CENTRE FOR
CYBER SECURITY
BELGIUM

UNDER THE AUTHORITY OF
THE PRIME MINISTER

CYBERSICHERHEITSSTRATEGIE BELGIEN 2.0 2021-2025

MAI 2021

.be


Security

Zusammenfassung

Die belgische Bevölkerung und Organisationen verfügen, dank der Präsenz und des Wachstums digitaler Dienste und Technologien, über verschiedene Entwicklungsmöglichkeiten. Allerdings sind Behörden, Bürger und Organisationen auch zunehmend mit (fortgeschrittenen) Cyberbedrohungen konfrontiert, die die Risiken erhöhen können und die Chancen digitaler Dienste und Technologien gefährden können. Das Ziel dieser aktualisierten nationalen Cybersicherheitsstrategie ist es, die Möglichkeiten von Dienstleistungen, Waren, Menschen und Kapital grenzüberschreitend zu schützen.

Die Zielsetzung dieser Strategie ist es, um eine zukunftsorientierte Vision eines offenen, freien und sicheren Cyberraumes zu präsentieren. Sie soll eine Antwort auf potenzielle Cyberbedrohungen bieten, denen Belgien gegenübersteht oder gegenüberstehen könnte. Dieses Dokument identifiziert die verschiedenen Akteure, die wichtigsten Bedrohungen, legt eine klare Mission fest und schlägt auf dieser Basis, strategische Ziele und Prioritäten für die kommenden Jahre sowie die notwendigen Mittel zu deren Umsetzung vor. Da Cybersicherheit in erster Linie eine gemeinsame Verantwortung ist, werden die verschiedenen Rollen der beteiligten Akteure beschrieben. Das Zentrum für Cybersicherheit Belgien (ZCB) ist für die Koordination der Cybersicherheit zuständig und spielt daher eine Schlüsselrolle bei der Umsetzung dieser Cybersicherheitsstrategie 2.0.

Centre for Cyber Security Belgium, Brussels, May 2021

Inhaltsverzeichnis

1. Einführung

Unsere Gesellschaft und Wirtschaft befinden sich im ständigen Wandel, ein Prozess, der durch die digitale Transformation beschleunigt wird. Menschen, Organisationen, Geräte, Daten und Prozesse verbinden und interagieren zunehmend über Online-Kanäle wie das Internet, mobile Geräte, das Internet der Dinge (IdD), oder die Nutzung der Cloud zur Speicherung von (persönlichen) Dateien und Fotos. Die zunehmende Nutzung neuer Technologien geht mit der Zunahme von Cyberangriffen sowie deren Schweregrad und Auswirkungsrate einher. Sensible Daten, einschließlich personenbezogener Daten, Kundendaten und politisch sensibler Daten (z.B. militärische Geheimdienstinformationen) sind zunehmend von der Offenlegung bedroht. Daher ist es von größter Wichtigkeit, diese Daten durch Sicherung der digitalen Umgebung zu schützen.

1.1 Politischer Kontext

Im Jahr 2012 entwarf Belgien seine erste Cybersicherheitsstrategie, die sich auf die Erkennung der Cyberbedrohung, die Verbesserung der Sicherheit und die Ausarbeitung von Maßnahmen zur angemessenen Reaktion auf Vorfälle konzentrierte. Mit dem kontinuierlichen Wandel in der Cyber-Landschaft besteht ein Bedarf an einer neuen belgischen Cybersicherheitsstrategie, die auf aktuelle und zukünftige Risiken und Bedrohungen eingeht.

Die Cybersicherheitsstrategie 2.0 prägt die belgische Politik und hat zum Ziel, die Cyber-Landschaft auf allen Ebenen und für alle betroffenen Parteien zu sichern. Die Überwachung, Koordination und Beaufsichtigung der Umsetzung der belgischen Cybersicherheitsstrategie liegt in der Verantwortung des Zentrums für Cybersicherheit Belgien (ZCB). Die Cybersicherheitsstrategie 2.0 setzt Ziele bis 2025 und wird in regelmäßigen Abständen überprüft bzw. angepasst.

Diese Strategie ist auch in einen internationalen Kontext eingebettet. Die Europäische Union arbeitet zum Beispiel an einer Reihe von Initiativen zur Förderung und Verbesserung der Cyber-Resilienz innerhalb der EU. Im Juli 2016 wurde die NIS-Richtlinie (*Network and Information Security)* verabschiedet, die in Belgien mit dem Gesetz vom 7. April 2019 umgesetzt wurde: *Gesetz zur Schaffung eines Rahmens für die Sicherung von Netz- und Informationssystemen von öffentlichem Interesse für die öffentliche Sicherheit*. Artikel 7 dieser Richtlinie (in Artikel 10 des belgischen Gesetzes

übernommen) schreibt vor, dass die Mitgliedsstaaten eine nationale Strategie im Rahmen von der Sicherheit von Netzwerk- und Informationssystemen ausarbeiten müssen.

Darüber hinaus trat im Juni 2019 der europäische Rechtsakt zur Cyber-Sicherheit („Cybersecurity Act") in Kraft, welcher unter anderem ein neues, permanentes Mandat für die europäische Cyber-Sicherheitsagentur ENISA einführte. Diese Verordnung unterstreicht zusätzlich die Notwendigkeit eines europäischen Zertifikats für Cybersicherheit in der Informations- und Kommunikationstechnologie, um das Vertrauen in und die Sicherheit von Produkten und Dienstleistungen zu erhöhen, was für den digitalen Binnenmarkt entscheidend ist.

Schließlich sollten auch die nationalen Engagements für Resilienz im Rahmen des *Cyber Defense Pledge* der NATO im Auge behalten werden.

1.2 Cybersicherheit

Cybersicherheit ist das Ergebnis einer Reihe von Sicherheitsmaßnahmen, die
das Risiko einer Unterbrechung oder eines unbefugten Zugriffs auf Informations- und Kommunikationssysteme (IKT) minimieren.

Cybersecurity, oder Cybersicherheit, umfasst alle angemessenen und akzeptablen Maßnahmen zum Schutz der IKT von Bürgern, Unternehmen, Organisationen und Behörden vor Cyberbedrohungen. Es geht um den Schutz von Systemen (wie Hardware, Software und zugehörige Infrastruktur), Netzwerken, sowie der darin enthaltenen Daten. Maßnahmen gegen die Nutzung von IKT, um z. B. Betrug zu begehen oder Terroristen zu rekrutieren, liegen streng genommen außerhalb des Anwendungsbereichs dieser Strategie.

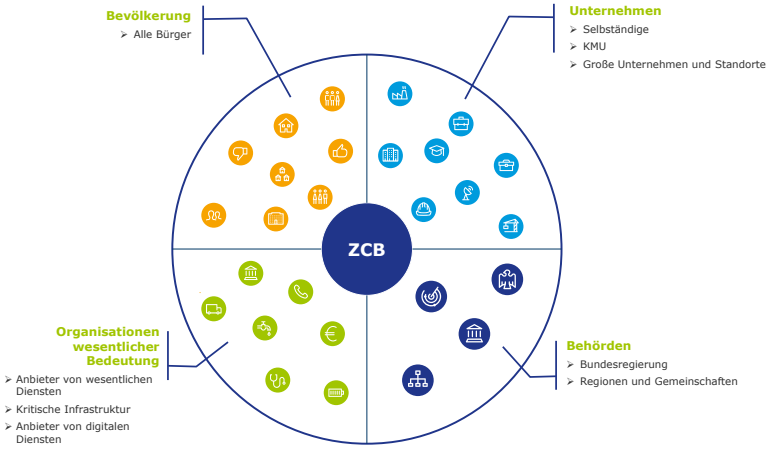
Dies erfordert die Entwicklung und Stärkung von technischen und organisatorischen Maßnahmen. Zunächst müssen die richtigen Ziele identifiziert werden, sowie die entsprechenden Sensibilisierungskampagnen zum Thema Cybersicherheit für alle betroffenen Parteien. Es ist erforderlich, sich mit der Implementierung von Präventivmaßnahmen zum Schutz sensibler

Daten vor Cyberbedrohungen und -Vorfällen zu befassen, um unbefugten Zugriff auf diese Daten zu verhindern. Es ist auch notwendig, eventuelle Bedrohungen zu überwachen und zu analysieren. Wenn ein Vorfall doch eintritt, ist es wichtig, darauf vorbereitet zu sein, um effizient reagieren zu können und ihn auf effiziente Weise zu lösen.

Die Festlegung eines „Governance-Rahmens"für Cybersicherheit ist wichtig, um die Cybersicherheitsziele zu erreichen. Daher ist es entscheidend, Rollen und Aufgaben zu bestimmen, sowie die Verantwortung aller betroffenen Parteien zu verdeutlichen. Die Festlegung eines nationalen Governance-Rahmens ermöglicht den Dialog und die Koordination der verschiedenen Aktivitäten.

Die Datenschutz-Grundverordnung, und „Datenschutz" im Allgemeinen sind nicht Teil der Cybersicherheit strictu sensu, aber sie sind offenkundig eng mit der Aufgabe des ZCB verbunden, Vorfälle und Bedrohungen zu erkennen. Eine gute Zusammenarbeit mit der belgischen Datenschutzbehörde ist daher notwendig. Auch die Bekämpfung von Online-Desinformationskampagnen ist kein eigentlicher Teil der Cybersicherheit, aber sie ist mit ihr verknüpft. Auch hier ist die Zusammenarbeit mit den zuständigen Nachrichten- und Sicherheitsdiensten unerlässlich.

1.3 Zielgruppen



Cybersicherheit ist nicht nur die Verantwortung des Staats. Es ist eine gemeinschaftliche Anstrengung, zu der alle betroffenen Parteien beitragen können. Dank der Bemühungen aller Beteiligten wird die allgemeine Sicherheit verbessert.

i. Bevölkerung
Bürger sind in erster Linie selbst für den Schutz ihres Eigentums verantwortlich. Dazu gehören Smartphones, Laptops, Tablets, aber auch die darauf befindlichen Anwendungen (z. B. Bankanwendungen) und damit die darin enthaltenen Daten. Der Schutz der eigenen Geräte und Anwendungen und deren angemessene Nutzung macht es für Angreifer schwieriger, um Cyberangriffe auszuführen. Mit Unterstützung des Staats und der Medien, wie zum Beispiel Safeonweb.be und Risico-info.be, kann sich die Bevölkerung der wichtigsten Cyberbedrohungen bewusst sein/werden und sich in die Sicherung der Cyberumgebung einbezogen fühlen.

ii. Unternehmen
Companies play a big role in protecting their own infrastructure and their employees' data. Small and Medium Enterprises (SMEs, less than 250 employees) have an important place in this, as they comprise more than 99% of Belgian companies. This group of stakeholders includes educational institutions and suppliers of security products. Security products such as firewalls, virus scans, encryption or other software and hardware products make IT systems a lot safer and reduce the likelihood of incidents. Investing in these security products, supporting suppliers of them, and facilitating users of IT systems in the use of these products is important. Developing a basic cybersecurity certification that allows a company to demonstrate that it is paying due attention to the most common cyber threats is a not insignificant aspect of this approach and can also serve as a competitive advantage. In 2019, the European Union also launched a cybersecurity certification framework in this vein.

iii. Behörden
Belgien hat eine komplexe Regierungsstruktur, die eine koordinierte Cybersicherheitspolitik für Behörden nicht einfach macht. Die Bundesbehörde verfügt über horizontale, vertikale und programmatische Dienste. Regionen und Gemeinschaften haben Ministerien und Direktorien. Das Zentrum für Cybersicherheit Belgien (ZCB) entwickelt Ratschläge und Richtlinien, die allen Behörden zur Verfügung stehen.

