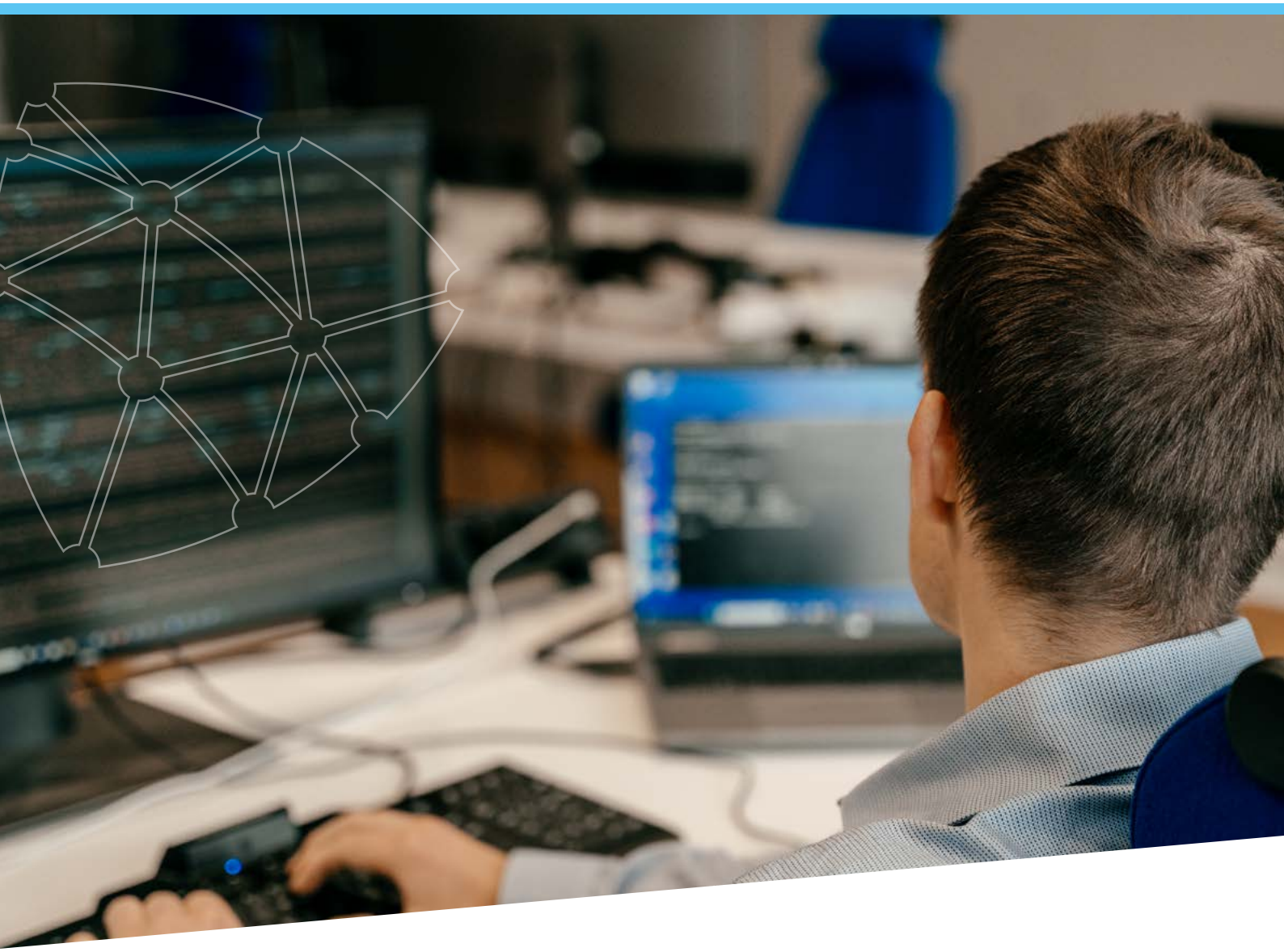
CENTRE FOR
CYBERSECURITY
BELGIUM



CYBERSICHERHEIT

ZCB-BERICHT 1.1.2023 - 30.9.2023

Centre for Cybersecurity Belgium
Unter der Autorität des Premierministers

Inhalt

Mitteilung des Direktors

Die nationale Cybersicherheit zu verbessern und ein Land weniger verwundbar zu machen, ist ein schwieriges Unterfangen. Schließlich ist der Cyberspace zu fast 100 % ein privates Umfeld. Darum fällt es staatlichen Stellen schwer, Bedrohungen und Zwischenfälle abzuwehren, zu erkennen und auf sie zu reagieren.

Wie in den meisten Ländern arbeitet das auch das „Zentrum für Cybersicherheit Belgien (ZCB)“ daran, die Widerstandsfähigkeit zu stärken: durch nationale und internationale Zusammenarbeit, durch Partnerschaften zwischen dem öffentlichen und privaten Sektor, Informationsaustausch, Kapazitätsaufbau und Schulungen, Sensibilisierung, Forschung, KI-gesteuerte Erkennung und Reaktion, Quantum-ready Crypto, nationale Übungen zur Cybersicherheit usw. Obgleich diese sämtlichen Maßnahmen notwendig und nützlich sind, reichen sie nicht aus und verhindern für sich genommen nicht, dass Cyberkriminalität und Online-Betrug zunehmen.

Sie erscheinen nicht spezifisch genug und bewirken konkrete Aktionen und Ergebnisse oft erst dann, wenn sie in kleinere, konkretere, zielgerichtete Projekte und Dienste umgesetzt werden. Ein Marathon ist erst beendet, wenn die letzte Meile geschafft ist! Und genau das wollen wir im ZCB erreichen: die letzte Meile für all diese wichtigen Konzepte und Initiativen laufen. Jedes Mal wollen wir uns fragen:

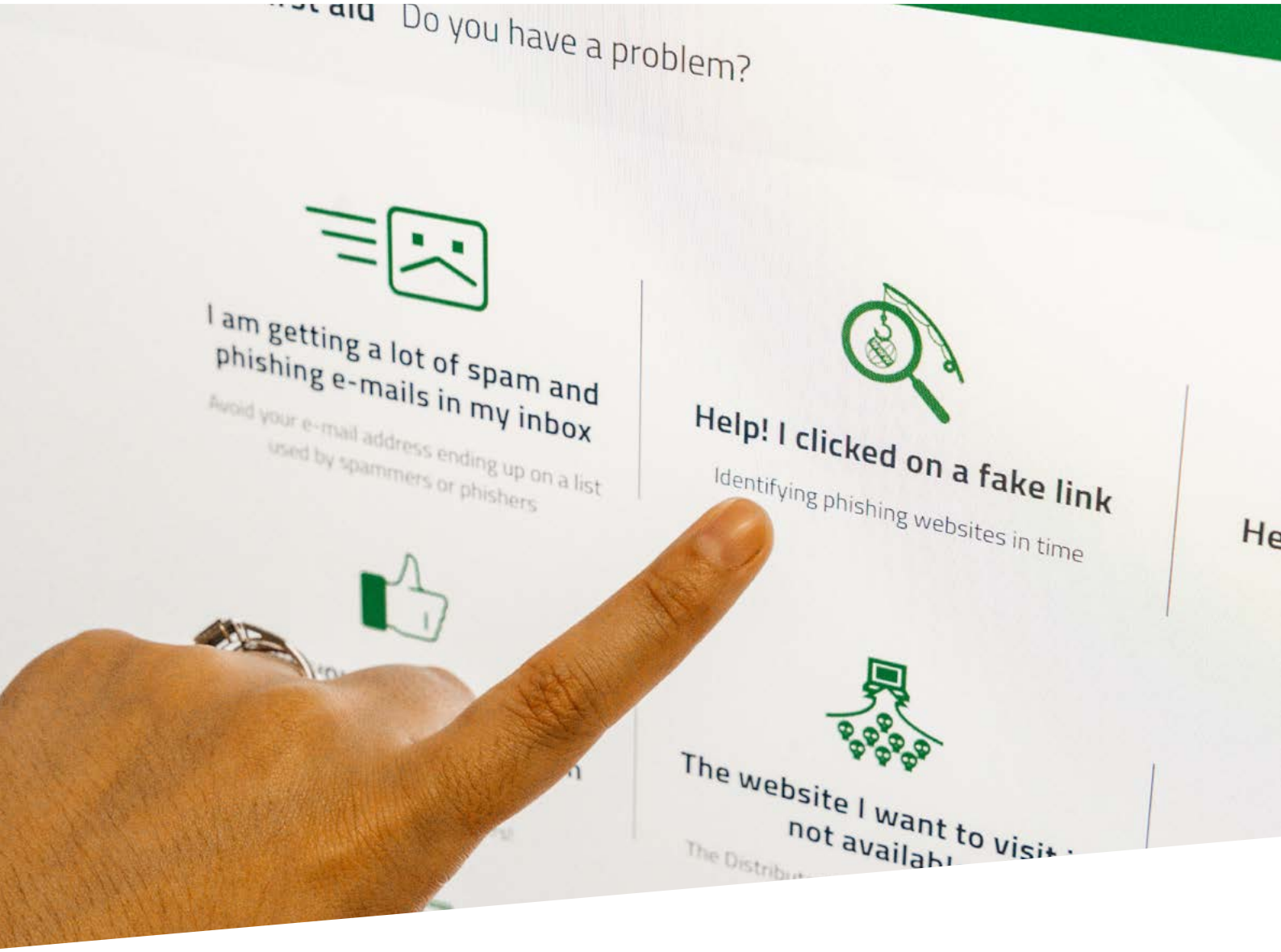
> Was bedeutet das real für Bürger, Unternehmen, Behörden oder unentbehrliche Infrastrukturen?

Diese letzte Meile wurde in eine Politik der „Active Cyber Protection“ (ACP; Aktiver Cyberschutz) umgesetzt, die aus fünf Teilbereichen besteht: Erstens wollen wir die Eigentümer der bedrohten Systeme oder Accounts einbeziehen, zweitens die Kommunikation mit zu 100 % schädlicher Infrastruktur national filtern, drittens die Cybersicherheit in einen für alle Unternehmen zugänglichen Routinebereich verwandeln, viertens anfällige Systeme in Belgien identifizieren und die Eigentümer direkt warnen („Spear Warning“) und schließlich fünftens die Entwicklung validierter Dienste fördern, damit jeder, der über das Internet Informationen empfängt, erkennen kann, ob die Identität des Absenders validiert wurde.

Das Kerngeschäft des ZCB lautet: die sich entwickelnden Cyber-Bedrohungslandschaft bewerten und darauf, zusammen mit unseren Partnern, mit konkreten Projekten reagieren. Unsere Kunden müssen erkennen können, wie wir die letzte Meile zurücklegen – dafür müssen wir sorgen!

Miguel De Bruycker
Der Generaldirektor,
Zentrum für Cybersicherheit Belgien

Brüssel, Dezember 2023


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

NATIONALE PROJEKTE UND INTERNATIONALE PRIORITÄTEN

Die Projekte und Initiativen des „Zentrums für Cybersicherheit Belgien“ als nationale Behörde für Cybersicherheit sollen bei öffentlichen Einrichtungen, Unternehmen, Hochschulen und Endnutzern die Cybersicherheit und Widerstandsfähigkeit stärken. So setzt sich das Zentrum aktiv dafür ein, dass Belgien in puncto Cybersicherheit bis 2025 zu einem der am wenigsten gefährdeten europäischen Länder wird.

Die rotierende Präsidentschaft des Rates der EU

Vom 1. Januar bis zum 30. Juni 2024 leitet Belgien den Rat der EU.

Dann wird das ZCB seine internationale Verantwortung wahrnehmen und eine führende Rolle bei der Förderung der belgischen Prioritäten und des Präsidentschaftsprogramms zur Cybersicherheit bei anderen Mitgliedstaaten und im Ausland spielen. So wollen wir das Ziel Nr. 6 unserer nationalen Strategie zur Cybersicherheit fördern: das nachdrückliche internationale Engagement Belgiens in der Cybersicherheit aufrechtzuerhalten.

DER VORSITZ UMFASST VERPFLICHTUNGEN UND CHANCEN GLEICHERMASSEN

Das ZCB wird den rotierenden Vorsitz in mehreren offiziellen europäischen Netzwerken zur Cybersicherheit gewährleisten, in denen es der offiziell ernannte Vertreter Belgiens ist (die NIS-Kooperationsgruppe, das EU Cybercrisis Liaison Network - EU-CyCLONe, das EU-CSIRT-Netzwerk u. a.). Dabei wird es die gesetzlichen Verantwortlichkeiten dieser Netzwerke nachverfolgen und für all diese Gruppen den Vorsitz führen, ihre Tagesordnung festlegen und ihre Sitzungen an verschiedenen Orten in Belgien ausrichten – u. a. auch, um unser Land zu präsentieren.

