CENTRE FOR
CYBER SECURITY
BELGIUM

Guide towards a cybersecure Belgian Presidency of the EU

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

UNDER THE AUTHORITY
OF THE PRIME MINISTER

.be

CENTRE FOR CYBER SECURITY BELGIUM

I. Preface

In the first half of 2024 Belgium will hold the rotating presidency of the Council of the European Union. During this period, Belgium will be in the international spotlight for 6 months. This will offer significant opportunities for our country, but being in the spotlight also comes with significant additional threats, including cyberthreats.

The Presidency will be a period filled with events, organized by, or under the auspices of, Belgian public administrations. To facilitate a modern, pleasant and efficient audience experience, these events will often be supported by many different digital technologies, including video conferencing tools, online registration products, websites in general, mobile applications or other connected instruments.

To assure that all these events go smoothly, and to protect the availability, integrity and authenticity of all the digital traffic associated in any way to the Presidency, a high level of cybersecurity of these tools and their use is needed. Such heightened cybersecurity is equally needed to build confidence among the other EU Member States, and in the global community, in the capability of our country to lead the Council. The efforts to strengthen our EU Presidency will also support the mission of the National Cybersecurity Strategy 2021-2025: making Belgium one of the least cyber vulnerable countries of Europe.

The National Crisis Center (NCCN) performed a risk-analysis on the Belgian presidency of the European Union and highlighted herein four cyber related threats: disturbance of services (Distributed Denial of Service -DDoS- attacks), ransomware, misinformation and espionage.

The Center for Cybersecurity Belgium (CCB), supported by other Security & Intelligence Services, has therefore written a guiding document on how to assure a higher level of cybersecurity during the Belgian Presidency. The target audience of this document are in first instance the coordinators and organizers of events during the presidency period, but also their suppliers of event management services.

This guide document describes in more detail the cyber threats that were identified during the NCCN risk analysis, as well as possibly associated phenomena. More practically, the document offers a set of **eight key cybersecurity requirements** and tips to take into account when selecting and using appropriate digital tools in order to mitigate the risks associated

with the outlined threats. These measures were drafted based on the CyberFundamentals Framework published by the CCB earlier this year.

Furthermore, this document lays out **four additional CCB services** to help prevent and respond to cybersecurity incidents. Where relevant, this document also provides links to more in-depth existing advisories.

This document contains many recommendations, but two core measures we cannot emphasize enough as being truly essential:

1) Install multi-factor authentication on all external connections
2) Make sure all systems and software are patched and updated.

At the end of the document we equally provide a contact point to which organizations can reach out for support, either before or after the occurrence of a cyber incident that might impact the functioning of presidency related events.

Let's use the Presidency to showcase how we together make Belgium one of the least cyber vulnerable countries in Europe!

Miguel De Bruycker
Director-General CCB

CENTRE FOR CYBER SECURITY BELGIUM

II. Table of Contents

III. Scope

This document is intended as a guide for all (collaborators of) Public Administrations who organize events on the occasion of the Belgian Presidency of the Council of the European Union, and will use digital tools during these events or during their preparation. The document is equally meant for the ICT managers – and for some aspects also for the communication departments – associated to these organizers, as well as their (digital) service providers, be they regular or specifically under contract for Presidency events.

Consequently the document includes high level advise, as well as technical steps to take, including references to more specific publications.

The document is meant for Federal as well as Regional Public Administrations, and is of particular importance if you organize events outside the standard locations in Brussels.

Organizers of events related to the Belgian Presidency are strongly advised to take into account the advisories described in this document, specifically for the following digital tools:

- Videoconferencing tools (such as MS Teams, Webex and others), including associated instruments (chats, registration, etc.).
- Registration platforms
- Websites containing info about events
- Social Media
- Applications that are developed or used specifically for the Belgian Presidency
- Wifi networks that are set up at Presidency events
- Internal communication systems for event organizers,
- File Storage and sharing systems

For all events that are hosted in the Egmont Palace, most digital services, including their cybersecurity services, will be provided by the ICT services of the Federal Public Service for Foreign Affairs and its digital service providers.

For all events in the Council buildings, the ICT and cybersecurity related services will be provided by the General Secretariat of the Council. This includes the general Presidency registration platform (PPI).

However**, if you organize events or host tools in relation to such events, it is essential that organizers check with either of these institutions what the exact scope of these services includes and whether you have to accommodate tools yourself.**

Organizers should further check with other providers whether basic cybersecurity measures can be taken. Some examples of service providers could be:

- hotels or event halls, who offer videoconferencing, Wifi networks, or even mobile apps
- individually procured applications
- event organizers, contracted to acquire for your organization any of the tools listed above
- the ICT services of your own administration.

