ACTIVE CYBER PROTECTION (ACP)

Policy document, June 2024

Table of contents

Table of figures

Table of tables

A

A

1. Vision for the Future

The world is only at the start of the digital transition. To benefit fully from the opportunities that this transition will offer our society and economy, it is crucial that our citizens, businesses and governments can maintain trust in the digital domain. To ensure such trust, cybersecurity is crucial.

In the last years, much national and international effort has been directed at improving the cybersecurity of organisations and potential victims. However, while these efforts are crucial for bolstering a country's resilience, recent trends indicate that such efforts may be insufficient, as cybersecurity incidents, cybercrime and online fraud continue to rise. According to the Centre for Cybersecurity Belgium (CCB), the cause for this are vulnerabilities: both human and technical vulnerabilities. As a national cybersecurity agency, we see it as our job to assist organisations and citizens in overcoming these vulnerabilities.

Over the course of the last years, the CCB has therefore developed several projects to address these vulnerabilities via a more proactive approach, which we group under the initial concept of Active Cybersecurity, later renamed to Active Cyber Protection (ACP). An important policy step was achieved when the NIS2 Directive recognised the importance of a proactive approach, and included ACP as a legal requirement in the definition of national cybersecurity strategies. Consequently, it is now imperative for EU Member States to integrate policies in their national cybersecurity strategies that implement ACP as part of a comprehensive preventive and resilience strategy. This development underscores the importance of proactive measures in safeguarding cyber infrastructure and ensures the security of digital communication across the EU.

The CCB is strongly convinced about the opportunity to promote ACP and wishes to encourage not only EU Member States, but also other countries, to uptake ACP policies. In this guide we wish to outline our understanding of the ACP concept and to share some of our experiences, if they can be to the benefit of others and if they could foster collaboration.

Cybersecurity is not a project, it is a journey.

Director-General of the Centre for Cybersecurity Belgium,
Miguel De Bruycker, June 2024

2. Introduction

The concept of Active Cyber Protection (ACP) is referenced – for the first time legally – in the EU Directive 2022/2555 concerning measures for a high common level of security of network and information systems across the Union, the so-called NIS 2, under recital 57 and article 7.

The directive specifies that "*as part of their national cybersecurity strategies, Member States should adopt policies on the promotion of active cyber protection as part of a wider defensive strategy.*"[1] The previous NIS directive already required Member States to adopt national cybersecurity strategies, outlining strategic objectives and priorities. Now, ACP holds the promise of emerging as a key focal point for national authorities and policymakers tasked with revising, updating, and adopting National Cybersecurity Strategies as part of their NIS2 implementation obligations

However, as EU Member States are still in the process of transposing NIS 2 into national law, there is not yet a common understanding, or better a common definition, of what ACP exactly means, and how ACP policy(ies) could be transposed at national level. In this policy document the CCB wishes to outline its understanding of the concept and share best practices in its implementation.

Recital 57 of NIS 2 describes ACP as:
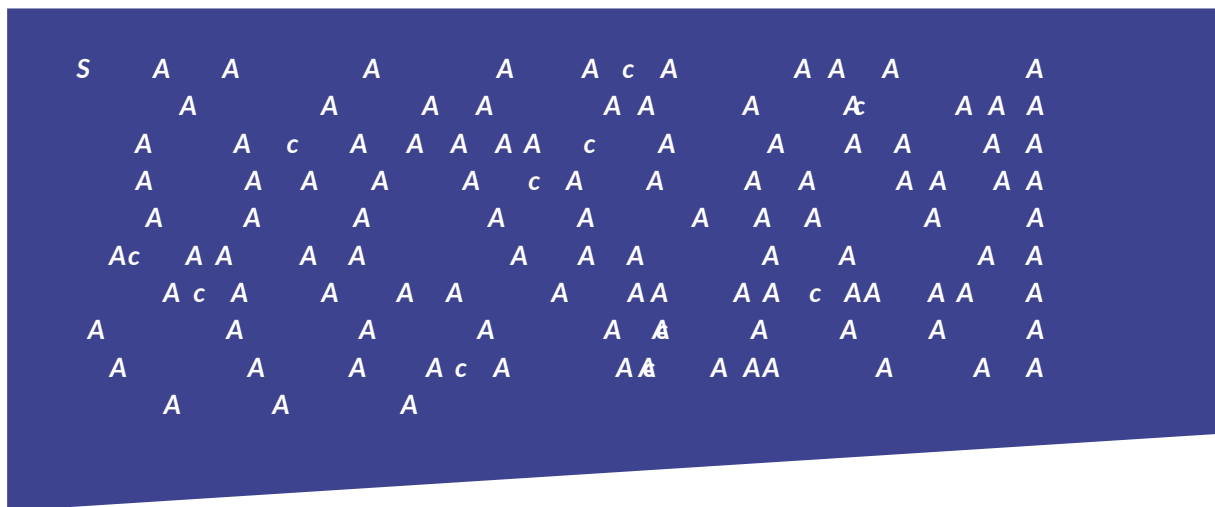
The CCB, the national authority for cybersecurity in Belgium, and responsible for coordinating European obligations and representation, considers ACP as a proactive, tailored, automated and participative approach to cybersecurity.

