechnung tragen und auf ihren Sektor und ihre Systemkonfiguration zugeschnitten sind. Anstatt Warnungen zu verbreiten, fördert ACP die Weitergabe von Informationen oder das Angebot von Diensten für die einzelnen Interessengruppen, die für sie relevant sind, um eine Informationsüberlastung zu vermeiden.
Automatisiert	In einer sich rasch verändernden Cybersicherheitslandschaft ist Schnelligkeit entscheidend. Es müssen automatisierte Lösungen, vorzugsweise in großem Maßstab, entwickelt werden, um Systeme vor zunehmend automatisierten Angriffen zu schützen. Eine solche Automatisierung und Skalierbarkeit des Schutzes kann auch dazu beitragen, den zunehmenden Fachkräftemangel im Bereich der Cybersicherheit zu überwinden.
Partizipativ	ACP ermutigt alle Akteure, von Einzelpersonen bis hin zu großen Organisationen, sich aktiv an der Ermittlung und Behebung von Schwachstellen zu beteiligen, so dass ihre Organisation und nach Möglichkeit die gesamte Gesellschaft davon profitieren. Anstatt dass es nur ein schwaches Glied braucht, um einen Angriff zu ermöglichen, will ACP diese Logik umkehren: Es sollte nur einen aufmerksamen Bürger brauchen, um ein System zu schützen. Jeder kann einen Beitrag zum Schutz leisten.

Dementsprechend betont das CCB den aktiven Aspekt von ACP. Das bedeutet, dass es als nationales CSIRT die **Nutzer aktiv einbeziehen und ihnen helfen** will**, ihr eigenes digitales Umfeld zu stärken und ihr Vertrauen in den digitalen Bereich dynamisch zu festigen**. Vor allem Bürger und Unternehmen sollten in ihren eigenen Schutz einbezogen werden, da die Aktivierung zu einer besseren Zusammenarbeit führt. Belgien möchte die Nutzer aktiv mit Informationen über konkrete Bedrohungen, die für sie relevant sind, versorgen. Dieser aktive Ansatz baut auf einer soliden Basis von Politiken und Leitlinien, der Veröffentlichung von Warnungen oder dem Aufbau von Fachwissen und Fähigkeiten auf - und will darüber hinausgehen.

3. Die aktuellen Projektpfeiler des aktiven belgischen Cyberschutzes

Das CCB betrachtet ACP als ein zuverlässiges Konzept, um seine proaktive Schutzstrategie zu kapseln, die mit den Initiativen mehrerer EU-Mitgliedstaaten und ihrer jeweiligen Cyber-Agenturen übereinstimmt. **Die Hauptaufgabe des CCB besteht darin, Belgien zu einem der am wenigsten durch Cyberangriffe gefährdeten Länder Europas zu machen**. Um dieses Ziel zu erreichen, **entwickelt** das CCB **nationale Projekte, die sich nicht nur mit technischen Schwachstellen wie bösartigem Code, sondern auch mit menschlichen Schwachstellen wie Phishing befassen.**

Diese **Projekte sind derzeit in fünf operative Säulen gegliedert**: Identifizierung und Abschaltung bösartiger Infrastrukturen, Einbeziehung der Nutzer, Speerwarnung, Cybersicherheit als Routine und validierte Dienste.

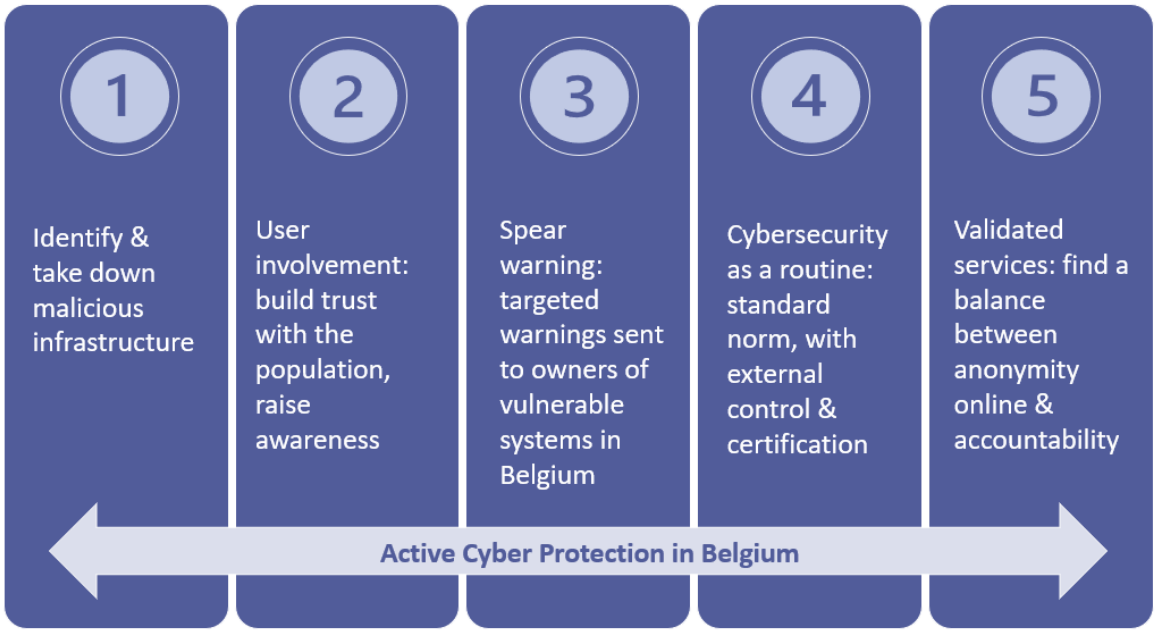

Abbildung 1 Die aktuellen ACP-Projektsäulen des CCB

Bevor diese Säulen im Einzelnen erörtert werden, ist es wichtig klarzustellen, dass das ACP-Konzept **des CCB kein statisches Unterfangen mit einem endlichen Ziel ist, sondern ein fließender und progressiver Prozess**. Da er ständig überarbeitet und verfeinert wird, wird er eher als eine fortlaufende Reise, denn als eine Aufgabe mit einer Ziellinie betrachtet. Ziel der CCB ist es, einen Gesamtrahmen zu schaffen, der die nötige Flexibilität für die Anpassung an neue Cyberangriffsmethoden bietet. Diese proaktive Herangehensweise ist von entscheidender Bedeutung, um in der stetig fortschreitenden Welt der Cyber-Bedrohungen einen Wettbewerbsvorteil zu erlangen. Die folgenden fünf Säulen, wie sie hier beschrieben sind, werden zukünftigen Anpassungen unterliegen.

Säule I - Identifizierung und Beseitigung bösartiger Infrastrukturen

Projekte zur Segmentierung von Infrastrukturen beinhalten die systematische Identifizierung von Infrastrukturen, die von böswilligen Akteuren genutzt werden, mit dem Ziel, rechtzeitig vor solchen Infrastrukturen zu warnen. Anschließend werden geeignete Maßnahmen ergriffen, um diese Bedrohungen herauszufiltern, wenn dies als notwendig erachtet wird. Dieser Infrastruktur-"Segmentierungs"-Ansatz konzentriert sich auf das Verständnis der Aktivitäten bösartiger Akteure und ermöglicht einen gezielteren Schutz unserer belgischen Infrastruktur.

Eine der zentralen Initiativen des CCB im Rahmen dieser Projektsäule ist das **belgische Anti-Phishing-Schutzschild** (BAPS). Siehe den entsprechenden Anhang für weitere Einzelheiten. Das 2021 gestartete BAPS Projekt gibt Warnungen vor bösartigen Websites auf der belgischen DNS-Ebene aus und entspricht damit der in der NIS 2 beschriebenen Dimension der "aktiven Schadensbegrenzung".

