CENTRE FOR
CYBERSECURITY
BELGIUM

GUIDE POUR

UNE PRÉSIDENCE BELGE DE L'UE EN TOUTE CYBERSÉCURITÉ

Centre pour la Cybersécurité Belgique
Sous l'autorité du Premier Ministre

I. Préface

La Belgique assurera la présidence tournante du Conseil de l'Union européenne au cours du premier semestre 2024. Durant ces six mois, tous les regards se tourneront vers la Belgique. Une attention porteuse d'opportunités significatives pour notre pays, mais qui s'accompagne également de menaces supplémentaires considérables, y compris des cybermenaces.

La présidence sera une période riche en événements, organisés par les services publics belges ou sous leurs auspices. Pour pouvoir offrir une expérience moderne, agréable et efficace au public, ces événements seront souvent soutenus par de nombreuses technologies numériques, comme des outils de visioconférence, des produits d'enregistrement en ligne, des sites Internet en général, des applications mobiles ou d'autres instruments connectés.

Pour garantir le bon déroulement de tous ces événements et protéger la disponibilité, l'intégrité et l'authenticité de tout le trafic numérique associé d'une manière ou d'une autre à la présidence, il est nécessaire d'assurer un niveau élevé de cybersécurité de ces outils et de leur utilisation. Ce renforcement de la cybersécurité s'impose également pour consolider la confiance des autres États membres de l'UE et de la communauté internationale dans la capacité de notre pays à présider le Conseil. Les efforts visant à renforcer notre présidence de l'UE soutiendront également la mission de la Stratégie nationale de cybersécurité 2021-2025 : faire de la Belgique l'un des pays les moins cybervulnérables d'Europe.

Le Centre de crise national (NCCN) a effectué une analyse des risques liés à la présidence belge de l'Union européenne et a épinglé quatre cybermenaces : perturbation des services (attaques par déni de service distribué, ou DDoS), ransomware (rançongiciel), désinformation et espionnage.

Le Centre pour la cybersécurité Belgique (CCB), avec le soutien d'autres services de sécurité et de renseignement, a donc rédigé un guide permettant d'assurer un niveau plus élevé de cybersécurité pendant la présidence belge. Le public cible de ce document est en premier lieu les coordinateurs et les organisateurs d'événements pendant la période de présidence, mais également leurs fournisseurs de services de gestion d'événements.

Ce guide décrit plus en détail les cybermenaces identifiées lors de l'analyse des risques du NCCN, ainsi que les phénomènes pouvant en découler. Plus concrètement, le document propose une série de **huit exigences et conseils clés en matière de cybersécurité** à prendre en compte lors de la sélection et de l'utilisation d'outils numériques appropriés afin d'atténuer les risques associés aux menaces épinglées. Ces mesures ont été élaborées sur la base du cadre des Cyberfondamentaux publié par le CCB au début de l'année.

Il présente également **quatre services supplémentaires proposés par le CCB** pour aider à prévenir les incidents de cybersécurité et à y répondre. Le cas échéant, ce document fournit également des liens vers des avis existants plus détaillés.

Ce document contient de nombreuses recommandations, mais nous ne saurions trop insister sur deux mesures essentielles :