Finally, it is important to stress that this document is meant to give advice. Every system owner retains the final responsibility for adequately protecting their own environment. The measures advised in this document are a list of basic steps to take and do not guarantee that all attacks will be prevented. It remains up to system owners to take those measures according to the specific risks they are facing.

IV. Cyber threats

As a preparation to the Belgian Presidency of the Council of the European Union, the National Crisis Centre (NCCN) performed a general Risk Analysis. This risk analysis highlights four cyber threats that merit particular attention during the EU presidency:

1. disturbance of online services or events,
2. ransomware (including data theft)
3. misinformation (through the use of social media) and
4. espionage.

Associated cyber incidents may affect the functioning of events related to the presidency.

These risks are each sometimes associated to specific threat actors, but one must take into account four types of cyber threat actors in general:

a. Foreign military and intelligence services
b. Cybercriminals, who use networks to obtain financial gain
c. Hacktivists, who perform intentional cyber activities with the intention of promoting a political agenda, religious belief or social ideology.
d. Terrorists, who use the internet to commit acts of violence for the purpose of gaining a political advantage and instilling fear in the population.

In the current dynamically changing geo-political landscape, often these threat actor types either mix or collaborate.

In what follows each phenomenon is briefly described. Appropriate mitigating actions and recommendations are provided in the next chapter, so that you and your suppliers can take these threats into account during your events and especially during the preparations of these events.

1. Disturbance of online services or events

Malicious actors, such as hackers or hacktivists may desire to disturb high-profile events or services, and this in order to shame its organizer, or to bring their proper action points under the attention.

The most common way for a threat actor to make such disruption is by launching a (distributed) denial-of-service (DDOS) attack.[1] This would mean that more demand for the service is generated than capacity available to deal with these demands. This results in the

[1] The network bandwidth and availability of resources is currently so large for most organizations that a single attacking machine can usually not cause a DoS. This is the reason why attacks are happening in a coordinated way. The attack is distributed across multiple attacking computers, hence Distributed Denial of Service (DDoS). It is important to stress that although distributed in nature the computers taking part in a DDoS share a common goal and the attack is coordinated.

system outage. Especially Pro-Russian hacktivist groups have been associated with large scale DDoS campaigns recently.

Such an attack could entail that registration platforms, videoconferencing platforms, websites or apps containing important practical information for participants of events, or even communication tools could be made unavailable at key moments. This would severely disturb meetings or their preparation.

Apart from the disruptive effects themselves, such attacks can cause significant damage to the government's reputation, including loss of public trust.

2. Ransomware, extortion, data theft and credential leakage

The threat of ransomware has consistently ranked at the top in the ENISA Threat Landscape for the past few years. Ransomware is malicious software (malware) that encrypts the data of users with the intention to make it unavailable unless a payment of a ransom has been paid.

Most often, the deployment of Ransomware is used in an approach of multiple extortion, whereby data will not only be encrypted but also stolen and/or destroyed, each step of which may or may not be additionally connected to a ransom. Such data theft might sometimes also be linked to espionage.

Cybercriminals may desire to launch ransomware or linked extortion tactics, during Belgian's EU Presidency, not only for monetary objectives, but also to disrupt our working and to weaken the public image of our country or government institutions.

Additionally, phishing often remains the main attack vector to illicitly get into systems.

One of the biggest associated risks is that of credential leakage. Data theft can include passwords, which subsequently circulate on the dark web, and will be used to gain illicit access to other networks. The tools of the Belgian Presidency must thus be well protected to avoid this type of exposure. Inversely, stolen credentials might help attackers to gain more easily access to systems concerning our Presidency. Installing Multi Factor Authentication could help mitigate this particular risk.

3. Foreign Information Manipulation and Interference/ Information Operations (through the use of social media)

State and non-state actors, including their proxies, use Influence activities to manipulate and even to change the perception (and behavior) of a domestic or a foreign Target Audience.

To obtain these strategic goals, Psychological Operations (PSYOPS) are used in combination with a toolbox of online (and offline) Tactics, Technics and Procedures (TTPs) in order to change *"the hearts and the minds"*.

FIMI (=Foreign Information Manipulation and Interference) combine these activities and are mostly patterns of non-illegal behavior, that threaten or have the potential to negatively impact values, procedures and political processes.