Das Projekt soll bösartige Links identifizieren und dann alle belgischen Nutzer - Kunden der großen belgischen Internetdienstanbieter - von dieser Seite wegleiten. Wenn eine von einem Internetnutzer aufgerufene Website auf einer Liste mit verdächtigen Links steht (die Liste wird vom CCB geführt), wird der Nutzer auf eine Warnseite umgeleitet. Durch die Zusammenarbeit mit den belgischen Internetanbietern und der Öffentlichkeit konnten im Jahr 2022 nicht weniger als **13 Millionen Klicks auf verdächtige Websites verhindert werden**, was etwa 25 Warnungen an belgische Internetnutzer pro Minute entspricht. Im ersten Quartal 2024 führte BAPS zu 3.03.984 Zugriffen auf die Warnseite, was einem Tagesdurchschnitt von 97.838 Zugriffen entspricht. Durch das System werden jeden Tag fast 98.000 Belgier, die auf einen bösartigen Link geklickt haben, davor geschützt, die bösartige Infrastruktur aufzurufen.

Das Projekt ist somit proaktiv, automatisiert, maßgeschneidert und - wie die zweite Säule zeigt - auch partizipativ.

Säule II - Einbindung der Nutzer

Die Projekte, die sich um die Säule der Einbindung der Zielgruppen gruppieren, konzentrieren sich auf den Aufbau von Vertrauen bei der belgischen Bevölkerung (d. h. Medien, Nutzer, Unternehmen, Bürger) und die Verbreitung des Bewusstseins für die Cybersicherheit. Diese Projekte werden unter dem Namen "Safeonweb" geführt und richten sich sowohl an die Öffentlichkeit (@Home) als an Organisationen (@Work).

- **Safeonweb@home** nutzt eine Mischung aus verschiedenen Kommunikationsmitteln, um die belgischen Bürger schnell zu informieren und sie über Online-Sicherheit und digitale Bedrohungen zu beraten. Hierdurch wird die Gefahr verringert um Opfer von Betrügern und Cyberkriminellen zu werden. Die Website www.safeonweb.be bietet ständigen Zugang zu allen Informationen zur Cybersicherheit. Dies geschieht auch über Social-Media-Kanäle, die Presse und unsere mehr als 500 Partner während unserer jährlichen Sensibilisierungskampagne, die alle Sektoren - öffentlich, privat, akademisch - und Werbung (eigene, verdiente und bezahlte) vertreten. Unsere Partner (z. B. die Cybersecurity Coalition und Febelfin) helfen uns nicht nur bei der Verbreitung der

Botschaft, sondern auch bei der Entwicklung des Inhalts der jährlichen Sensibilisierungskampagne. Dank ihres Fachwissens vor Ort konnten wir die Botschaft verfeinern und präzisieren, so dass sie möglichst viele Menschen erreicht, die geeignete Maßnahmen ergreifen, um sich vor allen Arten von Cyber-Bedrohungen zu schützen, insbesondere aber vor Phishing - der wahren Geißel unserer Zeit.

  - Ein Teil der Safeonweb-Dienste ist die Safeonweb-Mobil-App, mit der Internetnutzer schnell über neue Phishing-Versuche informiert werden und neue Sicherheitstipps erhalten (siehe Anhang C für weitere Einzelheiten).

- Ein neues Projekt ist **Safeonweb@work**. Ziel dieses Projekts ist es, sicherzustellen, dass auch belgische Unternehmen in einer zunehmend digitalisierten Welt wettbewerbsfähig sind. Belgische Unternehmen konnten durch die Digitalisierung ihre Organisation und ihrer Produktionsmethoden optimaliseren, ihre Investitionskosten senken und näher an ihre Kunden herankommen. Als Gegenreaktion auf diese exponentielle Transformation vergrößern zunehmend vernetzte und voneinander abhängige Systeme die Angriffsfläche von Organisationen und schaffen neue Herausforderungen: die Umsetzung von Cybersicherheitsmaßnahmen zum Schutz ihrer Aktivitäten und Investitionen. Aus diesem Grund und aufbauend auf dem Erfolg und der Anerkennung von Safeonweb.be für die Öffentlichkeit, hat das CCB im November 2023 eine spezielle Plattform Safeonweb@work (https://atwork.safeonweb.be/) ins Leben gerufen. Über diese Plattform können belgische Unternehmen und Organisationen ihre Domains und IP-Bereiche registrieren, um von den Safeonweb@work-Diensten zu profitieren. Die Safeonweb@work-Plattform nutzt das bestehende Frühwarnsystem und bietet eine Light-Version an, so dass Unternehmen auf der Grundlage der von ihnen registrierten, technischen Informationen Warnungen erhalten können. Auf diesem Portal können Unternehmen auch Reifegradbewertungen vornehmen und verschiedene Beratungsdokumente, Werkzeuge, Unterstützung, Vorlagen und Referenzen finden, die ihnen helfen, ihr Cybersicherheitsniveau zu erhöhen. Siehe Anhang E für weitere Einzelheiten.

Eines der Vorzeigeprojekte von CCB Safeonweb im Kampf gegen Phishing ist das **BePhish-Projekt (siehe Anhang D)**. Seit vielen Jahren kann sich das CCB auf die Beteiligung der Öffentlichkeit durch die Meldung verdächtiger Nachrichten verlassen. Das CCB hat die E-Mail-Adresse suspicious@safeonweb.be (in vier Sprachen) eingerichtet, an die die Bürger verdächtige Nachrichten (E-Mails oder Textnachrichten) weiterleiten können. Jeden Tag erhalten wir Tausende von verdächtigen Nachrichten.

Die Beteiligung der Bevölkerung an den Safeonweb-Projekten, insbesondere am BePhish-Projekt, ist ein echtes Beispiel für ACP und steht daher in direktem Zusammenhang mit dem Aspekt der "Beteiligung" in der NIS-2-Richtlinie. Im Jahr 2021 wurden 4.500.000 Nachrichten an suspicious@Safeonweb.be weitergeleitet. Im Jahr 2022 stieg diese Zahl weiter auf 7 Millionen Nachrichten an, mit mehr als 660.000 verdächtigen URLs, was einem Durchschnitt von 15.000 analysierten Nachrichten pro Tag entspricht. Im Jahr 2023 stieg diese Zahl sogar auf fast 10 Millionen, was einem Durchschnitt von 27.000 E-Mails pro Tag entspricht. Alle diese

weitergeleiteten Links werden dann für andere Projekte wie BAPS verwendet.

Säule III – Speerwarnverfahren (Spearwarning)

Während Spear Phishing erfolgreich eingesetzt wird, um gezielte Nachrichten an Einzelpersonen zu senden, um in deren Systeme einzudringen, verwendet das CCB den gleichen Ansatz, jedoch mit dem Ziel zu schützen.

Ein wichtiger Bestandteil von ACP ist die **Erkennung von Bedrohungen in Echtzeit**. Die rechtzeitige Erkennung ermöglicht es Unternehmen, schnell zu reagieren und so den potenziellen Schaden zu minimieren. Speerwarn-Projekte sind speziell darauf ausgerichtet, Unternehmen dabei zu helfen, anfällige Systeme zu identifizieren.

Das CCB sammelt systematisch Informationen über gefährdete Systeme, einschließlich Bedrohungen, Schwachstellen und Einbrüche, und führt eine Liste der gefährdeten Systeme in Belgien, die am ehesten ausgenutzt werden können. Anschließend versucht das CCB proaktiv, die Eigentümer dieser gefährdeten Systeme zu identifizieren. Nach der Identifizierung verfasst das CCB eine individuelle und maßgeschneiderte Warnung an den Eigentümer des gefährdeten Systems, wobei automatisierte Prozesse zur schnellen und direkten Änderung eingesetzt werden. **Dieser Ansatz trägt aktiv dazu bei, die Angriffsfläche einer Organisation zu verkleinern, so dass es für potenzielle Angreifer schwieriger wird, Systemschwächen auszunutzen.** Das CCB hat wiederholt festgestellt, dass gezielte Warnungen die Handlungsbereitschaft verwundbarer Organisationen deutlich erhöhen.