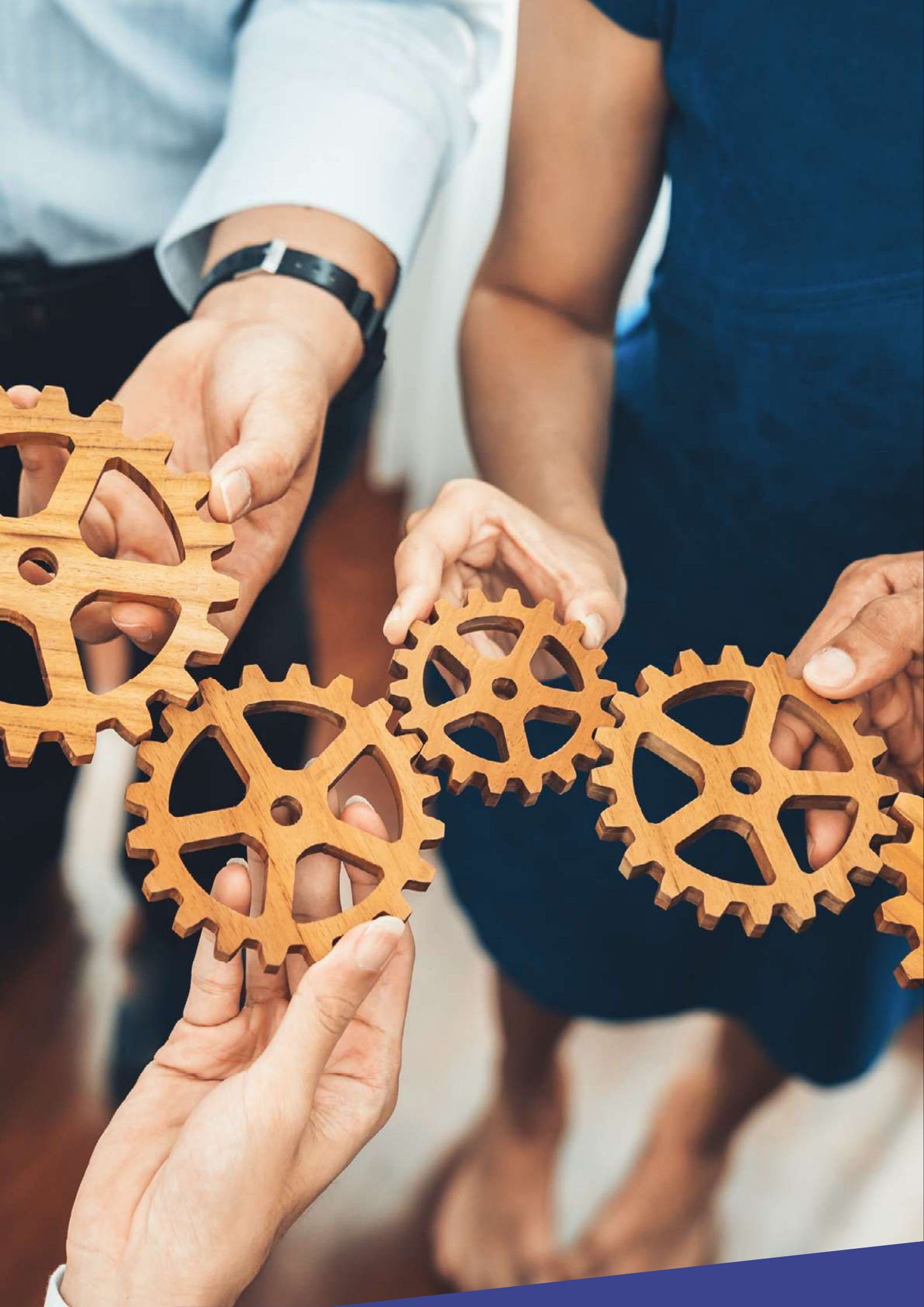
1. Installer l'authentification multifactorielle sur toutes les connexions vers l'extérieur.
2. S'assurer que tous les systèmes et logiciels sont corrigés et mis à jour.

À la fin du document, les organisations trouveront également les coordonnées du point de contacts vers qui se tourner pour obtenir de l'aide, que ce soit avant ou après la survenue d'un cyberincident susceptible d'avoir un impact sur le fonctionnement des événements liés à la présidence.

Profitons de la présidence pour montrer comment, ensemble, nous faisons de la Belgique l'un des pays les moins cybervulnérables d'Europe!

Miguel De Bruycker
Directeur général du CCB

II. Table des matières



III. Portée

Ce document se veut un guide à l'attention de tous les (collaborateurs des) administrations publiques qui organisent des événements utilisant des outils numériques (au cours des événements ou lors de leur préparation) à l'occasion de la Présidence belge du Conseil de l'Union européenne. Il s'adresse par la même occasion aux gestionnaires ICT – et pour certains aspects aussi aux services de communication – associés à ces organisateurs, ainsi qu'à leurs fournisseurs de services (digitaux), qu'ils soient réguliers ou sous contrat dans le cadre de la présidence.

Par conséquent, il comprend des conseils de haut niveau, ainsi que des mesures techniques à prendre, y compris des références à des publications plus spécifiques.

Ce document est destiné aux services publics tant fédéraux que régionaux, et est surtout d'importance pour les événements qui sont organisés hors des locations standards à Bruxelles.

Il est vivement conseillé aux organisateurs d'événements liés à la Présidence belge de tenir compte des conseils décrits dans ce document, en particulier pour les outils numériques suivants :

- Outils de visioconférence (Par exemple MS Teams, Webex, etc.), y compris les instruments associés (chats, inscription, etc.).
- Plateformes d'inscription ou accréditation
- Sites Internet contenant des informations sur les événements
- Médias sociaux
- Applications développées ou utilisées spécifiquement dans le cadre de la présidence belge
- Réseaux Wi-Fi mis en place lors des événements de la présidence
- Systèmes de communication interne pour les organisateurs d'événements
- Systèmes de stockage et de partage de fichiers

Pour tous les événements organisés au Palais d'Egmont, la plupart des services numériques, y compris les services de cybersécurité, seront fournis par les services ICT du Service public fédéral Affaires étrangères et leurs fournisseurs de service numérique.

Pour tous les événements organisés dans les bâtiments du Conseil, les services ICT et liés à la cybersécurité seront fournis par le Secrétariat général du Conseil. Ceci inclut la plateforme d'inscription générale de la Présidence (PPI).

Cependant, si vous organisez des événements ou hébergez des outils en rapport avec ces événements, il est essentiel que les organisateurs vérifient auprès de l'une ou l'autre de ces institutions quelle est l'étendue exacte de ces services et si vous devez héberger les outils vous-même.