Table 1 Characteristics of the CCB approach to ACP

Proactive	Rather than just reacting to attacks, ACP entails a proactive search for potential threats, vulnerabilities and vulnerable systems, before they can be widely exploited. Thereby ACP supports the prevention of major cybersecurity breaches in organisations.
Tailored	Because there is no "one size fits all" solution, ACP promotes customised solutions taking into account the different needs and cyber posture of stakeholders, from individuals and small organisations to large firms and public administrations, tailored to their sector and system set-up. Rather than broadcasting warnings, ACP encourages information sharing or service offering per stakeholder only of what is relevant to them, to avoid information overload.
Automated	In a rapidly changing cybersecurity landscape, speed is essential. Automated solutions, preferably at scale, need to be developed to protect systems from increasingly equally automated attacks. Such automation and scalability in the protection can also help overcome the increasing cybersecurity skills shortage.
Participative	ACP encourages an active involvement of all actors, from individuals to large organisations, in identifying and fixing vulnerabilities in a manner that benefits their organisation and if possible, the wider society. Rather than it only taking one weak link to allow an attack, ACP wants to turn this logic around: it should only take one vigilant citizen to help protect a system. Everyone can play a part in protection.

Accordingly, the CCB emphasizes the active aspect of the ACP. Meaning that, as the national CSIRT, it seek00887 0 od

l e180nole180no a i ynaill-11yp s84thig53( )-5-5uop-6( )-5-5(th)87(g)-3ia-r-12( )-5-5(rs)-7uos82t, n thg l mai

Aove 711(a)9(l-79(l-79(,)-9(6)9(c)7(i)-7(ti)-9(zen)39(s)-7(6)9(a)9(dg)-3(6)9b(u)-4(s))7(i)-7nzes)-9(s)-7((s)-7(6)

3. The Current Project Pillars of Belgium's Active Cyber Protection

The CCB views ACP as a reliable concept to encapsulate its proactive protective strategy, aligning with initiatives underway in several EU Member States and their respective cyber agencies. The core mission of the CCB is to make Belgium one of the least cyber vulnerable countries in Europe. To achieve this goal, the CCB develops national projects that address not just technical vulnerabilities such as malicious code, but also human vulnerabilities such as phishing.

These projects are currently grouped along the lines of five operational pillars: identify and take down malicious infrastructure, user involvement, spear warning, cybersecurity as routine and validated services.
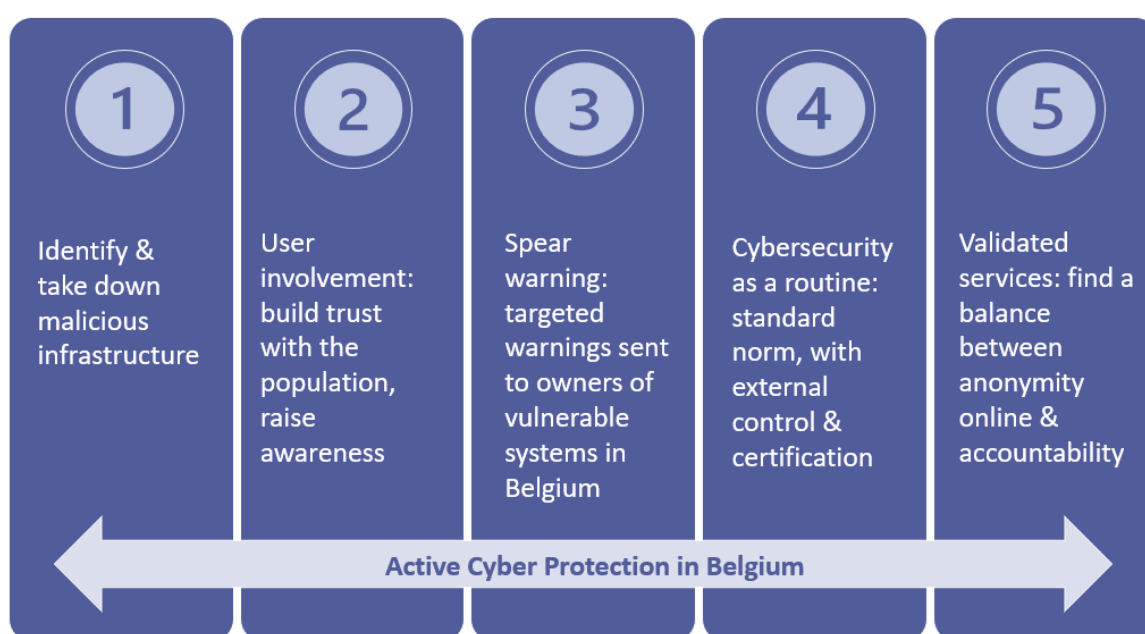
Figure 1 CCB's current ACP project pillars

Before discussing these pillars more in detail, it is important to clarify that the CCB approach to ACP does not aim to be a static endeavour with a finite goal; instead, it is a fluid and progressive effort. Constantly being revised and honed, it is seen as an ongoing journey rather than a task with a finishing line. The objective for CCB is to create an overall framework that can promote the flexibility needed to adapt to emerging cyberattacks methods. This proactive stance is essential for staying ahead in the ever-evolving realm of cyber threats. The five current pillars outlined below will undoubtedly by adapted in the future.

