SICHER SURFEN WÄHREND DER WAHLKAMPAGNE

Empfehlungen für einen Wahlkampf im Zeichen der Cybersicherheit

MÄRZ 2024

CENTRE FOR CYBERSECURITY BELGIUM
ADIV - SGRS
VSSE veiligheid van de staat sûreté de l'état
.be

SICHER SURFEN WÄHREND DER WAHLKAMPAGNE

Empfehlungen für einen Wahlkampf im Zeichen der Cybersicherheit

Der Leitfaden „Sicher Surfen während der Wahlkampagne“ enthält Empfehlungen, wie Sie die verschiedenen digitalen Werkzeuge, mit denen Sie täglich arbeiten, sicherer verwenden können.

Wahlen sind der Grundpfeiler des demokratischen Prozesses. Terroristische Gruppen, Kriminelle oder politisierte Instanzen können versuchen, das Ergebnis zu beeinflussen. Politische Parteien und ihre Kandidaten stellen daher ein wichtiges potenzielles Ziel dar. Die Agentur der Europäischen Union für Cybersicherheit (ENISA)[1] hat die störenden Auswirkungen von Chatbots und der Manipulation von Informationen durch künstliche Intelligenz (KI) aufgezeigt. Sie registrierte zwischen Juli 2022 und Juni 2023 rund 2.580 Vorfälle, deren Ziel oftmals öffentliche Verwaltungen waren.

Mit diesem Leitfaden möchten wir Ihnen alle notwendigen Informationen an die Hand geben, um Ihre Kenntnisse im Bereich der Cybersicherheit zu verbessern, die Gefahren im Zusammenhang mit der Cybersicherheit einzudämmen und digitale Schwachstellen zu verringern.

Die meisten dieser Tipps und Tricks werden Ihnen selbstverständlich erscheinen und vielleicht bereits von Ihnen angewendet. Falls nicht, hilft Ihnen dieses Dokument dabei, Ihre Interessen und Ihre digitale Sicherheit besser zu schützen. Darüber hinaus ist es wichtig, dass sich auch Ihre Mitmenschen gründlich schützen. Teilen Sie diese Tipps und Tricks daher mit Ihrer Familie und Ihren Freunden!

Der Leitfaden „Sicher Surfen während der Wahlkampagne“ ist eine Initiative der Staatssicherheit (VSSE), des Zentrums für Cybersicherheit Belgien (ZCB) und des Allgemeinen Nachrichten- und Sicherheitsdienstes (ANSD). Jede Behörde hat dabei ihr spezifisches Fachwissen eingebracht und so die Erstellung dieses Leitfadens ermöglicht.

Brüssel, März 2024
Mit freundlichen Grüßen,

Miguel DE BRUYCKER
Generaldirektor des Zentrums für Cybersicherheit Belgien

Francisca BOSTYN
Stellvertretende Generaladministratorin der Staatssicherheit

Stéphane DUTRON
Generalmajor und Leiter des Allgemeinen Nachrichten- und Sicherheitsdienstes

1 : ENISA Threat Landscape 2023, *Impact of social engineering & information manipulation campaigns.* Siehe auch Kapitel 4 „Addressing FIMI During Electoral Processes“ im *2nd EEAS Report on Foreign Information Manipulation and Interference Threats* (Januar 2024).

INHALTSVERZEICHNIS

1

ICH ERKENNE VERDÄCHTIGE NACHRICHTEN

DER BEGRIFF „PHISHING“ BEZEICHNET ONLINE-BETRÜGEREIEN MITHILFE VON BETRÜGERISCHEN E-MAILS, WEBSITES ODER NACHRICHTEN. SOLCHE E-MAILS UND IHRE LINKS UND ANHÄNGE SIND HÄUFIG EIN TÜRÖFFNER FÜR CYBERANGRIFFE. HIER KOMMEN EINIGE HINWEISE, AUF DIE SIE ACHTEN SOLLTEN, BEVOR SIE SICH ENTSCHEIDEN, AUF EINEN LINK ODER EINEN ANHANG ZU KLICKEN.

> **Der Absender.** Kennen Sie den/die Absender/in persönlich? Ist das seine/ihre übliche E-Mail-Adresse? Sieht die E-Mail-Adresse seriös aus? Schickt mir diese Person oder Organisation häufig solche Dokumente? Rufen Sie im Zweifelsfall die Person oder Organisation an, die Ihnen die E-Mail zugeschickt hat.

> **Die Art der Anfrage.** Werden Sie um persönliche oder sensible Informationen gebeten? Geben Sie im Zweifelsfall niemals persönliche oder sensible Daten weiter.

> **Der Wortlaut der Nachricht.** Enthält die E-Mail Rechtschreib- oder Grammatikfehler? Wird versucht, Ihre Neugier zu wecken? Werden Ihnen Versprechungen gemacht, die zu schön sind, um wahr zu sein? Werden Sie um Geld gebeten? Wird ein Gefühl der Dringlichkeit erzeugt? Klicken Sie im Zweifelsfall nicht.