Les organisateurs doivent également vérifier auprès d'autres prestataires si des mesures de cybersécurité de base peuvent être prises. Voici quelques exemples de prestataires de service :

- les hôtels ou les salles de réception, qui offrent des services de visioconférence, des réseaux Wi-Fi, voire des applications mobiles
- les applications achetées individuellement
- les organisateurs d'événements, chargés d'acquérir l'un des outils cités ci-dessus pour votre organisation
- les services ICT de votre propre administration.

Enfin, il est important de souligner que ce document a pour but de conseiller. Chaque propriétaire de système conserve la responsabilité finale de la protection adéquate de son propre environnement. Les mesures conseillées dans le présent document constituent une liste d'actions de base et ne garantissent pas une protection contre toutes les attaques. Il appartient aux propriétaires de systèmes de prendre ces mesures en fonction des risques spécifiques auxquels ils sont confrontés.

IV. Cybermenaces

Le Centre de crise national (NCCN) a effectué une analyse générale des risques dans le cadre de la préparation de la présidence belge du Conseil de l'Union européenne. Cette analyse des risques met en évidence quatre cybermenaces méritant une attention particulière pendant la présidence de l'UE :

1. la perturbation de services ou d'événements en ligne,
2. les ransomwares (y compris le vol de données),
3. la désinformation (par le biais des médias sociaux) et
4. l'espionnage.

Les cyberincidents pouvant en découler peuvent affecter le fonctionnement des événements liés à la présidence.

Ces risques sont parfois associés à des acteurs spécifiques, mais en général, il convient de tenir compte de quatre types d'acteurs de cybermenaces :

1. les services militaires et de renseignement étrangers
2. les cybercriminels, qui utilisent les réseaux pour obtenir de l'argent
3. les hacktivistes, qui mènent des cyberactivités intentionnelles dans le but de promouvoir un programme politique, une croyance religieuse ou une idéologie sociale
4. les terroristes, qui utilisent Internet pour commettre des actes violents dans le but d'obtenir un avantage politique et d'instiller la peur dans la population.

Dans le paysage géopolitique actuel, en constante évolution, ces types d'acteurs se mélangent ou collaborent souvent.

Nous vous fournissons ici une brève description de chaque phénomène. Le chapitre suivant propose des mesures d'atténuation et des recommandations appropriées, afin que vous et vos fournisseurs puissiez tenir compte de ces menaces lors de vos événements et surtout lors de la préparation de ces événements.

1. PERTURBATION DE SERVICES OU D'ÉVÉNEMENTS EN LIGNE

Les acteurs malveillants, comme les hackers ou les hacktivistes, peuvent vouloir perturber des événements ou des services de premier plan et ce, afin d'humilier leurs organisateurs ou d'attirer l'attention sur leurs propres revendications.

Le modus operandi adopté le plus souvent dans ce cas est l'attaque par déni de service (distribué) (DDoS)[1]. La demande de service est alors supérieure à la capacité disponible pour y répondre et il en résulte une panne du système. Les groupes hacktivistes pro-russes, en particulier, ont récemment été associés à des campagnes DDoS de grande envergure.

Une telle attaque pourrait impliquer que les plateformes d'accréditation, les plateformes de visioconférence, les sites Internet ou les applications contenant des informations pratiques importantes pour les participants aux événements, voire les outils de communication, soient rendus indisponibles à des moments clés. Cela perturberait gravement les réunions ou leur préparation.

Outre les perturbations en elles-mêmes, de telles attaques peuvent causer des dommages importants à la réputation des autorités, y compris la perte de confiance du public.

2. RANSOMWARE, EXTORSION, VOL DE DONNÉES ET FUITE DE DONNÉES D'IDENTIFICATION

La menace des ransomwares se classe en tête du paysage de l'ENISA Threat Landscape depuis quelques années. Les ransomwares sont des logiciels malveillants qui cryptent les données des utilisateurs dans l'intention de les rendre indisponibles et de demander une rançon.

Le plus souvent, le déploiement d'un ransomware s'inscrit dans une approche d'extorsion multiple, durant laquelle les données sont non seulement cryptées, mais aussi volées et/ou détruites, chaque étape pouvant ou non être liée au paiement d'une rançon. Un tel vol de données peut parfois être lié à l'espionnage.

Les cybercriminels peuvent vouloir lancer des ransomwares ou utiliser des tactiques d'extorsion liées, pendant la présidence belge de l'UE, non seulement pour des objectifs financiers, mais aussi pour perturber notre travail et affaiblir la réputation de notre pays ou de nos institutions publiques.

En outre, le phishing reste souvent le principal vecteur d'attaque pour s'introduire illicitement dans les systèmes.

L'un des plus grands risques associés à ce type d'attaque est également la fuite de données d'identification. Un vol de données peut notamment inclure des mots de passe, qui circuleront ensuite sur le dark web, et seront utilisés pour obtenir un accès illicite à d'autres réseaux. Les outils de la présidence belge doivent donc être protégés efficacement pour éviter ce type d'exposition.