Sicherheit und insbesondere Cybersicherheit sind Bundesangelegenheiten und werden auf nationaler Ebene behandelt.

iv. Organisationen von wesentlicher Bedeutung
Die Organisationen von wesentlicher Bedeutung unseres Land müssen optimal vor Cyberangriffen geschützt werden, da Vorfälle in Bezug auf diese Organisationen weitreichende, nationale Auswirkungen haben können.

In diesem Zusammenhang bezieht sich der Begriff Organisationen von wesentlicher Bedeutung auf öffentliche und private Einrichtungen, die eine wesentliche Dienstleistung für die belgische Bevölkerung erbringen, und dafür Netzwerk- und Informationssysteme benutzen. Dazu gehören mindestens die Betreiber kritischer Infrastrukturen, die Anbieter wesentlicher Dienste und digitalen Diensten, sowie die kerntechnischen Anlagen (wie in den jeweiligen Rechtsrahmen genannt)[1].

A priori bestimmen die sektoralen Behörden, in Abstimmung mit dem Nationalen Krisenzentrum (NCCN) und mit dem ZCB, wer die Organisationen von wesentlicher Bedeutung sind. Der Begriff ist evolutionär zu verstehen und umfasst die Bereiche Energie, Mobilität, Telekommunikation, Finanzen, Trinkwasser, öffentliche Gesundheit, digitale Dienstleister und Behörden.

1.4 Vision

Belgien setzt sich für einen offenen, freien und sicheren Cyberraum ein, in dem sich Bürger und Unternehmen vollständig entfalten können, in dem sie sich international engagieren können und in dem die Grundrechte gesichert und geschützt sind. Um das notwendige Vertrauen der Gesellschaft in den Cyberraum aufzubauen und zu gewährleisten, ist Cybersicherheit von notwendiger und entscheidender Bedeutung. Dies ist eine gemeinsame Verantwortung aller betroffenen Parteien und erfordert einen breit angelegten Ansatz.

1 Obwohl das wissenschaftliche und wirtschaftliche Potenzial des Landes und die Organisationen, die wesentliche Dienstleistungen innerhalb des öffentlichen Sektors erbringen, in den beabsichtigten Anwendungsbereich der „Organisationen von wesentlicher Bedeutung" fallen, muss zunächst ein klarer Cyber-Governance-Rahmen für diese Sektoren entwickelt werden

1.5 Mission

Bis 2025 soll Belgien im Cyber-Bereich eines der am wenigsten gefährdeten Länder in Europa sein.

Die Cybersicherheitsstrategie 2.0 hat das Ziel, Belgien bis 2025 zu einem der am wenigsten gefährdeten Länder in Europa im Bereich der Cybersicherheit zu machen. Dies wird durch die Entwicklung von Aktionsplänen zum Schutz aller betroffenen Parteien, von der Bevölkerung über private Organisationen bis hin zu Organisationen von wesentlicher Bedeutung konkretisiert. Die Strategie ist mit den Investitionsstrategien der Regierung und des privaten Sektors für zukünftige Entwicklungen abgestimmt und gewährleistet diese Investitionen und die Schaffung neuer Möglichkeiten und Arbeitsplätze. Darüber hinaus ermöglichen die strategischen Ziele es, auf neue technologische Entwicklungen und die damit verbundenen potenziellen Risiken vorbereitet zu sein.

2. Risikobewertung

Die belgische nationale Risikobewertung 2018-2023 des Nationalen Krisenzentrums betrachtet Cyber als eines der Hauptrisikocluster, mit denen unser Land in den kommenden Jahren konfrontiert werden wird. Innerhalb dieses Clusters werden Cyberkriminalität und Hacktivismus gegen Unternehmen und kritische Infrastrukturen als nationale Hauptrisiken identifiziert.

2017 sahen wir, wie sich die Ransomware WannaCry in mehr als 150 Ländern ausbreitete und Geschäftsaktivitäten unterbrach, und wie Malware NotPetya im Handumdrehen zum teuersten Cybervorfall aller Zeiten wurde.

Darüber hinaus ist die Entwicklung der Cyberbedrohung von finanziell motiviert zu geopolitisch motiviert äußerst besorgniserregend. Westliche Länder sind mit einer Bedrohung im Cyberspace konfrontiert, die die Gefahr physischer Angriffe übersteigt. Diese Cyberbedrohungen können schwerwiegende unmittelbare Folgen haben, zum Beispiel für unsere Stromverteilung, für unsere Bankensysteme oder für die Verfügbarkeit aller Online-Dienste. Die fortgesetzte Berichterstattung über Cybervorfälle, sogar über kleinere, kann dazu führen, dass die Bevölkerung das Vertrauen in die digitale Umgebung und die Dienste verliert, was schädliche wirtschaftliche Folgen haben kann.

Als Teil der hybriden Bedrohung kann die Cyberbedrohung benutzt werden, um die Auswirkungen anderer Angriffsmethoden zu verstärken. Bei dieser Bedrohung kann eine Kombination aus zum Beispiel einem physischen Angriff mit einer Reihe von Cyberangriffen die Auswirkung erheblich verstärken und vorübergehend eine Atmosphäre von Chaos schaffen.

Diese Strategie definiert die nationalen Ziele für den Zeitraum 2021-2025, um dieser sich ständig verändernden Cyberlandschaft gerecht zu werden. Um bei der Formulierung dieser Ziele die richtigen Prioritäten zu setzen, ist es notwendig, ein klares Bild von den verschiedenen Cyberrisiken und -bedrohungen zu haben, mit denen Belgien in diesem Zeitraum konfrontiert werden kann. Dieses Kapitel bietet einen prägnanten Überblick über die wichtigsten Bedrohungsakteure und technologischen Risiken.

Es sollte jedoch erwähnt werden, dass die Risikobewertung ein fortlaufender Prozess ist. Geeignete Konsultationsplattformen, wie der Koordinierungsausschuss für Geheimdienste und Sicherheitsbehörden und die

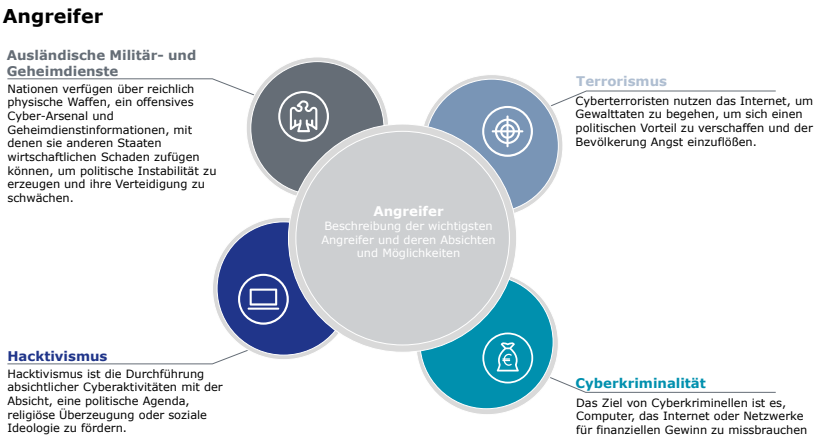
dazugehörige Plattform 4 Cyber, werden daher weiterhin die ergriffenen Maßnahmen evaluieren, Cybertrends überwachen und die Ziele bei Bedarf anpassen. Die Ausarbeitung eines belgischen Beitrags zur europäischen 5G-Risikobewertung im Jahr 2019 ist ein Beispiel dafür.

Darüber hinaus sieht das Nationale Krisenzentrum als Folgemaßnahme zur belgischen nationalen Risikobewertung 2018-2023 eine eingehendere Analyse der Hauptrisikocluster (zu denen auch Cyber gehört) mit allen betroffenen Parteien vor. Ziel ist es, die zugrundeliegenden Ursachen und Folgen besser zu identifizieren, um Entscheidungsträgern einen klaren Überblick im Umgang mit dem Risiko zu geben.

Schließlich finden auf dem belgischem Hoheitsgebiet regelmäßig Veranstaltungen statt, die ein erhöhtes Cyberrisiko mit sich bringen (ein internationales Gipfeltreffen, Wahlen, …). Diese Art von Veranstaltung kann eine außergewöhnliche Risikobewertung erfordern, um erhöhte Risiken zu identifizieren und geeignete Maßnahmen zu empfehlen.

2.1 Bedrohungsakteure

Da sich die Motivationen und Möglichkeiten von Angreifern ständig ändern, ist es entscheidend, die größten Bedrohungsakteure zu kennen und zu überwachen. Dies ermöglicht es auch zu verstehen, wie sich die Cyberlandschaft weiter entwickelt. Belgien sieht in den folgenden Bedrohungsakteure die größte Bedrohung für den belgischen Staat und die Bevölkerung: Cyberkriminelle, ausländische Militär- und Geheimdienste, terroristische Gruppen und Hacktivisten



2.1.1 Cyberkriminalität

Die (potenzielle) Auswirkung von Cyberbedrohungen, ausgehend von Cyberkriminellen, ist in den letzten Jahren immer deutlicher geworden. Dazu gehören nicht nur Bedrohungen, die unsere Infrastruktur stören könnten, sondern auch Bedrohungen der Integrität, Verfügbarkeit und Vertraulichkeit der Informationen, die wir digital erfassen, analysieren und austauschen. Die Digitalisierung von Dingen oder Waren (Internet der Dinge) impliziert, dass diese „hackbar"sind. Dies hat unmittelbare Auswirkungen auf die allgemeine Sicherheit jedes Bürgers, bedeutet aber auch, dass sie digitale Spuren enthalten können, die bei der Aufklärung von Verbrechen von Interesse sein könnten.

Das Hauptziel krimineller Akteure, sowohl von Einzelpersonen als auch im Rahmen der organisierten Kriminalität, ist in der Regel die Generierung von Geld und Gewinn, beispielsweise durch Phishing, Datendiebstahl oder Ransomware. In manchen Fällen verfolgen sie zusätzlich destruktive Zwecke, zum Beispiel Datensabotage oder Cyberangriffe. Cyberkriminelle spezialisieren sich auf spezifische Dienste, die sie dann im Dark Web gegen Bezahlung anbieten. So kann ein Krimineller zum Beispiel ein Exploit Kit abonnieren, mit dem er sich ohne technische Kenntnisse die neuesten digitalen Einbruchstechniken zunutze machen kann. Cyberkriminelle bieten ihre Dienste jedem an, der bereit ist, dafür zu bezahlen. Daher sollten neben dem Cyberterrorismus auch kriminelle Organisationen (oder Einzelpersonen), die versuchen, materiellen und/oder physischen Schaden zu verursachen, als potenzielle Angreifer auf nationaler Ebene in Betracht

gezogen werden. Die potenziellen Auswirkungen von Cyberangriffen auf kritische Infrastrukturen können derart sein, dass sie die Stabilität staatlicher Institutionen unter Druck setzen.

2.1.2 Ausländische Militär- und Geheimdienste

Nationen und Staaten verfügen über viel Wissen und physische Rüstung, aber auch über ein offensives Cyber-Arsenal. Es ist jedoch möglich, dass sie diese für andere Zwecke als den Schutz ihrer eigenen Bürger einsetzen wollen. So können Militär- und Geheimdienste dieses Wissen und diese Aufrüstung ausnutzen, um anderen Staaten wirtschaftlichen Schaden zuzufügen, dort politische Instabilität zu erzeugen und/oder die dortige Verteidigung zu schwächen. Ausländische Militär- und Geheimdienste führen nicht nur vermehrt Cyberangriffe durch, um sich einen Wettbewerbsvorteil im Bereich der Geheimdienste zu verschaffen: immer häufiger werden fortschrittliche Techniken eingesetzt, um den Betrieb von Organisationen - und damit indirekt auch die Länder, in denen sie ansässig sind – zu stören, indem beispielsweise vertrauliche Informationen preisgegeben werden.