Zu einer Zeit, in der die Umsetzung der NIS2-Richtlinie in nationales Recht in die Endphase eintritt, wird es entscheidend, all diese Netzwerke miteinander zu koordinieren. Innerhalb des EU-Netzwerks „CyCLONe“ werden auch Belgien und das ZCB damit betraut sein, den ersten Bericht an den Rat und das EU-Parlament fertigzustellen.

Sollten sich schwerere Zwischenfälle im Bereich Cybersicherheit ereignen, wird das ZCB auch bei der Koordinierung einer europäischen Reaktion innerhalb der EU-Netzwerk „CyCLONe“ und „CSIRTs“ führend agieren müssen.

Ferner wird das ZCB eine führende Rolle bei der legislativen und politischen Arbeit innerhalb der „Arbeitsgruppe des Rates zur Cybersicherheit“ spielen. Wir werden die belgischen Attachés im Rat dabei unterstützen, die belgischen Ziele zu erreichen und die Arbeit an wichtigen Akten wie dem „Cyber Resilience Act“ (EU-Gesetz über Cyberresilienz), dem „Cyber Solidarity Act“ (Gesetz über die Cyber-Solidarität) oder den Änderungen am „Cybersecurity Act“ (Gesetz zur Cybersicherheit) voranzutreiben oder abzuschließen.

UND DIE WAHLEN …

Am 9. Juni 2024 – während unserer Präsidentschaft also – finden in Belgien neben nationalen und regionalen Wahlen auch die Europawahlen statt. All das könnte, zusätzlich zum anhaltenden Krieg in der Ukraine oder anderen unerwarteten Ereignissen, eine erhöhte Wachsamkeit und noch stärkere Zusammenarbeit erfordern. Auch für die große halbjährliche Übung „Cyber-Europe“ der Agentur der Europäischen Union für Cybersicherheit (ENISA) ist ein bedeutender Koordinationsaufwand erforderlich.

NIS2: Auswirkungen auf belgische Sektoren und Einrichtungen

Um der sich ausweitenden Cyber-Bedrohungslandschaft und den neuen Herausforderungen zu begegnen, hat die EU eine neue Rechtsvorschrift zu Maßnahmen für ein hohes gemeinsames Niveau der Cybersicherheit in der Union verabschiedet (Richtlinie 2022/2555 vom 14. Dezember 2022 - die sog. „NIS2-Richtlinie“). Diese ersetzt die „NIS1-Richtlinie“ (Richtlinie 2016/1148 vom 6. Juli 2016 über Maßnahmen für ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der Union).

Die NIS2-Richtlinie umfasst gegenüber NIS1 einige wichtige Änderungen: die Erweiterung der erfassten Sektoren und Einrichtungen, neue Auswahl- und Registriermethoden, mehr Cybersicherheits-Anforderungen, neue Fristen für die Meldung von Zwischenfällen und die Stärkung der Überwachungsmechanismen.

Darüber hinaus soll die NIS2-Richtlinie die nationalen Kapazitäten und Strategien zur Cybersicherheit verbessern. Was die nationale Politik betrifft, umfasst dies die nationale Strategie zur Cybersicherheit, nationale Rahmen für das Cyber-Krisenmanagement, die Rolle zuständiger Behörden sowie die nationale oder internationale Zusammenarbeit.

KOORDINIERUNG UND UMSETZUNG DER NIS2-RICHTLINIE

Als nationale Behörde für Cybersicherheit wird das ZCB eine Schlüsselrolle bei der Koordinierung und Umsetzung dieser Richtlinie spielen. Es übernimmt dann die Aufgaben der zuständigen Behörde für alle Sektoren (in Zusammenarbeit mit potenziellen sektoralen Behörden), des nationalen CSIRT, des nationalen einheitlichen Ansprechpartners, des Vertreters in der Kooperationsgruppe, CSIRT-Netzwerk und CyCLONe.

Um die Risiken der Cybersicherheit beherrschen zu können, müssen wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, betriebliche und organisatorische Maßnahmen ergreifen, um die Gefahren für die Sicherheit des Netzes und jener Informationssysteme zu beherrschen, welche die betreffende Einrichtungen für ihren Betrieb oder die Erbringung ihrer Leistungen einsetzen, und um die Auswirkungen von Zwischenfällen auf die Empfänger besagter Dienste zu verhindern oder zu minimieren. Solche Maßnahmen fußen auf einem Allgefahren-Ansatz, für den das ZCB mit der Verabschiedung des CyberFundamentals-Framework klare Vorgaben gemacht hat. Hierbei können sich die Organisationen zunutze machen, dass dann von ihrer Konformität mit den Vorschriften ausgegangen wird, wenn sie eine Zertifizierung bzw. das Label CyberFundamentals oder ISO/IEC 27001 erhalten.

Als nationales CSIRT wird das ZCB von den NIS-Einrichtungen über bedeutende Zwischenfälle benachrichtigt, um deren potenzielle Ausbreitung einzudämmen, den Einrichtungen zu ermöglichen, Hilfe hinzuzuziehen, Krisensituationen bestmöglich zu bewältigen und mit anderen Einrichtungen relevante technische Informationen zu teilen.

Schließlich wird das ZCB über seinen Inspektionsdienst (in Zusammenarbeit mit potenziellen sektoralen Behörden) auch bei der Überwachung der betroffenen Einrichtungen mitwirken.

Das CyberFundamentals-Framework

Zur Cybersicherheit besehen internationale Rahmen und verschiedene internationale Standards. Dieser sind sich die belgischen Organisationen bewusst. Dennoch fehlt es meist an einer spezifischen Auslegung für die Lage Belgiens, wodurch die Rahmen sehr allgemein bleiben. Folglich sind die von den Organisationen durchführbaren Maßnahmen risikobasiert festzulegen. Für Organisationen, die nicht unbedingt über Cyber-Spezialisten verfügen bzw. diese beschäftigen, ist dies besonders schwierig.

Belgien soll bis 2025 im Cyberbereich zu einem der am wenigsten gefährdeten europäischen Länder werden. Das ist die Mission der belgischen Nationalen Strategie zur Cybersicherheit 2.0 und auch des belgischen Zentrums für Cybersicherheit. Um diesem Ziel Substanz zu verleihen, hat die ZCB-Zertifizierungsbehörde das Rahmenwerk CyberFundamentals entwickelt.

DAS RISIKO VON CYBERANGRIFFEN VERRINGERN

Dieses Rahmenwerk soll unsere Daten schützen, das Risiko von Cyberangriffen merklich senken und die Widerstandsfähigkeit belgischer Organisationen erhöhen.

Mit diesem ganzheitlichen, risikobasierten Ansatz wollen wir das Vertrauen in die Digitalisierung der Gesellschaft stärken. Dazu teilen wir unser Wissen und geben Einblicke in verschiedene Cyber-Bedrohungen. Hierfür integrieren wir vom belgischen „Cyber Emergency Response Team“ (Team zur Abwehr von Cybergefahren; CERT) erhaltene, reale Daten in den Rahmen und nutzen diese (neben anderen Methoden), um den Rahmen zu validieren.

Der Rahmen fußt auf dem weltweit anerkannten NIST-CSF-Framework und umfasst verschiedene Elemente der in Belgien weit verbreiteten Normen ISO 27001 und ISO 62443 sowie des CIS Security Framework. Die Schritte „Identifizieren“, „Schützen“, „Erkennen“, „Reagieren“ und „Wiederherstellen“ ziehen sich als roter Faden durch das Rahmenwerk. Es wurde als Programm zur Konformitätsbewertung geschrieben und soll anzeigen, ob Konformität mit den Maßnahmen des Rahmenwerks vorliegt.

SICHERHEITSSTUFEN

Ferner orientiert sich der Rahmen an den Sicherheitsstufen des Cybersicherheitsgesetzes „Cyber Security Act“. Es umfasst drei Sicherheitsstufen: „Basic“, „Important“ und „Essential“, ergänzt durch eine Einstiegsstufe „Small“.

Auf diese Weise und teilweise auch durch einen einbezogenen Reifegradansatz soll der Rahmen angemessen auf die Anforderungen kleiner bis großer Organisationen reagieren, so dass diese ihre Cybersicherheit schrittweise verbessern können.

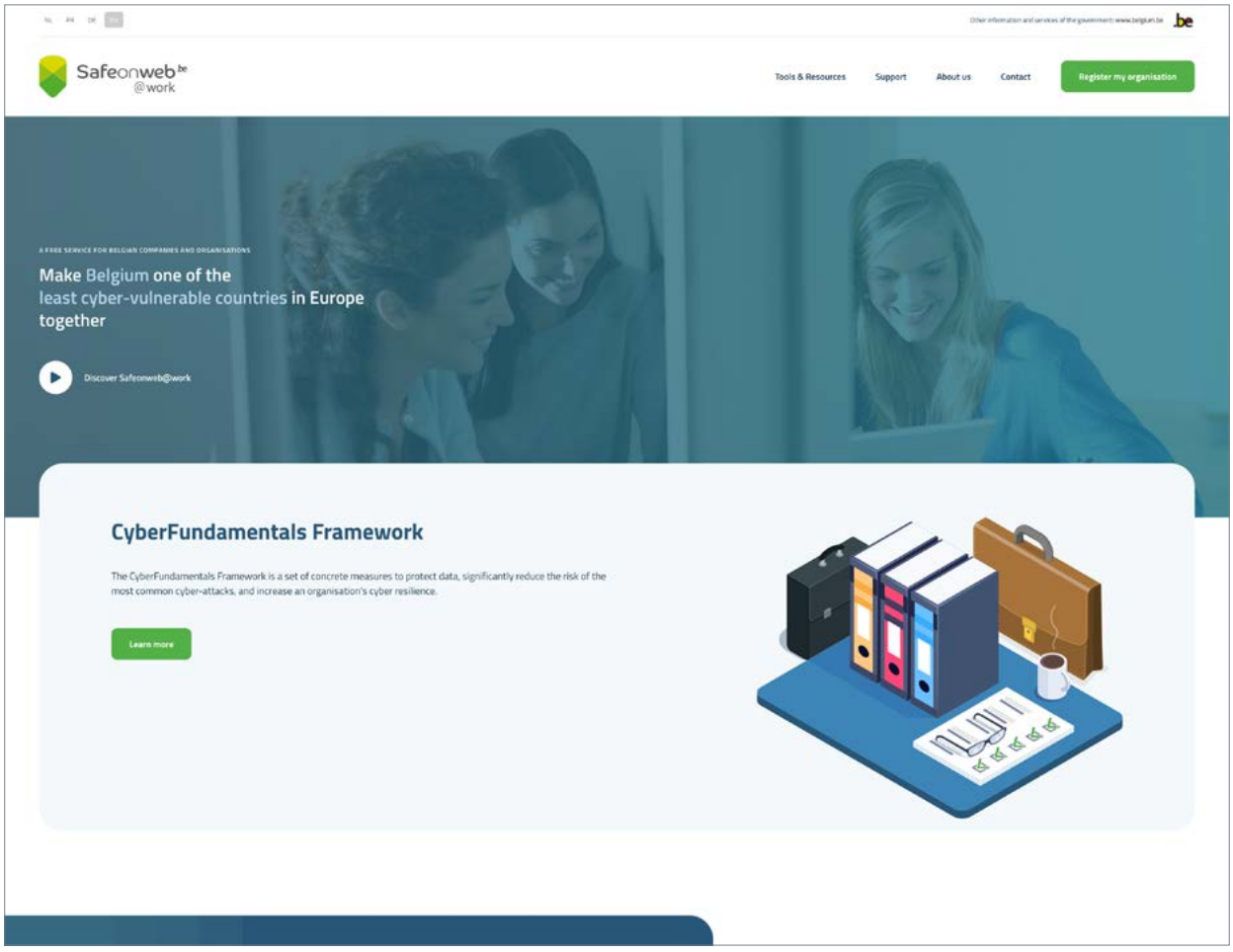
Um die Umsetzung des Rahmenwerks zu unterstützen, bietet das ZCB letztlich noch verschiedene Tools an: von einer Risikoanalyse zur Bestimmung des nach NIS2 erforderlichen Sicherheitsniveaus über ein Selbstbewertungs-Tool bis hin zu einer Zuordnung zu jenen verschiedenen Rahmenwerken und Standards, welche die Grundlage des Rahmenwerks bilden.