Inversement, des données d'identification volées, notamment de la part du personnel de la Présidence, pourraient aussi permettre aux criminels d'accéder plus facilement à des systèmes concernant notre présidence. L'installation d'une authentification multifactorielle pourrait contribuer à atténuer ce risque particulier.

1. Aujourd'hui, la bande passante du réseau et la disponibilité des ressources de la plupart des organisations sont tellement élevées qu'une attaque menée par une seule machine ne peut généralement pas provoquer un DoS. Les attaques sont donc coordonnées. Elles sont réparties sur plusieurs ordinateurs attaquants, d'où le déni de service distribué (DDoS). Il est important de souligner que, bien que répartis par nature, les ordinateurs participant à un DDoS partagent un objectif commun et que l'attaque est coordonnée.

3. FOREIGN INFORMATION MANIPULATION AND INTERFERENCE (FIMI) / OPÉRATIONS D'INFORMATION (VIA LES MÉDIAS SOCIAUX)

Les acteurs étatiques et non étatiques, y compris leurs mandataires, utilisent des activités d'influence pour manipuler et même changer la perception (et le comportement) d'un public cible national ou étranger.

Pour atteindre ces objectifs stratégiques, ils mènent des opérations psychologiques (PSYOPS) en combinaison avec une série de tactiques, techniques et procédures (TTP) en ligne (et hors ligne) afin de changer « les cœurs et les esprits ».

Les FIMI (= *Foreign Information Manipulation and Interference*) combinent ces activités et sont principalement composés de comportements non illégaux, qui menacent ou ont le potentiel d'avoir un impact négatif sur les valeurs, les procédures et les processus politiques.

La désinformation n'est qu'un des vecteurs du large éventail d'activités découlant des FIMI. Elle est principalement conçue sur mesure, en fonction du public cible. La clé du succès réside dans la répétition du message. Les principaux objectifs des FIMI sont de semer la division ou le discrédit dans une société, de détourner l'attention, etc.

L'on combine alors la diffusion de la propagande ou de la désinformation, en utilisant différentes techniques telles que le déploiement massif de bots/trolls, les opérations de piratage et de fuite, *l'astroturfing*, et d'autres, afin de parvenir à tromper un public.

Les activités de FIMI bien menées sont souvent coordonnées et semblent inauthentiques. Il ne faut toutefois pas oublier que les messages organiques en ligne peuvent aussi avoir un impact considérable.

Pendant les élections fédérales et européennes de 2019, le SGRS et la VSSE ont surveillé et analysé l'espace en ligne/virtuel afin de détecter d'éventuelles activités de FIMI. Par la suite, la pandémie de COVID-19, la campagne de vaccination, l'invasion russe en Ukraine, etc. ont engendré une augmentation substantielle de la manipulation de l'information en ligne, ce qui a donné lieu à la « guerre de l'information » que nous connaissons actuellement.

Une taskforce fédérale, la « Agile Taskforce Information Operations » (ATFIO), dirigée par le SGRS, a été lancée en amont des élections de 2024. Cette taskforce rassemble toutes les entités fédérales nécessaires pour faire face à d'éventuelles activités de FIMI.

4. ESPIONNAGE

La Présidence belge de l'UE et les événements qui l'entourent peuvent également être la cible d'activités d'espionnage.

Les événements rassemblent des acteurs intéressants autour d'un certain sujet et sont donc l'occasion rêvée pour les services de renseignement hostiles de se faire des contacts, de repérer des personnes et même d'établir le premier contact qui peut déboucher sur un recrutement. Il est donc important d'analyser les participants et le public de votre événement en fonction de la sensibilité des sujets abordés.

Mais pourquoi un service de renseignement hostile ferait-il l'effort d'envoyer un infiltré réel à un événement, alors qu'il est tout aussi facile de suivre l'événement en ligne et de collecter toutes les adresses mail ?

V. Mesures de protection fondamentales

Le CyberFundamentals framework propose des mesures de base à mettre en œuvre pour garantir la sécurité d'un événement. Les mesures de base sont résumées ci-dessous et adaptées aux organisateurs d'événements. Il est conseillé aux organisateurs de veiller à la mise en œuvre de ces mesures, le cas échéant et dans la mesure du possible, en fonction des risques. Le CyberFundamentals framework et les normes en découlant vous offriront davantage d'informations, tels qu'ils figurent sur le site web du CCB.

1. FORMEZ VOS COLLABORATEURS À LA SÉCURITÉ DE L'INFORMATION ET À LA CYBERSÉCURITÉ

En tant qu'organisateur, vous devez penser à rédiger un document d'instructions expliquant les pratiques acceptables et les attentes vis-à-vis des sous-traitants (hôtels, sociétés d'hébergement) et des collaborateurs de l'événement. Cela permet de sensibiliser et d'aider à la mise en œuvre correcte des mesures. Ces instructions doivent être spécifiques à votre événement et à votre organisation, mais peuvent en grande partie se fonder sur les avertissements ci-dessus et les lignes directrices reprises dans ce document.