Die Kapazitäten der verschiedenen nationalen Militär- und Geheimdienste werden immer ausgefeilter. Daher wird es immer schwieriger, solche Cyberangriffe zu erkennen und sich präventiv dagegen zu wehren. Folglich ist die tatsächliche Aktivität dieser Bedrohungsakteure viel häufiger, als es die Statistiken vermuten lassen.

2.1.3 Hacktivismus

Hacktivismus ist die Durchführung verschiedener absichtlicher Cyberaktivitäten mit dem Ziel, eine politische Agenda, religiöse Überzeugung oder soziale Ideologie zu fördern. Es kann sich um eine politisch motivierte Bewegung handeln, die diese Tätigkeit ausübt. Die derzeit am häufigsten verwendeten Angriffsmethoden in diesem Zusammenhang sind Doxing2, DDoS3, Web-Defacement4 und die unrechtmäßige Übernahme von Identitäten und Social-Media-Kanälen.

2 Doxing ist die meist unrechtmäßige öffentliche Verbreitung von Informationen oder Dokumenten einer Person.

3 DDoS steht für Distributed-Denial-of-Service-Angriffe, bei denen eine große Datenmenge an ein bestimmtes System gesendet wird, um dessen normalen Betrieb zu stören.

4 Ein Web Defacement ist die unrechtmäßige Veränderung des Inhalts einer Website oder Seite.

2.1.4 Terrorismus

Cyberterrorismus ist die Durchführung von gewalttätigen Aktivitäten unter Verwendung des Internets, mit dem zugrunde liegenden Ziel, durch Einschüchterung und Anschüren von Angst einen politischen Vorteil zu erlangen. Diese Handlungen können zu Zerstörung, Verlust von Menschenleben und/oder körperlichen Schäden führen. Die offensichtlichsten Ziele von Cyberterroristen sind öffentliche Dienste, Industrien, kritische Infrastrukturen, usw.

Beispielsweise benutzen einige terroristische Gruppen die Online-Welt als Propaganda- und Rekrutierungskanal für Terrorismus. Seit 2016 ist allerdings ein deutlicher Übergang bei der Nutzung von Twitter und Facebook zu mehr verschlüsselten Kommunikationskanälen zu beobachten. Aktuelle Entwicklungen deuten auch auf eine zunehmende Nutzung von Cyber-Tools zur Finanzierung von Terrorismus hin, z. B. durch Ransomware, Kryptomining oder sogar Crowdfunding. In diesem Zusammenhang besteht große Besorgnis, dass auch terroristische Organisationen vermehrt Cyberangriffe durchführen würden. Es scheint jedoch, dass diese Angriffstechniken ziemlich begrenzt bleiben. Um DDOS-Angriffe auszuführen, kaufen Gruppen immer noch Domain-Hosting-Dienste, laden Software herunter und mieten Botnetze, anstatt eigene Cyberwaffen zu entwickeln.

2.2 Technologische Trends und Risiken

Die Technologielandschaft steht nicht still, und ständig kommen neue Produkte auf den Markt. Organisationen setzen diese neuen Technologien ein, um wettbewerbsfähig zu bleiben und neue Möglichkeiten zu erschließen. Allerdings sind mit diesen technologischen Entwicklungen auch Risiken verbunden, auch weil sie dazu beitragen, die Fähigkeiten von Angreifern weiterzuentwickeln. Es ist daher entscheidend, sich stets über die Entwicklungen der Technologien bewusst zu sein und die damit verbundenen Risiken zu erkennen.

Technologische Trends und Risiken

2.2.1 Abhängigkeit

Organisationen setzen neue Technologien ein, um neue Möglichkeiten zu erschließen und ihre Produktivität oder Effizienz zu steigern. Die zunehmende Nutzung dieser Technologien führt daher zu einer immer stärkeren Abhängigkeit von IKT. Dies geht mit einer erhöhten Gefährdung durch Cyberbedrohungen einher. Generell ist auch zu beobachten, dass die Inbetriebnahme von Technologien schneller steigt als deren Sicherheit.

Organisationen werden sich mehr für die Bereitstellung und Nutzung neuer Technologien engagieren als für die Bereitstellung von Budgets für ihre Sicherheit. Es wird oft übersehen, dass neue Technologien nicht immer sofort ausgiebig getestet werden. Es ist daher ein großes Risiko, davon auszugehen, dass es noch keine Angriffe gibt oder, dass es sicher erscheint, die Technologie auf den üblichen Wegen zu implementieren und abzusichern. Schließlich dauert es oft ein paar Monate oder Jahre, bis die meisten Angriffe und Vektoren auf eine bestimmte Technologie bekannt werden und angemessen dagegen geschützt werden kann. Secure Development - unter Berücksichtigung der Sicherheit – sollte daher in den Entwicklungsprozess neuer Software und Technologien einbezogen werden.

Auch die Abhängigkeit von so genannten Drittanbietern nimmt bei jedem Schritt des Entwicklungs-, Herstellungs-, Wartungs- und Verarbeitungsprozesses immer mehr zu. Dies erhöht das Risiko und die potenziell kritischen Auswirkungen von ‚Supply-Chain-Angriffen'.

Die Vernetzung von Produkten kann ebenfalls zu einer „hazardization"führen. Dies ist die Situation, die entsteht, wenn ein Produkt sicher ist, wenn es von einem Verbraucher erworben wird, aber wenn es an ein Netzwerk angeschlossen wird, aufgrund von böswilligen, falschen oder unsorgfältigen Änderungen am operationellen Code gefährlich wird.

2.2.2 Technologiespezifische Risiken

Neue Anwendungen, die sich aus aufkommenden Technologien ergeben, bieten oft große Vorteile gegenüber traditionellen Methoden; zum Beispiel in Bezug auf Effizienz und Skaleneffekte. Allerdings sind damit manchmal spezifische Sicherheitsrisiken verbunden.

Ein gutes Beispiel ist Cloud Computing. Der große Vorteil ist, dass die Infrastruktur nicht mehr gewartet werden muss und alles mit dem Wachstum der Organisation skaliert. Eine zentrale Cloud-Infrastruktur kann daher professionell gut gesichert werden. Das Risiko besteht jedoch darin, dass ein unberechtigter Zugriff plötzlich die Kompromittierung einer sehr großen Menge an Informationen bedeutet.

In diesem Zusammenhang können auch zwei wirtschaftliche Bedrohungen formuliert werden. Erstens ist die Welt der Cloud-basierten Anwendungen durch das Vorhandensein einer begrenzten Anzahl von globalen Akteuren gekennzeichnet, bei denen Skaleneffekte ausgespielt werden können, wodurch ein Konzentrationsrisiko entsteht. Auf der anderen Seite werden Innovationen in diesem Markt oft von neuen, viel kleineren Akteuren angeboten. Diese jungen Organisationen sind oft nicht auf dem gleichen Stand, was die Leistungsfähigkeit und den Reifegrad der Prozesse angeht. Dies kann zu falschem Vertrauen in diese Anwendungen führen.

Die zunehmende technologische Entwicklung bei neuen (Arten von) IKT-basierten Produkten und Dienstleistungen in vielen wirtschaftlichen Teilbereichen erfordert auch von den Aufsichtsbehörden eine rasche Weiterentwicklung der Marktaufsicht- und Kontrollkapazitäten. Andererseits bieten diese Technologien aber zum Teil auch Vorteile, um die Marktüberwachung effizienter zu gestalten.

Behörden schenken den personenzentrierten Aspekten rund um ‚Sicherheit' und ‚Datenschutz' bereits große Aufmerksamkeit. Die produktbezogenen Aspekte dieser Themen, wie Regulierung und Kontrolle, werden von den Aufsichtsbehörden jedoch noch kaum abgedeckt. Es besteht daher die Notwendigkeit, den bestehenden Rechtsrahmen anzupassen. Dies sollte

hauptsächlich in einem europäischen/internationalen Rahmen geschehen. Der europäische Rechtsakt zur Cyber-Sicherheit („Cybersecurity Act") ist ein wichtiger Schritt in diese Richtung und erfordert eine klare belgische Implementierung.

Ein weiteres häufiges Risiko ist der individuelle Schutz von Geräten, die mit dem Internet verbunden sind. Die größte aktuelle Herausforderung in diesem Bereich ist das Internet der Dinge (IdD).

Es ist sehr wichtig, die Risiken einzuschätzen und die notwendige Sicherheit zu schaffen, bevor neue Technologien eingesetzt werden. Die Geschwindigkeit bei der Entwicklung und Einführung neuer Technologien wie künstliche Intelligenz, Quanten-Computing, Blockchain, und Smart Meters&Grids macht eine angemessene Bewertung aller Risiken (und den Schutz davor) zu einer großen Herausforderung.

2.2.3 War On Talentt

Mit dem digitalen Wandel und der Anwendung neuer Technologien steigt auch der Missbrauch dieser Systeme. Daher ist es wichtig, dass man als Unternehmen in die Rekrutierung von IT-Profilen, aber auch von IT-Sicherheitsprofilen investier. Auf dem Arbeitsmarkt herrscht jedoch ein Mangel an Talenten im Bereich der Cybersicherheit. Es gibt wenige Ausbildungen, in denen Cybersicherheit ein (Haupt-)Bestandteil ist. Oft wird es als Ergänzungsfach gelehrt, wodurch wenig Wissen erworben oder in die Praxis übertragen wird.

Infolgedessen gibt es einen deutlichen Mangel an Fachkräften für Cybersicherheit. Viele Unternehmen werden daher diese Positionen nicht besetzen können oder sie mit anderen Profilen besetzen. Die Herausforderung, kompetente und verlässliche Mitarbeiter zu finden, geht offensichtlich Hand in Hand mit einer Insider-Bedrohung..

3. Strategische Ziele und Ansatz

Der Zweck der Erstellung einer Cyberstrategie ist es, auf die technologischen Entwicklungen zu reagieren und die dringende Notwendigkeit des Schutzes der Öffentlichkeit, des privaten und öffentlichen Sektors sowie der lebenswichtigen Sektoren zu erfüllen. Die Cyberstrategie 2.0 enthält sechs strategische Ziele für die nächsten vier Jahre. Diese Strategie schreibt eine Reihe von Maßnahmen vor, um diese strategischen Ziele zu erreichen. Erreicht werden soll dies mit der Hilfe verschiedener Parteien.

3.1 Stärkung der digitalen Umgebung und Erhöhung des Vertrauens in die digitale Umgebung

3.1.1 Investition in eine sichere Netzwerkinfrastruktur

Gemeinsam mit den Internetdienstanbietern (ISP) wird an der Schaffung einer sichereren Basis-Netzwerkinfrastruktur gearbeitet. Neue Schutztechniken werden den technologischen Entwicklungen folgen, wie dem Internet der Dinge (IoT) und neuen Generationen von Fest- und Mobilnetzen.

Die Sicherheit der Netzwerkinfrastruktur kann durch die Übernahme von sichereren Internetstandards (DNS-Sicherheit, sicheres Routing, Verschlüsselung, usw.) verbessert werden. Diese Standards bieten einen sicheren Weg, um Daten auszutauschen (sichere Daten-Transportschicht). Der Online-Datenaustausch ist dann flächendeckend sicher. Dadurch wird das Risiko eines Angriffs auf eine Schwachstelle in der Kette reduziert.

Solche Standards können auch für vertrauenswürdigere Identitäten und Veröffentlichungen im Internet sorgen. Dies kann zum Beispiel durch die Förderung des Einsatzes von Technologien wie Itsme und von Extended Validation Certificates auf Websites geschehen.