Disinformation is only one vector of a large set of FIMI activities. Disinformation is mostly tailor-made, depending on the Target Audience. Key of success is continuously repetition of the message. Main objectives of FIMI are to sow division into a society, discredit credibility, distract,…

Spreading propaganda or disinformation, using different techniques such as deploying massively bots/trolls, hack and leak operations, astroturfing, and others, are combined in order to be able to reach an audience with the intent to deceive.

Well-executed FIMI activities are often coordinated and display inauthentic behavior. However awareness needs to be raised that also online organic messaging might have serious impact.

During the Federal and European elections in 2019, SGRS together with VSSE, monitored and analyzed the online/virtual space for FIMI activities. Later on, the COVID-19 pandemic, the vaccination campaign, Russian invasion into Ukraine,… have shown a substantial increase in online manipulation of information resulting in a current “Information War”.

A Federal taskforce, the “Agile Taskforce Information Operations” (ATFIO), led by ADIV is put in place in order to be ready for the elections of 2024. This taskforce brings together all necessary federal entities in tackling possible FIMI activities.

4. Espionage

The Belgian EU presidency and the events around it may also be a target for espionage activities.

Events bring together interesting crowds of people around a certain topic, which is a good occasion for hostile intelligence services to collect contacts, spot people and even make the first contact which may lead to a recruitment. It is therefore important to make an evaluation of the attendees and the audience of your event in function of the sensibility of the topics discussed.

But why would a hostile intelligence service (only) go through the effort of sending a real-life infiltrator to an event, when it is just as easy to follow the event online and get all the email addresses?

V. Fundamental protection measures

Based on the CyberFundamentals framework guidelines, general measures are proposed to protect events. The basic measures are summarized below and tailored to event organizers. Organizers are advised to assure the implementation of these measures, where appropriate and possible, based on risk. More detailed information can be found in the CyberFundamentals framework and linked standards, as can be found on the CCB website.

1. Instruct collaborators on information security and cybersecurity

As an organizer you should think to write an instruction document explaining acceptable practices and expectations towards subcontractors (hotels, web hosting companies) and event collaborators. This raises the awareness and helps to implement the measures in a correct way. These instructions will be specific to your event and organization, but can in large part be based on the warnings above and guidelines below in this document.

Instructions to your employees should include at least basic measures to prevent phishing attempts. Common phishing techniques can be found on www.safeonweb.be. Instructions to forward suspicious mails to suspicious@safeonweb.be can moreover help the CCB to protect other users.

Instructions should also inform your collaborators about the risk of disinformation (FIMI) through misuse of the event communication channels (websites and social media). The document should also include instructions on the monitoring *and* reporting disinformation attested on your channels. Communication services should also best cooperate with ICT security services for mitigating these threats. We also remind that the Belgian National Security Council has imposed a temporary ban on the use of TikTok on federal public service devices, citing privacy and security concerns.

The instructions towards collaborators and providers should include an overview of responsibilities and first contacts in case of an incident (see chapter VI) and could link to the following CCB publications:

- https://ccb.belgium.be/en/document/ransomware-how-protect-and-respond
- https://ccb.belgium.be/en/document/how-respond-ransomware-attack-12-steps

2. Install Multifactor Authentication (MFA) & Manage credentials

Enforce authentication of users wherever possible. Two factor authentication is a key measure that should be enforced whenever possible.

In complement to the multi factor authentication, password routine rules should be followed:

- Change all default passwords
- Ensure that no one works with administrator privileges for daily tasks.
- Keep a limited and updated list of system administrator accounts.

- Enforce password rules, e.g. passwords must be longer than a state-of-the-art number of characters with a combination of character types and changed periodically or when there is any suspicion of compromise.
- Use only individual accounts and never share passwords.
- Immediately disable unused accounts
- Rights and privileges are managed by user groups.

3. Manage physical and digital access

A registration desk for physical access to an event is good practice, but also prevent the unauthorized physical access to your digital devices on your event, such as servers or communication tools.

The same principle should be used in digital events as to create user dedicated login URLs for digital events where threats on espionage, FIMI or data theft are relevant. This includes access to video conferences, Wifi networks etc.

For event organizers, the principle of 'least privilege' should be applied, which means limiting collaborator's access to data and information to the systems and specific information they need to do their jobs.

Once collaborators change jobs or leave the organization, their access should be changed or deleted.

4. Secure your digital access points & separate internal from guest networks

When wireless networking is used, ask your technical support to change the administrative password upon installation of a wireless access points, and set router to use at least Wifi Protected Access with the Advanced Encryption Standard (AES) for encryption.