Les instructions données à vos collaborateurs doivent au minimum comprendre des mesures de base visant à prévenir les tentatives de phishing. Le site Internet www.safeonweb.be reprend les techniques de phishing les plus fréquentes. Signaler les mails suspects à l'adresse suspect@safeonweb.be permet également au CCB de protéger les autres utilisateurs.

Les instructions doivent également informer vos collaborateurs du risque de désinformation (FIMI) par une mauvaise utilisation des canaux de communication de l'événement (sites Internet et médias sociaux). Le document doit aussi contenir des instructions sur la surveillance et le signalement de la désinformation attestée sur vos canaux. Les services de communication devraient également coopérer au mieux avec les services de sécurité des ICT pour atténuer ces menaces. Nous rappelons également que le Conseil national de sécurité a imposé une interdiction temporaire de l'utilisation de TikTok sur les appareils des services publics fédéraux, en invoquant des problèmes de confidentialité et de sécurité.

Les instructions destinées aux collaborateurs et aux fournisseurs devraient également inclure un aperçu des responsabilités et des premiers contacts en cas d'incident (voir chapitre VI) et pourraient renvoyer aux publications suivantes du CCB :

- Ransomware : protection et prévention | Centre pour la Cybersécurité (belgium.be)
- Comment répondre à une attaque par ransomware en 12 étapes | Centre pour la Cybersécurité (belgium.be)

2. INSTALLEZ L'AUTHENTIFICATION MULTIFACTORIELLE (MFA) ET GÉREZ LES DONNÉES D'IDENTIFICATION

Imposez l'authentification des utilisateurs dès que possible. L'authentification à deux facteurs est une mesure clé qui devrait être appliquée dès que possible.

Outre l'authentification multifactorielle, il convient de respecter les règles de routine en matière de mots de passe :

- Changez tous les mots de passe par défaut
- Veillez à ce que personne ne travaille avec des privilèges d'administrateur pour des tâches quotidiennes
- Conservez une liste limitée et actualisée des comptes d'administrateurs système
- Appliquez les règles relatives aux mots de passe (longueur spécifique, combinaison de différents types de caractères, modifications périodiques ou en cas de suspicion de compromission, etc.)
- N'utilisez que des comptes individuels et ne jamais partager les mots de passe

- Désactivez immédiatement les comptes inutilisés
- Gérez les droits et privilèges par groupes d'utilisateurs

3. GÉREZ LES ACCÈS NUMÉRIQUES ET PHYSIQUES

Il peut être utile d'installer un bureau d'enregistrement pour l'accès physique à un événement, mais il convient également empêcher l'accès physique non autorisé à vos dispositifs numériques sur votre événement, tels que les serveurs ou les outils de communication.

Le même principe devrait être utilisé pour les événements numériques, à savoir créer des URL de connexion dédiées aux utilisateurs pour les événements numériques où les menaces d'espionnage, de FIMI ou de vol de données sont pertinentes. Cela comprend l'accès aux visioconférences, aux réseaux Wifi, etc.

Le principe du « moindre privilège » doit être appliqué pour les organisateurs d'événements, ce qui signifie que l'accès des collaborateurs aux données et aux informations doit être limité aux systèmes et aux informations spécifiques dont ils ont besoin pour accomplir leurs tâches.

Lorsque les collaborateurs changent de poste ou quittent l'organisation, leur accès doit être modifié ou supprimé.

4. SÉCURISEZ VOS POINTS D'ACCÈS NUMÉRIQUES ET SCINDEZ LES RÉSEAUX INTERNES ET RÉSEAUX « VISITEURS »

En cas d'utilisation d'un réseau sans fil, demandez à votre support technique de modifier le mot de passe administratif lors de l'installation d'un point d'accès sans fil, et réglez le routeur pour qu'il utilise au moins l'accès protégé Wi-Fi avec la norme de cryptage avancée (AES) pour le cryptage.

Veillez à ce que l'accès et les réseaux des participants à l'événement, des présentateurs et des organisateurs soient séparés les uns des autres. En particulier, l'accès aux outils pour les participants ainsi que les réseaux qu'ils utilisent doivent être autant que possible séparés de ceux des organisateurs, par exemple en segmentant les réseaux Wi-Fi, ainsi que les liens d'accès. Dans tous les cas, les réseaux internes doivent être séparés des réseaux destinés aux invités.

Comme indiqué plus haut, il convient d'utiliser l'authentification multifactorielle (authentification à deux facteurs), pour les accès aux réseaux internes, car il s'agit de la mesure la plus efficace contre les fuites de données d'identification qui découlent de toutes les menaces.

Pour les événements plus sensibles, il convient d'imposer une politique de login et de mot de passe personnels afin de décourager l'espionnage et le vol d'informations.