Pillar I – Identify And Take Down Malicious Infrastructure

Infrastructure segmentation projects entail the systematic identification of infrastructure used by malicious actors with the objective of providing timely warnings about such infrastructures. Subsequently, appropriate measures are implemented to filter out these threats when deemed necessary. This infrastructure "segmentation" approach is centred on understanding the activities of malicious actors, allowing for a more targeted safeguarding of our Belgian infrastructure.

One of CCB's pivotal initiatives under this project pillar is the Belgian Anti-Phishing Shield (BAPS), see the respective Annex for more details. Launched in 2021, BAPS operates by issuing warnings for malicious websites at the Belgian DNS level, thereby aligning with the dimension of "active mitigation" outlined in NIS 2.

The project is set up to identify malicious links, and then redirect any Belgian user – customers of the major Belgian Internet Service Providers (ISPs) – away from that page. If a website requested by an internet user is on a list with suspicious links (the list is maintained by the CCB) the user will be redirected to a warning page. Collaboration with the Belgian ISPs and public prevented no less than 13 million clicks to suspicious websites in 2022, or about 25 warnings to Belgian Internet users per minute. In the first quarter of 2024, BAPS resulted in 3.03.984 hits on the landing page, translating into a daily average of 97.838 hits. Through the system, every day almost 98.000 Belgians that clicked on a malicious link are nevertheless protected from going to the malicious infrastructure – thereby rendering it ineffective.

The project is thereby proactive, automated, tailored, and – as Pillar II demonstrates – it is also participative.

Pillar II – User Involvement

Projects grouped around the pillar of target involvement focus on building trust with the Belgian population (i.e., media, users, companies, citizens) and spread awareness on cybersecurity. These projects are branded under the "Safeonweb" name, targeting both the public (@Home) and organizations (@Work).

- Safeonweb@home uses a mix of communication tools to quickly inform Belgian citizens and advise them on online security and digital threats to reduce the like hood of falling victim to scammers and cybercriminals. The www.safeonweb.be website provides continuous access to cybersecurity advice. This is also done via social media channels, press and our 500 + partners during our annual awareness campaign, representing all sectors - public, private, academic – and advertisement (owned, earned and paid). Safeonweb@home also includes our annual awareness campaign in October. In addition to helping us spread the message, our partners (e.g., the Cybersecurity Coalition and Febelfin) also help develop the content of the campaign. Their field expertise has allowed us to refine and clarify the message, so it reaches a maximum number of people undertaking the appropriate actions to protect themselves from all kinds of cybersecurity threats but especially phishing - the real scourge of our time.

- o Part of the Safeonweb's set of services is the Safeonweb mobile app to quickly inform internet users of new phishing attempts and to send out new security tips (See Annex for more details).
  - A recent addition is Safeonweb@work. The goal of this project is to make sure that also Belgian businesses are ready to compete in an increasingly digitalized world. In fact, by digitising their organisation and production methods, Belgian companies have been able to reduce their investment costs, optimise their processes and get closer to their customers. As a backlash to this exponential transformation, increasingly connected and interdependent systems are increasing the vulnerable surface of organisations and creating new challenges: implementing cybersecurity measures to protect their activities and investments. Therefore, and building on the success and recognition of Safeonweb.be for the public, the CCB launched a specialized platform Safeonweb@work in November 2023 (https://atwork.safeonweb.be/). Via this platform, Belgian companies and organizations can register their domains and IP ranges to benefit from the Safeonweb@work services. The Safeonweb@work platform uses the existing Early Warning System and offers a light version so that companies can receive alerts based on the technical information they have registered. On this portal, organizations will also be able to make maturity assessments, and find various advisory documents, tools, support, templates, and references to help them raise their cybersecurity level. See Annex for more details.

One of CCB Safeonweb flagship projects in the fight against phishing is the BePhish project (see Annex). For many years now, the CCB has been able to rely on the participation of the public through the notification of suspicious messages. The CCB created the email address suspicious@safeonweb.be (in four languages) to which citizens can forward suspicious messages (emails or text messages). Every day we receive thousands of suspicious messages.

The participation of the population in the Safeonweb projects, especially the BePhish project, is a true illustration of ACP and is therefore directly connected to the aspect of "involvement" in the NIS 2 directive. In 2021, 4.500.000 messages were forwarded to suspicious@Safeonweb.be. In 2022, this figure rose further to 7 million messages, resulting in the detection of more than 660.000 suspicious URLs, an average of 15.000 messages analysed per day. In 2023 this rose even further to almost 10 million, or an average of 27.000 mails per day. All these forwarded links are then used to feed into other projects, such as BAPS.