Ensure that the access and networks for event participants, presenters and organizers are separated from each other. Especially the access to tools for participants as well as the networks they use, should be as much as possible separate from those for organizers, e.g. by segmenting the wifi networks, as well as access links. Internal networks should in any case be separated from the networks for guests.

As already stated: For all access to the internal networks multi factor authentication (two-factor authentication) should be used since it is the most feasible measure against credential leaks that is associated with all threats.

For events with more sensitive information a personal login and password policy should be imposed to discourage espionage and information theft.

For your event organizers with admin rights, separate the administrative account from the personal account to reduce the risk on deployment of ransomware.

5. Keep an inventory of hardware and software used in the organization of your event.

An inventory of relevant hardware (computers, tablets, smartphones, communication systems for event organizers), software platforms, applications and information storage media is a prerequisite to prevent theft-related intrusions (espionage). It also provides a tool to manage protective measures, respond to early warnings and patch your systems with the latest security updates in a timely manner.

It is also useful to structure post-event information removal measures. For example, electronically wiping or sanitizing computers for reuse prevents data theft.

6. Install updates and keep all your software up to date

Many incidents happen based on vulnerabilities for which an update had been available for a long time. It is therefore crucial to ensure that patches and security updates on operating systems and software are installed in a timely manner. Federal public administrations can onboard on the CCB EWS warning system and react to EWS warnings received (see Chapter VI.2 below). Professional providers should be subscribed to a professional provider of warnings.

Ensure equally the installation and updates of anti-virus, anti-spyware and other malware programs.

7. Ensure your network integrity management together with your provider

Check, demand and make sure that your internal or external technical providers apply the following basic measures (see also chapter VII):

- This includes installing, activating and patching of firewalls on all your networks.
- Segmentation of your network to avoid that DDoS attacks could influence the event or the reputation of the event.
- Where this is relevant installing intrusion detection systems and network traffic monitoring should be considered by the provider.
- To enhance DDOS protection of your online services such as websites, broadcasting and registration platforms, ‘rate limiting thresholds’ could be considered. Detailed guidelines of

the CCB on this matter can be used (https://ccb.belgium.be/sites/default/files/DDoS-proactive-reactive.pdf)

- Regarding video conferencing, make sure that the configuration allows the following measures:
  - Provide the access details (URL and or password) to registered participants only.
  - Consider requiring participants to authenticate themselves before joining a meeting to ensure that only authorized users attend.
  - (Note: the list of participants can only be published with the consent of each participant)
  - Utilise secure video conferencing platforms that use end-to-end encryption, so that the content cannot be intercepted.
  - Enable the option to assign a moderator to monitor the meeting and look for any suspicious behavior, such as unauthorized participants or unusual activity. The moderator should be empowered to remove anyone who is not authorized or acting inappropriately.
  - Make sure that the platform provides functionality for host control such as “mute all”, “forced exit” and password verification.
  - Use virtual backgrounds whenever sharing your video, instead of showing your actual surroundings. This in order to prevent sensitive or private information from being inadvertently displayed.
  - If you opt for recording a meeting, make sure that all participants are aware of the recording and provide their consent. Ensure that recordings are stored securely and are only accessible by authorized individuals during a limited period of time.
- Ensure that web- and e-mail filters are installed and used.
- Ensure that the activity logging functionality of protection/detection hardware or software (e.g. firewalls, antivirus) is enabled, reviewed and stored for a predetermined period of time. The logs should be reviewed for unusual or undesirable trends (e.g. high usage of social media websites ...) that indicate possible intrusions or other problems that result in the need for stronger protection in a particular area.

8. Ensure back-ups of your data

In event organizing almost all information is business critical, especially for high level events. This includes not only applications and data (including on participants), but also configuration data and system data.

Ensure a regular backup and put it offline periodically.

Test back-ups to ensure a swift restoring in case of an incident before or during your event.

Don’t store the organization's data backup on the same network as the system on which the original data resides and provide an offline copy. Among other things, this prevents file encryption by hackers (risk of ransomware).

Having a good and verified backup of all your business-critical files and personal data mitigates the risk and impact of incidents shortly before or during the event.

VI. CCB Services and toolbox to help event organizers

1. Incident reporting

You can report cyber incidents or request assistance at CERT.be of the CCB, before, during or after the Belgian EU Presidency: https://cert.be/en/report-incident

The link above equally gives many information on how to deal with cybersecurity incidents, including basic steps to take when under attack, as well as advice concerning transparent communication during an incident. Read the incident response plan beforehand and take the necessary measures to be able to continue your event in case of an incident or to recover ASAP

The CERT.be of the CCB will try to assist in a secondary line of support. In case your ICT service or cybersecurity service provider can't handle a certain emergency, you can reach out to CERT.be by phone: +32 (0)2 501 05 60, or via the incident reporting form above.