Rahmenwerk und Tools sind frei verfügbar.

www.cyfun.be

Safeonweb @work

Die Initiative **Safeonweb@work** richtet sich an belgische Organisationen und Unternehmen, deren Cybersicherheit sie stärken soll. Dazu liefert sie Ratschläge, Empfehlungen und Tools an die Institutionen, um die Schwachstellen in deren Systemen zu identifizieren und zu entschärfen, und um sie vor Cyber-Bedrohungen zu warnen. Dank der verschiedenen Dienste können die Organisationen proaktiv geeignete Maßnahmen ergreifen, um das Risiko von Cyberangriffen merklich zu senken und letztlich an unserem Ziel mitzuwirken, Belgien bis 2025 zu einem am wenigsten durch Cyberangriffe gefährdeten europäischen Länder zu machen.



DIE DIENSTE VON SAFEONWEB@WORK UMFASSEN:

Warnungen vor Cyber-Bedrohungen
Dieser Service warnt das Netzwerk früh vor Bedrohungen. Wenn in dem registrierten Netzwerk auf der Plattform eine Schwachstelle oder Infektion gemeldet wurde, versendet Safeonweb@work eine spezifische Warnung.

Schnellscan-Bericht
Über diesen Dienst kann man einen Bericht anfordern, der die Assets der Organisation skizziert, potenzielle Schwachstellen identifiziert und Empfehlungen zur Behebung gibt.

Richtlinien-Vorlagen
Ein Satz aus anpass- und editierbaren Dokumenten für Richtlinien zur Cybersicherheit, welche die Umsetzung des Informationssicherheits-Managements in einer Organisation erleichtern.

Selbstbewertung
Ein Formular zur Selbstbewertung, über das sich der Reifegrad der Cybersicherheit einer Organisation bewerten und unsere praktischen Empfehlungen einholen lassen, um festgestellte Sicherheitslücken zu schließen.

Inhalt
Nachrichten, Tipps, Warnungen, Webinare, Empfehlungen zu bewährten Verfahren in Sachen Cybersicherheit und häufige Bedrohungen sowie verschiedene Tools zur Verbesserung des Niveaus der Cybersicherheit einer Organisation.

atwork.safeonweb.be

Browser-Erweiterung „Safeonweb“

Das ZCB hat die Browser-Erweiterung Safeonweb entwickelt, mit der Bürger und Organisationen leichter beurteilen können, ob die Identität des Website-Besitzers gründlich validiert wurde, woraus sich u. U. die Zuverlässigkeit der Website ableiten ließe. Die Erweiterung ist gratis und liefert Informationen, um die die Zuverlässigkeit der Betreiber (nicht den Inhalt) der Website zu prüfen.

WIE FUNKTIONIERT DIE SAFEONWEB-BROWSERERWEITERUNG NUN?

Die Erweiterung vergibt für die Websites eine Punktzahl:

Grün (OK)
Bewertung 4 von 4: Der Eigentümer der Website verfügt über ein „Extended Validation“-Zertifikat von einer Zertifizierungsstelle oder ist auf atwork.safeonweb.be registriert (nur für belgische Organisationen).

Deshalb gilt:

- Auf der betreffenden Website kann man ruhig weiter surfen
- und Daten teilen.

Gelb (!)
Bewertung 1 bis 3 von 4: Der Eigentümer der Website verfügt über ein Zertifikat „Organisation Validation“ oder ein von einer Zertifizierungsstelle ausgestelltes Domain-Validierungs-Zertifikat. Die Website ist aber nicht auf atwork.safeonweb.be registriert.

Deshalb gilt:

- Auf der betreffenden Website kann man ruhig weiter surfen
- Im Zweifel sollten Sie auf dieser Website keine Daten teilen.

Rot (X)
Bewertung 0 von 4: Die Website hat keine grundlegenden Sicherheitsmerkmale oder ist als Schad-Website bekannt. Ihr Eigentümer verfügt über kein Zertifikat und wurde folglich nicht validiert. Deshalb gilt:

Deshalb gilt:

- Sie sollten diese Website nicht besuchen und dort keine Daten teilen.

Weitere Informationen über das Projekt sowie Installationsanleitungen finden Sie unter:

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

Innovationen in der Cybersicherheit für belgische KMU fördern: „Financial Support for Third Parties“ (Finanzielle Unterstützung für Drittparteien) (FSTP)

Das Projekt „Financial Support for Third Parties“ (Finanzielle Unterstützung für Drittparteien; FSTP) wurde vom **„Belgian National Coordination Centre“ (Nationales Koordinierungszentrum Belgiens**; (NCC-BE) innerhalb des ZCB umgesetzt. Diese Initiative konzentriert sich darauf, mittels EU-Investitionen (FSTP u. a.), Start-ups, KMU und Midcap-Unternehmen Unternehmen zu befähigen, ihre Cybersicherheitskapazitäten zu stärken und so zu einem sichereren digitalen Umfeld beizutragen.

DIE CYBER-RESILIENZ FÜR KMU STÄRKEN

FSTP ist mehr als nur ein schickes Akronym, FSTP ist Ihr Ticket zur Cyber-Resilienz!

FSTP, auch „Cascading Funding“ genannt, ist ein wichtiger Mechanismus, mit dem die Europäische Kommission Start-ups und KMU dabei unterstützt, für mehr Cybersicherheit zu sorgen. Mittels FSTP stärkt NCC-BE Belgiens Cybersicherheit, indem es entsprechende innovative Lösungen verbreitet.

DIE WIRKUNG VON FSTP: STÄRKER, SICHERER, INTELLIGENTER!

Man geht davon aus, dass die FSTP-Initiative zu signifikanten Ergebnissen führt, welche die belgische Cybersicherheit wie folgt positiv beeinflussen werden:

- Erhöhte Cyber-Resilienz: Die KMUs werden besser auf innovative Cybersicherheitslösungen zugreifen können, um sich neu entstehenden Cyberbedrohungen besser zu widersetzen.
- Innovation fördern: Werden Innovationen im KMU-Sektor gefördert, entstehen Spitzentechnologien für die Cybersicherheit, so dass Belgien ausgeklügelte Cyber-Bedrohungen weitaus besser bekämpfen kann.
- Kooperation zwischen Öffentlich und Privat Wenn das NCC-BE und privaten KMUs kooperieren, wird der Informationsaustausch optimiert und ein kohärenter Ansatz für die Cybersicherheit gefördert, was wiederum der nationalen Cyber-Resilienz insgesamt dient.
- Wirtschaftswachstum: Das FSTP fördert das Wirtschaftswachstum, indem es die Position der KMU in Sachen Cybersicherheit stärkt, denn es schützt unentbehrliche digitale Werte und wirkt an einem günstigen Umfeld für die Geschäftstätigkeit mit.

Das vom NCC-BE geleitete FSTP trägt entscheidend dazu bei, dass die Cybersicherheit in Belgien stets die diesbezüglichen europäischen Ziele erfüllt. Achten Sie auf weitere Updates auf den Kanälen des ZCB und NCC-BE.

Finanzierung und Ausschreibungen (europa.eu)

LANDSCHAFT DER CYBER-BEDROHUNGEN 2023

Die aktuelle Cyber-Bedrohungslage

DIE GLOBALE CYBER-BEDROHUNGSLANDSCHAFT

Die globale Cyber-Bedrohungslandschaft war 2023 weiterhin von Cyber-Angriffen durch verschiedene Bedrohungsakteure geprägt. Dazu zählten Hacktivisten- und Ransomware-Gruppen sowie staatlich gestützte Hackergruppen. Cyberkriminelle wollen meist finanziell profitieren. Dagegen sind Geopolitik einerseits sowie Cyberangriffe durch Hacktivisten und staatlich geförderte Akteure andererseits eng miteinander verbunden.

Der Ukraine-Russland-Konflikt

Der Konflikt zwischen der Ukraine und Russland hat seit 2022 den Hacktivismus reaktiviert. Er zeigte zudem, dass diese Gruppen einen wichtigen Faktor darstellen und Aufmerksamkeit erregen können, um die physischen und ideologischen Aktivitäten während eines Konflikts zu unterstützen. Die hacktivistischen Aktivitäten 2023 bezogen sich primär auf den Konflikt zwischen Russland und der Ukraine. Seit dessen Beginn erschienen viele Hacktivisten-Gruppen in der Online-Szene und bauten ihre Aktivitäten stark aus, um so die Interessen und Politik einer der beteiligten Seiten zu unterstützen. Bevorzugter Modus Operandi waren störende DDoS-Angriffe (Distributed Denial-of-Service), Web-Defacements und „Hack-and-Leak"-Operationen.

Die pro-russischen Hacktivistengruppen griffen neben der Ukraine auch viele andere europäische Länder an, darunter Belgien. Sie attackierten vor allem Regierungs- und Militäreinrichtungen, aber auch Organisationen in den Bereichen Energie, Transport (Häfen und Flughäfen), Logistik, Banken, Telekommunikation und sogar im Gesundheitswesen. Es sollten Vergeltung für die nationale militärische, finanzielle, humanitäre oder politische Unterstützung der Ukraine durch europäische Länder geübt werden, was durchweg den strategischen Zielen Russlands diente. Neben den Hacktivismus-Aktivitäten zum besagten Konflikt verbreitet sich der Hacktivismus auch in anderen Regionen der Welt als fortlaufende Reaktion auf die sich wandelnden, globalen Probleme in Politik und Gesellschaft sowie auf bestehende Konflikte. Im Jahr 2023 bedingten politische Themen, soziale Spannungen sowie anhaltende Konflikte in verschiedenen Zonen der Welt die hacktivistischen Aktivitäten.

Die Tätigkeiten von Cyberkriminellen folgten den makroökonomischen Veränderungen und wandelten bzw. entwickelten sich beträchtlich; es wurden mehr Fähigkeiten und Taktiken genutzt und auch neue Ziele anvisiert: Regierungsbehörden, öffentliche Einrichtungen und Organisationen in kritischen Sektoren u. a.

Ransomware

Angriffe durch Ransomware waren weiterhin die wichtigste cyberkriminelle Aktivität, unter der Organisationen (einschließlich kritischer Infrastrukturen) in Europa und den USA, litten. Ransomware-Betreiber griffen vor allem folgende Branchen an: Fertigung, Software und Informationstechnologie (IT), Gesundheitswesen, Bildung, Unternehmens- und Beratungsdienste, Recht, Finanzen und Banken. Seit Ausbruch des Ukrainekrieges gibt es verstärkt Ransomware-Angriffe auf Gemeinden und öffentliche Einrichtungen in europäischen Ländern, darunter auch Belgien.

APT-Kampagnen und Cyberspionage

Wichtigste Triebkraft für die Entwicklung von APT-Kampagnen ist nach wie vor die Geopolitik. Hauptziel von APT-Angriffen ist die Cyberspionage (Ausschleusung und Sammlung sensibler Daten). Die APT-Angriffe gingen meist auf das Konto staatlich gesponserter Hackergruppen und beeinträchtigten die attackierte Infrastruktur erheblich. Das ganze Jahr über meldeten Cybersicherheitsunternehmen und nationale Behörden mehrere Cyberspionage-Kampagnen, die sich meist gegen das Regierungsumfeld, aber auch auf einige strategische Sektoren richteten.

Weiterhin weltweit aktiv waren bekannte, staatlich gesponserte Hackergruppen, wie APT 28 (Fancy Bear), APT 29 (Cozy Bear), Emissary Panda, APT 33, Charming Kitten oder Lazarus Groups, um nur einige zu nennen. Ferner deuteten Berichte auf intensive Aktivitäten gegen verschiedene europäische Ziele hin; von neuen Gruppen wie der von Microsoft gemeldeten Storm-0978, die in diesem Jahr eine Phishing-Kampagne gegen den NATO-Gipfel führte, bis hin zu Storm-0558, einer ebenfalls von Microsoft aufgespürten Bedrohungs-

gruppe, die vor allem westeuropäische Regierungsbehörden angreift und sich auf Spionage, Datendiebstahl und Zugriff auf Zugangsdaten konzentriert. Ebenfalls beobachtet wurde, wie staatlich finanzierte Bedrohungsfaktoren zum Kampf gegen ihre Ziele neue Tools und Fähigkeiten entwickelten und einsetzten, um anhaltend aktiv sein zu können, um unentdeckt zu bleiben und um ihre Ziele zu erreichen.

DIE LANDSCHAFT DER CYBER-BEDROHUNGEN IN BELGIEN

2023 fielen belgische Organisationen in erster Linie Ransomware und DDoS-Angriffen zum Opfer, waren aber auch von anderen Arten von Cyber-Zwischenfällen betroffen: Datenlecks, CEO-Betrug, Bedrohungsspuren im Dark Web und in speziellen Foren mit beworbenen gestohlenen Daten und für Cyberoperationen verwendeten, kompromittierten belgischen IP-Adressen.