Es kann auch eine Testumgebung (‚*testbed*') für Infrastruktur aufgebaut werden. Ein *testbed* ist eine Plattform, die es ermöglicht, neue Infrastruktur in einer zuverlässigen, kontrollierten und sicheren Umgebung zu testen, bevor sie auf breiter Basis eingesetzt wird.

3.1.2 Einrichten eines Cyber Green House

Die Einrichtung eines Cyber Green House wird der Innovation im Bereich der Cybersicherheit einen deutlichen Schub geben. Die Einrichtung eines Innovationszentrums zielt darauf ab, innovative Cyberlösungen und

Geschäftsmodelle in einer risikofreien Umgebung zu testen und *Cybersecurity Guidelines* und *Best Practices* zu verbreiten.

3.1.3 Expertise und Wissen fördern

Um dem Bedarf an mehr Sicherheit und dem Bedarf an mehr Sicherheitsexperten gerecht zu werden, ist es unumgänglich, mehr in Expertise und Wissen zu investieren. Bildungseinrichtungen leisten einen wichtigen Beitrag zur Cybersicherheitslandschaft. Einerseits spielen sie eine wichtige Rolle bei der Vermehrung des Wissens, indem sie Forschungen durchführen. Andererseits tragen sie zur Entwicklung und Bereitstellung von relevanten Ausbildungen bei.

Es wird weitere Investitionen in Forschung & Entwicklung (F&E) im Bereich der Cybersicherheit geben. Der private Sektor und Bildungseinrichtungen wie Universitäten und Hochschulen werden eng zusammenarbeiten.

Europäischen Initiativen in diesem Rahmen werden mit Blick auf dieses Ziel bewertet.

Sicherheitsbeauftragte öffentlicher Einrichtungen sollten durch Schulungsprogramme für öffentliche Bedienstete auf ein angemessenes Sicherheitsniveau ausgebildet werden.

Um dem Mangel an Fachkräften für Informationssicherheit sowohl im öffentlichen als auch im privaten Sektor zu begegnen, sollten mehr junge Menschen ermutigt werden, MINT-Fächer (Mathematik, Informatik, Naturwissenschaften und Technik) zu belegen. Zu diesem Zweck müssen Kontakte zu den Gemeinschaften hergestellt und eine kohärente Politik zu diesem Thema in Zusammenarbeit mit relevanten Partnern festgelegt werden. So können beispielsweise Sensibilisierungs- und Informationsmaterialien für Schulen bereitgestellt oder Mentorenprogramme organisiert werden.

3.1.4 Cybersicherheitszertifizierung und Bezeichnung von Produkten, Dienstleistungen und Prozessen

Belgien wird einen Rahmen schaffen, der es Unternehmen ermöglicht, die Sicherheit von IKT-Produkten, -Dienstleistungen und -Prozessen zu bewerten und zu zertifizieren.

Dieser Rahmen wird mit dem europäischem Rechtsakt zur Cyber-Sicherheit 2019 und den laufenden Entwicklungen auf europäischer Ebene in Einklang gebracht. Der europäische Rechtsakt zur Cyber-Sicherheit zielt

auf eine europäische Anerkennung der gelieferten Zertifikate, sowie auf eine maximale Angleichung an bestehende europäische und internationale Referenzrahmen ab.

Zu diesem Zweck wird Belgien, wie vom europäische Rechtsakt zur Cyber-Sicherheit gefordert, eine *Nationale Cybersicherheits-Zertifizierungsbehörde* (NCCA) gründen. Diese NCCA wird in Absprache mit u.a. den Marktaufsichtsbehörden, anderen sektoralen Behörden und dem NCCN, die notwendige Expertise im Bereich der Cybersicherheitszertifizierung koordinieren, Zertifikate mit hohen Sicherheitsanforderungen autorisieren und eine enge Zusammenarbeit mit BELAC (der belgischen Akkreditierungsorganisation) aufbauen, indem sie die bestehenden Prozesse, Verfahren und Vorschriften optimal nutzt.

Ein Anerkennungsmechanismus für Cybersicherheit für Unternehmen, mit besonderem Fokus auf KMU, die ein Minimum an grundlegenden Cybersicherheitsanforderungen, Best Practices und Richtlinien nachweisen wollen, wird ebenfalls entwickelt. Es ist wichtig, einen integrierten Ansatz für strategische Sektoren in Betracht zu ziehen, der IT-Aspekte, physischen Schutz und die Überprüfung des Personals kombiniert.

Diese Initiativen unterstützen nachdrücklich die Vision dieser Cybersicherheitsstrategie und werden das Vertrauen der Kunden in die Sicherheit der digitalen Umgebung stärken.

3.1.5 Stärkung der Cyberfähigkeiten von Geheimdiensten und Sicherheitsbehörden

Um auf die schnell wachsende Bedrohung angemessen reagieren zu können, müssen die Kapazitäten und Kompetenzen unserer Geheimdienste und Sicherheitsbehörden mindestens Schritt halten. Das Humankapital der technischen Experten im Bereich der Cybersicherheit stellt die beste Waffe gegen diese neuen Bedrohungen auf nationaler Ebene dar.

Um unsere Dienste mit den notwendigen Fachkräften zu versorgen, werden alternative Rekrutierungs- und Beschäftigungsmethoden bewertet und nach Möglichkeit eingesetzt. Denn der Bedarf an jungen und gut ausgebildeten Computerexperten ist nicht nur bei unseren Sicherheitsbehörden vorhanden. Der „War on Talent" wird zwischen spezialisierten Unternehmen, großen multinationalen Konzernen und allen Sicherheitsbehörden in Europa und darüber hinaus ausgetragen. Um ihr Wissen zu erweitern, suchen technische Experten oft nach neuen Herausforderungen

und sind in der Regel nicht auf der Suche nach einem Job fürs Leben. Ein hinreichend flexibles Rekrutierungssystem und eine wettbewerbsfähigere Vergütung sollten unsere Sicherheitsbehörden in die Lage versetzen, sich auf dem Arbeitsmarkt besser behaupten zu können.

Darüber hinaus müssen die Behörden ihren technischen Experten im Bereich Cybersicherheit eine ausreichend hochwertige technische Ausbildung anbieten. Dies ist nicht nur ein wichtiger Motivationsfaktor, sondern garantiert auch ausreichend technisches Wissen und Know-how.

3.2 Schutz von Benutzern und Verwaltern von Computern und Netzwerken

Das Internet besteht aus Infrastruktur und Systemen, die sich fast vollständig in Privatbesitz befinden. Es ist daher von großer Bedeutung, dass jeder Besitzer eines Computersystems oder Netzwerks ausreichend gewappnet ist, um es vor Cyberbedrohungen und Angriffen zu schützen.

3.2.1 Bewusstsein schärfen und engagieren

Neben dem Informieren der Bürger über potenzielle Bedrohungen ist der Staat bestrebt, die Bürger dafür zu sensibilisieren, wie sie sich besser vor potenziellen Cyberrisiken schützen können.

Zum Schutz von Systemen und Computernetzwerken sind einerseits technische Schutzmaßnahmen notwendig, andererseits muss jeder Benutzer diese verantwortungsvoll einsetzen. Wer ausreichend bewusst und wachsam ist, wird schnell zum besten Erkennungssystem für Cyberangriffe. Die Website www.safeonweb.be bietet der Öffentlichkeit alle Informationen über spezifische Bedrohungen, wie man sie erkennt und wie man sich schützen oder reagieren kann.

Das Internet gehört allen und ist für alle da. Auch seine Sicherheit ist eine Gemeinschaftsleistung. Daher wird die Bevölkerung aufgefordert, sich an der Sicherheit zu beteiligen. Zum Beispiel kann jeder verdächtige E-Mails an suspicious@safeonweb.be weiterleiten. Derartige Initiativen werden ausgeweitet.

Das ZCB organisiert eine jährliche Sensibilisierungskampagne über die Medien und bettet sie in europäische Initiativen ein. Auch die europäische

Agentur ENISA organisiert jedes Jahr im Oktober den europäischen Monat der Cybersicherheit.

Durch gute Kooperationen soll der Kontakt zwischen Bürgern und Diensteanbietern im Bereich der Cybersicherheit in unserem Land erleichtert werden. Ein solcher optimierter Kontakt sollte es den Bürgern ermöglichen, Sicherheitsvorfälle anzugehen und Probleme zu neutralisieren.

Die Sensibilisierung wirkt sich auch direkt auf die Geschäftswelt aus und schafft eine allgemeine Kultur der Besorgnis und Sicherheit. Sensibilisierungskampagnen, zum Beispiel durch Webinare, Leitfäden oder das Cybersecurity KIT, sollten weiter eingesetzt werden.

3.2.2 Informieren über Bedrohungen und Sicherheitslücken

Die rechtzeitige Warnung vor aufkommenden und bedeutenden Bedrohungen oder Sicherheitslücken ist entscheidend.

Das ZCB analysiert permanent alle verfügbaren Informationen über Cyberbedrohungen oder Sicherheitslücken und versendet gegebenenfalls entsprechende Warnungen. Für die Bevölkerung verfügt das ZCB über die notwendigen digitalen Medien und pflegt eine unmittelbare und transparente Beziehung zu den allgemeinen Medien. BE-Alert vom Nationalen Krisenzentrum (NCCN) kann die Verbreitung von Warnungen unterstützen und innerhalb einer bestimmten Region versenden.

Unternehmen und Organisationen wird empfohlen, eine „Coordinated Vulnerability Disclosure Policy"zu veröffentlichen. Über sektorale Behörden, Berufsverbände und die Cyber Security Koalition Belgien werden sie über bedeutende Bedrohungen oder Sicherheitslücken informiert. Organisationen von wesentlicher Bedeutung erhalten außerdem gezielte und nicht-öffentliche Warnungen über das Frühwarnsystem (*Early Warning System (EWS)*) des ZCB.

Das ZCB hat mit dem nationalen *Computer Emergency Response Team* (CERT.be) und als nationales CSIRT (*Computer Security Incident Response Team*) die Aufgabe, Online-Sicherheitsprobleme und Sicherheitslücken aufzuspüren, zu analysieren und Benutzer diesbezüglich zu informieren. Dies kann jedoch nicht ohne die Unterstützung der Internetdienstanbieter geschehen, die die Warnungen schnell an ihre gefährdeten oder bedrohten Kunden weiterleiten müssen.

3.2.3 Verbreitung der Cybersicherheitsrichtlinien und „best practices"

Die Cyberbedrohungen und die verwendeten Angriffstechniken entwickeln sich sehr schnell weiter. Wissensaustausch und die Weitergabe von *„best practices"sind* daher sehr wertvoll. Dies bereichert nicht nur das Wissen und generiert neue Ideen zur Bewältigung der Bedrohungen, sondern erleichtert auch die Entscheidungsfindung. Wissen über Cybersicherheit wird über bestehende oder zukünftige Plattformen geteilt.

Das ZCB verwaltet einen Online-Referenzleitfaden über Cybersicherheit, um Organisationen bei der Entwicklung einer Cybersicherheitsstrategie zu unterstützen. Der Leitfaden bietet „grundlegende"und „fortgeschrittene Empfehlungen" in Bezug auf Planung, Risikomanagement, Sicherheitsmaßnahmen und Bewertungen beim Einsatz von Computern und Computernetzwerken. Die Identifizierung und das Management von Risiken ist in diesem Zusammenhang entscheidend. Die angebotenen Richtlinien basieren auf internationalen Standards und werden vom ZCB kontinuierlich aktualisiert. Unternehmen wird daher dringend empfohlen, diese Richtlinien in ihrer Cybersicherheitspolitik zu verwenden.