> **Klicken Sie nicht auf Links oder QR-Codes in gefälschten Nachrichten und öffnen Sie auf keinen Fall Anhänge.** Wenn Sie Zweifel haben, suchen Sie in einer Suchmaschine nach der Website.

> **Lernen Sie** mit dem E-Learning-Modul „Surfen ohne Risiko“, **wie Sie einen falschen Link erkennen können:** https://surfenohnerisiko.safeonweb.be/de/modules/1

> **Geben Sie niemals Ihre persönlichen Daten an.**

> **Leiten Sie verdächtige Nachrichten** an verdacht@safeonweb.be **weiter.**

> **Installieren Sie die Safeonweb-Browsererweiterung.** Die Safeonweb-Erweiterung ist ein Tool, mit dem Sie die Vertrauenswürdigkeit einer Website bewerten können. Die Safeonweb-Browsererweiterung zeigt Ihnen für jede Website, die Sie besuchen, an, ob der Eigentümer validiert wurde (grün) oder nicht (orange).

Für weitere Informationen:
- https://safeonweb.be/de/erkennen-sie-gefaelschte-e-mails
- https://surfenohnerisiko.safeonweb.be/de/modules/1

2

ICH SCHÜTZE MEINE KONTEN UND VERWENDE DIE ZWEI-FAKTOR-AUTHENTIFIZIERUNG (2FA)

BEI DER WAHL IHRER KENNWÖRTER MÜSSEN SIE UNBEDINGT VORSICHT WALTEN LASSEN. SIE BENÖTIGEN STETS KENNWÖRTER, UM IHRE GERÄTE, DATEN, NETZWERKE (Z. B. WI-FI) UND KONTEN (Z. B. IHRE E-MAILS ODER SOZIALEN MEDIEN) ZU SICHERN. DOCH SELBST DAS STÄRKSTE KENNWORT GARANTIERT KEINE VOLLSTÄNDIGE SICHERHEIT.

Die Zwei-Faktor-Authentifizierung erhöht die Sicherheit beim Zugriff auf Ihre Konten und Geräte. Auf diese Weise kann ein/e Cyberkriminelle/r, selbst wenn er/sie an Ihr Kennwort gelangt, nicht auf Ihre Konten zugreifen, ohne die anderen Sicherheitsebenen zu überwinden.

> **Aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA), wann immer es möglich ist.** Die meisten Dienste, die von den großen digitalen Plattformen (wie den sozialen Medien) angeboten werden, sowie viele Geräte bieten diese Möglichkeit (z. B. durch Fingerabdruck und/oder Gesichtserkennung) an.

> **Verwenden Sie mehrere Kennwörter.** Am sichersten ist es, wenn Sie für jeden sensiblen Dienst (Ihre Bank, Ihre E-Mail, Ihren Zugang zu sozialen Medien usw.) ein anderes Kennwort verwenden. Wenn dann eines Ihrer Kennwörter missbraucht wurde, ist nur ein Dienst betroffen.

> **Lang und originell.** Je länger Ihr Kennwort ist, desto sicherer ist es. Vermeiden Sie es, ein einzelnes Wort aus dem Wörterbuch zu wählen. Bevorzugen Sie Kombinationen aus mehreren Wörtern, die in keinem offensichtlichen Zusammenhang stehen, aber leicht zu merken sind.

> Sie können auch einen **Kennwort- bzw. Passwortmanager** verwenden. Das ist ein Programm, das alle Ihre Kennwörter verwaltet) und dabei selbst gut geschützt ist.

> **Keine Spuren.** Schreiben Sie Ihr Kennwort nicht auf ein Post-it neben Ihren Computer, in eine E-Mail oder in eine Computerdatei.

> **Teilen Sie Ihre Kennwörter und Konten nicht mit Dritten.** Wenn Sie Ihre Konten teilen, besteht die Gefahr, dass Sie die Verantwortung für die betreffenden Konten verschleiern und somit die Nachvollziehbarkeit der im Namen des Nutzers vorgenommenen Handlungen verringern.

Für weitere Informationen:
- https://safeonweb.be/de/nutzen-sie-starke-passwoerter
- https://safeonweb.be/de/nutzen-sie-die-zwei-faktor-authentisierung
- https://atwork.safeonweb.be/de/MFA

3

ICH VERWENDE AKTUELLE UND OFFIZIELLE GERÄTE UND PROGRAMME

GEBEN SIE CYBERKRIMINELLEN ODER ANDEREN EINDRINGLINGEN KEINE GELEGENHEIT, SICH ZUGANG ZU IHREM GERÄT ODER IHREN DATEN ZU VERSCHAFFEN, INDEM SIE REGELMÄSSIG SICHERHEITSUPDATES DURCHFÜHREN, UND ZWAR SOWOHL FÜR IHRE BETRIEBSSYSTEME ALS AUCH FÜR IHRE PROGRAMME UND ANWENDUNGEN. ALLE PROGRAMME ENTHALTEN SCHWACHSTELLEN, DIE ES CYBERKRIMINELLEN ERMÖGLICHEN, IHNEN ZU SCHADEN ODER DIE KONTROLLE ÜBER IHR GERÄT ZU ERLANGEN. DIESE SCHWACHSTELLEN WERDEN ENTDECKT UND BEHOBEN, WENN SIE EIN UPDATE DURCHFÜHREN.