Where relevant, the National Cyber Emergency Plan will be activated to coordinate all severe incidents above a certain threshold.

Please also always file a complaint with the police in case of an incident.

2. CCB's Early Warning System

The Early Warning System (EWS) provides quick and targeted warnings about new cyber threats and attacks, with the goal of making your organization more secure and less vulnerable. With EWS you will receive reports about the threat landscape, warnings about imminent threats, a security rating on your attack surface, indicators of compromise which can help with correlating events, access to the connect and share events of the CCB and spear warnings. Spear warnings are individualized warnings on intrusions, leaked credentials, vulnerable systems, etc. Such individualized warnings allow constituents to quickly obtain relevant information from a reliable source, so that they can take action as quickly as possible to protect themselves.

Federal public administrations who organize events or host tools in the context of the Belgian Presidency of the Council can contact ews@cert.be to benefit from the EWS-services. You should motivate why your public administration would like to make use of the services (i.e. what role you have in the Presidency), and provide contact details as well as a functional (i.e. not a personal) e-mail address for the registration process.

3. SafeOnWeb

With Safeonweb.be, the CCB informs internet users about online security in a quick and accurate manner. Where Cyber Fundamentals is targeted truly to organizations (ranging from small to large and mature), SafeOnWeb is there for all citizens.

- Please don't hesitate to refer your users or visitors to SafeOnWeb for basic cyber hygiene tips.
- Please always forward suspicious emails to suspicious@safeonweb.be , and ask your users and visitors to do the same. This helps protect others from clicking on phishing links.

4. Consider using relevant CCB Advisories

- The CyberFundamentals Framework is a set of concrete measures to protect data, significantly reduce the risk of the most common cyber-attacks and increase an organization's cyber resilience. https://ccb.belgium.be/en/cyberfundamentals-framework
- CCB Technical Guidance on cyber secure **Supply Chain management**: https://ccb.belgium.be/en/document/supply-chain-proces-guidelines)
- CCB Technical Guidance on multi factor authentication: https://www.cert.be/en/news/take-most-important-step-against-cyber-attacks-now-install-two-factor-authentication-2fa-all
- CCB Technical Guidance on mitigation of **DDoS** attacks: https://ccb.belgium.be/sites/default/files/DDoS-proactive-reactive.pdf
- CCB Technical Guidance on protection and response in case your organization would be hit by a **ransomware** attack.
  - https://ccb.belgium.be/en/document/ransomware-how-protect-and-respond
  - https://ccb.belgium.be/en/document/how-respond-ransomware-attack-12-steps

VII. Contracting event organizers and other service providers

When you set up your event, request your supplier to take at least the measures described in this document. In case you contract a service provider, make sure to include where possible contractual clauses that cover these requirements.

More stringent and detailed requirements that can be required from service providers can be found in the CyberFundamentals framework as mentioned above. Additionally, the CCB published a more detailed guideline to manage the cybersecurity of your supply chain. The purpose of this document is to describe control objectives to protect confidentiality, integrity and availability (CIA triad) within the supply chain of network assets and services. The document is targeted to Operators of Essential Services, but could equally be used by Public Administrations and their security officers. https://ccb.belgium.be/en/document/supply-chain-proces-guidelines

If the services you request are of a high technological order and/or the event has high visibility or deals with sensitive data, it might be useful to have a private cybersecurity incident responder under contract – either as support to your own ICT team, or as a requirement to be put on your service provider. Such an incident response entity could be put on standby during the event to immediately be able to act when an incident happens, and assure availability, integrity and confidentiality of your service and data.

It would prove worthwhile to demand from your service providers to perform penetration testing of all systems to test their (outward) exposure to attacks.

In rare and critical cases, the CERT.be of the CCB could be contacted to perform occasional pentesting. The CCB can also assist in referring to concrete funding opportunities to acquire pentesting.

VIII. Questions

If you would have additional related questions, please do not hesitate to get in touch with the CCB at: info@ccb.belgium.be .

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

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

The information provided:

- are exclusive of a general nature and do not intend to take into consideration all particular situations;
- are not necessarily exhaustive, precise or up to date on all points;

Responsible editor:
Centre for Cybersecurity Belgium
Mr. De Bruycker, General Director
Rue de la Loi, 18
1000 Brussels

Legal Deposit:
D/2023/14828/006