3.3 Schutz von Organisationen von wesentlicher Bedeutung vor allen Cyberbedrohungen

Organisationen von wesentlicher Bedeutung sind weltweit mit einer schnell wachsenden und immer komplexeren Cyberbedrohung konfrontiert. Angesichts der Tatsache, dass Cyberangriffe auf diese Organisationen erhebliche Auswirkungen auf unsere Gesellschaft und die nationale Sicherheit haben können, ist es entscheidend, sie bei ihrem Schutz angemessen zu unterstützen.

3.3.1 Optimierung des Informationsaustauschs und Versenden von Warnungen

Das ZCB erhält als nationale Cybersicherheitsbehörde alle relevanten Bedrohungsinformationen von seinen Partnern. Es analysiert diese empfangenen Informationen kontinuierlich und sendet Warnungen über sein „Early Warning System"(EWS) oder andere Kanäle aus.

Organisationen von wesentlicher Bedeutung werden somit kontinuierlich (über das Frühwarnsystem (EWS) des ZCB) über relevante Cybersicherheitsbedrohungen, Sicherheitslücken oder Vorfälle informiert.

In Belgien haben die sektoralen Behörden eine entscheidende Verantwortung bei der Identifizierung, Regulierung und Überwachung der Organisationen von wesentlicher Bedeutung. Eine Konsultationsplattform zwischen diesen sektoralen Behörden (Cyber Security Sectoral Authorities Platform - CySSAP) soll dazu beitragen, den Informationsaustausch mit den Organisationen von wesentlicher Bedeutung auch im Hinblick auf grenzüberschreitende Abhängigkeiten zu optimieren.

3.3.2 Verbesserter Schutz für internationale Institutionen

Belgien ist die Heimat vieler internationaler Institutionen, darunter die NATO (Nordatlantikvertrag) und Institutionen der Europäischen Union. Die belgischen Organisationen von wesentlicher Bedeutung, die diese Institutionen unterstützen, werden identifiziert, damit ein angemessener Schutz gewährleistet werden kann.

Darüber hinaus ist ein guter Dialog und Zusammenarbeit mit den internationalen Institutionen in unserem Land wichtig und notwendig, um die Effektivität des Schutzes und der Reaktion auf Cyberangriffe zu erhöhen.

3.3.3 Die Fähigkeit, Vorfälle mit nationalen Auswirkungen zu behandeln

Der nationale Cybernotfallplan wird weiter operationalisiert. Durch eine optimale Zusammenarbeit zwischen dem nationalen *Computer Emergency Response Team* (CERT.be) des CCB, den integrierten Polizeidiensten und dem Nationalen Krisenzentrum (NCCN) werden Vorfälle schnell und effektiv bearbeitet und werden juristische Ermittlungen sofort integriert.

Vorfälle mit nationalen Auswirkungen werden auf die entsprechende Ebene eskaliert und von *ad hoc* zusammengesetzte *Rapid Reaction Teams* bearbeitet, in die auch andere Dienste und Partner effizient einbezogen werden.

3.3.4 Übungen

Der belgische Cybernotfallplan wurde 2017 vom Ministerrat genehmigt und beschreibt die Verfahren, die von den verschiedenen Diensten im Falle eines Cybereignisses zu befolgen sind. Dieser Plan sollte jedes Jahr bewertet und bei Bedarf angepasst werden. Das ZCB spielt dabei eine koordinierende Rolle. Die Durchführung regelmäßiger Übungen ist wichtig, um die Widerstandsfähigkeit gegenüber Vorfällen zu erhöhen und die Wirksamkeit des Notfallplans zu testen. Die aus diesen Übungen gewonnenen Erkenntnisse können dann in die jährlichen Bewertungen dieses Plans einfließen.

Daher ist die Teilnahme der belgischen Sicherheitsbehörden, anderer Behörden und Organisationen von wesentlicher Bedeutung an internationalen und nationalen Übungen sehr wünschenswert. Die Koordinierung der belgischen Teilnahmen an solchen Übungen wird durch Konsultation zwischen dem ZCB, dem FÖD Auswärtige Angelegenheiten, dem NCCN und dem Verteidigungsministerium sichergestellt.

3.4 Reaktion auf die Cyberbedrohung

Um der zunehmenden Cyberkriminalität und den staatlichen Bedrohungen schnell begegnen zu können, muss in die schnelle Erkennung von und Reaktion auf Bedrohungen für unsere Bevölkerung, unsere Wirtschaft oder für Organisationen von wesentlicher Bedeutung investiert werden.

3.4.1 Einschätzung der internationalen Bedrohung

Die kontinuierliche Überwachung und Einschätzung der internationalen Cyberbedrohung ist entscheidend für die Reduzierung des Risikos von Cyberangriffen und -Vorfällen. Es ist der erste Schritt jeder Verteidigung.

Die Cyberabsichten und die Möglichkeiten von „Akteuren" gegen unsere wesentlichen und vitalen Interessen müssen erfasst und die potenziellen Quellen verfolgt werden. Um unsere Computernetzwerke schützen zu können, muss die Entwicklung ihrer technischen Taktiken, Techniken und Verfahren so gut wie möglich bekannt sein, und unsere Schutzmittel müssen im Verhältnis zu ihnen bewertet werden.

3.4.2 Störung der kriminellen Cyberinfrastruktur

Cyberkriminelle spezialisieren sich und verwenden die im *Dark Web* kursierenden Angriffstechniken und -Software wieder. Um ihre Hightech- oder groß angelegten Cyberangriffe durchführen zu können und auch um anonym zu bleiben, benutzen sie sowohl eigene als auch kompromittierte Computersysteme im Internet.

Die Störung dieser kriminellen Cyberinfrastruktur untergräbt teilweise das Geschäftsmodell der Kriminellen. Dies kann geschehen durch:

- Aufspüren und Neutralisation der Infrastruktur auf juristischem Weg
- Erkennen der kompromittierten Systeme und Benachrichtigung des Eigentümers
- Schutz der Kommunikation der Bevölkerung und der Unternehmen vor bekannter bösartiger Infrastruktur

· Nationaler und internationaler Austausch von Informationen

Dies erfordert eine enge Zusammenarbeit zwischen allen Geheim- und Sicherheitsdiensten.

3.4.3 Entwicklung einer angemessenen Repressionskapazität

Um die Verwundbarkeit Belgiens im Cyberbereich zu reduzieren, sind präventive Maßnahmen der Schlüssel. Gut informierte und widerstandsfähige Bürger, Unternehmen und Behörden werden Cyberkriminelle in Zukunft abwehren und entmutigen. Mit jeder Investition in die Prävention sinkt der Zustrom von Strafverfahren. Infolgedessen dürfen Polizei und Justiz nicht mehr nur die Symptome bekämpfen, sondern müssen in der Lage sein, die Ursachen zu bekämpfen.

Gleichzeitig ist es klar, dass Cyberkriminalität auch weiterhin bestehen wird. Ein effektives und sachkundiges Repressionssystem ist daher nach wie vor erforderlich, um die verbleibende Kategorie der Computerkriminalität so effektiv wie möglich zu bekämpfen. Die Täter von Cyberkriminalität müssen identifiziert und festgenommen werden, Beweise für ihre Beteiligung müssen gesammelt werden, die kriminelle Infrastruktur muss aufgedeckt und aufgelöst werden, illegale Vermögenswerte müssen beschlagnahmt und eingezogen werden, und die Verdächtigen müssen strafrechtlich verfolgt und angemessen bestraft werden. Da Cyberkriminelle vornehmlich im internationalen Kontext agieren, erfordert dies auch die Abstimmung mit anderen, beteiligten Ländern.

Dieser strategische Plan hat die Ambition, die Entwicklung einer angemessenen repressiven Kapazität zu unterstützen. Eine solche repressive Kapazität muss in der Lage sein, Cyberkriminalität angemessen und kompetent aufzudecken, zu untersuchen, zu verfolgen und zu bestrafen.

Ziel ist es zunächst, auf allen Ebenen der integrierten Polizei (sowohl bei der lokalen Polizei als auch bei den dekonzentrierten Diensten und den zentralen Diensten der föderalen Polizei) die entsprechenden Kapazitäten und Expertise aufzubauen, damit die von jeder Ebene erwarteten Bildgebungs- und Ermittlungskapazitäten in einer digitalen Umgebung effektiv und schnell durchgeführt werden können.

Damit soll weiter sichergestellt werden, dass die Staatsanwaltschaften und Gerichte aller Gerichtsbezirke und Amtsbereiche über ausreichend Staatsanwälte, Ermittlungsrichter und Amtsrichter mit Interesse an Cybersicherheit

und Cyberkriminalität verfügen, die ein entsprechendes Schulungsprogramm absolvieren. Diese Magistrate werden von spezialisierten internen Netzwerken unterstützt, in denen sie Erfahrungen, Probleme und *best practices* austauschen und diskutieren können. Dabei muss sich die Ermittlungs- und Strafverfolgungstätigkeit der Justiz an einer durchdachten Strafrechtspolitik im Cyberbereich orientieren.

3.4.4 Entwicklung einer angemessenen Verteidigungskapazität

Das Internet wird zunehmend zur Zielscheibe und zum Mittel in internationalen Konflikten.

Alle Staats- und Regierungschefs der NATO haben erklärt, dass der Cyberraum als eine neue operative Domäne (zusätzlich zu den klassischen Land-, Luft- und Seedomänen) betrachtet werden sollte, in der militärische und geheimdienstliche Operationen durchgeführt werden können.

Gegner benutzen jede Gelegenheit im und mittels des Cyberraumes, um ihre Informationsposition zu stärken, unsere zivilen und militärischen Systeme zu stören und das Vertrauen in die Informationen zu untergraben, die unsere Operationen unterstützen. Der weitere Ausbau der Cyberkapazität innerhalb des militärische Abschirmdienstes (ADIV) und der Verteidigung ist daher eine der Prioritäten im Orientierungsdokument des Verteidigungsministers und im Strategieplan des Verteidigungsministeriums. Mit der Zeit muss es auch zur Einrichtung einer fünften Komponente führen, die sich speziell auf die Cyberbedrohung konzentriert. Das Ziel ist ein zwei Komponenten: ein besseres Verständnis der Cyberbedrohung und ein besserer Schutz dagegen, aber auch ein besseres Verständnis der Möglichkeiten. In der Cyberstrategie des Verteidigungsministeriums werden diese Ziele konkretisiert. Darüber hinaus wird diese Kapazität eine wichtigen Doppelrolle zur Unterstützung der Gesellschaft im Falle von (hybriden) Krisen haben.

3.4.5 Attribution

Die Identifizierung und Zuordnung eines Cyberangriffs zu einer bestimmten Person, Gruppe oder einem Staat spielt in der Weltpolitik eine immer wichtigere Rolle. Die Diskussion um die Notwendigkeit und mögliche internationale Koordination der Attribution eines Cyberangriffs steht ganz oben auf der internationalen Agenda unter anderem von der NATO, der EU und der VN. Attribution bleibt jedoch eine politische und souveräne Entscheidung mit großem Einfluss auf die Außenpolitik. Eine mögliche Attribution wird daher in einem koordinierten nationalen Verfahren gründlich analysiert und beschlossen. Hierfür ist Kapazitätsaufbau entscheidend.

3.5 Verbesserung der öffentlichen, privaten und akademischen Zusammenarbeit

Bei der Vorbeugung, Reduzierung, Behandlung und Überwachung von Cyberbedrohungen und -Vorfällen ist die Zusammenarbeit zwischen den betroffenen Parteien, sowohl auf nationaler als auch auf internationaler Ebene, ein wesentlicher Erfolgsfaktor.

3.5.1 Förderung der Koordination und Zusammenarbeit

Jede betroffene Partei, die eine Rolle in Belgiens Cybersicherheit spielt, hat seine spezifischen Verantwortlichkeiten. Es ist jedoch entscheidend, alle Initiativen zentral zu koordinieren. Das ZCB ist als nationale Behörde für die Koordination zwischen den betroffenen Parteien verantwortlich, einschließlich der öffentlichen Dienste, aber auch des privaten und wissenschaftlichen Sektors.