Eine Vorreiterinitiative im Rahmen dieses Pfeilers ist das **Frühwarnsystem EWS (siehe Anhang B).** Diese Initiative ist darauf zugeschnitten, Organisationen von vitalem Interesse (wie NIS-Betreiber, kritische Infrastrukturen, Kernkraftwerksbetreiber, die Datenschutzbehörde) und Organisationen von besonderem Interesse auf nationaler Ebene in Belgien zu warnen. Die Einführung von EWS fügt sich nahtlos in das Konzept der "aktiven Schadensbegrenzung" ein, dass in der NIS-Richtlinie 2 dargelegt ist.

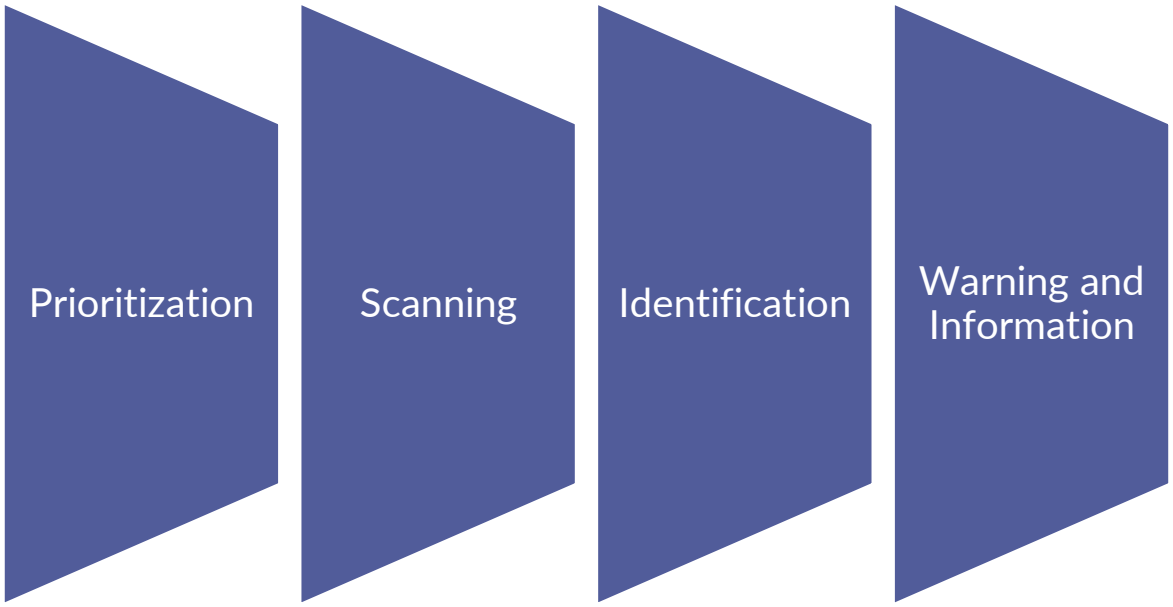

Abbildung 2 Die vier verschiedenen Phasen des EWS

Der von der EWS durchgeführte Vorwarnprozess läuft in vier verschiedenen Phasen ab: Prioritätensetzung, Scanning, Identifizierung, Warnung und Information. Im Detail:

- **Priorisierung:** Gemeinsam mit unserem kommerziellen Partner Recorded Future bewerten wir die Schwachstellen, die am ehesten ausgenutzt werden können.
- **Scanning:** Anschließend führt das CCB einen eingehenden Scan des belgischen IP-Raums durch, um die wichtigsten anfälligen Systeme für die priorisierten Schwachstellen zu ermitteln. Hierfür haben wir ein gesetzliches Mandat. Da Länder keine exakten IP-Grenzen haben, können wir nur die IP-Bereiche scannen, die mit hoher Sicherheit als in Belgien liegend angesehen werden können. Was als "belgischer IP-Raum" betrachtet werden kann, ist natürlich unscharf, aber der Anteil der Systeme, die aus diesem Grund nicht gescannt werden können, ist trivial.
- **Identifizierung:** Der nächste Schritt besteht darin, die Eigentümer der anfälligen Systeme zu ermitteln. In den meisten Fällen muss die Liste der IP-Adressen und Zeitstempel pro ISP aufgeteilt werden, und wir müssen die ISPs um die Kontaktinformationen der Eigentümer bitten.
- **Warnen und Informieren:** In einem letzten Schritt werden gezielte Warnungen an die Besitzer gefährdeter Systeme versandt. Dies wird durch automatisierte Prozesse für eine rasche Kommunikation erleichtert. Die E-Mails werden in der Regel an den IT-Manager des gefährdeten Systems geschickt.

Das CCB hat festgestellt, dass eine direkte, gezielte und maßgeschneiderte Benachrichtigung durch die nationale Behörde für Cybersicherheit im Vergleich zu einer allgemeinen Warnung vor einer Sicherheitslücke eine deutlich größere Wirkung hat. Allerdings wenden noch immer nicht alle gewarnten Eigentümer die notwendigen und dringenden Software-Updates sofort an. Häufig bleiben aktiv ausgenutzte Schwachstellen zu lange ungepatched, weil die IT-Verantwortlichen die Dringlichkeit nicht erkennen. Aus

diesem Grund versendet das CCB auch vom Generaldirektor des CCB unterzeichnete Schreiben auf Papier an den Geschäftsführer oder einen anderen gesetzlichen Vertreter der Organisation.

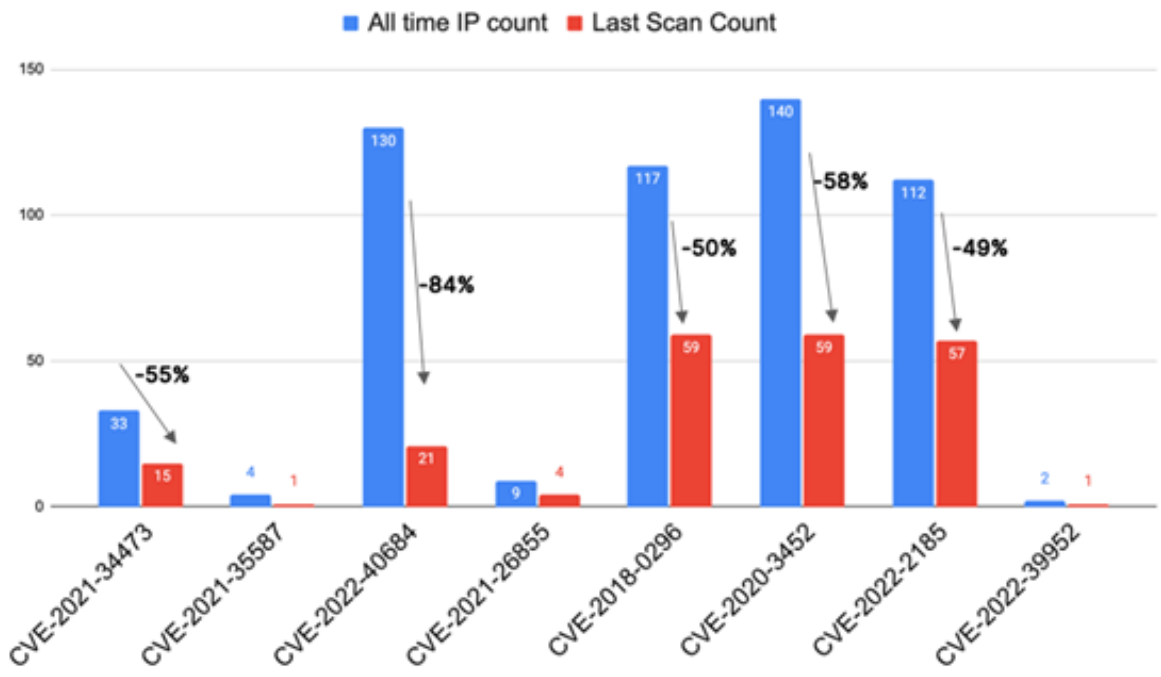

Abbildung 3 Verringerungsrate nach dem Speerwarnverfahren

Im ersten Quartal 2024 wurden 5757 Spear-Warnungen an belgische Organisationen und Einzelpersonen verschickt. Da sich die Cyber-Bedrohungslandschaft ständig weiterentwickelt, hat das CCB damit begonnen, neben den Warnungen vor Sicherheitslücken auch Warnungen vor durchgesickerten Anmeldeinformationen und Malware-Infektionen zu versenden, die zu erheblichen Schäden führen können. Diese Art von Infektionen führt häufig zu Ransomware-Angriffen. Es ist daher anzunehmen, dass das CCB dank dieser Kampagne einige Ransomware-Vorfälle verhindern konnte, auch wenn wir nie erfahren werden, wie viele genau.