Si des organisateurs disposent de droits d'administrateur, veillez à séparer le compte d'administrateur du compte personnel afin de réduire le risque de ransomware.

5. TENEZ UN INVENTAIRE DU MATÉRIEL ET DES LOGICIELS UTILISÉS POUR L'ORGANISATION DE VOTRE ÉVÉNEMENT

Tenir un inventaire du matériel informatique (ordinateurs, tablettes, smartphones, systèmes de communication pour les organisateurs d'événements), des plateformes logicielles, des applications et des supports de stockage d'informations est une condition préalable à la prévention des intrusions liées au vol (espionnage). Il s'agit également d'un outil permettant de gérer les mesures de protection, de répondre aux alertes précoces et de protéger vos systèmes avec les dernières mises à jour de sécurité en temps opportun.

Il est également utile de structurer les mesures de suppression des informations après l'événement. Par exemple, le nettoyage électronique des ordinateurs en vue de leur réutilisation permet d'éviter le vol de données.

6. INSTALLEZ LES MISES À JOUR ET MAINTENEZ TOUS VOS LOGICIELS À JOUR

De nombreux incidents se produisent en raison de vulnérabilités pour lesquelles une mise à jour est disponible depuis longtemps. Il est donc essentiel de veiller à ce que les correctifs et les mises à jour de sécurité des systèmes d'exploitation et des logiciels soient installés en temps voulu. Les services publics fédéraux peuvent avoir accès au système d'alerte EWS du CCB et réagir aux alertes EWS reçues (voir chapitre VI.2 ci-dessous). Les fournisseurs professionnels devraient être abonnés à un fournisseur professionnel d'alertes.

Veillez également à l'installation et à la mise à jour des programmes antivirus, antispyware et autres programmes de lutte contre les logiciels malveillants.

7. ASSUREZ LA GESTION DE L'INTÉGRITÉ DE VOTRE RÉSEAU EN COOPÉRATION AVEC VOTRE FOURNISSEUR

Exigez et vérifiez que vos prestataires techniques internes ou externes appliquent les mesures de base suivantes (voir également le chapitre VII) :

- Il s'agit notamment d'installer, d'activer et de corriger les pare-feu sur tous vos réseaux.
- Optez pour une segmentation de votre réseau pour éviter que des attaques DDoS n'influencent l'événement ou sa réputation.
- Le cas échéant, le fournisseur devrait envisager d'installer des systèmes de détection d'intrusion et de surveillance du trafic réseau.
- Vous pouvez également envisager des « seuils de limitation du débit » pour renforcer la protection DDoS de vos services en ligne tels que les sites Internet, les plateformes de diffusion et d'inscription. Le CCB propose des lignes directrices détaillées à ce sujet (https://atwork.safeonweb.be/fr/tools-resources/attaque-ddos).
- En ce qui concerne la visioconférence, assurez-vous que la configuration permet les mesures suivantes :
  - Fournissez les détails d'accès (URL et/ou mot de passe) uniquement aux participants enregistrés.
  - Demandez aux participants de s'authentifier avant de rejoindre une réunion afin de vous assurer que seuls les utilisateurs autorisés y participent.
  - (Note : la liste des participants ne peut être publiée qu'avec le consentement de chacun d'entre eux)
  - Utilisez des plateformes de visioconférence sécurisées qui utilisent le cryptage de bout en bout, afin que le contenu ne puisse pas être intercepté.
  - Activez l'option permettant de désigner un modérateur chargé de surveiller la réunion et de détecter tout comportement suspect, tel que des participants non autorisés ou une activité inhabituelle. Le modérateur doit être habilité à exclure toute personne non autorisée ou agissant de manière inappropriée.
  - Assurez-vous que la plateforme offre des fonctionnalités de contrôle, telles que la « mise en sourdine », la « sortie forcée » et la vérification du mot de passe.
  - Utilisez des arrière-plans virtuels lorsque vous partagez votre vidéo, au lieu de montrer votre environnement réel, afin d'éviter que des informations sensibles ou privées ne soient affichées par inadvertance.
  - Si vous optez pour l'enregistrement d'une réunion, assurez-vous que tous les participants sont au courant de l'enregistrement et qu'ils y consentent. Veillez à ce que les enregistrements soient stockés en toute sécurité et ne soient accessibles qu'aux personnes autorisées pendant une période limitée.
- Assurez-vous que des filtres sont installés et utilisés pour Internet et les services de messagerie électronique.
- Veillez à ce que la fonctionnalité d'enregistrement des activités du matériel ou des logiciels de protection/détection (par exemple, pare-feu, antivirus) soit activée, examinée et stockée pendant une période prédéterminée. Les enregistrements doivent être examinés pour détecter des tendances inhabituelles ou indésirables (utilisation élevée des sites Internet de médias sociaux, etc.) qui indiquent d'éventuelles intrusions ou d'autres problèmes nécessitant une protection plus forte dans un domaine particulier.