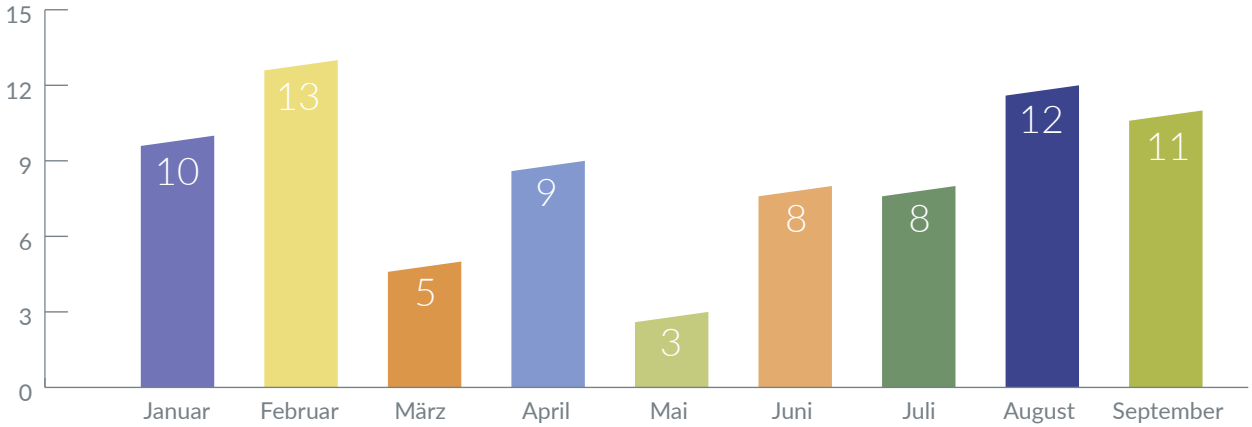
Ransomware

Wie in anderen europäischen Ländern blieb Ransomware in puncto Anzahl und Wirkung die bedeutendste und konstanteste Cyberbedrohung. Verschiedene Ransomware-Gruppen, (darunter die berüchtigtsten wie LockBit, Play oder Cl0p) griffen belgische Organisationen an.

> Die meisten belgischen Opfer erpresste unseren Daten nach die Gruppe LockBit, was deren weltweiten Aktivitäten entspricht.
>
> Auch die Ransomware-Bande Cl0p, die massenweise die kritische Sicherheitslücke MOVEit ausnutzt, hat in der Hierarchie der Ransomware-Angreifer die Spitze erklommen.

Attackiert wurden private und öffentliche Einrichtungen verschiedener Sektoren, wie Regierungen, lokale Verwaltungen, das Gesundheitswesen, die Fertigung, die IT-Branche sowie die Lebensmittel- und Getränkeindustrie. Die Opfer waren wenig bis stark betroffen; je nach angegriffener Organisation, Cybersicherheits-Infrastruktur und vorhandenen Praktiken und Richtlinien. In einigen Fällen erpressten Cyberkriminelle ihre Ziele doppelt, und den Ransomware-Angriffen folgten Datenlecks und die Veröffentlichung der gestohlenen Informationen auf der den Ransomware-Gruppen gehörenden Data Leak Site. In solchen Situationen sind die Folgen stets gravierender, denn die Angriffe verringern nicht nur die Verfügbarkeit der Infrastrukturen, sondern schädigen auch das Image der angegriffenen Unternehmen. Bis einschließlich September 2023 meldeten öffentliche oder private Einrichtungen in Belgien dem ZCB 79 Fälle von Ransomware.

Ransomware-Angriffen: Januar – September 2023



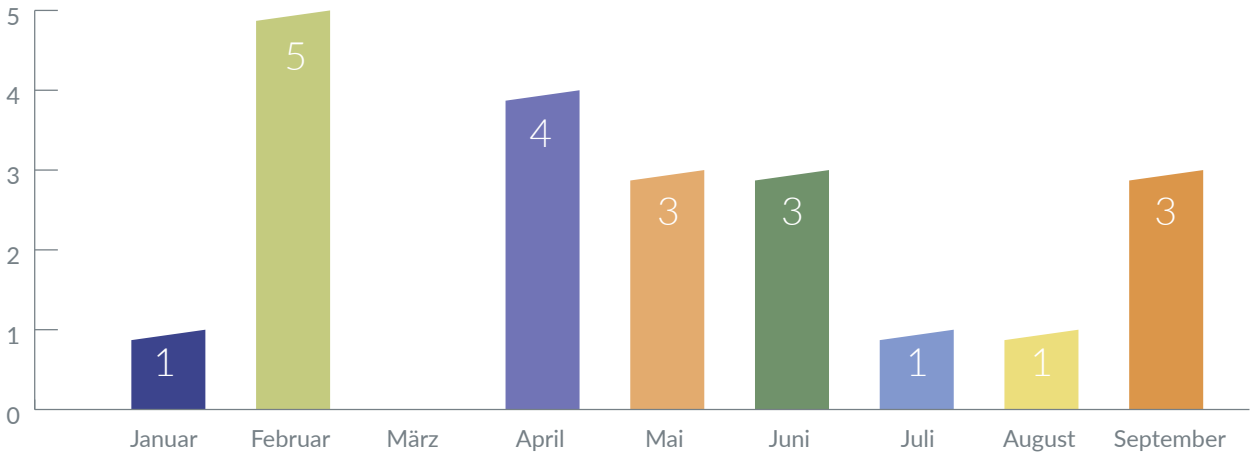
DDoS

DDoS-Angriffe gegen belgische Unternehmen waren eine konstante Bedrohung, ihre Folgen waren jedoch gering. Durch die Angriffe war bei der betroffenen Organisation vorübergehend die Verfügbarkeit einiger Ressourcen oder Dienste eingeschränkt. Meist wurde die Lage jedoch korrekt gehandhabt, und die Dienste waren wieder verfügbar und funktionstüchtig. Einige Angriffe, zu denen sich die pro-russischen Hacktivistengruppen KillNet, NoName057(16) und NET-WORKER ALLIANCE bekannten, standen im Zusammenhang mit den offiziellen belgischen Positionen zum Fortgang des Konflikte zwischen der Ukraine und Russland oder mit der militärischen Unterstützung Belgiens für die Ukraine.

Dennoch ist unbedingt zu erwähnen, dass die DDoS-Angriffe der pro-russischen Hacktivisten mit Kommunikationsarbeit einhergehen, um ein hohes Maß an Aufmerksamkeit der Medien zu erlangen. Auf diesem Weg sollen die Berichte über die Nichtverfügbarkeit von Diensten bzw. die übertriebene Darstellung der Auswirkungen den Ruf des Unternehmens schädigen und langfristig weitaus schwerere Folgen verursachen.

Andere DDoS-Angriffe, zu denen sich keine pro-russischen Hacktivistengruppen bekannten, zielten vorrangig auf öffentliche Einrichtungen ab. So wurden zwischen Januar und September 2023 insgesamt 21 Angriffe gemeldet.

DDos-Angriffen: Januar – September 2023



Und 2024?

Ransomware-Angriffe werden weiterhin zu den häufigsten und folgenreichsten Cyber-Bedrohungen gegen Belgien zählen.

Je nach der Entwicklung der anhaltenden Konflikte und der geopolitischen Lage sowie den von Belgien getroffenen Entscheidungen und Maßnahmen besteht auch 2024 die Gefahr von DDoS-Angriffen durch Hacktivistengruppen auf belgische Ziele.

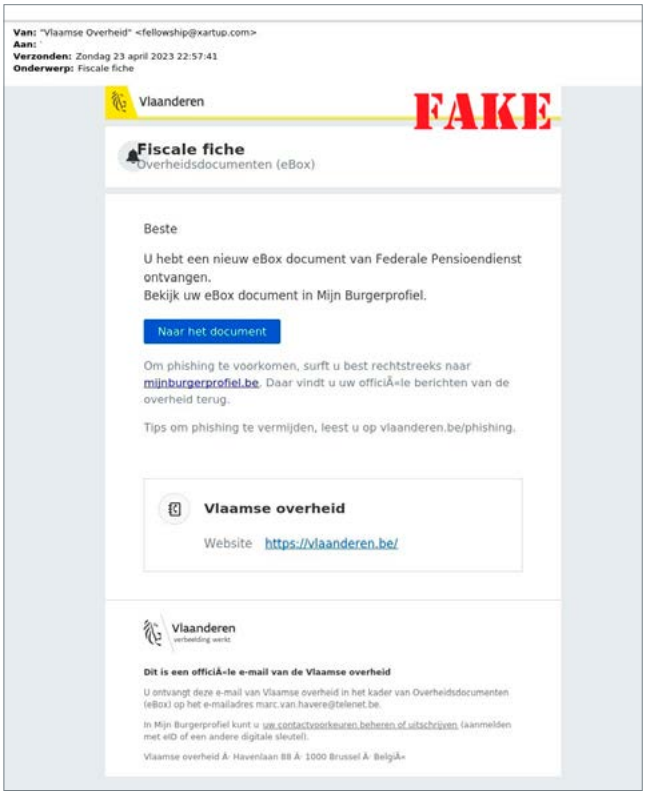
Mit Brüssel als Hauptstadt und Sitz zahlreicher internationaler Unternehmen, Organisationen und EU-Institutionen wird Belgien auch künftig Ziel von Cyberspionage sein.

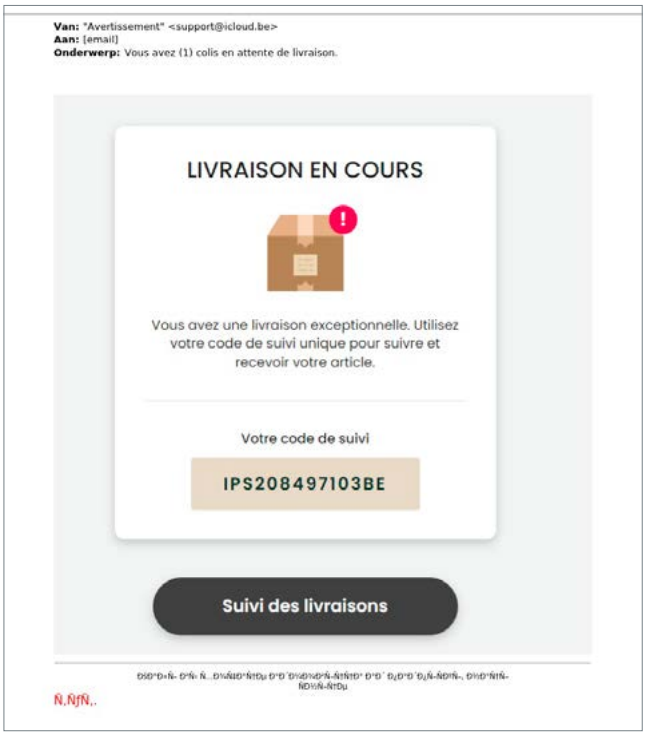
Beispiele für Angriffe auf belgische Organisationen: Januar – Oktober 2023

	Typ	Beschreibung oder Aktivität
12.03.2023	Ransomware	Von Ransomware betroffene Einrichtung im Gesundheitswesen
11.05.2023	Ransomware	Einrichtung im Gesundheitssektor fiel Ransomware zum Opfer
20.06.2023	DDoS	Pro-russischer DDoS-Angriff gegen belgische Einrichtungen im maritimen Sektor. Hinter diesem Angriff steckt NoName057(16).
27.06.2023	DDoS	Ein DDoS-Angriff richtete sich gegen die belgische Bundesregierung
14.07.2023	Ransomware	Eine belgische Gemeinde wurde zur Zielscheibe eines Cyberangriffs
2.08.2023	Ransomware	Ein belgischer Verband wurde von Ransomware angegriffen
22.08.2023	Ransomware	Cyberangriff auf die Infrastruktur für eine belgische Gemeinde
24.08.2023	Cyberangriff	Die Regierung wurde Opfer eines DDoS-Angriffs (Distributed Denial of Service).
12.10.2023	DDoS	NoName057(16) Attackiert wurden belgische Regierungsstellen als Vergeltung für versprochene militärische und finanzielle Unterstützung der Ukraine.

Das Anti-Phishing-Projekt

Phishing ist noch immer einer der wichtigsten **Angriffsvektoren**, mit denen Kriminelle Malware in Zielsystemen installieren. Phishing ist aber ebenso eine der häufigsten **Angriffsarten, um Informationen**, wie personenbezogene Daten und Zugangsdaten, zu stehlen und Cyber-Betrug zu begehen. Phishing-Angriffe nutzen weitgehend **„Social-Engineering"-Techniken**, die eher auf menschlichem Schwächen als auf technischen Schwachstellen beruhen, und sie **gefährden sowohl belgische Organisationen als auch einzelne Personen.**





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

Le service clients Proximus

Cher(e) Client(e) ,

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

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

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

CONFIRMER & CONTINUER

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

Die von den Angreifern verwendeten **Betreffe** und **Köder** für Nachrichten und Phishing-E-Mails, um Daten von Belgiern zu stehlen, bezogen sich meist auf für die Bürger interessante Themen (Bankkommunikation, Pakete und andere Postdienste) und variierten je nach sozioökonomischem Kontext, der Jahreszeit oder den geopolitischen Umständen.