In Anbetracht dieser Zahlen und Maßnahmen ist es nicht verwunderlich, dass das Speerwarn Projekt den ersten Platz der Publica Awards 2023 in der Kategorie "Security & Safety" erhielt.

Säule IV - Cybersecurity als Routine

So wie Brandschutz oder Einbruchschutz zur Sicherheitsroutine eines Unternehmens gehören, **sollten nach Ansicht des CCB auch Cybersicherheitsstandards und -normen Teil der Sicherheitsroutine eines jeden Unternehmens sein**. Organisationen, die bereits strengen gesetzlichen Anforderungen an die Cybersicherheit unterliegen, können durch die Implementierung aktiver Cyberschutzmaßnahmen ihre Compliance-Standards einhalten. Organisationen, für die Cybersicherheitsanforderungen nicht zwingend vorgeschrieben sind, können durch den Aufbau einer Routine mit Standardnormen, Kontrollen, Kennzeichnungen und Zertifizierungen ihr Cybersicherheitsniveau erhöhen.

Das CCB hat daher die CyberFundamentals entwickelt, die auf vier grundlegenden Rahmenwerken basieren, um Standard-Sicherheitsnormen, externe Kontrollen und Zertifizierungen für alle Beteiligten auf allen Ebenen zu verankern. Um die internationale Nutzung zu erleichtern, wurden keine spezifischen Verweise auf die nationale Gesetzgebung aufgenommen. Das Modell besteht aus vier Ebenen: klein, grundlegend, wichtig und wesentlich, und ist in Bezug auf die Anzahl der Kontrollen in kohärenter Weise aufgebaut. Darüber hinaus sind **die CyberFundamentals um fünf Kernfunktionen herum aufgebaut**: Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen.

- **Identifizieren:** Diese Funktion hilft dabei, ein organisatorisches Verständnis dafür zu entwickeln, wie Cybersicherheitsrisiken in Bezug auf Systeme, Menschen, Vermögenswerte, Daten und Fähigkeiten zu handhaben sind.
- **Schutz:** Diese Funktion konzentriert sich auf die Entwicklung und Umsetzung von Schutzmaßnahmen, die erforderlich sind, um ein Cyber-Risiko zu mindern oder einzudämmen.
- **Erkennen: Mit** dieser Funktion soll die rechtzeitige Erkennung von Cybersicherheits-Ereignissen sichergestellt werden.
- **Reagieren: Bei** dieser Funktion geht es um die Kontrollen, die helfen, auf Cybersicherheitsvorfälle zu reagieren. Die Reaktionsfunktion unterstützt die Fähigkeit, die Auswirkungen eines potenziellen Cybersicherheitsvorfalls einzudämmen.
- **Wiederherstellung:** Diese Funktion konzentriert sich auf die Schutzmaßnahmen, die zur Aufrechterhaltung der Widerstandsfähigkeit und zur Wiederherstellung von Diensten beitragen, die von einem Cybersicherheitsvorfall betroffen waren.

Mit den CyberFundamentals kann die Cybersicherheit zur Routine werden. Zusätzlich wurde eine Toolbox erstellt, die Organisationen bei der Umsetzung des Rahmenwerks unterstützt. Die CyberFundamentals basieren auf dem Cybersecurity Framework des National Institute of Standards and Technology (NIST/CSF) und werden durch relevante Erkenntnisse aus anderen Normen ergänzt, darunter ISO 27001/ISO 27002 (für die Einrichtung eines Informationssicherheitsmanagementsystems), IEC 62443 (Cybersicherheit für Betriebstechnik in Automatisierungs- und Steuerungssystemen) und die CIS Critical Security Controls (ETSI TR 103 305-1). Das Schema wurde vom Federal Cyber Emergency Response Team (CERT.be) validiert, dass die (anonymisierten) realen Cyberangriffsdaten zur Verfügung stellte. Diese Daten wurden verwendet, um die Angriffsabdeckungsraten zu ermitteln. Die CyberFundamentals werden unter Berücksichtigung des Feedbacks der Interessengruppen, des sich entwickelnden Risikos spezifischer Cybersicherheitsbedrohungen, der Verfügbarkeit technischer Lösungen und fortschreitender Erkenntnisse weiterhin aktualisiert und verbessert.

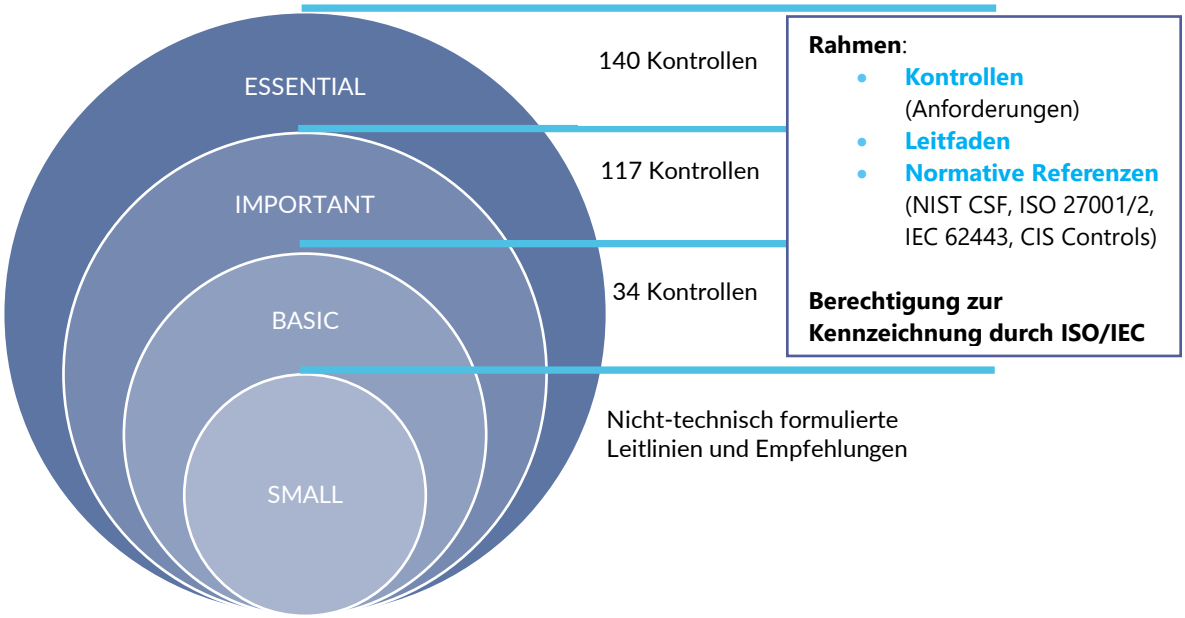

Abbildung 4 Überblick über das CyberFundamentals Framework

Auf der Grundlage historischer CCB-Daten wurden erfolgreiche Cyberangriffe anhand anonymisierter Daten nachgebessert. Die Schlussfolgerung ist, dass Maßnahmen der Sicherheitsstufe "basic" 82 % der Angriffe abdecken konnten; Maßnahmen der Sicherheitsstufe "important" konnten 94 % der Angriffe abdecken; Maßnahmen der Sicherheitsstufe "essential" konnten 100 % der Angriffe abdecken. Auf der Grundlage dieser Angriffe wurden auf jeder Stufe Schlüsselmaßnahmen ermittelt, um die Gegenmaßnahmen zum Schutz vor den bekannten Cyberangriffen, die für die jeweilige Sicherheitsstufe relevant sind, zu priorisieren. Für weitere Informationen siehe Anhang F.