> **Aktivieren Sie die automatische Aktualisierung von Geräten und Software.** Dadurch wird sichergestellt, dass Ihr Gerät besser geschützt ist, wenn eine Schwachstelle entdeckt wird.

> **Nutzen Sie nur offizielle Websites.** Wenn Sie Software oder deren Updates herunterladen müssen, tun Sie dies nur von der offiziellen Website des Herstellers.

> **Installieren Sie nur sichere Anwendungen und Programme.** Installieren Sie Anwendungen, die aus einem Standard-App-Store (Google Play, App Store) stammen, und Programme von einem offiziellen Verkäufer. Beschränken Sie den Zugriff auf Ihre Anwendungen auf das Nötigste. Beispielsweise sollte eine Anwendung, die als Taschenrechner dient, keinesfalls Zugriff auf Ihren Standort oder Ihre Kontakte haben. Überprüfen Sie regelmäßig die Daten, die Ihre Anwendungen verwenden, um illegalen Datenverkehr zu erkennen.

> **Umgehen Sie nicht das standardmäßige Sicherheitssystem Ihres Geräts** (z. B. durch Jailbreaking[2] oder Routing[3]). Auch wenn solche Manipulationen den Eindruck erwecken, dass Sie mehr Kontrolle über Ihr Gerät haben und immer auf Sicherheitsfunktionen zugreifen können, erhöhen sie das Risiko erheblich.

> **Schalten Sie Ihr Gerät jeden Tag aus.** Updates werden in der Regel automatisch durchgeführt, wenn das Gerät gestartet wird.

Weitere Informationen zu Aktualisierungen:

- https://safeonweb.be/de/fuehren-sie-regelmaessige-updates-durch
- https://atwork.safeonweb.be/de/tools-resources/how-manage-updates (auf Englisch).

2: Jailbreaking: Einem iPhone, iPod touch, iPad oder Apple TV das Laden von Softwareanwendungen erlauben, die von der Firma Apple nicht anerkannt werden.
3: Das Routing eines Smartphones oder Tablets besteht darin, eine Softwareaktualisierung durchzuführen, um auf das Administratorkonto des Geräts zuzugreifen, welches Zugriff auf alle Funktionen und Einstellungen hat.

4

ICH ACHTE DARAUF, MEINE GERÄTE RICHTIG ZU SICHERN

WENN EINES IHRER GERÄTE IN FALSCHE HÄNDE GELANGT, KÖNNEN SIE GROßE PROBLEME BEKOMMEN. ACHTEN SIE DAHER DARAUF, IHR SMARTPHONE, IHR TABLET, IHREN LAPTOP USW. RICHTIG ZU SICHERN.

> **Eine gute Sperrfunktion.** Aktivieren Sie die automatische Sperrfunktion Ihres Smartphones, wenn es inaktiv ist (maximal eine Minute). Ziehen Sie einen Code einem Muster vor. Wenn dieser Service angeboten wird, programmieren Sie eine zeitliche Sperre Ihres Smartphones nach mehreren Fehlversuchen und ein Löschen der Daten, wenn zu viele Zugriffsversuche registriert wurden. Stellen Sie natürlich sicher, dass qualitativ hochwertige Backups verfügbar sind.

> **Verschlüsseln Sie Ihre Geräte.** Wenn Sie die Möglichkeit haben, verschlüsseln Sie Ihre Geräte, ebenso wie USB-Sticks und externe Festplatten. Wenn Sie eine SD-Karte verwenden, verschlüsseln Sie diese ebenfalls.

> **Beschränken Sie den Zugriff.** Achten Sie darauf, dass Sie den Zugriff auf Wi-Fi, Bluetooth, Near Field Communication (NFC[4]), Ihre Daten, Geolokalisierung usw. nur dann aktivieren, wenn Sie ihn benötigen. Aktivieren Sie keine Selbstaktivierungsfunktionen (z. B. für Wi-Fi). Überprüfen Sie regelmäßig die Zugriffsrechte von Anwendungen.

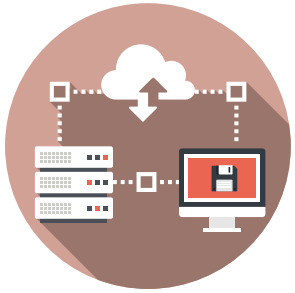
> **Behalten Sie die Kontrolle über Ihr Gerät.** Lassen Sie es nicht unbeaufsichtigt.