Das Wissen über Cybersicherheit und die Entwicklung der Cyberbedrohung wird über bestehende oder neue Plattformen zwischen den relevanten Sicherheitsbehörden, öffentlichen Behörden, dem privaten und wissenschaftlichen Sektor ausgetauscht. Regelmäßige Treffen ermöglichen es den Experten, im direkten Kontakt, Informationen und Erfahrungen auszutauschen und sich untereinander zu vernetzen. Der offene und strukturelle Dialog ermöglicht es dem ZCB, die dringendsten Bedürfnisse besser zu verstehen.

3.5.2 Unterstützung der Cyber Security Koalition

Die Cyber Security Koalition ist eine einzigartige Partnerschaft, in der sich Akteure aus dem akademischen Bereich, öffentlichen Institutionen und dem privaten Sektor im Kampf gegen Cyberkriminalität zusammenschließen. 2021 sind bereits 100 Organisationen aus drei Sektoren aktive Mitglieder, und tragen zur Mission und den Zielen der Koalition bei.

Die Koalition bietet eine Antwort auf den dringenden Bedarf an sektorübergreifender Zusammenarbeit:

- um Wissen und Erfahrung zu teilen
- um konkrete sektorübergreifende Initiativen zu initiieren, zu organisieren und zu koordinieren
- um das Bewusstsein von Bürgern und Organisationen zu stärken
- um die Entwicklung von Fachwissen zu fördern
- und, um Empfehlungen für effektivere Richtlinien und Vorschriften zu formulieren

Der Staat, und insbesondere das ZCB, werden die Cyber Security Koalition aktiv unterstützen und sich an Aktivitäten beteiligen.

3.6 Ein klares internationales Engagement

Die Cyberbedrohung ist global und kann nicht nur auf nationaler Ebene angegangen werden. Internationale Zusammenarbeit ist eine wichtige Säule einer entschlossenen nationalen Cybersicherheitspolitik. Cybersicherheit erfordert eine ganzheitliche Perspektive, die die verschiedenen Vektoren der internationalen Zusammenarbeit (diplomatisch, militärisch, wirtschaftlich, …) berücksichtigt. Daher ist es wichtig, dass die verschiedenen betroffenen Behörden, in enger Konsultation und in ihren jeweiligen Zuständigkeiten gut zusammenarbeiten.

Belgien unterstützt die legislative und diplomatische Rolle der EU, der NATO und anderer relevanter internationaler Organisationen in ihrem Beitrag zu einer offenen, freien und sicheren Cyberumgebung und wird sich aktiv daran beteiligen, wann immer dies möglich ist. Besondere Aufmerksamkeit gilt der Agentur für Cybersicherheit in Europa, ENISA. Seit ihrer Gründung im Jahr 2004 hat ENISA eine allgemeine Kultur und ein Bewusstsein für Netz- und Informationssicherheit in der Union geschaffen. Das ZCB wird Belgien weiterhin in den verschiedenen Organen und Plattformen von ENISA vertreten.

Auch die bilaterale Zusammenarbeit zwischen allen betroffenen Behörden in Belgien und ihren ausländischen Partnern optimiert die internationale Zusammenarbeit und kann das Vertrauensverhältnis stärken.

4 Zuständigkeiten

Zusammenarbeit und die Übernahme gemeinsamer Verantwortung sind kritische Erfolgsfaktoren bei der Entwicklung effektiver Cybersicherheit. Die Verteidigung der digitalen Umgebung in Belgien gegen (aufkommende) Bedrohungen liegt nicht nur in der Verantwortung des Staats. Auch die anderen betroffenen Parteien können relevante Beiträge zu den verschiedenen Zielen und den zugehörigen Aktionsplänen leisten, darunter die Bürger, Unternehmen und Organisationen von wesentlicher Bedeutung.

Wie in der realen Welt liegt es in der Verantwortung jedes IKT-Systembesitzers, sein System ordnungsgemäß zu sichern und es verantwortungsvoll zu verwalten und zu benutzen. Jeder Bürger sollte über die wichtigsten Risiken bei der Nutzung von IKT und Internet informiert und sich der Sicherheitshinweise bewusst sein und diese beachten. Konkret bedeutet dies, dass jeder Benutzer sowohl für die technische Sicherheit seiner Systeme sorgen als auch diese verantwortungsvoll nutzen muss. Unternehmen und öffentliche Institutionen müssen ihre Umgebung schützen und verstehen, dass sie Verantwortung tragen, wenn sie Opfer eines Cyberangriffs werden.

4.1 Das Zentrum für Cybersicherheit Belgien (ZCB)

Das ZCB verfolgt, koordiniert und überwacht die Umsetzung der belgischen Cybersicherheitspolitik. Von einem integrierten und zentralisierten Ansatz aus steuert sie die verschiedenen Projekte im Bereich der Cybersicherheit und sorgt für die Koordination zwischen den betroffenen Diensten und Behörden, sowie den öffentlichen Behörden und dem privaten oder wissenschaftlichen Sektor.

In Zusammenarbeit mit dem Nationalen Krisenzentrum stellt das ZCB das Krisenmanagement bei Cybervorfällen sicher. Für die Verwaltungen und öffentliche Institutionen gibt das ZCB Standards, Richtlinien und Sicherheitsnormen heraus.

Das ZCB sensibilisiert über die wichtigsten Cyberbedrohungen und wie man sich vor ihnen schützen kann. Spezifische Programme mit öffentlichen und privaten Entitäten sollen die Expertise im Bereich der Cybersicherheit erhöhen.

Das ZCB hat auch die Aufgabe, die belgische Vertretung in internationalen Cybersicherheitsforen zu koordinieren, die internationalen Verpflichtungen zu berücksichtigen und die nationale Position in diesem Bereich vorzuschlagen. Dies geschieht, im Hinblick auf ein kohärentes ausländisches Handeln, in enger Abstimmung mit dem FÖD Auswärtige Angelegenheiten und dem Verteidigungsministerium.

Das ZCB stellt den europäischen Institutionen die belgische Position vor, unter anderem bezüglich der Zertifizierung und Standardisierung von Produkten und Dienstleistungen.

4.1.1 CERT.BE

Als nationales CSIRT (*Computer Security Incident Response Team*) hat das ZCB auch eine wichtige Erkennungs- und Warnungsfunktion. Das *Computer Emergency Response Team* (CERT.be) ist, als operativer Dienst des ZCB, für das Erkennen, Beobachten und Analysieren von Online-Sicherheitsproblemen wie Cyberbedrohungen, Sicherheitslücken in IKT-Systemen oder Cybervorfällen zuständig. CERT.be wird die Bevölkerung,Unternehmen, Behörden und Organisationen von wesentlicher Bedeutung permanent darüber informieren. In diesem Sinne ist CERT.be die zentrale Drehscheibe für den Austausch von Cybersicherheitsinformationen.

4.2 Die föderale Polizei

Die integrierten Polizeidienste sind, in Zusammenarbeit mit ihren Partnern, für die Bekämpfung der Computerkriminalität zuständig.

Die örtliche Polizei ist als Primärpolizei die erste Anlaufstelle für Bürger, Unternehmen und Behörden. Von dieser Rolle aus schaltet es bei Bedarf die spezialisierten Dienste (RCCU/FCCU) ein.

Innerhalb der föderalen Kriminalpolizei sind die regionalen Computer Crime Units (RCCUs) und die föderale Computer Crime Unit (FCCU) für die juristische Bearbeitung von IKT-Kriminalität zuständig.

Die RCCUs sind zuständig für die spezialisierte Assistenz bei computerbasierten Ermittlungen – mit einer mit einer vor allem unterstützenden Rolle bei der forensischen Analyse von IKT-Material (PCs, Smartphones) - für Fälle, die alle Arten von Kriminalitätsphänomenen betreffen, sowohl für die lokale Polizei als auch für die föderale Kriminalpolizei des Bezirks, zu

dem sie gehört. Sie befasst sich zudem eigenständig mit der justiziellen Bearbeitung von Fällen der Computerkriminalität, die ihrem Bezirk betreffen. Hier ist die Sammlung digitaler Spuren wichtig, um die Täter zu ermitteln und vor Gericht zu bringen.

Als operativer Dienst ist die FCCU Teil der zentralen Abteilung zur Bekämpfung der schweren und organisierten Kriminalität. Neben einer unterstützenden forensischen Analysetätigkeit, hauptsächlich zur Unterstützung der zentralen Dienststellen, ist sie eigenständig für die gerichtliche Bearbeitung von Fällen von Computerkriminalität im Zusammenhang mit Angriffen auf die IKT-Infrastruktur kritischer Infrastrukturen oder Sektoren wesentlicher Bedeutung zuständig. Bei anderen komplexen Angriffen, die sich nicht einem Distrikt zuordnen lassen oder distriktübergreifend sind, übernimmt die FCCU eine koordinierende Rolle. Das FCCU dient auch als nationale Anlaufstelle im internationalen Vorgehen gegen Cyberkriminalität.

4.3 Die Staatsanwaltschaft

Die Ermittlungen im Allgemeinen, aber auch für Cyberkriminalität insbesondere, werden in jedem Gerichtsbezirk unter der Leitung des zuständigen Staatsanwalts geführt. Dieser erteilt den integrierten Polizeidiensten und ggf. anderen Ermittlungsdiensten die notwendigen Aufträge, um Spuren zu sammeln und die Wahrheit ans Licht zu bringen. Letztendlich ist es auch die Staatsanwaltschaft, die entscheidet ob ein Cyberverbrechen vor Gericht gebracht wird. Dabei verfügt der Staatsanwalt in der Regel über einen oder mehrere Referenzrichter für Cyberkriminalität, die vorrangig bei der Ermittlung von Cyberkriminalität eingesetzt werden.

Der Generalprokurator ist Teil der Staatsanwaltschaft und speziell mit der Durchführung von Strafverfahren für bestimmte Straftaten (einschließlich Terrorismus, Verletzungen des humanitären Rechts, usw.) beauftragt. Die Föderalstaatsanwaltschaft kann auch beauftragt werden, strafrechtliche Ermittlungen, die mehrere Rechtsgebiete betreffen oder eine internationale Dimension haben, in Absprache mit der Staatsanwaltschaft zu koordinieren. Die Föderalstaatsanwaltschaft verfügt über eine Cyber-Unit, in der Bundesrichter tätig sind, die sich speziell mit der Aufklärung von Cyberkriminalität befassen. Dazu gehören komplexe Cyberstraftaten mit einer großen internationalen Dimension, die von organisierten kriminellen Netzwerken unter Verwendung fortschrittlicher Techniken begangen werden, sowie Bedrohungen für nationale kritische IKT-Infrastrukturen.

Schließlich ist die Föderalstaatsanwaltschaft auch mit der Förderung der internationalen operativen Zusammenarbeit betraut und vertritt die Staatsanwaltschaft bei EUROJUST und dem European Judicial Cybercrime Network. Wenn eine Cyberstraftat nicht sofort in einem genau definierten Bezirk lokalisiert werden kann, kann die Föderalstaatanwaltschaft die ersten und dringendsten Ermittlungen anordnen.

Der Cyber-Notfallplan bezieht die Staatsanwaltschaft in das Management von Cyber-Vorfällen und -Krisen ein.