Sehr oft gaben sich die Betrüger als offizielle Behörden und öffentliche Einrichtungen aus. Dabei wurden einige Phishing-Methoden sehr professionell umgesetzt. Gleichzeitig bestehen noch immer viele leicht erkennbare Phishing-E-Mails und -Nachrichten. So wurden 2023 neben den bereits „traditionellen" Betreffen zu Lieferpaketen, letzte Mahnungen für angeblich fällige Zahlungen, neue Betreffe im Zusammenhang mit den **Energiesubventionen** und **Steuerhilfen** verwendet, während alte Betreff-Themen etwa zu COVID-19 nicht mehr verwendet wurden.

Phishing-Kampagnen sollen vor allem die Daten ihrer Opfer erfassen. Deshalb dienten die **Top 5 der am häufigsten verwendeten Malware dem Datendiebstahl**: Agent Tesla, xloader, remcos, snake keylogger, Loki Password Stealer.

TOP 10 der Malware-Familien

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

Quelle: CCB, 2023

Agent Tesla[1], die 2023 am häufigsten festgestellte Malware, ist ein fortschrittlicher **Remote-Access-Trojaner (RAT)**, der sich auf den Diebstahl sensibler Daten von infizierten Rechnern spezialisiert (**Datendiebstahl**). Erstmals tauchte Agent Tesla 2014 auf und wurde in den 2020er Jahren vor allem für Phishing-Kampagnen über COVID-19 genutzt.

Agent Tesla verschickt E-Mails mit *zip-*, *gz-*, *cab-*, *msi-* und *img*-Dateien sowie Microsoft Office-Dokumente mit bösartigen VBA-Makros (Visual Basic Application), um die angegriffenen Systeme zu kompromittieren. Die Phishing-Kampagnen sind dafür bekannt, dass sie Ton und Optik eines seriösen Unternehmens, einschließlich Logos und Schriftarten, genau nachbilden.

Die Malware kann verschiedene Datenarten sammeln, darunter Tastatureingaben und Anmeldedaten in Browsern, E-Mail-Clients, WLAN-Profilen sowie weitere wertvolle Informationen.

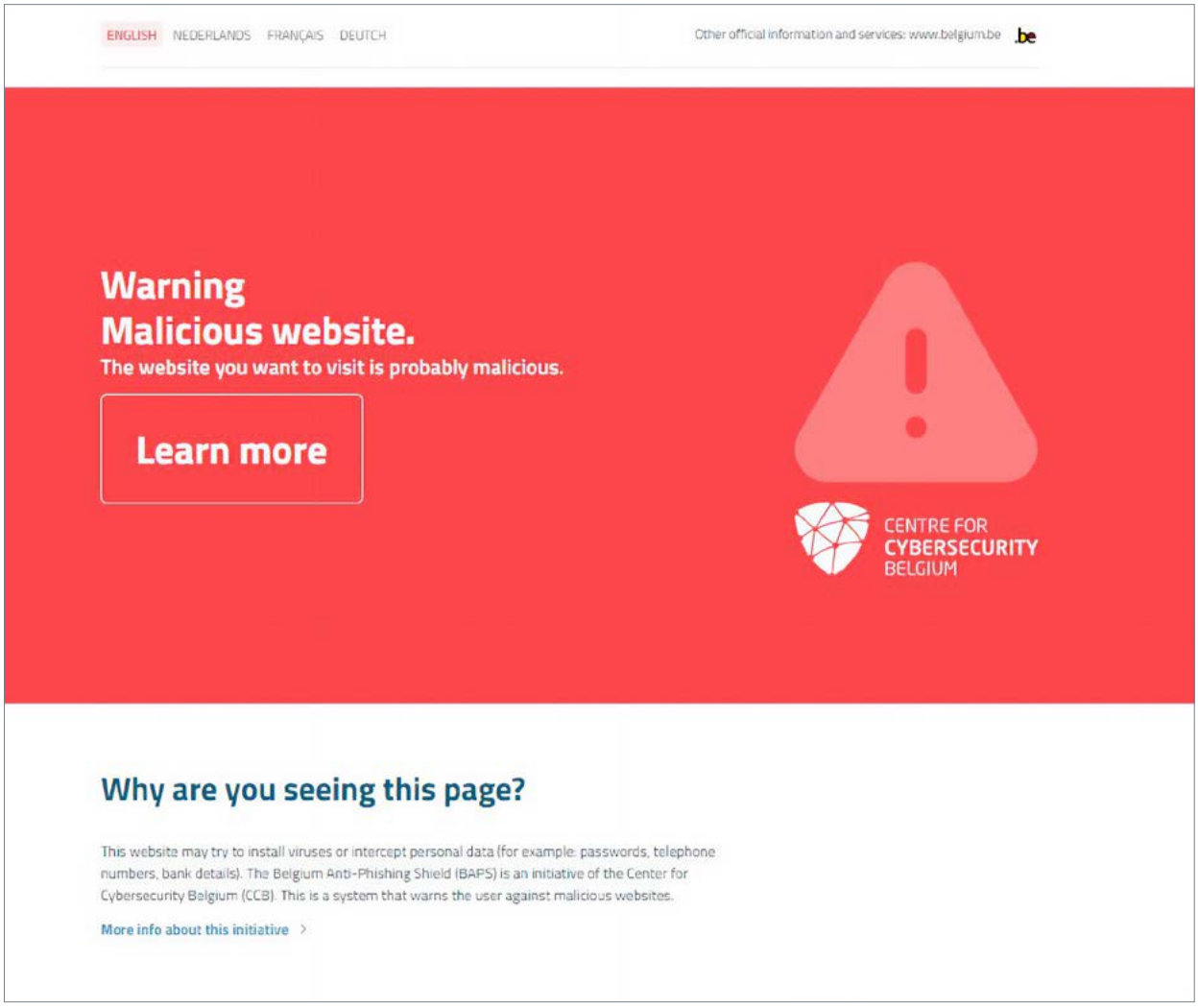
1 https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/agent-tesla
https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/agent-tesla-malware

SAFEONWEB UND DER BELGISCHE ANTI-PHISHING-SCHUTZSCHILD

Um die belgische Öffentlichkeit anhaltend online sicherer zu machen und besser vor Cyber-Bedrohungen und -Schwachstellen zu schützen, bietet das ZCB den Dienst Safeonweb an. Safeonweb präsentiert die nötigen aktuellen Informationen und spezielle Kampagnen zu bestimmten Themen. In der belgischen Strategie zur Cybersicherheit 2.0 heißt es: „Das Internet gehört allen und ist für alle da. Auch seine Sicherheit ist eine gemeinsame Aufgabe. Folglich ist die Bevölkerung dazu aufgefordert, die Sicherheit zu fördern."

Safeonweb ist ein hervorragendes Beispiel für die konstruktive Zusammenarbeit zwischen öffentlichen Institutionen und den Bürgern sowie dem privaten Sektor, bietet es doch die Möglichkeit, Phishing zu bekämpfen, indem man verdächtige Links und Nachrichten an suspicious@safeonweb.be sendet. Auf der Grundlage dieses Dienstes hat das ZCB innerhalb des „Active Cyber Protection"-Ansatzes die Initiative „Belgian Anti-Phishing Shield" (BAPS) initiiert. Sie warnt belgische Internetnutzer vor gefährlichen Websites (bspw. für Phishing-Angriffe) und postet die gemeldeten, verdächtigen Links auf unsere Warnseite.

In den ersten drei Quartalen 2023 gingen auf suspicious@safeonweb über 7 Mio. Nachrichten (7.207.167) ein, während es im gleichen Zeitraum des Vorjahres nur knapp 4 Mio. (3.954.641 im Jahr 2022) waren. Dies zeigt die große Reichweite und Akzeptanz unter den Bürgern. Dank dieser Meldungen konnte das ZCB 633.361 eindeutige URLs und 163.736 eindeutige Domains umleiten, die als bösartig gekennzeichnet waren. Zwischen Januar und September 2023 machte das BAPS-System 5.736.374 Mal belgische Bürger darauf aufmerksam, dass sie im Begriff waren, bösartige Websites oder Server zu besuchen.

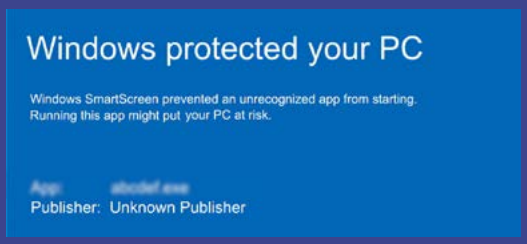


Quelle: https://baps.safeonweb.be/

Belgian Anti-Phishing Shield

Funktion

1. Das ZCB erhält seine Daten über potenziell bösartige Websites, indem Internetnutzer verdächtige Nachrichten an suspicious@safeonweb.be weiterleiten.
2. Aus den verdächtigen Nachrichten werden Anhänge und Links extrahiert, aus Screenshots und QR-Codes gewinnt das ZCB die URLs.
3. Das ZCB analysiert dann die Adresse/den Link/den Anhang. Handelt es sich laut Analyse um eine schädliche Website, wird eine Liste der bösartigen Sites an unsere Partner weitergeleitet (ISPs, Google Safe Browsing, Microsoft SmartScreen usw.).



4. Klickt ein User auf einen Link zu einer bösartigen Website, vergleicht der Internet-Provider die DNS-Anfrage mit der Liste bösartiger Websites.
5. Der Benutzer gelangt dann auf eine Warnseite, um nicht auf der schädlichen Site zu landen.

Aktiver Cyber-Schutz – Spear-Warnungen

Anfang 2021 führte das Zentrum für Cybersicherheit, Belgien (ZCB) das Konzept der Spear-Warnung ein. Spear-Warnungen sollen vor allem Unternehmen und Einzelpersonen rechtzeitig über eine Cyber-Bedrohung informieren, damit die Betroffenen zeitnah handeln und Cyberangriffe verhindern können. Das Wortspiel „Spear-Warnung" (SW) bezieht sich auf „Spear Phishing". Mit diesem Modus Operandi senden Cyberkriminelle überaus gezielte Phishing-E-Mails an potenzielle Opfer, meist um sie dazu zu verleiten, persönliche Angaben preiszugeben. Spear-Warnungen gehören auch zum Konzept des aktiven Schutzes vor Cyberangriffen (Active Cyber Protection, ACP), das nun als Begriff in die EU-Richtlinie NIS2 aufgenommen wurde.

Durch das Konzept der Spear-Warnungen sollen Internetnutzer (Unternehmen oder Endnutzer) „aktiv" per E-Mail, Brief oder sogar telefonisch kontaktiert werden (die schnellste und effizienteste Kontaktmethode bei bevorstehenden Bedrohungen), um sie rechtzeitig und proaktiv über Cyber-Bedrohungen oder Schwachstellen zu unterrichten. Dass diese persönliche Nachricht direkt vom ZCB kommt, müsste im Prinzip noch mehr Aufmerksamkeit erregen.

VERHINDERN, DASS DER BEDROHUNGSAKTEUR SEINE AKTIONEN DURCHFÜHREN KANN

Durch die versandten Spear-Warnungen will das ZCB den Bedrohungsakteur daran hindern, seine Ziele zu erreichen (Systeme kompromittieren bzw. unzugänglich machen, Daten entschleusen o.ä.).

Die Spear-Warnungen des ZCB gehören oft zu langfristigen Kampagnen und beziehen sich meist auf:

- anfällige, mit dem Internet verbundene IT-Systeme, die Cyberkriminelle leicht kompromittieren/angreifen/ausnutzen können
- kritische Schwachstellen, die belgische Organisationen beeinträchtigen könnten
- Lecks von Anmeldedaten und unbefugte Zugriffe auf belgische Unternehmen, die in Cybercrime-Foren angeboten werden und weiteren Spear-Phishing-Kampagnen dienen können.
- Systeme, die mit für einen größeren Cyberangriff verwendbarer Malware infiziert sind. Das ist der Fall, wenn belgische Infrastrukturen mit als Wegbereiter für Ransomware-Angriffe verwendeter Malware infiziert sind
- verdächtige Zertifikate und Domainregistrierungen
- Benachrichtigungen über kompromittierte Assets.