Pillar III – Spear Warning Process

Whereas Spear Phishing is successfully used to send targeted messages to individuals in order to get into their systems, the CCB uses the same approach but with the goal of protection.

An important part of ACP involves real-time threat detection. Timely identification enables organizations to respond swiftly thereby minimizing potential damage. Spear warning projects are specifically designed to help organisations pinpoint vulnerable systems.

The CCB systematically collects information on vulnerable systems, encompassing threats,

vulnerabilities, intrusions and maintains a list of the most likely to be exploited vulnerable systems in Belgium. Subsequently, the CCB proactively seeks to identify the owners of these vulnerable systems. Upon identification, the CCB initiates an individual and tailored spear warning to the owner of the vulnerable system, employing automated processes for fast and direct altering. This approach actively contributes to the reduction of an organization's attack surface making it more difficult for potential attackers to exploit system weaknesses. The CCB has repeatedly noticed how targeted warnings significantly increase the degree to which vulnerable organizations take action.

A flagship initiative under this pillar is the Early Warning System (EWS, see Annex). This initiative is tailored to provide warnings to Organizations of Vital interest (such as NIS operators, critical infrastructures, nuclear operators and the data protection agency) and Organisation of Special interest at the national level in Belgium. The implementation of EWS aligns seamlessly with the concept of "active mitigation" outlined in the NIS 2 Directive.

| Prioritization | Scanning | Identification | Warning and Information |

Figure 2 the four distinct phases of EWS

The spear warning process undertaken by EWS unfolds in <u>four distinct phases</u>: prioritization; scanning; identification; warning and informing. In detail:

- Prioritization: together with Recorded Future, our commercial partner, we evaluate the vulnerabilities most likely to be exploited.
- Scanning: then, the CCB conducts an in-depth scan of the Belgian IP space to identify key vulnerable systems to the prioritized vulnerabilities. For this we have a legal mandate. As countries do not have exact IP borders, we can only scan those IP-ranges that can be considered with high confidence being in Belgium. What can be considered as "the Belgian IP space" is of course fuzzy, but the portion of systems that cannot be scanned because of this is trivial.

- Identification: the next step is to identify the owners of the vulnerable systems. Most of the time the list of IP addresses and timestamps per ISP need to be split up and we need to ask for the contact information of the owners to the ISPs.
- Warning and Informing: in a final step, targeted warnings are sent out to the owners of vulnerable systems. This is facilitated through automated processes for swift communication. Emails are usually sent to the IT manager of the vulnerable system.

The CCB has noticed the impact a direct, targeted and tailored notification has when written by the national authority for cybersecurity versus a generic warning about a vulnerability. Though still not all warned owners apply the necessary and urgent software updates immediately. Quite often, actively exploited vulnerabilities remain unpatched for too long due to a lack of urgency felt at the IT manager's level. This is why the CCB also send out letters signed by the Director General of the CCB on paper to the CEO, or other legal representative, of the organisation.

Figure 2 Reduction rate following spear warning process

During the first quarter of 2024, 5757 spear warnings were sent to Belgian organisations and individuals. Moreover, as the cyber threat landscape is always evolving, besides the warnings for vulnerabilities, CCB started to send out warnings also on leaked credentials and for malware infections that might lead to significant damage. This kind of infection often leads to ransomware attacks. Therefore, it could be assumed that thanks to this campaign, CCB was able to prevent some ransomware incidents, although we will never know how many exactly.

Considering these figures, and actions, it does not come as a surprise that the Spear Warning Project was awarded the **first place** of the Publica Awards in 2023, in the category "security & safety".

Pillar IV – Cybersecurity As A Routine

Just as fire safety or intrusion security is part of an organization's security routine, the CCB believes cybersecurity standards and norms should be part of every organization's security routine as well. For those organisations who are already under strict regulatory cybersecurity requirements, implementing active cyber protection measures can aid in meeting their compliance standards. For those organizations where cybersecurity requirements are not mandatory, building a routine with standard norms, controls, labels, and certifications will help them augment their level of cybersecurity.

The CCB therefore developed the CyberFundamentals, based on four fundamental frameworks, to instore standard security norms, external controls, and certifications for all stakeholders at all levels. To facilitate international use, no specific references were included regarding national legislation. The model is made up of four levels: small, basic, important and essential, and built up in terms of the number of controls in a coherent way. Moreover, the CyberFundamentals is built around five core functions: identify, protect, detect, respond, and recover.

- Identify: this function helps develop an organisational understanding of how to manage cybersecurity risks related to systems, people, assets, data, and capabilities.
- Protect: this function focused on developing and implementing the safeguards necessary to mitigate or contain a cyber risk.
- Detect: the purpose of this function is to ensure the timely detection of cybersecurity events.
- Respond: this function is all about the controls that help respond to cybersecurity incidents. The respond function supports the ability to contain the impact of a potential cybersecurity incident.
- Recover: this function focuses on those safeguards that help maintain resilience and restore services that have been affected by a cybersecurity incident.