4: Bei der „Near Field Communication“ oder „NFC“ handelt es sich um eine drahtlose Kommunikation, mit der kleine Informationsmengen in einem Radius von 10 Zentimetern ausgetauscht werden können, z. B., um eine Verbindung mit einem Bezahlsystem oder einem Smartphone herzustellen.

5

ICH SORGE FÜR DIE KORREKTE SICHERUNG MEINER DATEN

AUCH MIT DEN DATEN, DIE SIE AUF IHREM COMPUTER AUFBEWAHREN, SOLLTEN SIE VORSICHTIG UMGEHEN. WENN IHRE DATEN VERLOREN GEHEN, IST DAS NICHT NUR PERSÖNLICH ÄRGERLICH, SONDERN SIE KÖNNEN AUCH IN SCHWIERIGKEITEN GERATEN, WENN BEISPIELSWEISE PERSONEN MIT NEGATIVEN ABSICHTEN DIE DATEN VON MITGLIEDERN IHRER PARTEI STEHLEN UND AUSNUTZEN.



> **Machen Sie Back-ups.** Ein Back-up ist eine Sicherungskopie der für Sie wichtigen Daten. Mithilfe des Back-ups können Sie die Daten erneut auf Ihrem Gerät installieren, wenn Sie von einem Virus befallen werden. Außerdem ist es im Falle eines Diebstahls, Verlusts oder eines technischen Problems beruhigend, ein Back-up zu haben. Sie können dann das gesamte System neu installieren und Ihre zuvor gesicherten Daten wieder aufspielen. Dies gilt natürlich auch für Ihre mobilen Geräte.

> **Datensicherung.** Richten Sie ein System ein, um Ihre Daten regelmäßig automatisch zu sichern. Dezentrale Cloud-Lösungen können einen klaren Vorteil bieten, sofern Ihr Anbieter vertrauenswürdig ist.

> **Verwenden Sie einen Virenscanner.** Ein Virenscanner macht Ihren Computer undurchlässig für Viren. Es ist die wichtigste Software zum Schutz Ihres Computers und Ihrer Daten.

> **Ausschalten.** Schalten Sie Ihre Geräte aus, wenn Sie sie nicht benutzen (Urlaub, Wochenende usw.) und deaktivieren Sie die Funktionen, die Sie nicht benötigen (Wi-Fi, Bluetooth, NFC, Geolokalisierung).

> **Seien Sie vorsichtig, wenn Sie USB-Sticks verwenden.** Ein USB-Stick ist praktisch, um Daten zu transportieren, aber er kann auch leicht verloren gehen. Achten Sie besonders auf USB-Sticks, die Sie von anderen Personen erhalten oder die Sie z. B. auf dem Boden finden. Sie können nämlich Viren enthalten. Wir empfehlen Ihnen daher, vor der Verwendung eines USB-Sticks einen professionellen Virenscan durchführen zu lassen. Sichern Sie regelmäßig den Inhalt Ihrer USB-Sticks und löschen Sie regelmäßig nicht benötigte Dokumente auf ihnen.

Weitere Informationen zu Back-ups:
- https://safeonweb.be/de/machen-sie-back-ups
- https://atwork.safeonweb.be/de/tools-resources/how-manage-backups (auf Englisch).

Weitere Informationen zum Virenschutz:
- https://safeonweb.be/de/scannen-sie-ihren-computer
- https://atwork.safeonweb.be/de/tools-resources/antivirus-software (auf Englisch).

Weitere Informationen zu USB-Sticks:
- https://cyfun.be (Cyber-Grundlagen - Stufe ‚Small', unter „3. Antivirus installieren").

6

ICH VERWENDE EIN SICHERES WI-FI-NETZ

EIN GUT GESICHERTES NETZWERK IST EINE GRUNDVORAUSSETZUNG FÜR HOCHWERTIGE PRÄVENTION. WENN SICH EIN/E CYBERKRIMINELLE/R ODER EIN ANDERER EINDRINGLING ZUGANG ZU IHREM NETZWERK VERSCHAFFT, HAT ER/SIE GLEICHZEITIG AUCH ZUGRIFF AUF ALLE ANGESCHLOSSENEN GERÄTE. DAS DRAHTLOSE SYSTEM WI-FI HAT DIE VERBINDUNG VON ELEKTRONISCHEN GERÄTEN MIT VERSCHIEDENEN NETZWERKEN (INTERNET, PRIVATES NETZWERK, FIRMENNETZWERK USW.) ERHEBLICH VEREINFACHT. WIE KÖNNEN SIE IHR WI-FI-NETZ MAXIMAL ABSICHERN?