DAS VERFAHREN

Zu den wichtigsten Teilen des Konzepts der Spear-Warnung, der zu den satzungsgemäßen Aufgaben des ZCB zählt, gehört es, für den gesamten belgischen Cyberspace Cyber-Bedrohungen und Schwachstellen zu erkennen. Zur Erfassung nutzt das ZCB verschiedene Techniken und Verfahren: technische Lösungen, (offene und kommerzielle) Informationsquellen sowie Partnerschaften. Das ZCB hat das nationales Projekt „Schwachstellenmanagement" eingeführt, um Schwachstellen zu priorisieren und um zu bestimmen, welche anhand von Warnungen zu veröffentlichen sind. Nachdem eine Schwachstelle ausgewählt wurde, beginnt der Prozess für die Spear-Warnung, über den die betroffenen Organisationen zu folgenden Punkten informiert werden:

- Risiko- und Auswirkungsanalyse der Schwachstelle,
- empfohlene Maßnahmen,
- aktive Ausnutzung durch Cyberkriminelle.

Eine andere Version dieses Konzepts besteht darin, automatisierte Nachrichten über Schwachstellen und Infektionen der IT-Infrastruktur an Organisationen zu senden, die für diesen Dienst registriert sind und den IP-Bereich mit dem ZCB teilen, so dass hierbei die IP-Identifizierung entfällt. Danke des Projekts safeonweb@work kann sich jedes Unternehmen für diesen Dienst registrieren.

Manchmal, bspw. bei umfangreicheren Zwischenfällen, fließen Spear-Warnungen in ein größeres Eskalationsverfahren ein. Diese umfasst außerdem Pressemitteilungen, die Veröffentlichung von Hinweisen auf den Websites, den Versand von Warnungen via Frühwarnsystem und sogar die Organisation spezieller Webinare. Spear-Warnungen fördern weitgehend den offiziellen Auftrag des ZCB, Belgien zu einem der am wenigsten gefährdeten Cyberräume in der EU zu machen. Organisationen besser zu informieren, heißt, ihre Cybersicherheit deutlich zu erhöhen. So sind ihre IT-Systeme weniger anfällig für die Angriffe von Cyberkriminellen, die stets den Weg des geringsten Widerstands gehen.

Wenn Organisationen vom ZCB eine Spear-Warnung erhalten, melden sie oft zurück, dass sie sich des Sicherheitsproblems, der Schwachstelle, der Datenverletzung oder der Infektion ihrer IT-Systeme gar nicht bewusst waren. Als das Opfer vom ZCB eine Spear-Warnung erhielt, lief der Angriff mitunter gerade oder wurde umfassend vorbereitet. So konnte das Opfer noch rechtzeitig reagieren.

Das Zentrum für Cybersicherheit, Belgien (ZCB) ist stolz darauf, dass es mit seinem bahnbrechenden Projekt „Spear-Warnung“ den Publica Award in der Kategorie „Security and Safety“ erringen konnte. Mit den Publica Awards werden herausragende öffentliche Projekte gewürdigt. Darum ist das ZCB hocherfreut, diesen prestigeträchtigen Wettbewerb am 16. November 2023 in Brüssel gewonnen zu haben.

„Wir sind sehr froh und dankbar für die Anerkennung, die wir durch die Publica Awards erhalten haben. Diese Auszeichnung bestätigt die Wirkung und das Innovationspotential des Projekts „Spear-Warnung“. Sie zeigt, dass proaktive Maßnahmen wie diese entscheidend sind, um die digitalen Widerstandsfähigkeit unserer Gesellschaft zu stärken. Wir werden uns auch künftig dafür engagieren, die Cybersicherheit zu verbessern und unsere Bürger und Unternehmen vor den sich ständig weiterentwickelnden Bedrohungen zu schützen.“

Miguel De Bruycker, Generaldirektor des ZCB

SPEAR-WARNUNG – HAFNIUM: DER ERSTE GROSSE ANWENDUNGSFALL

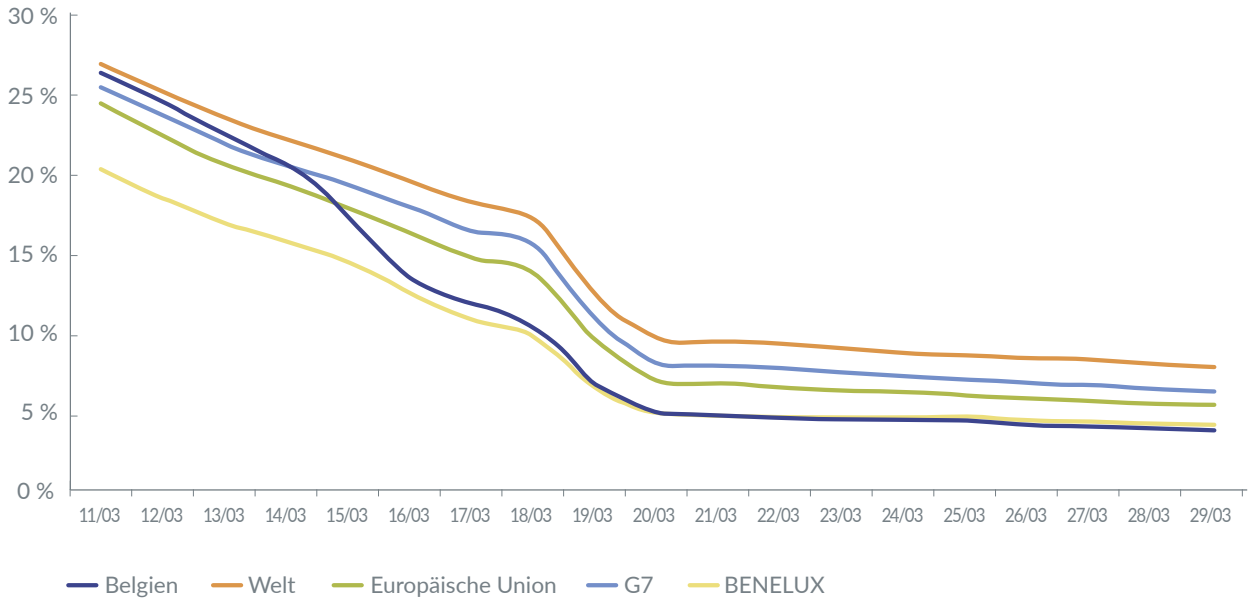
Hafnium. Dieser Akteur nutzte eine Sicherheitslücke in Microsoft Exchange. Damals waren viele belgische Exchange-Installationen anfällig und Angriffen aus dem Internet ausgesetzt. Belgien hatte prozentual die meisten angreifbaren Microsoft Exchange-Systeme. Die Einführung der Spear-Warnungen markierte jedoch den Beginn eines positiven Wandels: Durch die erste Spear-Warnung an potenzielle Opfer sank die Zahl der gefährdeten Systeme spürbar.

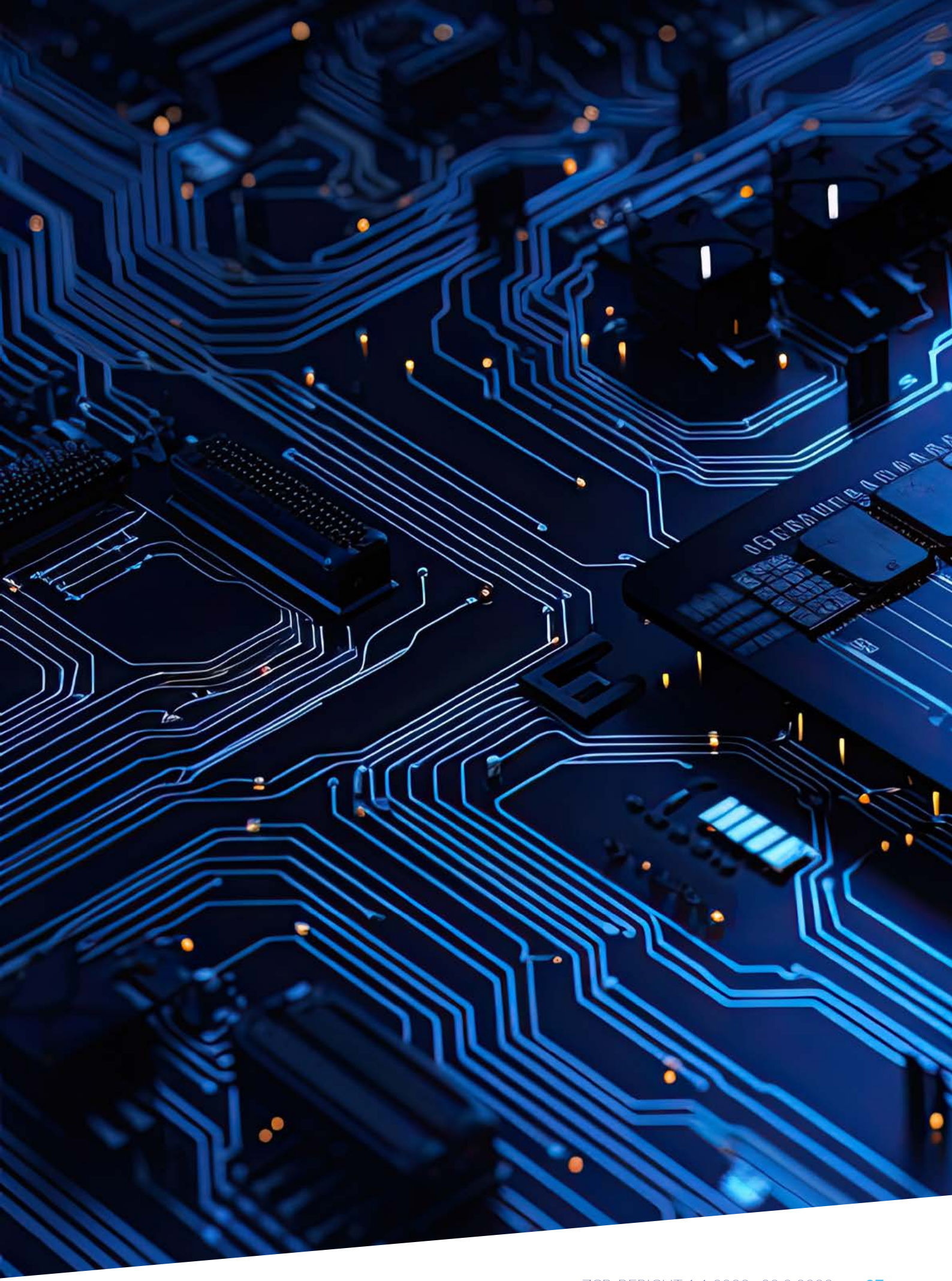
Die zweite Spear-Warnung verbesserte die Lage weiter und brachte schließlich eine bemerkenswerte Wende mit sich: Belgien wandelt sich vom Land mit den meisten gefährdeten Systemen zum Land mit den wenigsten, was belegt, wie wirksam das Spear-Warnung ist.

- Planung und Leitung: Formulierung eines strategischen Plans und Vorbereitung auf die genaue Ermittlung der Schwachstellen, die sich am stärksten auf den belgischen Cyberspace auswirken.
- Erfassung: Umfassender Scan, um in ganz Belgien verwundbare Systeme aufzuspüren.
- Verarbeitung und Nutzung: Identifizierung der Eigentümer dieser anfälligen Systeme.
- Analyse und Produktion: Initiierung von Kommunikation, um die Systembesitzer über ihre Schwachstellen zu informieren.
- Verbreitung: Nach einer bestimmten Zeit erneute Überprüfung, um festzustellen, ob die Systeme weiterhin anfällig sind.
- Rückmeldung: Ggf. Versand von Erinnerungsmeldungen an die Systemeigentümer.

2021

Benachrichtigungen wurden an 1259 gefährdete Organisationen versandt.
Benachrichtigungen wurden an 355 betroffene Organisationen versandt.
Danach wurden mehrere Erinnerungen versandt.





KRITISCHE SCHWACHSTELLEN

Kritische Schwachstellen, welche die Landschaft der Cyberbedrohungen zwischen Januar und September 2023 verschärft haben

Bedrohungsakteure mit unterschiedlichen Interessen beuten für ihre Angriffe kritische Schwachstellen aus. Sie nutzen Zero-Day-Schwachstellen stets schneller zu ihrem Vorteil aus, als die Organisation ihre Maßnahmen zur Cybersicherheit aktualisieren kann. Wie ferner beobachtet wurde, profitieren Bedrohungsakteure weiter erfolgreich von bereits bestehenden Schwachstellen in ungepatchter Software, wenn Unternehmen laxe oder unzureichende Sicherheitsmaßnahmen ergreifen.