With the CyberFundamentals cybersecurity can be made into a routine. An additional toolbox was created to guide organisations in the implementation of the framework. The CyberFundamentals is based on the National Institute of Standards and Technology's Cybersecurity Framework (NIST/CSF) and complemented by relevant insights from other standards including ISO 27001/ISO 27002 (for establishing an information security management system), IEC 62443 (cybersecurity for operational technology in automation and control systems.), the CIS Critical Security Controls (ETSI TR 103 305-1). The scheme is validated by the Federal Cyber Emergency Response Team (CERT.be) who provided the (anonymized) real-world cyberattack information. This data was used to obtain the attack coverage rates. The CyberFundamentals will continue to be updated and improved considering feedback received from stakeholders, evolving risk of specific cybersecurity threats, availability of technical solutions and progressive insight.
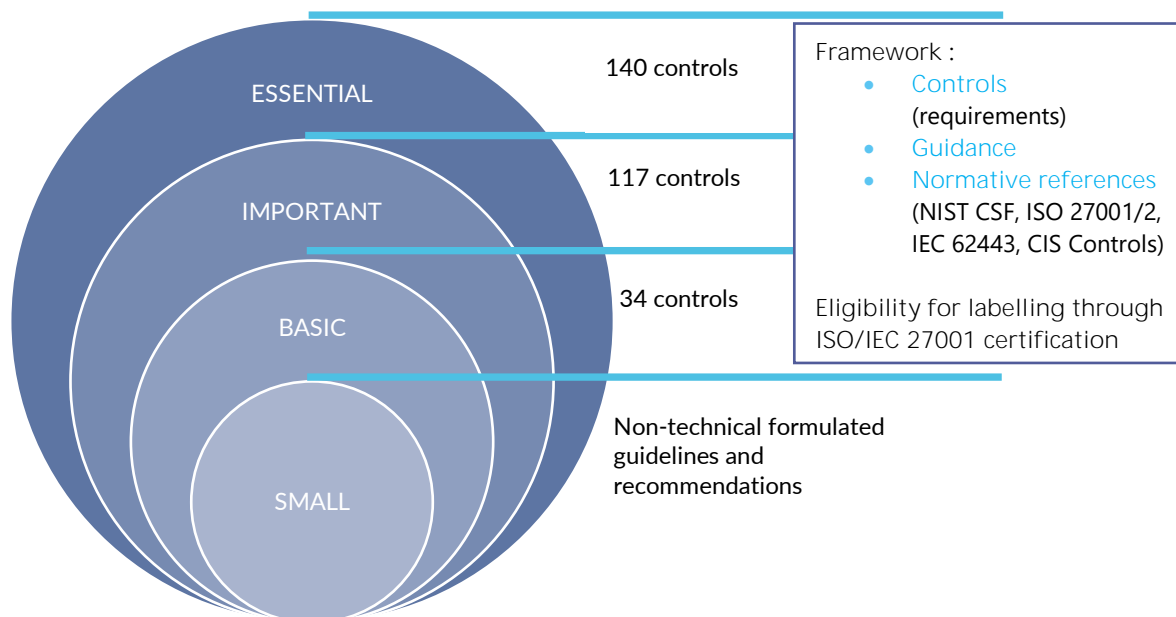
Figure 3 Overview of the CyberFundamentals Framework

Based on CCB historical data, retrofitting was done on successful cyberattacks using anonymised fata. The conclusion is that: measures in assurance level basic were able to cover 82% of the attacks; measures in assurance level important were able to cover 94% of the attacks; measures in assurance level essential were able to cover 100% of the attacks. Based on these attacks, key measures were identified at each level to prioritize the countermeasures to protect against the known cyberattacks relevant for that assurance level. For more information see Annex.

Pillar V – Validated Services

The internet offers users anonymity. However, the concept of anonymity is a double-edged sword. While it can foster a sense of liberation, it also has the potential to boost malicious activities. Without accountability, individuals might exploit anonymity to engage in harmful activities. This led to a growing need for some validation to counteract these negative aspects. As fraud prevention technology gets more sophisticated, account takeover tactics are keeping pace. According to researchers, account takeover attacks are still rising, representing a problem when it comes to monetary losses and the unquantifiable loss of credibility and customer trust.

Moreover, recent technologies, such as generative AI, seem to fuel previous techniques such as clever social engineering, phishing and other types of attacks, giving hackers an unparalleled access to personally identifiable information, allowing them to start a consumer account takeover. This is why authenticity becomes more and more complex to prove.

It is this specific conundrum – how to make sure that what appears online is safe and validated – that led the CCB to start wondering how to ensure that online presence can be secured. Because of the rise in the number of fraudulent websites used for phishing purposes, i.e., to obtain users' personal data for illegal purposes, the CCB created the Validated Services pillar of ACP.