Die Kriminalpolitik und die gute allgemeine und koordinierte Arbeitsweise der Staatsanwaltschaft liegen in der Verantwortung des Kollegiums der Staatsanwaltschaft. Das Kollegium der Generalstaatsanwälte kann diesbezüglich Weisungen erteilen, die für alle Mitglieder der Staatsanwaltschaft verbindlich sind. Unterstützt werden sie vom nationalen Expertennetzwerk (REN), die sich aus einer Vielzahl relevanter Partner zusammensetzen. In Bezug auf Cyberkriminalität ist dies das REN CYBERCRIME, dessen Hauptkoordination von der Generalstaatsanwaltschaft in Antwerpen wahrgenommen wird. Bei strategischen Fragen ist das REN CYBERCRIME in diesem Sinne der richtige Ansprechpartner.

4.4 Das Verteidigungsministerium

Das Verteidigungsministerium entwickelt eine Cyberstrategie, einen Strategieplan und die notwendigen Fähigkeiten, um militärische und geheimdienstliche Operationen aus der Cyber-Domäne heraus unterstützen und durchführen zu können. Diese Investitionen werden es Belgien ermöglichen, langfristig über technische/technologische Kapazitäten zu verfügen, um die notwendige Infrastruktur vor Cyberangriffen zu schützen und, gegebenenfalls einen Gegenangriff durchzuführen.

Das Verteidigungsministerium wird über eine Hightech-Cyberkapazität verfügen, um seine Handlungsfreiheit im und durch den Cyberraumes bei militärischen Operationen zu wahren.

Darüber hinaus unterstützt das Verteidigungsministerium die nationale Cybersicherheitspolitik durch:

- Loyale Erfüllung der Verpflichtungen, die im Nationalen Cybernotfallplan festgelegt sind;

- Ihre Kapazitäten bei Bedarf als technischer Experte zur Unterstützung bestimmter Rechtsfälle oder als technische Unterstützung für bestimmte CERT.be-Fälle einzusetzen;

- Anbieten einer Malware-Analyse auf Senior-Expertise-Niveau für nationale betroffene Parteien;

- Integration relevanter *cyberthreat intelligence* in die nationale *cyberthreat intelligence Platform*;

- Überwachung von Akteuren mit Absichten und Möglichkeiten für Cyberangriffe auf nationale wesentliche Interessen und Strukturen;

- Koordinierung der belgischen Teilnahme an internationalen Cybersicherheitsübungen, gegebenenfalls in Absprache mit dem Außenministerium und dem ZCB;

- Bereitstellung der mil.cert-Infrastruktur als Backup-Site für das Incident Management von CERT.be, in Krisensituationen, in denen die nationale Infrastruktur nicht verfügbar ist;

- Bei nationalen Krisen seine intrusive und offensive Kapazitäten einzusetzen, um mit einem eigenen Cyberangriff zu reagieren, um den Angriff zu neutralisieren und die Täter zu identifizieren.

4.5 Das Nationale Krisenzentrum (NCCN)

Das NCCN stellt zusammen mit dem ZCB die Organisation und Koordination des Cybernotfallplans auf nationaler Ebene sicher. Das NCCN und das ZCB sind gemeinsam für das Krisenmanagement verantwortlich.

Die Verwaltung der direkten und indirekten gesellschaftlichen Folgen einer Krise bleibt das Vorrecht des NCCN, der sektoralen Behörden und der Mitglieder der betroffenen Behörde. Das NCCN organisiert und leitet die Kommunikation im Falle einer nationalen Cyberkrise (siehe nationaler Cybernotfallplan).

Die Notrufstelle des NCCN stellt die 24/7-Verfügbarkeit von CERT.be sicher, das bei nationalen Vorfällen und Krisen erste Unterstützung leistet.

Das NCCN unterstützt die sektoralen Behörden rechtlich und organisatorisch bei der Identifizierung von kritischen Infrastrukturen und Anbietern wesentlicher Dienste. Das NCCN trägt auch zur Durchführung von Cyberrisikobewertungen bei, die den Betrieb von Organisationen von wesentlicher Bedeutung oder bestimmte Veranstaltungen stören können (siehe Kapitel 3).

Das NCCN verwaltet die Liste der Organisationen von wesentlicher Bedeutung und ist für die Koordinierung der Weiterverfolgung und Anpassung der entsprechenden Vorschriften verantwortlich. Schließlich analysiert das NCCN laufend die wichtigsten nationalen Risiken (einschließlich Cyber-Risiken) und führt bei besonderen Sachverhalten mit erhöhtem Risiko Adhoc-Risikoanalysen in Zusammenarbeit mit allen beteiligten Partnern durch.

4.6 Staatssicherheit (VSSE)

Die Aufgabe der Staatssicherheit (VSSE) ist es, Informationen über Aktivitäten zu sammeln, zu analysieren und zu verarbeiten, die die innere Sicherheit des Staates, die äußere Sicherheit des Staates oder das wissenschaftliche und wirtschaftliche Potenzial des Landes bedrohen oder bedrohen könnten.

Als Teil dieser Aufgabe wird die Staatssicherheit die entsprechenden Kontakte zu ausländischen Partnern pflegen und Informationen von diesen sammeln und die erhaltenen Informationen so weit wie möglich mit CERT.be und anderen relevanten Partnern teilen.

4.7 Der Föderale Öffentliche Dienst Auswärtige Angelegenheiten

Die Rolle des Föderalen Öffentlichen Dienstes Auswärtiger Angelegenheiten im Rahmen der Cybersicherheit kann wie folgt beschrieben werden:

- Internationaler *zentraler Ansprechpartner* auf diplomatischer Ebene, sowohl auf bilateraler Ebene als auch innerhalb relevanter multilateraler Organisationen (u.a. EU, NATO, OSZE), insbesondere in Krisenzeiten.

- In Absprache mit den zuständigen belgischen Behörden die Vertretung Belgiens bei internationalen Verhandlungen und Dialogen festlegen.

- Informieren der zuständigen belgischen Behörden über einschlägige internationale Entwicklungen.

- In Absprache mit allen betroffenen belgischen Behörden eine Position in internationalen Angelegenheiten definieren.

- Die koordinierte internationale Attribution von bösartigen Cyberaktivitäten.

- Bereitstellen von Erfahrungen, sowie das Umfeld eines internationalen Netzwerks zur Beobachtung und Analyse von Online-Sicherheitsproblemen, wie Cyberbedrohungen, Sicherheitslücken in IKT-Systemen, oder Cybervorfällen an zuständige Behörden (ZCB).

4.8 Die nationale Sicherheitsbehörde (NVO)

Die nationale Sicherheitsbehörde ist vor allem auf dem Gebiet der Informationssicherheit tätig, selbst wenn es sich um höchst sensible Daten oder „klassifizierte"Informationen handelt.

Die Cybersicherheitsstrategie in diesem Dokument richtet sich an vier verschiedene Zielgruppen. Drei dieser Zielgruppen gehören auch zu denen, auf die sich die nationale Sicherheitsbehörde konzentriert:

· Unternehmen
· Öffentliche Dienste
· Organisationen von wesentlicher Bedeutung

Für Unternehmen und öffentliche Dienste entwickelt die NVO eine Reihe von Produkten, die einen besseren Schutz von klassifizierten Informationen in einer Cyberumgebung ermöglichen. Der Einsatz, der von der NVO entwickelten Datenverschlüsselung, kann die Sicherheit von Verschlusssachen im Cyberbereich auf ein höheres Niveau heben, sowohl im privaten als auch im öffentlichen Bereich. So wird beispielsweise das nationale klassifizierte Netzwerk, dessen Einsatz und Organisation noch ausgearbeitet werden muss, den sicheren Informationsaustausch zwischen den öffentlichen Diensten erleichtern und damit Cyberrisiken reduzieren.

Für bestimmte Organisationen von wesentlicher Bedeutung kann die NVO auch Sicherheitsüberprüfungen durchführen (Sicherheitsberatung oder

Überprüfung von sensiblen Berufen). Dazu müssen diese Organisationen zunächst eine Risikoanalyse, eine Bedrohungsanalyse und eine Auswirkungsanalyse durchführen und die Sicherheitsmaßnahmen ihrer Informationssysteme abbilden. Dieser Prozess sensibilisiert nicht nur, sondern verstärkt auch die Maßnahmen, die diese Organisationen im Cyberbereich ergreifen.

4.9 Das Koordinierungsorgan für die Bedrohungsanalyse (KOBA)

Zu den Aufgaben des Koordinierungsorgans für die Bedrohungsanalyse gehört die Bewertung der Bedrohung durch Terrorismus und Extremismus. Im Falle von Cyberbedrohungen oder -Vorfällen, die (potenziell) mit terroristischen oder extremistischen Gruppen, oder ideologisch oder religiös inspirierten Hacktivisten in Verbindung stehen, kann das KOBA in Zusammenarbeit mit seinen Partnerdiensten eine Bedrohungsanalyse für das Nationale Krisenzentrum durchführen.

4.10 Sektorale Behörden

Das NIS-Gesetz vom 7. April 2019 (Gesetz zur Schaffung eines Rahmens für die Sicherheit von Netzwerk- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit) und der ausführende Königliche Erlass vom 12. Juli 2019 legen fest, wie in Belgien die sektoralen Behörden jeweils für die Identifizierung, Standardisierung und Inspektion von Anbietern wesentlicher Dienste in ihrem Sektor verantwortlich sind. Das ZCB und das Nationale Krisenzentrum haben dabei eine wichtige beratende Rolle. Das NIS-Gesetz identifiziert sechs verschiedene Sektoren von Anbietern wesentlicher Dienste: Energie, Transport, Finanzen, digitale Infrastruktur, Gesundheitswesen und Trinkwasser. Hinzu kommen digitale Dienste (wie Cloud-Computing-Dienste, Online-Suchmaschinen und Online-Marktplätze).

4.11 Das belgische Institut für Postdienste und Telekommunikation (BIPT)

Das belgische Institut für Postdienste und Telekommunikation (BIPT) überwacht die Sicherheit der elektronischen Kommunikationsnetze und -dienste von Telekommunikationsbetreibern. Das BIPT überwacht die Einhaltung der Gesetzgebung (z. B. Risikoanalysen und damit verbundene Sicherheitsmaßnahmen) und seiner Entscheidungen durch die Betreiber,

bearbeitet Meldungen über Sicherheitsvorfälle (einschließlich Vorfälle, die eine Verletzung des Schutzes personenbezogener Daten darstellen, zusammen mit dem GBA) und hat verschiedene Zuständigkeiten, um seine Aufgabe zu erfüllen (einschließlich der Erteilung verbindlicher Anweisungen an einen Betreiber). Das BIPT verfügt auch über ein Krisenreaktionsteam für den Fall der oben genannten Vorfälle.

BIPT ist auch die sektorale Behörde und der Inspektionsdienst für den Sektor der digitalen Infrastruktur (Internet Exchange Points, Anbieter von DNS-Diensten und Registrierungen von Top-Level-Domain-Namen) gemäß dem NIS-Gesetz und für die Sektoren der elektronischen Kommunikation und digitalen Infrastruktur gemäß dem Gesetz „kritische Infrastrukturen".

Das BIPT ist auch für die Überwachung der Anwendung der gesetzlichen Bestimmungen zur Umsetzung der Funkanlagenrichtlinie [RED (2014/53/EU)] in Bezug auf Produkte mit einer Funkfunktion verantwortlich.

4.12 Föderaler Öffentlicher Dienst Wirtschaft

Der Föderale Öffentliche Dienst Wirtschaft, K.M.B., Mittelstand und Energie hat die Aufgabe, die Bedingungen für ein wettbewerbsfähiges, nachhaltiges und ausgewogenes Funktionieren des Waren- und Dienstleistungsmarktes in Belgien zu schaffen. Angesichts der zunehmenden Digitalisierung unserer Gesellschaft und Unternehmen ist der FÖD Wirtschaft in mehreren Bereichen der Cybersicherheit tätig.

Sie ist die zuständige Verwaltung für die Identifizierung, Standardisierung und Überwachung der Bereiche Energie und digitaler Dienstleister nach dem NIS-Gesetz.