8. ASSUREZ LA SAUVEGARDE DE VOS DONNÉES

Lors de l'organisation d'événements, presque toutes les informations sont critiques pour l'entreprise, en particulier pour les événements de haut niveau. Cela concerne les applications et les données (y compris celles des participants), mais aussi les données de configuration et les données système.

Assurez une sauvegarde régulière et stockez-la hors ligne périodiquement.

Testez les sauvegardes pour garantir une restauration rapide en cas d'incident avant ou pendant votre événement.

Ne stockez pas la sauvegarde des données de l'organisation sur le même réseau que le système sur lequel se trouvent les données originales et conservez une copie hors ligne. Cette précaution permet notamment d'éviter le cryptage des fichiers par des hackers (risque de ransomware).

En disposant d'une bonne sauvegarde vérifiée de tous les fichiers critiques de l'entreprise et des données personnelles, vous atténuez le risque et l'impact d'incidents survenant peu avant ou pendant l'événement.

VI. Services et outils du CCB à destination des organisateurs d'événements

1. SIGNALEMENT DES INCIDENTS

Vous pouvez signaler des cyberincidents ou demander de l'aide avant, pendant et après la présidence belge de l'UE : Signaler un incident | Cert

Le lien ci-dessus contient également de nombreuses informations sur la manière de gérer les incidents de cybersécurité, y compris les mesures de base à prendre en cas d'attaque, ainsi que des conseils sur comment adopter une communication transparente pendant un incident. Lisez le plan d'intervention en cas d'incident à l'avance et prenez les mesures nécessaires pour pouvoir poursuivre votre événement en cas d'incident ou pour rétablir la situation le plus rapidement possible.

Le CCB pourra intervenir en tant que soutien secondaire. Si votre fournisseur de services ICT ou de cybersécurité n'est pas en mesure de gérer une certaine urgence, vous pouvez contacter le CCB par téléphone : +32 (0)2 501 05 60, ou via le formulaire de signalement des incidents ci-dessus.

Le cas échéant, le plan national d'urgence cybernétique sera activé pour coordonner tous les incidents graves dépassant un certain seuil.

Veillez également toujours à déposer plainte auprès de la police en cas d'incident.

2. EARLY WARNING SYSTEM DU CCB

L'Early Warning System (EWS) fournit des avertissements rapides et ciblés concernant les nouvelles cybermenaces et attaques, dans le but de rendre votre organisation plus sûre et moins vulnérable. Avec ce système, vous recevrez des rapports sur le paysage des menaces, des avertissements sur les menaces imminentes, une note de sécurité sur votre surface d'attaque, des indicateurs de compromission qui peuvent aider à corréler les événements, l'accès aux événements de connexion et de partage du CCB et des « spear warnings ». Les « spear warnings » sont des avertissements individualisés sur les intrusions, les fuites d'informations d'identification, les systèmes vulnérables, etc. Ces avertissements individualisés permettent aux personnes concernées d'obtenir rapidement des informations pertinentes auprès d'une source fiable, afin de pouvoir prendre des mesures le plus rapidement possible pour se protéger.

Les services publics fédéraux qui organisent des événements ou accueillent des outils dans le cadre de la Présidence belge du Conseil peuvent contacter ews@cert.be pour bénéficier des services EWS. Vous devrez expliquer pourquoi votre service public souhaite utiliser les services (c'est-à-dire le rôle que vous jouez dans le cadre de la présidence) et fournir vos coordonnées ainsi qu'une adresse électronique fonctionnelle (c'est-à-dire non personnelle) pour le processus d'inscription.