One of the fundamental aspects of a safe online environment is seeking the balance between anonymity and validation. It is important that the freedom anonymity provides, does not oppose the increasing need for validation online for security purposes. It is equally important to introduce layers of liability and accountability to provide validated services. Validation mechanisms should be implemented where personal/sensitive/critical information is used, for both privacy and security reasons. Digital identities linked to real credentials can deter malicious actors and establish an environment of trust and credibility.

With the Validated sites project, CCB developed a browser extension to assess and indicate to users the level of reliability of websites (strong publisher validation, no publisher validation owner, or known malicious website), and will be available on laptops and desktop with an objective of 90% green light experience in Belgium when surfing online (see Annex for more details). The validated services projects are directly connected to the dimension of "trust" as used to define ACP in NIS 2. At the same time, the validated sites project is in line with the EUid Regulation, which reviews the previous eIDAS Regulation. With this regulation, the EU has the objective of promoting website authentication services, as a way to enhance trust in online services, by providing users with assurance that there is a genuine and legitimate entity standing behind the website that they are visiting.

4. Conclusions and way forward

Cybersecurity it not a project, it is a journey. It is an ongoing process that demands continuous adaptation, and collaboration. In today's interconnected world, cyber threats are constantly evolving, requiring a dynamic and proactive approach. Organizations and individuals must not view cybersecurity as a one-time endeavor with a defined endpoint but rather as an ongoing expedition towards resilience and preparedness. This policy document provides insight into the strategic framework adopted by the CCB. In this regard, emphasizing the importance of proactive, tailored, automated and participative projects along five current pillars.

Consequently, the CCB recognizes the significant role of national cybersecurity agencies taking proactive measures and supporting users in identifying and rectifying vulnerabilities before succumbing to cyber threats. **Acknowledging the regulatory obligations delineated in the NIS 2 Directive, and the comprehensive definition of ACP,** the CCB acknowledges that this endeavour cannot be pursued in isolation. **Agencies need to work together, not just with the private sector, but with each other.** Thus, it underscores the importance of considering the international dimension of ACP initiatives, recognizing their role in fostering international relations and cooperation within the cyber domain, and the opportunities to strengthen ACP projects.

Considering this perspective, the CCB extends invitations to international partners, encompassing both public and private sectors, to engage in the endeavours and collectively brainstorm innovative strategies. **The CCB encourages all interested parties to reach out, expressing interest in collaborating or sharing information on the principles articulated in this document.**

Interested parties are already encouraged to explore the Annexes, accompanying this document, where detailed information regarding CCB specific projects, integral to the ACP framework, is provided. This Annex serves as a succinct repository for best practices and offers avenues for potential cooperation. By perusing these details, interested stakeholders can gain insight into CCB ongoing initiatives, facilitating exchange of expertise and resources. The annex thus becomes a vital resource for those seeking to deepen their engagement with the ACP framework as translated by the CCB and contribute to its objectives of enhancing cyber resilience on a national and international scale.

By fostering an environment of collaboration and shared expertise, Belgium aims to bolster its cyber resilience and contribute to the global efforts in combating cyber threats.

Annex

THE BELGIAN ANTI PHISHING SHIELD (BAPS)	
Webpage	WARNING (BAPS) (Safeonweb.be)
Aim	To reduce the click-rate of malicious websites in the Belgian cyberspace.
Project	The Belgian Anti Phishing Shield (BAPS) was launched in 2021 to warn internet users about malicious websites at the Belgian DNS level. If the requested website by an internet use is on a list with suspicious links - maintained by the CCB - the user will be redirected to a warning page.
How it works	BAPS is built on the BePhish project (see below). Suspicious weblinks are sent to the CCB via the email address suspicious@safeonweb.be. Domains are checked for content and end up on the so-called "BAPS list" with malicious websites if no content can be found. Suspicious URLs are passed on to Google Safe Browsing and Microsoft SmartScreen. The browsers then use this information to warn internet users about malicious websites. Since the CCB has no control over the speed at which Google and Microsoft react to this list of malicious links, the CCB and the Belgian Internet service providers Belnet, Proximus, Telenet and Orange developed a procedure to warn internet users in real time: every time a user clicks on a link, a DNS request is sent to the Internet Service Provider (ISP). Thanks to BAPS, the DNS server of the ISP compares the requested website with the list of malicious websites. **If the requested website is on this list, the ISP's DNS server will redirect the user to a warning page**. The list of malicious websites is again fuelled by the forwarded messages received via the BePhish project.
Figures	Collaboration with the Belgian public prevented no less than 13 million clicks to suspicious websites in 2022, or about 25 warnings to Internet users per minute. In the second quarter of 2023, BAPS resulted in 2.064.378 hits on the landing page, translating into a daily average of 33.842 hits.