CVEs steht für „Common Vulnerability Exposures“ (Häufige Schwachstellen). Immer dann, wenn Sicherheitsforscher oder Organisationen neue Schwachstellen finden, fügen sie diese der von der MITRE Corporation gepflegten CVE-Liste hinzu. Der Schwachstelle wird eine CVE-ID zugewiesen, die Identifizierung und Schutz erleichtert.

Fünf der kritischsten Schwachstellen, die Cyber-Bedrohungsakteure auch 2023 ausnutzten, waren:

CVE-2023-0669

CVE-2023-0669, eine Zero-Day-Schwachstelle im Managed File Transfer-Tool (MFT) GoAnywhere von Fortra (diese Plattform, zentralisiert die Kontrolle über interne und externe Dateiübertragungen), wurde aktiv von Bedrohungsakteuren, einschließlich Ransomware-Gruppen, ausgenutzt. Die Schwachstelle ermöglicht eine sog. Remotecode-Ausführung (RCE), was ggf. zur Kompromittierung der betroffenen Systeme, zu umfangreichen Datensicherheitsverletzungen und finanzieller Erpressung führen kann. Mit der verwalteten Dateiübertragungs-Software eines Opfers lassen sich dann andere Opfer infizieren, indem bösartige Dateien versendet werden. Gelingt das Eindringen, kann die Lieferkette ernsthaft beschädigt werden. Die Ransomware-Gruppe Clop visierte speziell ca. 490.000 Personen an, deren persönliche Daten durch diese ausgenutzte Sicherheitslücke kompromittiert wurden.

CVE-2023-2868

Durch die Sicherheitslücke CVE-2023-2868 in den Barracuda Email Security Gateway-Geräten lassen sich Benutzereingaben als Systembefehl ausführen, wodurch Angreifer Systembefehle mit erheblichen Privilegien aus der Ferne manipulieren können. Diese, von Mandiant als UNC4841 identifizierte Schwachstelle wurde von Oktober 2022 bis Mai 2023 von einem hochqualifizierten Angreifer in weitreichenden Kampagnen ausgenutzt. Fast ein Drittel der betroffenen Organisationen waren Regierungsbehörden in allen Regionen. Wie Mandiant schlussfolgerte, handelte es sich um eine Aktivität mit Bezug zu China und, dem beobachteten Zielprofil zufolge, u. U. um eine Spionagekampagne.

CVE-2023-34362

CVE-2023-34362 ist eine kritische Zero-Day-Schwachstelle in MOVEit Transfer, einer Lösung zur Dateiübertragung. Diese Schwachstelle ermöglicht potenziell erweiterte Privilegien und unbefugten Zugriff auf die Umgebung, wodurch die Ransomware-Gruppe Cl0p en masse Daten von Unternehmen stehlen konnte. Die Betreiber hinter der Ransomware Cl0p behaupteten, sie hätten auf die Daten „Hunderter“ Unternehmen zugreifen können, die alle die Software MOVEit verwenden, und sie begannen, die Opfer auf ihrer Data Leak Site (DLS) aufzuführen.

CVE-2023-23397

um eine kritische Erhöhung der Sicherheitsanfälligkeit in allen unterstützten Versionen des E-Mail-Clients von Microsoft Outlook für Windows. Durch diese Schwachstelle konnten Angreifer Authentifizierungsschritte umgehen und so leichter unbefugt auf vertrauliche Daten zugreifen und innerhalb von Organisationen die Identitäten von Benutzern stehlen.

CVE-2023-38831

CVE-2023-38831 ist eine Sicherheitslücke im Archivierungstool WinRAR für Windows. Mit ihr können Angreifer jeden beliebigen Code ausführen, sobald ein Benutzer eine nicht infizierte Datei in einem ZIP-Archiv betrachten will. Cyberkriminelle Organisationen und staatlich geförderte Bedrohungsakteure (APT 28, Sandworm, DarkPink, APT40 usw.) nutzten diese Anfälligkeit, um großflächig Remote-Codes für illegale Zwecke zu einzusetzen.

Das ZCB veröffentlicht fortlaufend technische Hinweise, in denen es vor möglichem Missbrauch von Sicherheitslücken warnt und die korrekten Schritte zur Risikominderung, einschließlich Patches, empfiehlt.

Bei kritischen Schwachstellen, die ein hohes Risiko für Belgien darstellen, gibt das ZCB Speerwarnungen heraus, in denen belgische Organisationen direkt über die Bedrohung und die dringende Notwendigkeit von Patches informiert werden Dieser proaktive Ansatz trägt dazu bei, belgische Opfer zu schützen und drohende Angriffe, wie z.B. Ransomware-Angriffe mit ausnutzbaren Schwachstellen, erfolgreich zu verhindern.

Überblick über die belgischen Cyber-Metriken im Jahr 2023

2023	Q1	Q2	Q3
PHISHING			
Empfangene E-Mails	2.695.345	2.381.106	2.130.716
Einzigartige URLs, die als bösartig eingestuft wurden:	186.792	237.740	211.031
Einzigartige Domains, die als bösartig gekennzeichnet wurden:	12.382	93.481	59.727
BAPS			
Anzahl der Zugriffe auf die Landing-Page	2.031.888	2.464.489	1.239.997
WARNUNGEN			
Technische Hinweise veröffentlicht auf www.cert.be	35	39	41
Technische Tweets	67	67	79
Spear-phishing-warnungen			
Automatisch verarbeitet	1.193	863	1.221
Manuell verarbeitet	1.653	946	1.255
Gesamt	2.846	1.809	2.476
ZWISCHENFÄLLE			
Ransomware (gemeldet)	28	20	31
Denial of Service	6	10	5
KOMMUNIKATION			
Websites			
Sitzungen www.safeonweb.be	674.243	615.379	450.365
Nachrichten Safeonweb	22	19	16
ZCB-Veranstaltungen			
Connect und Share- Veranstaltungen	2	2	0

BELGISCHEN CYBER-METRIKEN IM JAHR 2023

Bewusstsein schärfen und eine starke Gemeinschaft von Experten für Cybersicherheit aufbauen

Im Rahmen der ZCB-Initiative Connect und Share, die darauf abzielt, das Bewusstsein zu schärfen und eine Gemeinschaft aufzubauen, indem Experten für Cybersicherheit zusammengebracht werden, um ihre Gedanken zu den verschiedenen Cyber-Bedrohungen in Belgien und auf der ganzen Welt auszutauschen, wurden im Jahr 2023 mehrere Veranstaltungen organisiert, die gut besucht waren, live oder hybrid:

12. JANUAR 2023 – VIERTELJÄHRLICHE VERANSTALTUNG ZUM CYBER-BEDROHUNGSBERICHT Q4 2022

Die Experten des ZCB untersuchten gemeinsam mit Experten von Cybersicherheitsunternehmen die Cyber-Bedrohung mit Schwerpunkt auf Cloud-Sicherheit und dem Energiesektor.

19. JANUAR 2023 – ICS RAPID RESPONSE-VERANSTALTUNG

Die Veranstaltung wurde von SANS und dem ZCB organisiert und bot sowohl erfahrenen ICS-Spezialisten als auch Nicht-ICS-Spezialisten die Möglichkeit, Vorträge zu einer Reihe von Themen zu hören, darunter: Five Critical Controls, Defensible Architecture, OT Visibility, Threat Intelligence und OSINT.

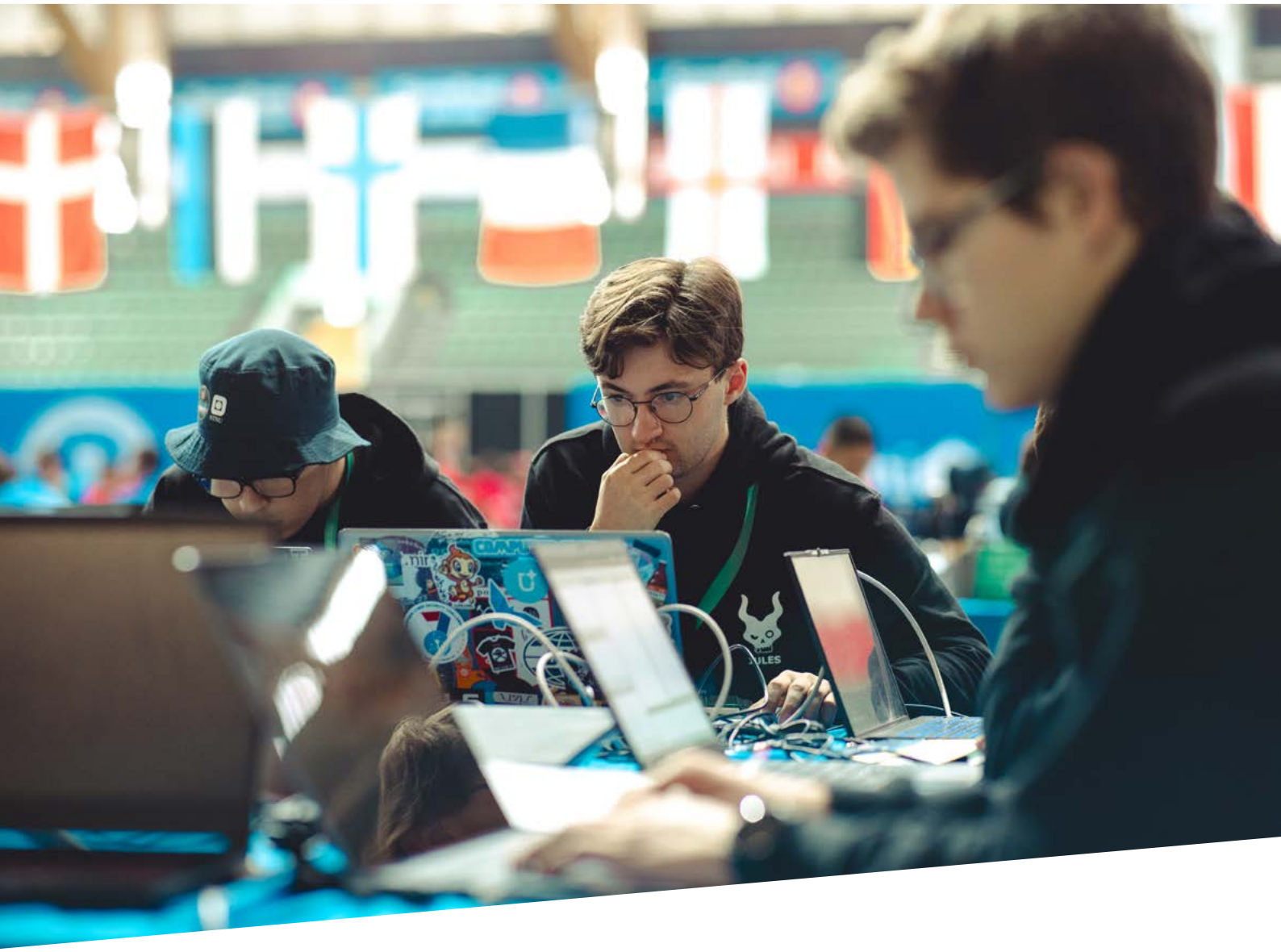
20. APRIL 2023 – VERANSTALTUNG ZUM VIERTELJÄHRLICHEN CYBER-BEDROHUNGSBERICHT Q1 2023

Das ZCB organisierte eine neue Veranstaltung, um die Beobachtungen aus dem ersten Quartal 2023 zu überprüfen und Themen wie DDoS-Angriffe, Wi-Fi-Sicherheit, Malware und die neuesten Beobachtungen zu Spionage und Hacktivismus zu diskutieren. Es war auch eine Gelegenheit für Experten, ihre neuesten Forschungsergebnisse vorzustellen.

25. MAI 2023 – 11. EU MITRE ATTUNDCK® GEMEINSCHAFTSWORKSHOP

Das ZCB organisierte gemeinsam mit MITRE Engenuity eine hybride Veranstaltung, um die neuesten Erkenntnisse über die Nutzung des ATTundCK®-Frameworks zur Verbesserung der bedrohungsbasierten Verteidigung zu präsentieren. Experten des ZCB, MITRE Engenuity und andere Entwickler von Systemen und Tools, die das ATTundCK® Framework unterstützen, hielten während der Veranstaltung Vorträge.