Säule V - Validierte Dienste

Das Internet bietet den Nutzern Anonymität. Das Konzept der Anonymität ist jedoch ein zweischneidiges Schwert. Es kann zwar ein Gefühl der Befreiung vermitteln, aber auch bösartige Aktivitäten fördern. Ohne Rechenschaftspflicht könnten Einzelpersonen die Anonymität ausnutzen, um sich an schädlichen Aktivitäten zu beteiligen. Dies führte zu einem wachsenden Bedarf an einer gewissen Validierung, um diesen negativen Aspekten entgegenzuwirken. Während die Technologie zur Betrugsbekämpfung immer ausgefeilter wird, halten die Taktiken zur Übernahme von Konten Schritt. Forschern zufolge nehmen die Angriffe zur Übernahme von Konten weiter zu und stellen ein Problem dar, wenn es um finanzielle Verluste und den nicht quantifizierbaren Verlust von Glaubwürdigkeit und Kundenvertrauen geht.

Darüber hinaus scheinen neuere Technologien wie generative KI frühere Techniken wie cleveres Social Engineering, Phishing und andere Arten von Angriffen zu verstärken und Hackern einen beispiellosen Zugang zu personenbezogenen Daten zu verschaffen, der es ihnen ermöglicht, ein Verbraucherkonto zu übernehmen. Aus diesem Grund wird es immer schwieriger, die Authentizität nachzuweisen.

Genau dieses Problem - wie kann sichergestellt werden, dass das, was online erscheint, sicher und validiert ist - hat das CCB dazu veranlasst, sich Gedanken darüber zu machen, wie eine

sichere Online-Präsenz gewährleistet werden kann. Aufgrund der steigenden Zahl betrügerischer Websites, die für Phishing-Zwecke genutzt werden, d. h. um die persönlichen Daten der Nutzer für illegale Zwecke auszuspionieren, hat das CCB die **Säule "Validierte Dienste" des ACP** geschaffen**.**

Einer der grundlegenden Aspekte einer sicheren Online-Umgebung ist die Suche nach einem Gleichgewicht zwischen Anonymität und Validierung. Es ist wichtig, dass **die Freiheit, die die Anonymität bietet, nicht im Widerspruch zu dem zunehmenden Bedarf an Online-Validierung zu Sicherheitszwecken steht**. Ebenso wichtig ist es, Schichten der Haftung und Verantwortlichkeit einzuführen, um validierte Dienste anzubieten. Validierungsmechanismen sollten dort eingeführt werden, wo persönliche/sensible/kritische Informationen verwendet werden, sowohl aus Gründen des Datenschutzes als auch der Sicherheit. Digitale Identitäten in Verbindung mit echten Berechtigungsnachweisen können böswillige Akteure abschrecken und ein Umfeld des Vertrauens und der Glaubwürdigkeit schaffen.

Im Rahmen des Projekts "Validierte Websites" hat das CCB ein **Browser-Plugin** entwickelt, mit dem der Grad der Zuverlässigkeit von Websites bewertet und den Nutzern angezeigt werden kann (starke Validierung des Herausgebers, keine Validierung des Inhabers des Herausgebers oder bekannte bösartige Website). Das Plugin wird auf Laptops und Desktops verfügbar sein, mit dem Ziel, dass in Belgien 90 % der Nutzer beim Online-Surfen grünes Licht erhalten (weitere Einzelheiten siehe Anhang G). Die Projekte für validierte Dienste stehen in direktem Zusammenhang mit der Dimension "Vertrauen", wie sie für die Definition von ACP in NIS 2 verwendet wird. Gleichzeitig steht das Projekt für validierte Websites im Einklang mit der EUid-Verordnung, die die vorherige eIDAS-Verordnung überarbeitet. Mit dieser Verordnung verfolgt die EU das Ziel, Website-Authentifizierungsdienste zu fördern, um das Vertrauen in Online-Dienste zu stärken, indem den Nutzern die Gewissheit gegeben wird, dass hinter der von ihnen besuchten Website eine echte und rechtmäßige Einrichtung steht.

4. Schlussfolgerungen und weiteres Vorgehen

Cybersicherheit ist kein Projekt, sie ist eine Reise. Es handelt sich um einen fortlaufenden Prozess, der eine kontinuierliche Anpassung und Zusammenarbeit erfordert. In der vernetzten Welt von heute entwickeln sich Cyber-Bedrohungen ständig weiter und erfordern einen dynamischen und proaktiven Ansatz. Organisationen und Einzelpersonen dürfen die Cybersicherheit nicht als einmaliges Unterfangen mit einem definierten Endpunkt betrachten, sondern müssen sich ständig auf dem Weg zu mehr Widerstandsfähigkeit und Bereitschaft befinden. Dieses Grundsatzdokument gibt einen Einblick in den vom CCB angenommenen strategischen Rahmen. In diesem Zusammenhang wird die Bedeutung **proaktiver, maßgeschneiderter, automatisierter und partizipativer Projekte entlang fünf aktueller Säulen** betont.

Folglich **erkennt das CCB die wichtige Rolle der nationalen Cybersicherheitsbehörden an, die proaktive Maßnahmen ergreifen und die Nutzer dabei unterstützen, Schwachstellen zu erkennen und zu beheben, bevor sie Cyber-Bedrohungen erliegen**. In Anbetracht der in der NIS-2-Richtlinie festgelegten regulatorischen Verpflichtungen und der umfassenden Definition des Begriffs "ACP" **erkennt der CCB an, dass diese Bemühungen nicht isoliert verfolgt werden können**. Die Agenturen müssen zusammenarbeiten, nicht nur mit dem privaten Sektor, sondern auch untereinander. Daher unterstreicht das CCB, die internationale Dimension des ACP-Konzeptes zu berücksichtigen und ihre Rolle bei der Förderung der internationalen Beziehungen und der Zusammenarbeit im Cyber-Bereich sowie die Möglichkeiten zur Stärkung der ACP-Projekte anzuerkennen.

In Anbetracht dieser Perspektive lädt das **CCB internationale Partner aus dem öffentlichen und privaten Sektor ein, sich an den Bemühungen zu beteiligen und gemeinsam innovative Strategien zu entwickeln**. Das CCB ermutigt alle interessierten Parteien, sich zu melden und ihr Interesse an einer Zusammenarbeit oder einem Informationsaustausch über die in diesem Dokument dargelegten Grundsätze zu bekunden.

Interessierte Parteien werden bereits jetzt ermutigt, die Anhänge dieses Dokuments zu studieren, das detaillierte Informationen über spezifische CCB-Projekte, die integraler Bestandteil des ACP-Konzeptes sind, enthalten. Diese Anhänge dienen als kurze Zusammenfassung bewährter Verfahren und bieten Möglichkeiten für eine Zusammenarbeit. Durch die Lektüre dieser Details können interessierte Akteure einen Einblick in die laufenden CCB-Initiativen gewinnen und den Austausch von Fachwissen und Ressourcen erleichtern. Der Anhang wird so zu einer unverzichtbaren Ressource für alle, die ihr Engagement, für das vom CCB umgesetzte ACP-Konzept vertiefen und zu dessen Zielen der Verbesserung der Cyber-Resilienz auf nationaler und internationaler Ebene beitragen wollen.