EARLY WARNING SYSTEM (EWS)	
Aim	To reduce the number of vulnerabilities and the time frame of threats for Organisation of Vital and Special Interest in Belgium.
Project description	The Early Warning System (EWS) is an online broadcast platform created to alert Organisations of Vital or Special Interest in Belgium in a fast and standardised way about vulnerabilities, intrusions and other cyber threats or attacks that are relevant for their sector or even their organization. A dedicated Cyber Threat and Intelligence Sharing team monitors the (dark) web daily on vulnerabilities such as credential leaks. The warnings are based on intel received by the CCB and filters from a wide array of both public and private partners, national and international. This information is shared both in a broadcasted and individually target manner. - After onboarding, registered organisations can freely consult a repository containing strategic and operational reports and notifications relevant for their sector. A general threat landscape report is also published daily on the portal. Notifications of newly available information are sent to onboarded constituents via email. This can be in real time or in a digest-form. - In a targeted manner alerts, indicators of compromise (IoC) and reports are sent directly to Organisations of Vital or Special Interest. Such alerts allow constituents to quickly obtain relevant information from a reliable source and act as quickly to protect themselves against active threats.
Legal framework	One of the most difficult parts of setting up a spear warning service on national level was obtaining all necessary legal provisions. It took the CCB quite some effort to find the right balance and convince political authorities. The CCB now has the legal mission to detect cyberthreats and vulnerabilities that could lead to significant cyberattacks and damage. While respecting proportionality, collecting only information necessary to identify the vulnerability, with the sole purpose of immediately informing the owner of the vulnerable system, the CCB can conduct non-discriminatory and non-intrusive scans. Another legislative initiative was needed to allow the CCB to obtain identity and contact information. Thanks to this new legal framework and a constructive collaboration with the Service Providers we can identify and notify most of the companies at risk within a few days after detecting the vulnerability.
Figures	The CCB sent out 8000 spear warnings in the first three quarters of 2023. Depending on the vulnerability we can measure a fast reduction ranging from 50% to 90% within days, rather than weeks or months. The effect is significant, even for older vulnerabilities for which several general warnings have already been published. Besides the warnings for vulnerabilities the CCB also started sending out warnings for leaked credentials and for malware infections that might lead to significant damage.

SAFEONWEB@HOME: SAFEONWEB APP	
Webpage	Safeonweb app | Safeonweb
Aim	The main human traits that cybercriminals exploit are ignorance and gullibility. With this project, the CCB wants to increase awareness on phishing and online swindles amongst the general population by showing that not every message can be trusted and that you can never be entirely sure who sent a message. Sending out a regular and effective warning about immediate threats can make a significant difference without wanting to create fear and excessive distrust.
Project	The Safeonweb app is a mobile application for Android and iOS mobile devices. The app sends alerts about actual cyber threats in Belgium in a comparable way to news flash apps. The Safeonweb app is provided free of charge for iOS (App Store) and Android (Google Play Store).

BEPHISH	
Webpage	What is suspicious@Safeonweb.be? | Safeonweb
Aim	Citizens are encouraged not just to be aware of suspicious mails via our app, but also to undertake action. They can forward suspicious emails or text messages to the CCB email address suspicious@safeonweb.be. This activation of the population keeps their attention to phishing messages longer and more engaged. The aim of BePhish is to further raise awareness about the latest phishing campaigns and reduce and counter as much as possible the success rate of phishing.
Project	The CCB appeals to internet users to forward suspicious messages to the email address suspicious@safeonweb.be (available in Dutch, French, German and English). It is also possible to send a screenshot of a fraudulent SMS and QR code messages. Our technology is able to detect URLs in images and QR codes. From the received suspicious messages and URLs the CCB extracts attachments and links. Next attachments are analysed in an automatic way. In the case of attachments, a sandbox is used. If the analysis shows that an URL is malicious, it is forwarded to Google Safe Browsing and Microsoft Smartscreen. These two lists of malicious websites are used by most browsers to provide a browser-level warning. This way, internet users are warned if they have clicked on a malicious link. Suspicious links "feed" the BAPS project (mentioned earlier). They are forwarded to Google and Microsoft Safe Browsing, which allows the big browsers to warn internet users. In this way, also less attentive internet users who click on the link are protected.
Figures	In 2021, 4.500.000 messages were forwarded to suspicious@safeonweb.be. In 2022, this figure rose further to 7 million messages, resulting in the detection of more than 660.000 suspicious URLs. In 2023, the CCB received almost 10.000.000 messages from the population, an average of 27.000 emails per day. This resulted in the detection of almost 1,3 million suspicious URLs.

SAFEONWEB@WORK	
Webpage	[Safeonweb@work - homepage	CCB Safeonweb](Safeonweb@work - homepage | CCB Safeonweb)
Aim A	The Safeonweb@work project aims to raise the level of cybersecurity of Belgian companies and organizations by providing them with content, tools and services such as vulnerability detection, alerts, templates, advice, and support.
Project	The Safeonweb@work platform is divided in 2 parts: a website and a portal with secured login. - The website is publicly available and gathers tools and services for Belgian companies and organisations to make maturity assessments, and find various advisory documents, tools, support, customizable policy templates to kickstart information security management, self-assessments to identify cybersecurity gaps and references to help them raise their level of cybersecurity both on the short and long-term. - The portal has an authentication mechanism based on eID (called "ItsMe" in Belgium) and rely on the Federal Authentication Service (FAS). Once authenticated in the portal, Belgian companies and organisation can fill in their contact information and their network information (domain names, IP addresses, IP ranges). The portal uses a 'light-version' of the existing Early Warning System to send out alters to registered companies based on the registered technical information. Once completed and thus registered, users can activate dedicated services such as the Cyber Threat Alerts (receive email alerts if a vulnerability or an infection is detected on their network assets), the Quick Scan Report (a yearly snapshot of the organization's domain and network identifying threats and describing mitigating actions).