> **Sichern Sie Ihren persönlichen Router.** Wenn Sie einen neuen Wi-Fi-Router (oder eine neue Wi-Fi-Box) erhalten, sollten Sie nicht die Standardeinstellungen beibehalten. Ändern Sie den Namen des Netzwerks (SSID) und fügen Sie keine offensichtlichen Elemente ein. Ändern Sie auch die Passwörter (einschließlich des Kennworts, das Ihren Router sichert).

> **Verwenden Sie eine WPA2-Sicherung.** Ihr Router kann wahrscheinlich mit WPA2, WPA oder WEP verschlüsselt werden. Entscheiden Sie sich für WPA2 und installieren Sie den Zugang umgehend, falls Sie es noch nicht getan haben.

> **Aktivieren Sie eine Firewall.**

> **Ein starkes Kennwort.** Beziehen Sie sich bei der Wahl des Kennworts für Ihr Wi-Fi-Netzwerk auf die oben genannten Tipps zu Kennwörtern. Geben Sie das Kennwort nur an vertrauenswürdige Personen weiter und wechseln Sie es regelmäßig.

> **Vermeiden Sie die Nutzung öffentlicher Wi-Fi-Netze.** Wir empfehlen Ihnen, keine Bankgeschäfte oder andere wichtige Transaktionen über ein öffentliches Wi-Fi-Netzwerk durchzuführen. Vermeiden Sie es, über ein öffentliches Wi-Fi-Netzwerk Konten mit Kennwörtern zu erstellen.

> **Installieren Sie ein Virtual Private Network (VPN).** Dabei handelt es sich um einen persönlichen und sicheren „Tunnel", der mithilfe des Wi-Fi-Netzwerks funktioniert. Sie können VPN-Dienste kostenlos oder kostenpflichtig online installieren. Auch verschiedene Virenscanner bieten VPN an.

Weitere Informationen zu Wi-Fi:
- https://safeonweb.be/de/nachrichten/gibt-es-auch-wi-fi
- https://atwork.safeonweb.be/de/tools-resources/protect-your-mobile-devices (auf Englisch).
- https://atwork.safeonweb.be/de/tools-resources/how-stay-vigilant-against-cyber-threats (auf Englisch).

Weitere Informationen zur WPA2-Sicherung:
- https://cyfun.be (Cyber-Grundlagen – Stufe ‚Small', unter „4. Sichern Sie Ihr Netzwerk").

7

ICH NUTZE SOZIALE MEDIEN MIT BEDACHT

DIE PRIVATSPHÄRE EINES POLITISCHEN ENTSCHEIDUNGSTRÄGERS/EINER POLITISCHEN ENTSCHEIDUNGSTRÄGERIN IST ANGREIFBARER ALS DIE ANDERER BÜRGER. WENN SIE IN DEN SOZIALEN MEDIEN AKTIV SIND, TRETEN SIE NICHT NUR MIT DER AUSSENWELT IN KONTAKT, SONDERN DIE AUSSENWELT KANN AUCH IHR PERSÖNLICHES PROFIL AUF DER GRUNDLAGE DER VON IHNEN GETEILTEN INFORMATIONEN ERSTELLEN, ANGEFANGEN BEI PERSÖNLICHEN FOTOS BIS HIN ZU IHREM PERSÖNLICHEN VERHALTEN, SAMT IHRER FILMAUSWAHL, IHREN ESSGEWOHNHEITEN UND INFORMATIONEN ÜBER IHRE FAMILIE, IHRE NETZWERKE UND IHREN AUFENTHALTSORT. DIESE INFORMATIONEN SIND DAHER ANFÄLLIG FÜR MISSBRAUCH. HIER SIND EINIGE TIPPS, WIE SIE IHRE PRIVATSPHÄRE SCHÜTZEN KÖNNEN:

> **Nutzen Sie unterschiedliche Geräte.** Wenn möglich, trennen Sie die Geräte, die Sie für Ihre politischen oder beruflichen Aktivitäten nutzen, von denen, die Sie für Ihr Privatleben verwenden.

> **Verwenden Sie mehrere E-Mail-Adressen.** Sie könnten z. B. eine E-Mail-Adresse für vertrauliche Dienste (Ihre Bank, Behörden usw.) und eine andere für weniger vertrauliche Dienste (Video-on-Demand, Foren, Spiele usw.) nutzen. Es ist ratsam, eine E-Mail-Adresse zu haben, die für Ihre öffentlichen Aktivitäten bestimmt ist.

> **Denken Sie an die Sicherheit Ihrer sozialen Medien.** Überprüfen Sie vor der Kampagne die Einstellungen der sozialen Medien, die Sie nutzen (insbesondere bestimmte automatische Postings). Treffen Sie vor jedem Beitrag eine Auswahl im Hinblick auf die Sichtbarkeit Ihrer Beiträge und stimmen Sie diese mit dem ab, was Sie mitteilen möchten. Aktivieren Sie eine starke Zwei-Faktor-Authentifizierung (2FA) für den Zugriff auf Ihre Konten.