CONNECT UND SHARE-VERANSTALTUNGEN



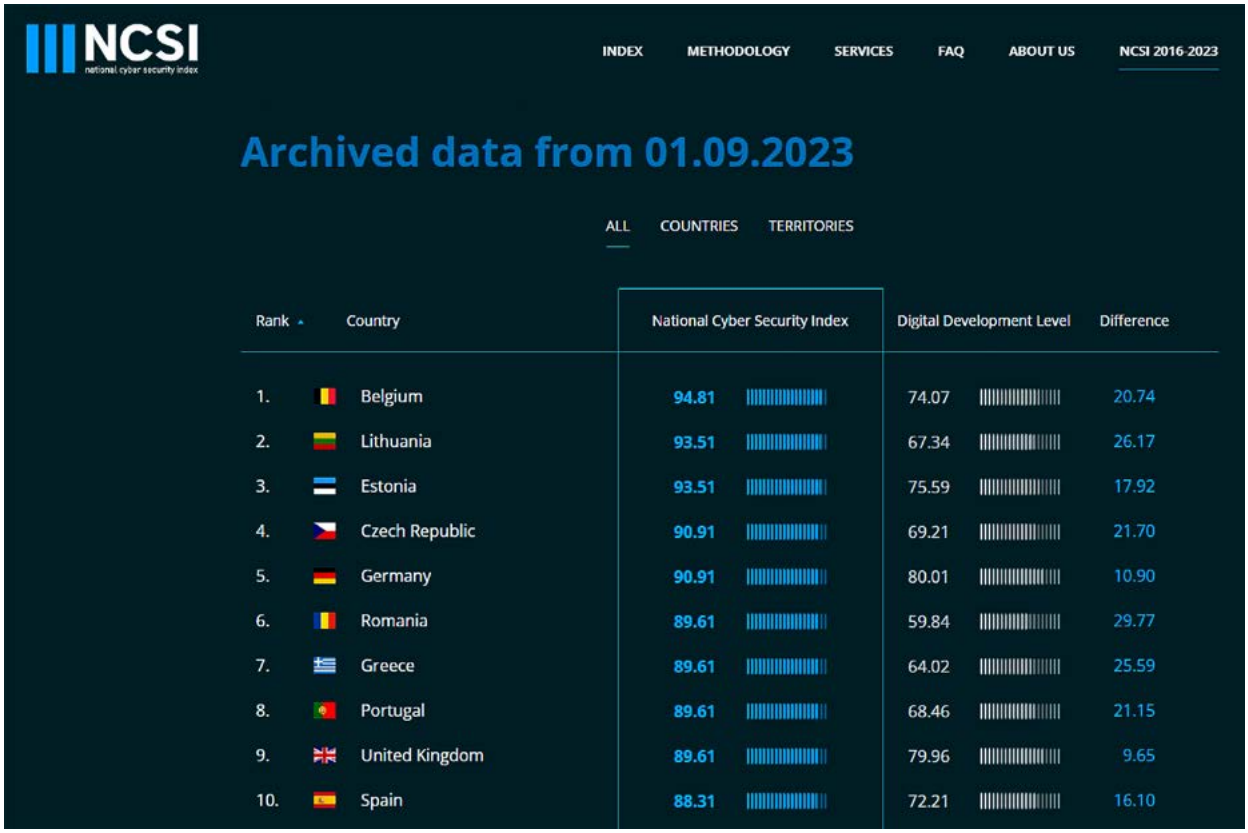
BELGIEN IN DER WELT

Belgisches Cybersicherheits-Ranking

Die insgesamt sehr gute Cybersicherheitslage Belgiens und die Bereitschaft, Cyberbedrohungen zu verhindern und Cyber-Zwischenfälle zu bewältigen, die nationale Organisationen betreffen, spiegelt sich auch im Cybersicherheits-Ranking Belgiens wider.

Im Jahr 2023 erreichte Belgien den ersten Platz in der Welt nach dem Nationalen Cybersicherheitsindex, dem globalen Live-Index, der die Bereitschaft von Ländern misst, Cyberbedrohungen zu verhindern und Cyber-Zwischenfälle zu bewältigen.

Der NCSI Score zeigt den Prozentsatz, den das Land vom Maximalwert der berücksichtigten Indikatoren auf der Grundlage der verwendeten Methodik erhalten hat.



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

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

Belgiens Cyber-Champions: Die Red Daemons auf der ECSC 2023

Im Oktober 2023 machte sich das belgische Team Red Daemons auf den Weg nach Hamar, Norwegen, um Belgien bei der 8. jährlichen European Cyber Security Challenge (ECSC) stolz zu vertreten. Im Wettbewerb mit Teams aus 29 anderen europäischen Ländern stellten sich die Red Daemons drei Tage lang intensiven sicherheitsrelevanten Herausforderungen und sammelten Punkte für ihre Lösungen. Dies war die sechste Teilnahme Belgiens an dieser prestigeträchtigen internationalen Veranstaltung.

Die zehn Cyber-Talente wurden traditionell aus den siegreichen Teams der nationalen Cyber Security Challenge Belgium (CSCBE) ausgewählt, die bereits im März dieses Jahres stattfand. In den vergangenen sieben Jahren hat die „Cyber Security Challenge Belgium" das Interesse tausender belgischer Studenten geweckt, die ihre Fähigkeiten testen, lernen und sich in der aufregenden Welt der Cybersicherheit engagieren wollten.

Die Nachfrage nach Experten für Cybersicherheit in Unternehmen, Organisationen, Sicherheits- und Polizeibehörden steigt stetig an. Die Teilnahme der belgischen Red Daemons wird durch eine Zusammenarbeit zwischen dem ZCB und NVISO ermöglicht. Diese Partner sind für die Organisation der Veranstaltung, die Bereitstellung von Sponsorengeldern und die Durchführung der jährlichen Vorbereitungsworkshops verantwortlich.

Der nationale Wettbewerb CSCBE wird jährlich von der NVISO organisiert und wird ebenfalls vom ZCB unterstützt.

Veranstaltungen wie die ECSC und die CSCBE spielen eine entscheidende Rolle, wenn es darum geht, junge Menschen zu inspirieren, eine dynamische Karriere im Bereich der Cybersicherheit zu verfolgen.

Folgen Sie den Belgian Red Daemons auf den sozialen Medien:

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

CYBER SPOTLIGHT: KI UND CYBERSICHERHEIT

Cyber Spotlight: KI und Cybersicherheit

Hinter dem aktuellen Hype um „KI“ in der Tech-Welt verbirgt sich ein echter Trend, der den Einsatz von KI in allen Bereichen vorsieht. Die Cybersicherheit bildet dabei keine Ausnahme und ist aufgrund ihrer Nähe zur Innovation und ihrer Querschnittsfunktion für viele Technologien ein erstklassiges Thema für KI-Anwendungen. Um die Wechselwirkungen zwischen diesen beiden Themen besser zu verstehen, lassen sich **3 Hauptbereiche der Konvergenz** wie folgt definieren:

- KI „im Dienste“ der Cybersicherheit: Wie können Cybersicherheitsexperten KI nutzen, um die Verteidigung ihrer Systeme zu verbessern? (z.B. Malware-Analyse und Angriffserkennung)
- KI „gegen“ die Cybersicherheit: Wie kann ein Hacker die Vorteile der KI nutzen, um seine Techniken und Taktiken zu verbessern? (z.B. Deepfake und Entdeckung von Schwachstellen)
- Die Sicherheit von KI-Anwendungen: Haben KI-Anwendungen Schwachstellen und wie kann man sie schützen? (z.B. Data Poisoning und Modellumgehung)

Diese verschiedenen Ansätze sind vielfältig und in ständiger Entwicklung, aber wir werden unser Bestes tun, um sie in einer Reihe von Artikeln zu behandeln. Der erste wird sich mit dem trendigen Einsatz von Chatbots und LLMs befassen, wir haben uns entschieden, uns auf den dritten Ansatz, die Sicherheit der KI, zu konzentrieren, und zwar aus der Sicht eines durchschnittlichen Benutzers.

ALLGEMEINE ÜBERLEGUNGEN ZUR SICHEREN UND VERANTWORTUNGSVOLLEN NUTZUNG VON KONVERSATIONELLEN TECHNOLOGIEN DER KÜNSTLICHEN INTELLIGENZ (KI)

Konversationsbasierte KI-Technologien wie ChatGPT und Bard, die auf großen Sprachmodellen (LLMs) basieren, erfreuen sich zunehmender Beliebtheit, und viele Belgier haben sie zur Verbesserung ihrer Produktivität eingesetzt. Vor diesem Hintergrund hat das ZCB erkannt, wie wichtig es ist, die mit diesen Technologien verbundenen Probleme klar zu definieren.

Wir möchten hier eine erste Liste von „guten Reflexen" vorstellen, die für den sicheren und verantwortungsvollen Einsatz dieser Technologien angenommen werden sollten.

Vorab: Auch wenn es dem gesunden Menschenverstand entspricht, ist es wichtig, den Antworten von Gesprächsagenten niemals blind zu vertrauen und immer einen kritischen Geist zu bewahren. Da die Antworten dieser Tools unvollkommen sind, sollten sie immer überprüft und korrigiert werden. Außerdem fehlt den Gesprächsagenten im Allgemeinen das logische Denken. Sie sind „probabilistisch" in dem Sinne, dass sie darauf trainiert sind, Wortfolgen mit einem hohen Maß an Wahrscheinlichkeit zu generieren.

Darüber hinaus muss den folgenden Aspekten besondere Aufmerksamkeit gewidmet werden:

- Schützen Sie vertrauliche Daten: Vermeiden Sie die Weitergabe vertraulicher Informationen, da KI-Agenten diese Daten speichern und wiederverwenden können. Deaktivieren Sie die Aufzeichnung des Gesprächsverlaufs wann immer möglich.
- Fehlererkennung: Konversationelle KI-Agenten machen Fehler, also betrauen Sie sie nur mit Aufgaben, für die Sie über ausreichende Kenntnisse verfügen (damit Sie die Ergebnisse überprüfen und kontrollieren können).
- Faktenüberprüfung: Überprüfen Sie unabhängig die Fakten (fact-checking), da in den von konversationellen KI-Agenten vorgeschlagenen Ergebnissen oft Quellen ausgelassen werden.
- Voreingenommenheit durch Automatisierung: Wenn man sie zu sehr einsetzt, kann man die von KI-Agenten generierten Ergebnisse bevorzugen und ihnen übermäßiges Vertrauen schenken, obwohl, wie wir gesehen haben, Menschen in vielen Bereichen kompetenter sind.
- Beschränkungen und Vorurteile: KI-Agenten können mit Vorurteilen behaftet sein und sind in ihrem Wissen durch ihre Trainingsdaten eingeschränkt. Konfrontieren Sie sie mit verschiedenen Quellen, um einen objektiven und vollständigen Kontext zu erhalten.
- Transparenz: Bevorzugen Sie den transparenten Einsatz von konversationellen KI-Agenten. Versuchen Sie nicht, ihren Einsatz zu verbergen, sondern berichten Sie darüber, um das Vertrauen und die Verantwortung zu stärken.
- Urheberrecht: Die Antworten von KI-Agenten können das Urheberrecht verletzen. Seien Sie daher vorsichtig, wenn Sie sie für akademische oder kommerzielle Zwecke verwenden.
- Menschlichkeit: Vergessen Sie nicht, dass konversationelle KI-Agenten kein Bewusstsein und keine Emotionen haben. Hüten Sie sich vor emotionaler Manipulation.

Wenn Sie all diese Aspekte berücksichtigen, sind wir davon überzeugt, dass Benutzer konversationelle KI-Agenten effektiv nutzen können, wenn sie ihre Grenzen kennen und verantwortungsbewusst handeln.

WER SIND WIR?

Wer sind wir?

Das „Zentrum für Cybersicherheit, Belgien (ZCB)“ ist die nationale Behörde für Cybersicherheit in Belgien. Es wurde per Königlichen Erlass vom 10. Oktober 2014 gegründet und untersteht dem Premierminister.

Durch einen optimalen Informationsaustausch können sich Unternehmen, die Regierung, Anbieter von wichtigen Dienstleistungen und die Bevölkerung angemessen schützen.

Das ZCB überwacht, koordiniert und kontrolliert auch die Anwendung der belgischen Strategie zur Cybersicherheit, die vom Nationalen Sicherheitsrat des Landes im Jahr 2021 verabschiedet wurde. Seine Aufgabe ist es, Belgien bis 2025 zu einem der am wenigsten gefährdeten Länder in Europa in Bezug auf Cybersicherheit zu machen.

Das ZCB spielt eine Schlüsselrolle dabei, Belgien bei der Erreichung dieses Ziels zu unterstützen, indem es seine Aufgaben wahrnimmt, wie z.B. die Information und Sensibilisierung für die wichtigsten Cyber-Bedrohungen und wie man sich dagegen schützen kann.

Folgen Sie dem „Zentrum für Cybersicherheit, Belgien“ in den sozialen Medien und auf unserer Website:

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

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

Gesetzliche Hinterlegung
D/2024/14828/004

Haftungsausschluss

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

Das ZCB übernimmt keine Verantwortung für den Inhalt dieses Dokuments.

Die bereitgestellten Informationen:

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