CYBERFUNDAMENTALS FRAMEWORK (CYFUN)	
Webpage	[CyberFundamentals Framework	CCB Safeonweb](CyberFundamentals Framework | CCB Safeonweb)
Aim	The CyberFundamentals Framework aims to increase an organisation's cyber resilience, significantly reduce the risk of the most common cyberattacks and protect data, ensure a maximum of companies are compliant with the basic cybersecurity fundamentals.
Project	CyFUN was developed based on international standards and frameworks in the field of ICT and Industrial cybersecurity. Implementing CyFUN can build trust between organizations and also provides support for regulatory compliance. The framework is built on four levels and can be used by any organization, regardless of size, sector, or cybersecurity maturity. The four levels build up in terms of the number of controls in a coherent way. CyFUN allows the cybersecurity maturity level to be increased over time so that invested resources can result in a coherent increase of cybersecurity **Assurance level SMALL** provides starting guidance for micro-entities or entities that do not have any experience in cybersecurity. **Assurance level BASIC** is able to cover 82% of the attacks, **Assurance level IMPORTANT** can cover 94 % of the attacks, **Assurance level ESSENTIAL** can cover 100% of the attacks, based on historical data. The CCB CyberFundamentals Framework is built around five core functions: identify, protect, detect, respond, and recover. These functions allow, regardless of the organization and industry, to promote communication around cybersecurity among both technical practitioners and stakeholders so that cyber-related risks can be incorporated into the overall risk management strategy of the organization. Certification or labelling is possible through impartial and competent accredited conformity assessment bodies (CAB's) that perform verification (BASIC/IMPORTANT) or certification (ESSENTIAL) audits. CyFUN can also be used as a tool for demonstrating compliance to the NIS2 cybersecurity requirements.
How it works	CyFUN is based on the National Institute of Standards and Technology's Cybersecurity Framework (NIST/CSF) and complemented by relevant insights from other standards including ISO 27001/ISO 27002 (for establishing an information security management system), IEC 62443 (cybersecurity for operational technology in automation and control systems.), the CIS Critical Security Controls (ETSI TR 103 305-1).The scheme is validated by the Federal Cyber Emergency Response Team (CERT.be) who provided the (anonymized) real-world cyberattack information. This data was used to obtain the attack coverage rates. **Starting level Small** allows an organisation to make an initial assessment. It is intended for micro-organisations or organisations with limited technical knowledge.

- **AL Basic** (34 security controls) contains the standard information security requirements for all enterprises. These provide an effective security value with technology and processes that are already available. Where justified, the measures are tailored and refined. Building on the Basic level, security requirements are added to protect organisations from increased cyber risks to achieve a higher level of assurance. 82% of CERT attack profiles are covered by requirements on level BASIC
- **AL Important** (117 security controls) is designed to minimise the risks of targeted cyberattacks by actors with common skills and resources in addition to known cybersecurity risks. 94% of CERT attack Profiles covered by requirements on level IMPORTANT
- **AL Essential** (140 security controls) goes a step further to also respond to the risk of advanced cyberattacks by actors with extensive skills and resources. 100% of CERT attack profiles are covered by requirements on level ESSENTIAL

SAFEONWEB BROWSER EXTENSION

Webpage   Safeonweb Browser Extension

	• 2/3 if you have obtained an Organisation Validation Certificate; • 1/3 if you have obtained a Domain Validation Certificate; or, • 0/3 if you have not obtained any type of Certificate for your website. The Certificate Authority score, is a score of 1 or 0 depending on whether the Certificate Authority that delivered your website's Certificate is a known actor on the market and referenced in the CCB's databases. The Domain Score reflects whether your domain is registered as malicious, in which case your total score will be brought down to 0.
Figures	As this project only launched a month ago at the time of writing, figures are limited. From October 2023 till end of November, the browser extension was downloaded (12000+) times.

Disclaimer

This document and its annexes have been prepared by the Centre for Cybersecurity Belgium (CCB), a federal administration created by the Royal Decree of 10 October 2014 and under the authority of the Prime Minister.

All texts, layouts, designs and other elements of any nature in this document are subject to copyright law. Reproduction of extracts from this document is authorised for non-commercial purposes only and provided the source is acknowledged.

The CCB accepts no responsibility for the content of this document.

The information provided:

are exclusive of a general nature and do not intend to take into consideration all particular situations;

are not necessarily exhaustive, precise or up to date on all points;