Durch die Förderung eines Umfelds der Zusammenarbeit und des Austausches von Fachwissen **will Belgien seine Cyber-Resilienz stärken und einen Beitrag zu den weltweiten Bemühungen im Kampf gegen Cyber-Bedrohungen leisten**.

Anhang

DAS BELGISCHE ANTI-PHISHING-SCHUTZSCHILD (BAPS)	
Webseite	WARNUNG (BAPS) (Safeonweb.be)
Ziel	Verringerung der Klickrate von bösartigen Websites im belgischen Cyberspace.
Projekt	Der belgische Anti-Phishing-Schutz (BAPS) wurde 2021 eingeführt, um Internetnutzer vor bösartigen Websites auf der belgischen DNS-Ebene zu warnen. Wenn die von einem Internetnutzer angeforderte Website auf einer Liste mit verdächtigen Links steht, die vom CCB geführt wird, wird der Nutzer auf eine Warnseite weitergeleitet.
Wie es funktioniert	BAPS basiert auf dem BePhish-Projekt (siehe unten). Verdächtige Weblinks werden über die E-Mail-Adresse suspicious@safeonweb.be an das CCB gesendet. Domains werden auf Inhalte geprüft und landen auf der so genannten "BAPS-Liste" mit bösartigen Websites, wenn keine Inhalte gefunden werden können. Verdächtige URLs werden an Google Safe Browsing und Microsoft SmartScreen weitergeleitet. Die Browser verwenden diese Informationen dann, um den Internetnutzer vor bösartigen Websites zu warnen. Da das CCB keinen Einfluss auf die Geschwindigkeit hat, mit der Google und Microsoft auf diese Liste bösartiger Links reagieren, haben der CCB und die belgischen Internetdienstleister Belnet, Proximus, Telenet und Orange ein Verfahren entwickelt, um Internetnutzer in Echtzeit zu warnen: Jedes Mal, wenn ein Nutzer auf einen Link klickt, wird eine DNS-Anfrage an den Internetdienstleister (ISP) gesendet. Dank BAPS vergleicht der DNS-Server des ISP die angeforderte Website mit der Liste der bösartigen Websites. **Wenn die angeforderte Website auf dieser Liste steht, leitet der DNS-Server des ISP den Benutzer auf eine Warnseite um**. Die Liste der bösartigen Websites wird wiederum aus den weitergeleiteten Nachrichten gespeist, die über das BePhish-Projekt eingehen.
Zahlen	Durch die Zusammenarbeit mit der belgischen Öffentlichkeit wurden im Jahr 2022 nicht weniger als 13 Millionen Klicks auf verdächtige Websites verhindert, was etwa 25 Warnungen an Internetnutzer pro Minute entspricht. Im zweiten Quartal 2023 führte BAPS zu 2.064.378 Zugriffen auf die Landing Page, was einem Tagesdurchschnitt von 33.842 Zugriffen entspricht.

FRÜHWARNSYSTEM (EWS)	
Ziel	Verringerung der Anzahl der Schwachstellen und des Zeitrahmens der Bedrohungen für Organisationen von vitalem Interesse und besonderem Interesse in Belgien.
Beschreibung des Projekts	Das Frühwarnsystem (Early Warning System, EWS) ist eine Online-Plattform, die geschaffen wurde, um Organisationen von vitalem oder besonderem Interesse in Belgien schnell und standardisiert über Schwachstellen, Eindringlinge und andere Cyber-Bedrohungen oder Angriffe zu informieren, die für ihren Sektor oder sogar ihre Organisation relevant sind. Ein spezielles Team für den Austausch von Cyber-Bedrohungen und -Intelligenz überwacht das (dunkle) Web täglich auf Schwachstellen wie z. B. das Auslesen von Zugangsdaten. Die Warnungen beruhen auf Informationen, die das CCB erhält und die von einer Vielzahl öffentlicher und privater Partner auf nationaler und internationaler Ebene gefiltert werden. Diese Informationen werden sowohl im Rundfunk als auch individuell weitergegeben. • Nach der Anmeldung können die registrierten Organisationen ein Repository mit strategischen und operativen Berichten und Meldungen, die für ihren Sektor relevant sind, frei konsultieren. Ein allgemeiner Bericht über die Bedrohungslage wird ebenfalls täglich auf dem Portal veröffentlicht. Benachrichtigungen über neu verfügbare Informationen werden den angemeldeten Teilnehmern per E-Mail zugesandt. Dies kann in Echtzeit oder in Form einer Zusammenfassung geschehen. • Warnungen, Kompromissindikatoren (Indicators of Compromise, IoC) und Berichte werden gezielt an Organisationen von vitalem oder besonderem Interesse gesandt. Solche Warnungen ermöglichen es den Betroffenen, schnell relevante Informationen aus einer zuverlässigen Quelle zu erhalten und ebenso schnell zu handeln, um sich vor aktiven Bedrohungen zu schützen.
Rechtlicher Rahmen	Einer der schwierigsten Aspekte bei der Einrichtung eines Speerwarndienstes auf nationaler Ebene war die Erlangung aller erforderlichen rechtlichen Bestimmungen. Es kostete das CCB einige Mühe, die richtige Balance zu finden und die relevanten Behörden zu überzeugen. Das CCB hat nun den gesetzlichen Auftrag, Cyberbedrohungen und -Schwachstellen aufzudecken, die zu erheblichen Cyberangriffen und Schäden führen könnten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit darf das CCB nur Informationen sammeln, die für die Identifizierung der Schwachstelle erforderlich sind, mit dem alleinigen Ziel, den Eigentümer des gefährdeten Systems unverzüglich zu informieren, und kann diskriminierungsfreie und nicht-intrusive Scans durchführen. Eine weitere Gesetzesinitiative war notwendig, um dem CCB die Möglichkeit zu geben, Identitäts- und Kontaktinformationen zu erhalten. Dank dieses neuen Rechtsrahmens und einer konstruktiven Zusammenarbeit mit den Dienstanbietern können wir die meisten der gefährdeten Unternehmen innerhalb weniger Tage nach der Entdeckung der Schwachstelle identifizieren

	und benachrichtigen.
Zahlen	Das CCB hat in den ersten drei Quartalen des Jahres 2023 8000 Speerwarnungen verschickt. Je nach Schwachstelle können wir einen schnellen Rückgang von 50 % bis 90 % innerhalb von Tagen statt von Wochen oder Monaten messen. Der Effekt ist signifikant, selbst bei älteren Schwachstellen, für die bereits mehrere allgemeine Warnungen veröffentlicht wurden. Neben den Warnungen vor Sicherheitslücken hat das CCB auch damit begonnen, Warnungen vor durchgesickerten Zugangsdaten und vor Malware-Infektionen zu versenden, die zu erheblichen Schäden führen können.

SAFEONWEB@HOME: SAFEONWEB APP	
Webseite	Safeonweb Anwendung | Safeonweb
Ziel	Die wichtigsten menschlichen Eigenschaften, die Cyberkriminelle ausnutzen, sind Unwissenheit und Leichtgläubigkeit. Mit diesem Projekt möchte das CCB die Bevölkerung für Phishing und Online-Betrügereien sensibilisieren, indem er aufzeigt, dass man nicht jeder Nachricht vertrauen kann und dass man nie ganz sicher sein kann, wer eine Nachricht geschickt hat. Eine regelmäßige und wirksame Warnung vor unmittelbaren Bedrohungen kann viel bewirken, ohne Angst und übermäßiges Misstrauen zu erzeugen.
Projekt	Die Safeonweb-App ist eine mobile Anwendung für Android- und iOS-Mobilgeräte. Die App sendet Warnmeldungen über aktuelle Cyber-Bedrohungen in Belgien, vergleichbar mit Nachrichten-Flash-Apps. Die Safeonweb-App wird kostenlos für iOS (App Store) und Android (Google Play Store) angeboten.