Opfer verschiedener Arten von Cyberbetrug können Cyberbetrug bei Meldpunt melden, einem Dienst des FÖD Wirtschaft, der relevante Daten rund um diese Meldungen mit dem ZCB teilt und Opfer von Cyberkriminalität an die Polizei weiterleitet.

Angesichts der Bedeutung der KMU für die belgische Wirtschaft wird der FÖD Wirtschaft enger mit dem ZCB zusammenarbeiten, um die Cybersicherheit dieser Gruppe von Unternehmen zu erhöhen.

4.13 Governance-Rahmen und Konsultationsplattformen

Neben den eigenen unterschiedlichen Verantwortlichkeiten ist die Zusammenarbeit zwischen den betroffenen Parteien ein wesentlicher Erfolgsfaktor bei der Vorbeugung, Reduzierung, Handhabung und Überwachung von Cyberbedrohungen und -Vorfällen. Wissen über Cybersicherheit und die Entwicklung der Cyberbedrohung wird zwischen den betroffenen Sicherheitsbehörden, öffentlichen Behörden, dem privaten und wissenschaftlichen Sektor über bestehende oder neue Plattformen ausgetauscht. Regelmäßige Treffen ermöglichen es den Experten, im direkten Kontakt Informationen und Erfahrungen auszutauschen und sich untereinander zu vernetzen.

In der Plattform 4 Cyber des Koordinierungsausschuss für Geheimdienste und Sicherheitsbehörden (CCIV) diskutieren die Geheimdienste und Sicherheitsbehörden über die allgemeine Cybersicherheitspolitik.

Konsultation zwischen den Aufsichtsbehörden von Organisationen von wesentlicher Bedeutung erfolgt über die Cybersecurity Sectoral Authority Plattform (CySSAP).

Das Expertise Network (REN) Cybercrime bringt Experten aus den Behörden im Bereich der Cyberkriminalität zu regelmäßigen Treffen zusammen. Dies wird von der Generalstaatsanwaltschaft in Antwerpen koordiniert.

Die CSI/DPO-Plattform (les Conseillers en Sécurité de l'Information/Data Protection Officers) bringt die Sicherheitsberater und Datenschutzbeauftragten der einzelnen Behörden zusammen. Jedes Quartal wird im Rahmen des Quarterly Cyber Threat Reportes des ZCB/CERT eine spezielle Sitzung zu Cyberthemen organisiert.

Die SIT (Synergy IT) ist die Plattform für den Wissensaustausch und Konsultation zwischen IT-Verantwortlichen aus allen föderalen öffentlichen Diensten (Föderale Öffentliche Dienste, Öffentliche Sozialversicherungsanstalten und Einrichtungen vom öffentlichem Interesse). Die SIT trifft sich monatlich mit dem Ziel, gemeinsame IT-Initiativen zu initiieren und weiterzuverfolgen, sowohl öffentliche Aufträge als auch Projekte, sowie technischen Input zu G-Cloud-Initiativen zu liefern.

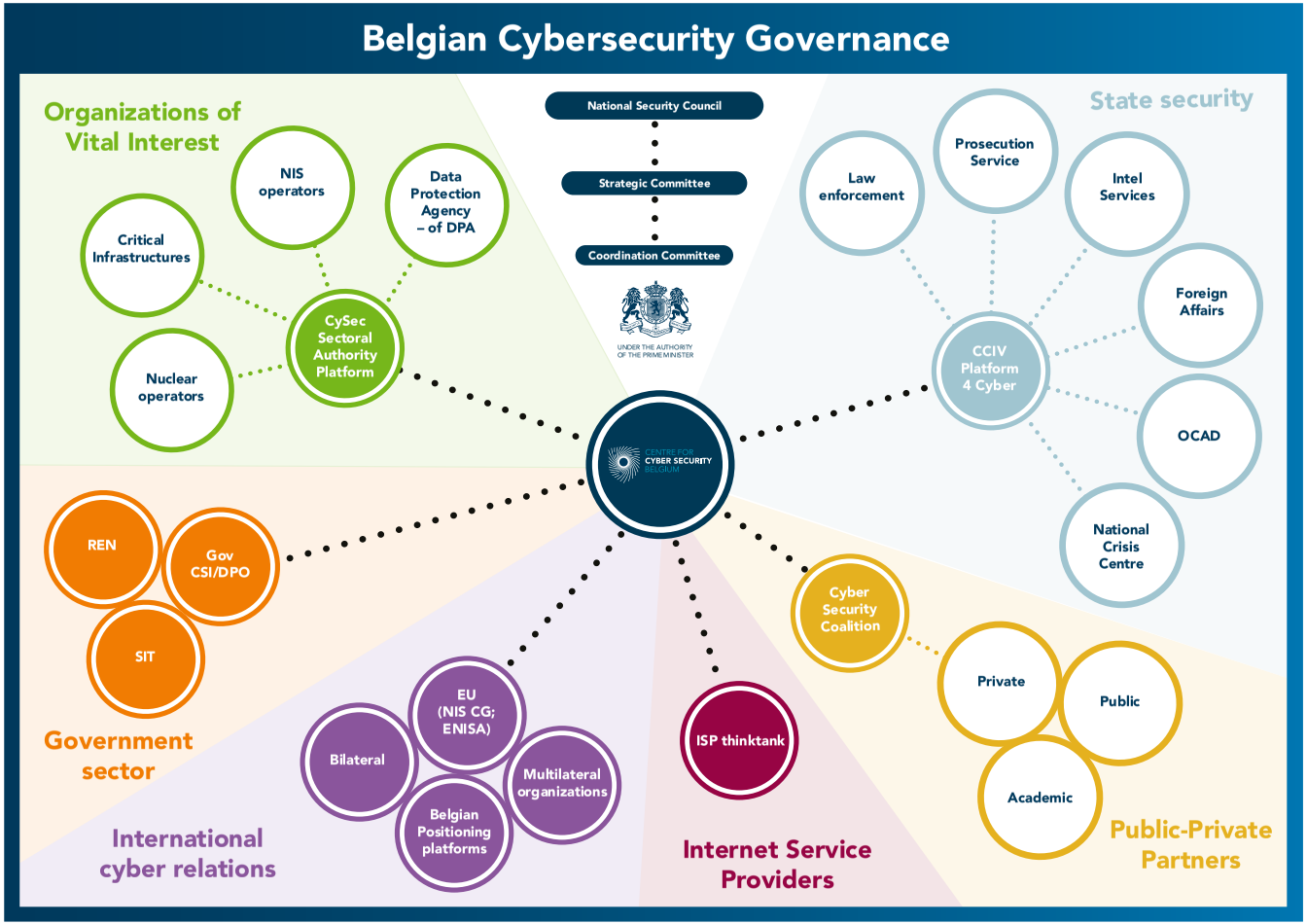
Die Entwicklung formeller belgischer Positionen in internationalen Diskussionen erfolgt über die entsprechenden Kanäle des FÖD Auswärtige Angelegenheiten.

Der Interministerielle Wirtschaftsausschuss (IEC) ist ein unabhängiger, flexibler, technisch-administrativer Koordinationsmechanismus im FÖD Wirtschaft, K.M.B., Mittelstand und Energie, der bei der Definition und Abstimmung der administrativen Positionen der föderalen und föderierten Behörden in nationalen, europäischen und internationalen Angelegenheiten helfen kann.

In der ISP-Denkfabrik berät das ZCB regelmäßig mit den größten Internetdienstanbietern in Belgien über konkrete Maßnahmen und Projekte, die die Cybersicherheit für belgische Bürger und Unternehmen erhöhen können.

Die vierteljährlichen Cyberbedrohungsberichte, die vom ZCB und CERT.be organisiert werden, bringen mehrere dieser Konsultationsplattformen zusammen und informieren alle Teilnehmer und Organisationen von wesentlicher Bedeutung über aktive Bedrohungen.

Die Cyber Security Koalition Belgien bringt regelmäßig Experten aus dem Bereich der privaten, akademischen und öffentlichen Sektoren zusammen. Dies geschieht bei Veranstaltungen zum Erfahrungsaustausch und in Fokusgruppen, in denen Best Practices, Erfahrungen oder Initiativen zu verschiedenen Themen (wie Cloud-Sicherheit, NIS, Krypto usw.) diskutiert werden.


Belgian Cybersecurity Governance
Organizations of Vital Interest
NIS operators
Data Protection Agency – of DPA
Critical Infrastructures
CySec Sectoral Authority Platform
Nuclear operators
National Security Council
Strategic Committee
Coordination Committee
UNDER THE AUTHORITY OF THE PRIME MINISTER
CYBERSECURITY BELGIUM
State security
Law enforcement
Prosecution Service
Intel Services
Foreign Affairs
CCIV Platform 4 Cyber
OCAD
National Crisis Centre
REN
Gov CSI/DPO
SIT
Government sector
Bilateral
EU (NIS CG; ENISA)
Multilateral organizations
Belgian Positioning platforms
International cyber relations
ISP thinktank
Internet Service Providers
Cyber Security Coalition
Private
Public
Academic
Public-Private Partners

5 Ressourcen

Um die beschriebene Vision und die sechs strategischen Ziele dieser ehrgeizigen Strategie umzusetzen, sind erhebliche, aber unerlässliche, zusätzliche Investitionen erforderlich. Ein deutliches Engagement des belgischen Staates zu diesen Ressourcen ist daher der elementare Schlussteil dieser aktualisierten nationalen Cybersicherheitsstrategie. Eine erhöhte Cyberkapazität ist von entscheidender Bedeutung, um unsere Wirtschaft, Behörden und Organisationen von wesentlicher Bedeutung effektiv und praktikabel gegen die ständig zunehmenden Cyberbedrohungen zu wappnen.

Investitionen in Cybersicherheit haben auch eine unmittelbare und deutliche wirtschaftliche Auswirkung. Wenn es der Regierung gelingt, das Vertrauen in das „digitale Leben" zu wecken und zu sichern, werden auch Unternehmen und Bürger eher bereit sein, in mehr digitale Anwendungen zu investieren. Dies wird die Produktivität und das Wirtschaftswachstum in unserem Land steigern, und Cyberangriffe werden noch besser vermieden werden können.

Mit dieser konkreten Investitionszusage folgt Belgien den signifikanten Initiativen in den Nachbarländern. Darüber hinaus schaffen die angesprochenen Investitionen wichtiges Vertrauen in die realistische Umsetzung unserer Ziele, insbesondere bei unseren europäischen und internationalen Partnern. Schließlich haben viele von ihnen gerade einen wichtigen Sitz oder eine Vertretung in unserem Land.

Die Mission, Belgien bis 2025 zu einem der am wenigsten gefährdeten Länder Europas im Cyberbereich zu machen, ist eine gemeinsame Anstrengung. Neben dem ZCB tragen auch andere Behörden, die Geheimdienste und Sicherheitsbehörden, sowie die Unternehmen, die Organisationen von wesentlicher Bedeutung, die akademische Welt und die Bürger jeweils ihre eigene Verantwortung, um die gesetzten ehrgeizigen Ziele zu erreichen.

Die Regierung hat dabei eine wichtige Verantwortung, die Richtung vorzugeben, aber auch mit gutem Beispiel voranzugehen. Sie wird daher eine glaubwürdige Cyberkapazität aufbauen, die mit anderen belgischen Akteuren mithalten kann, und versuchen, sich mit den Fähigkeiten unserer Nachbarländer zu verbinden.

Prepress en druk
Centrale drukkerij van de Kamer van Volksvertegenwoordigers

Brussel, mei 2021

Verantwoordelijke uitgever
Centrum voor Cybersecurity België
M. De Bruycker, Directeur
Wetstraat, 16
1000 Brussel

D/2021/14828/001