> **Seien Sie wachsam gegenüber Internet-Trollen.** Ihr Hauptziel ist es, Online-Diskussionen zu provozieren, zu beeinflussen, zu lenken und zu eskalieren. Zu diesem Zweck werden in den sozialen Medien vorab Konten von scheinbar gewöhnlichen Bürgern eingerichtet. Zum richtigen Zeitpunkt werden sie dann in Aktion gesetzt, um zu einem bestimmten Thema Stellung zu beziehen. Um den Troll zu stoppen, ist es wichtig, nicht so zu reagieren, wie er es möchte. Beteiligen Sie sich nicht an der Diskussion und regen Sie sich nicht auf.

> **Soweit möglich, vermeiden Sie Verknüpfungen zwischen Ihren Konten.** Manche Plattformen bieten die Möglichkeit, Ihr bestehendes Konto mit anderen sozialen Medien zu verknüpfen. Diese verknüpften Konten sind anfällig, da sich alle Ihre persönlichen Daten auf einer bestimmten Plattform befinden.

> **Die Datenschutzeinstellungen Ihrer Konten sollten regelmäßig überprüft werden.** Manchmal können Einstellungen einseitig vom Anbieter geändert werden, was z. B. bedeuten kann, dass die Eigentumsrechte an Ihren persönlichen Daten möglicherweise an den Plattformbetreiber übertragen werden.

> **Seien Sie sich bewusst, dass manche Social-Media-Plattformen Verbindungen zu bestimmten Ländern haben können.** TikTok zum Beispiel ist eine chinesische Plattform. Daher können die auf TikTok gespeicherten Daten von der chinesischen Regierung verwendet oder missbraucht werden. Überlegen Sie, ob Sie wirklich auf allen Social-Media-Plattformen präsent sein müssen.

8

ICH ERKENNE DESINFORMATION

DESINFORMATION IST EINE GEFAHR FÜR UNSERE DEMOKRATIE, DA SIE DIE WÄHLER DARAN HINDERN KANN, EINE FUNDIERTE POLITISCHE ENTSCHEIDUNG ZU TREFFEN. DIES GILT INSBESONDERE FÜR DIE VERBREITUNG FALSCHER ODER MANIPULIERTER INFORMATIONEN, ABER AUCH FÜR DIE KÜNSTLICHE VERSCHÄRFUNG VON SPALTUNGEN, DIE FÖRDERUNG VON MISSTRAUEN GEGENÜBER WAHLEN ODER DEN AUSSCHLUSS LEGITIMER STIMMEN IN DER DEBATTE. ALS POLITISCH VERANTWORTLICHE PERSON KÖNNTEN SIE ZUR ZIELSCHEIBE WERDEN, ABER AUCH SELBST UNWISSENTLICH ZUR FÖRDERUNG VON DESINFORMATION BEITRAGEN.

> **Informieren Sie sich über Desinformation.** Desinformation ist nicht unbedingt das Gleiche wie Propaganda oder „Fake News“. Darüber hinaus kann sie in vielen verschiedenen Formen auftreten. Denken Sie an gefälschte Nachrichtenseiten oder falsche Bilder, aber auch an gefälschte Audionachrichten oder verschwörungstheoretische Videos auf TikTok. Auf der Website des Nationalen Krisenzentrums wird ausführlich erklärt, was Desinformation genau ist und welche verschiedenen Einflusstechniken üblicherweise angewendet werden: https://krisenzentrum.be/de/desinformation

> **Setzen Sie Ihren gesunden Menschenverstand ein.** Sie können Desinformation erkennen, indem Sie sich ein paar Fragen stellen. Wer ist der Autor, der Ersteller oder der Verbreiter? Ist die Information wahr? Zu welchem Zweck wurde die Nachricht erstellt oder verbreitet? Weitere Tipps: Lesen Sie über die Überschrift hinaus, konsultieren Sie mehrere Quellen, prüfen Sie, wann eine Nachricht verfasst oder verbreitet wurde, und seien Sie kritisch im Hinblick auf die Form.

> **Hüten Sie sich vor „Deepfakes“.** Die rasante Entwicklung der generativen künstlichen Intelligenz macht es enorm einfach, Bilder zu manipulieren oder völlig unechte Fotos, Videos und Töne zu erstellen. Das Abspielen eines Videos in Zeitlupe kann eine erste Möglichkeit darstellen, solche „Deepfakes“ zu erkennen.