BEPHISH	
Webseite	Was ist suspicious@Safeonweb.be? | Safeonweb
Ziel	Die Bürger sind aufgefordert, nicht nur über unsere App auf verdächtige E-Mails aufmerksam zu werden, sondern auch Maßnahmen zu ergreifen. Sie können verdächtige E-Mails oder Textnachrichten an die CCB-E-Mail-Adresse suspicious@safeonweb.be weiterleiten. Diese Aktivierung der Bevölkerung sorgt dafür, dass die Aufmerksamkeit für Phishing-Nachrichten länger und intensiver erhalten bleibt. Das Ziel von BePhish ist es, das Bewusstsein für die neuesten Phishing-Kampagnen weiter zu schärfen und die Erfolgsquote von Phishing so weit wie möglich zu reduzieren.
Projekt	Das CCB appelliert an Internetnutzer, verdächtige Nachrichten an die E-Mail-Adresse suspicious@safeonweb.be (verfügbar in Niederländisch, Französisch, Deutsch und Englisch) weiterzuleiten. Es ist auch möglich, einen Screenshot einer betrügerischen SMS- und QR-Code-Nachricht zu senden. Unsere Technologie ist in der Lage, URLs in Bildern und QR-Codes zu erkennen. Aus den empfangenen verdächtigen Nachrichten und URLs extrahiert das CCB Anhänge und Links. Die nächsten Anhänge werden automatisch analysiert. Im Falle von Anhängen wird eine Sandbox verwendet. Wenn die Analyse ergibt, dass eine URL bösartig ist, wird sie an Google Safe Browsing und Microsoft Smartscreen weitergeleitet. Diese beiden Listen bösartiger Websites werden

	von den meisten Browsern verwendet, um eine Warnung auf Browserebene zu geben. Auf diese Weise werden die Internetnutzer gewarnt, wenn sie auf einen bösartigen Link geklickt haben. Verdächtige Links "füttern" das (bereits erwähnte) BAPS-Projekt. Sie werden an Google und Microsoft Safe Browsing weitergeleitet, was es den großen Browsern ermöglicht, die Internetnutzer zu warnen. Auf diese Weise werden auch weniger aufmerksame Internetnutzer, die auf den Link klicken, geschützt.
Zahlen	Im Jahr 2021 wurden 4.500.000 Nachrichten an suspicious@safeonweb.be weitergeleitet. Im Jahr 2022 stieg diese Zahl weiter auf 7 Millionen Nachrichten an, was zur Aufdeckung von mehr als 660.000 verdächtigen URLs führte. Im Jahr 2023 erhielt das CCB fast 10.000.000 Nachrichten aus der Bevölkerung, was einem Durchschnitt von 27.000 E-Mails pro Tag entspricht. Dies führte zur Aufdeckung von fast 1,3 Millionen verdächtigen URLs.

SAFEONWEB@WORK	
Webseite	Safeonweb@work - Startseite | CCB Safeonweb
Ziel	Das Projekt Safeonweb@work zielt darauf ab, das Niveau der Cybersicherheit in belgischen Unternehmen und Organisationen zu erhöhen, indem es ihnen Inhalte, Werkzeuge und Dienstleistungen wie Schwachstellenerkennung, Warnungen, Vorlagen, Beratung und Unterstützung zur Verfügung stellt.
Projekt	Die Safeonweb@work-Plattform ist in 2 Teile gegliedert: eine Website und ein Portal mit gesichertem Login. • Auf der öffentlich zugänglichen Website finden belgische Unternehmen und Organisationen Tools und Dienstleistungen zur Bewertung des Reifegrads, verschiedene Beratungsdokumente, Tools, Unterstützung, anpassbare Richtlinienvorlagen für den Start des Informationssicherheitsmanagements, Selbstbewertungen zur Ermittlung von Cybersicherheitslücken und Referenzen, die ihnen dabei helfen, ihr Cybersicherheitsniveau sowohl kurz- als auch langfristig zu erhöhen. • Das Portal verfügt über einen Authentifizierungsmechanismus auf der Grundlage von eID (in Belgien "ItsMe" genannt) und stützt sich auf den Föderalen Authentifizierungsdienst (FAS). Nach der Authentifizierung im Portal können belgische Unternehmen und Organisationen ihre Kontaktinformationen und ihre Netzwerkinformationen (Domänennamen, IP-Adressen, IP-Bereiche) eingeben. Das Portal verwendet eine "Light-Version" des bestehenden Frühwarnsystems, um auf der Grundlage der registrierten technischen Informationen Warnmeldungen an die registrierten Unternehmen zu senden. Sobald die Registrierung abgeschlossen ist, können die Nutzer spezielle Dienste aktivieren, z. B. die Cyber-Bedrohungswarnungen (sie erhalten E-Mail-Warnungen, wenn eine Schwachstelle oder eine Infektion in ihren Netzwerkressourcen entdeckt wird), den Quick Scan Report (eine jährliche Momentaufnahme der Domäne und des

	Netzwerks des Unternehmens, in der Bedrohungen identifiziert und Maßnahmen zur Abschwächung beschrieben werden).

CYBERFUNDAMENTALS FRAMEWORK (CYFUN)	
Webseite	CyberFundamentals Framework | CCB Safeonweb
Ziel	Der CyberFundamentals Rahmen zielt darauf ab, die Cyber-Resilienz einer Organisation zu erhöhen, das Risiko der häufigsten Cyber-Angriffe deutlich zu verringern und Daten zu schützen, um sicherzustellen, dass ein Maximum an Unternehmen die grundlegenden Cyber-Sicherheitsregeln einhält.
Projekt	CyFUN wurde auf der Grundlage internationaler Standards und Rahmenwerke im Bereich der IKT- und industriellen Cybersicherheit entwickelt. Die Implementierung von CyFUN kann das Vertrauen zwischen Organisationen stärken und bietet auch Unterstützung bei der Einhaltung von Vorschriften. Der Rahmen besteht aus vier Stufen und kann von jeder Organisation unabhängig von ihrer Größe, ihrem Sektor oder ihrer Cybersicherheitsreife verwendet werden. Die vier Stufen bauen in Bezug auf die Anzahl der Kontrollen auf eine kohärente Weise auf. Mit CyFUN kann der Reifegrad der Cybersicherheit im Laufe der Zeit erhöht werden, so dass investierte Ressourcen zu einer kohärenten Erhöhung der Cybersicherheit führen können • **Die Sicherheitsstufe SMALL** bietet eine erste Orientierungshilfe für Kleinstunternehmen oder Unternehmen, die noch keine Erfahrung im Bereich der Cybersicherheit haben. • **Die Sicherheitsstufe BASIC** kann 82 % der Angriffe abdecken, • **Die Sicherheitsstufe WICHTIG** kann 94 % der Angriffe abdecken, • **Die Sicherheitsstufe ESSENTIAL** kann 100 % der Angriffe abdecken, basierend auf historischen Daten. Das CCB CyberFundamentals Framework basiert auf fünf Kernfunktionen: identifizieren, schützen, erkennen, reagieren und wiederherstellen. Diese Funktionen ermöglichen es, unabhängig von der Organisation und der Branche, die Kommunikation rund um das Thema Cybersicherheit sowohl unter technischen Fachleuten als auch unter Interessenvertretern zu fördern, so dass cyberbezogene Risiken in die Gesamtstrategie des Risikomanagements der Organisation einbezogen werden können. Die Zertifizierung oder Kennzeichnung ist durch unparteiische und kompetente akkreditierte Konformitätsbewertungsstellen (CABs) möglich, die Verifizierungs- (BASIC/IMPORTANT) oder Zertifizierungsaudits (ESSENTIAL) durchführen. CyFUN kann auch als Instrument für den Nachweis der Einhaltung der NIS2-Cybersicherheitsanforderungen verwendet werden.
Wie es funktioniert	CyFUN basiert auf dem Cybersecurity Framework des National Institute of Standards and Technology (NIST/CSF) und wird durch relevante Erkenntnisse aus anderen Normen ergänzt, darunter ISO 27001/ISO 27002 (für die Einrichtung eines Informationssicherheits-Managementsystems), IEC 62443 (Cybersicherheit für Betriebstechnik in Automatisierungs- und Steuerungssystemen), die CIS Critical Security Controls (ETSI TR 103 305-1)