> **Überprüfen Sie selbst die Fakten.** Um die Richtigkeit von Bildern zu überprüfen, können Sie auch folgendermaßen vorgehen. Mithilfe einer Suchmaschine wie Google Reverse Image Search können Sie den tatsächlichen Kontext herausfinden. Schauen Sie genau hin und notieren Sie sich die verschiedenen Umgebungsmerkmale, die Ihnen mehr über den Ort verraten. Suchen Sie unabhängige Quellen, um Geschichten oder Bilder zu überprüfen. Weitere Tipps finden Sie unter https://belux.edmo.eu/de/werkzeug/toolkit-zur-faktenueberpruefung/

> **Teilen Sie keine zweifelhaften Inhalte.** Haben Sie noch Zweifel an der Richtigkeit oder Zuverlässigkeit einer Information? Dann sollten Sie diese Information oder Nachricht nicht weiterverbreiten. Dies ist nicht nur die Hoffnung der Verbreiter, sondern als Politikerin oder Politiker haben Sie auch eine sehr große Reichweite und verleihen der Desinformation zusätzliche Bedeutung, wenn Sie sie über Ihre Kanäle verbreiten.

> **Melden Sie Desinformation.** Sind Sie sicher, dass Sie es mit Desinformation zu tun haben? Dann können Sie diese bei EDMO BELUX unter https://belux.edmo.eu/de/berichterstattung-ueber-desinformation/ melden.

WAS KANN ICH TUN, WENN ICH OPFER GEWORDEN BIN?

1. ICH BIN OPFER EINES NOCH ANDAUERNDEN CYBERANGRIFFS

> Sie können die Folgen eines Cyberangriffs begrenzen, wenn Sie schnell reagieren.

> Sie können den Vorfall über das Formular auf der ZCB-Website oder per E-Mail incident@ccb.belgium.be an das ZCB melden. Weitere Möglichkeiten, einen Vorfall zu melden, finden Sie unter https://cert.be/de/einen-vorfall-melden-0

In dringenden Fällen können Sie das ZCB auch telefonisch erreichen: **+32 (0)2 501 05 60.**

> Schalten Sie Ihren Computer NICHT aus, da Sie sonst die Spuren der Cyberangreifer verwischen.

> Es ist auch besser, Ihre Passwörter von einem sicheren Computer aus zu ändern, da sie sich möglicherweise im Besitz des Täters befinden.

> Erstatten Sie bei der örtlichen Polizei Anzeige.

Weitere Informationen:
- https://ccb.belgium.be/de/cert/erste-hilfe-bei-einem-cyberangriff

2. MEIN KONTO WURDE GEHACKT

> Ändern Sie sofort alle Ihre Kennwörter. Tun Sie dies von einem sicheren Gerät aus, also von einem anderen als dem, von dem Ihre Daten gestohlen wurden.

> Installieren Sie umgehend eine Zwei-Faktor-Authentifizierung (2FA).

> Starten Sie Ihr Antivirenprogramm, damit es Ihren Computer scannt.

> Wenn Ihre Bank- oder Kreditkartendaten gestohlen wurden, benachrichtigen Sie Ihre Bank und überwachen Sie Ihre Konten. Wenden Sie sich an Card Stop unter **+32 (0)78 170 170.**

> Wenn Daten über Ihr politisches Leben gestohlen wurden, benachrichtigen Sie so schnell wie möglich Ihre Partei und machen Sie eine Meldung bei der Datenschutzbehörde.

> Informieren Sie Ihre Kontakte. Es besteht die Gefahr, dass sie Nachrichten erhalten, die in Ihrem Namen versendet wurden.

Weitere Informationen:
- https://safeonweb.be/de/mein-konto-wurde-gehackt

3. MEIN SMARTPHONE ODER TABLET IST WEG

> Wechseln Sie sofort sämtliche Kennwörter aller Accounts, die sich auf Ihrem Gerät befinden (E-Mail, Facebook, WhatsApp, usw.).

> Wenn sich Ihre Bank- oder Zahlungsdaten auf dem gestohlenen Gerät befinden, benachrichtigen Sie die Kontaktperson bei Ihrer Bank und behalten Sie Ihre Konten im Auge. Lassen Sie Ihre Bankkarten und Konten gegebenenfalls über Card Stop (www.cardstop.be (auf Französisch und Niederländisch) oder **+32 (0)78 170 170**) sperren.

> Sollten sich Daten über Ihre politischen Aktivitäten auf dem Gerät befinden, informieren Sie bitte Ihre Partei so schnell wie möglich.

> Wenn Ihr Gerät gestohlen wurde, erstatten Sie Anzeige bei der Polizei.

Weitere Informationen:
- https://safeonweb.be/de/mein-smartphone-oder-tablet-ist-weg

4. HILFE, ICH HABE EINEN VIRUS!

> Eins ist sicher: ein Virus muss möglichst umgehend gelöscht werden.

> Wenn Sie noch keinen Virenscanner haben und Ihr Gerät nicht blockiert ist, dann ist es höchste Zeit, ein Antivirenprogramm zu installieren, einen Scan durchzuführen und den Virus zu entfernen. Geben Sie bis dahin keine persönlichen Daten oder Zahlungsdetails ein, da einige Viren diese Informationen weiterleiten.