	Das Schema wurde vom Federal Cyber Emergency Response Team (CERT.be) validiert, das die (anonymisierten) realen Cyberangriffsdaten zur Verfügung stellte. Diese Daten wurden verwendet, um die Angriffsabdeckungsraten zu erhalten. • **Die Einstiegsstufe Small** ermöglicht es einer Organisation, eine erste Bewertung vorzunehmen. Sie ist für Kleinstorganisationen oder Organisationen mit begrenzten technischen Kenntnissen gedacht. • **AL Basic** (34 Sicherheitskontrollen) enthält die Standardanforderungen an die Informationssicherheit für alle Unternehmen. Diese bieten einen effektiven Sicherheitswert mit Technologien und Prozessen, die bereits verfügbar sind. Wo dies gerechtfertigt ist, werden die Maßnahmen angepasst und verfeinert. Aufbauend auf der Basisstufe werden Sicherheitsanforderungen hinzugefügt, um Organisationen vor erhöhten Cyber-Risiken zu schützen und ein höheres Maß an Sicherheit zu erreichen. 82 % der CERT-Angriffsprofile werden durch Anforderungen der Stufe BASIC abgedeckt. • **AL Wichtig** (117 Sicherheitskontrollen) soll die Risiken gezielter Cyberangriffe durch Akteure mit gemeinsamen Fähigkeiten und Ressourcen zusätzlich zu den bekannten Cybersicherheitsrisiken minimieren. 94 % der CERT-Angriffsprofile werden durch Anforderungen der Stufe WICHTIG abgedeckt • **AL Essential** (140 Sicherheitskontrollen) geht noch einen Schritt weiter und reagiert auch auf das Risiko fortgeschrittener Cyberangriffe durch Akteure mit umfangreichen Fähigkeiten und Ressourcen. 100 % der CERT-Angriffsprofile werden durch Anforderungen der Stufe ESSENTIAL abgedeckt.

SAFEONWEB BROWSER-ERWEITERUNG	
Webseite	Safeonweb Browser-Erweiterung
Ziel	Die Safeonweb-Browsererweiterung ist eine Internet-Browsererweiterung, die den Grad des Vertrauens in die von Ihnen besuchten Websites misst. So kann ein Besucher dieser Website sicher sein, dass es in Ordnung ist, persönliche Daten auf dieser Website zu hinterlassen. Wenn eine Website nicht in der Lage ist, ihren Eigentümer nachzuweisen, kann es sich immer noch um eine zuverlässige Website mit nicht bösartigem Inhalt handeln, aber man sollte es sich zweimal überlegen, bevor man persönliche Daten auf dieser Website hinterlässt, da es keine Garantie dafür gibt, welche Art von Organisation hinter dieser Website steht.
Projekt	Für jede Website, die Sie besuchen, zeigt Ihnen die Safeonweb-Browsererweiterung an, ob der Eigentümer validiert wurde (grün) oder nicht (gelb). Websites ohne validierten Eigentümer (gelb) sollten nur zum Lesen geeignet sein. Wenn Sie persönliche und sensible Informationen weitergeben möchten, sollten Sie davon ausgehen, dass der Eigentümer der Website

	validiert ist (Grün). Wenn ein Hacker bösartige Inhalte auf eine Website mit validiertem Eigentümer stellt, ändert sich der Validierungsstatus direkt nach der ersten Benachrichtigung auf Gelb oder Rot. Bekannte bösartige oder unsichere Websites werden als rot gekennzeichnet.
Wie es funktioniert	Die **Erweiterung** vergibt für die von Ihnen besuchten Websites eine Punktzahl: • Grün (OK) - 4 von 4 Punkten: Der Eigentümer der Website verfügt über ein Extended Validation-Zertifikat, das von einer Zertifizierungsstelle ausgestellt wurde, oder der Eigentümer der Website ist auf atwork.Safeonweb.be registriert (nur für belgische Organisationen). Daher: Das Surfen auf dieser Website sollte weiterhin möglich sein. Es sollte in Ordnung sein, Daten auf dieser Website auszutauschen. • Bernstein (!) - Bewertungen von 1 bis 3 von 4: Der Inhaber der Website verfügt über ein Organisationsvalidierungszertifikat oder ein von einer Zertifizierungsstelle ausgestelltes Domainvalidierungszertifikat, und die Website ist nicht auf atwork.Safeonweb.be registriert Daher: Das Surfen auf dieser Website sollte weiterhin möglich sein. Im Zweifelsfall sollten Sie von der Weitergabe von Daten auf dieser Website absehen. • Rot (X) - Wertung 0 von 4: Der Website fehlen grundlegende Sicherheitsmerkmale oder sie ist als bösartig bekannt. Der Eigentümer der Website hat kein Zertifikat und wurde daher nicht validiert. Daher: Wir raten davon ab, auf dieser Website zu surfen und Daten weiterzugeben. Dieser Wert basiert auf drei Variablen; Der **Zertifikatstyp-Score**, der die Validierungsstufe des Zertifikats widerspiegelt, das Sie für Ihre Website erworben haben. Dieser Wert wird wie folgt berechnet; • 3/3 wenn Sie eine beliebige Art von Zertifikat erhalten und Ihre Website auf dem Safeonweb@work-Portal registriert haben oder ein Extended Validation-Zertifikat erhalten haben; • 2/3, wenn Sie ein Organisationsvalidierungszertifikat erhalten haben; • 1/3, wenn Sie ein Domainvalidierungszertifikat erhalten haben; oder, • 0/3, wenn Sie kein Zertifikat für Ihre Website erhalten haben. Die **Bewertung der Zertifizierungsstelle** ist ein Wert von 1 oder 0, je nachdem, ob die Zertifizierungsstelle, die das Zertifikat Ihrer Website ausgestellt hat, ein bekannter Akteur auf dem Markt ist und in den Datenbanken der CCB referenziert wird. Der **Domain-Score** gibt an, ob Ihre Domain als bösartig registriert ist; in diesem Fall wird Ihr Gesamtscore auf 0 herabgesetzt.

Zahlen	Da dieses Projekt erst vor einem Monat gestartet wurde, sind die Zahlen zum Zeitpunkt der Erstellung dieses Artikels noch begrenzt. Von Oktober 2023 bis Ende November wurde das Plugin (mehr als 12000) Mal heruntergeladen.

Haftungsausschluss

Dieses Dokument und seine Anhänge wurden vom Zentrum für Cybersicherheit Belgien (CCB) erstellt, einer föderalen Verwaltung, die durch den Königlichen Erlass vom 10. Oktober 2014 geschaffen wurde und dem Premierminister untersteht.

Das CCB übernimmt keine Verantwortung für den Inhalt dieses Dokuments.

Die bereitgestellten Informationen:

- sind ausschließlich allgemeiner Natur und zielen nicht darauf ab, alle besonderen Situationen zu berücksichtigen;
- sind nicht notwendigerweise in allen Punkten erschöpfend, präzise oder auf dem neuesten Stand;

Verantwortlicher Redakteur:
Zentrum für Cybersicherheit Belgien
Herr De Bruycker, Generaldirektor
Rue de la Loi, 18
1000 Brüssel

Juristisches Depot:
D/2024/14828/006