Weitere Informationen:
- https://safeonweb.be/de/hilfe-ich-habe-einen-virus

KONTAKT

1. ZENTRUM FÜR CYBERSICHERHEIT BELGIEN (ZCB)

> Das ZCB ist sowohl während als auch nach der Wahl Ihr Ansprechpartner, wenn Sie einen Cybervorfall melden oder Fragen stellen möchten.

Sie erreichen diese Stelle entweder per E-Mail an incident@ccb.belgium.be oder Sie können einen Vorfall auf der Website https://ccb.belgium.be/de/cert melden.

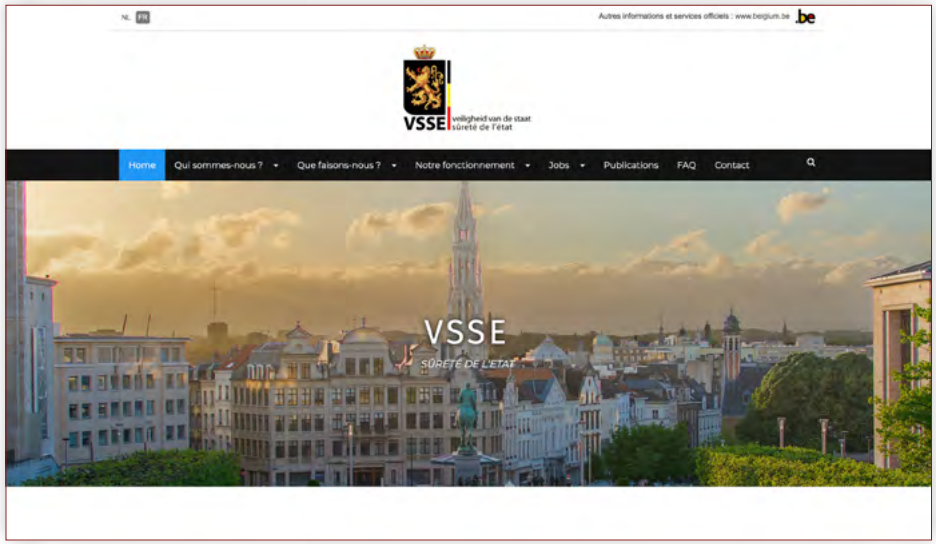
In dringenden Fällen ist das ZCB auch telefonisch erreichbar unter **+32 (0)2 501 05 60.**

2. STAATSSICHERHEIT (VSSE)

> Alle Informationen über die Aufgaben und die Arbeitsweise der Staatssicherheit finden Sie auf der Website www.vsse.be (auf Französisch und Niederländisch).

3. ALLGEMEINER NACHRICHTEN- UND SICHERHEITSDIENST (ANSD)

> Um mehr über die Rolle und die Zuständigkeiten des ANSD zu erfahren, wenden Sie sich bitte an diesen Dienst unter folgender Adresse: csoc@cyber.mil.be



WEITERE INFORMATIONEN

CYBERANGRIFFE:

> **Zentrum für Cybersicherheit Belgien:** https://ccb.belgium.be/de/cert

> **Safeonweb@work:** https://atwork.safeonweb.be/de

> **CyberFundamentals:** https://cyfun.be

> **Cyber Security Basics für Starter:** https://www.cybersecuritycoalition.be/cyber-security-basics-for-starters/ (auf Englisch).

> **Cyberscan (FÖD Wirtschaft):** https://economie.fgov.be/de/cyberscan

> **Datenschutzbehörde:** https://www.datenschutzbehorde.be/zivilist

> **Meldestelle bei Betrug:** https://pointdecontact.belgique.be/meldpunt/de/wilkommen

> **Safeonweb:** https://safeonweb.be/de

DESINFORMATION:

> **Desinformation (Nationales Krisenzentrum):** https://krisenzentrum.be/de/risiken-belgien/sicherheitsrisiken/desinformation/desinformation

> **European Centre of Excellence for Countering Hybrid Threats:** https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ (auf Englisch).

INFORMATIONEN ÜBER POTENZIELLE AUSLÄNDISCHE EINMISCHUNG:

> www.vsse.be (auf Französisch und Niederländisch).

Es steht jedem frei, die Empfehlungen dieses Leitfadens auf der Grundlage seiner eigenen Risikoanalyse zu befolgen. Sie wurden auf der Grundlage der zum Zeitpunkt der Veröffentlichung beobachteten Bedrohungslage erstellt. Wir können nicht garantieren, dass diese Empfehlungen die Sicherheit eines bestimmten Computersystems gewährleisten.

Sicher Surfen während der Wahlkampagne
Empfehlungen für einen Wahlkampf im Zeichen der Cybersicherheit

Verantwortlicher Herausgeber: Francisca BOSTYN
König-Albert-II.-Boulevard, 6 - 1000 Brüssel