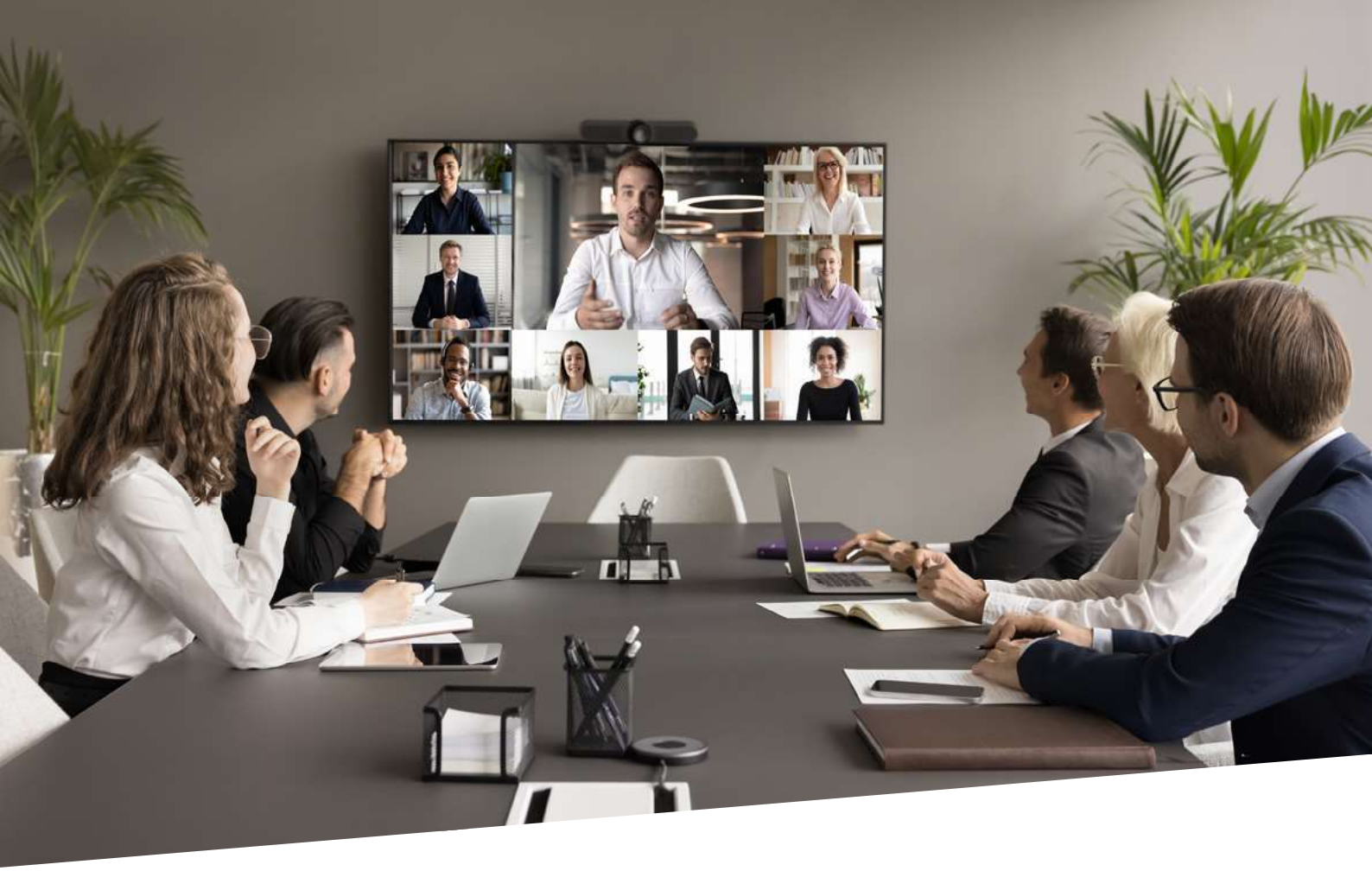
3. SAFEONWEB

Avec www.safeonweb.be, le CCB informe les internautes sur la sécurité en ligne de manière rapide et précise. Alors que les CyberFundamentals s'adressent aux organisations (des plus petites aux plus grandes), Safeonweb concerne tous les citoyens.

- N'hésitez pas à renvoyer vos utilisateurs ou visiteurs vers Safeonweb pour des conseils de base en matière de cyberhygiène.
- Veillez également à transmettre tous les emails suspects à suspect@safeonweb.be et demandez à vos utilisateurs et visiteurs de faire de même. Vous éviterez ainsi que d'autres personnes ne tombent dans le piège d'une tentative de phishing.

4. ENVISAGEZ D'UTILISER LES OUTILS PERTINENTS DU CCB

- Safeonweb at work : https://atwork.safeonweb.be
- Safeonweb : www.safeonweb.be
- Centre pour la Cybersecurité Belgique : www.ccb.belgium.be



VII. Engager des organisateurs d'événements et autres prestataires de services sous contrat

Lorsque vous organisez votre événement, demandez à votre fournisseur de prendre au moins les mesures décrites dans le présent document. Si vous passez un contrat avec un prestataire de services, veillez à inclure, dans la mesure du possible, des clauses contractuelles couvrant ces exigences.

Des exigences plus strictes et plus détaillées qui peuvent être demandées aux fournisseurs de services peuvent être trouvées dans le CyberFundamentals, comme mentionné ci-dessus. En outre, le CCB a publié un guide plus détaillé pour vous aider à gérer votre chaîne d'approvisionnement. Le but de ce document est de décrire les objectifs de contrôle pour protéger la confidentialité, l'intégrité et la disponibilité (triade CIA) au sein de la chaîne d'approvisionnement des actifs et des services du réseau. Ce document s'adresse en premier lieu aux opérateurs de services essentiels, mais il pourrait également être utilisé par les administrations publiques et leurs responsables de la sécurité. https://ccb.belgium.be/fr/document/lignes-directrices-«-gestion-sécuritaire-de-la-chaîne-d'approvisionnement-»-supply-chain

Si les services que vous demandez sont d'un niveau technologique élevé et/ou si l'événement a une grande visibilité ou traite de données sensibles, il peut être utile de conclure un contrat avec une entité privée de réponse aux incidents de cybersécurité - soit comme soutien à votre propre équipe ICT, soit comme exigence à l'égard de votre fournisseur de services. Cette entité de réponse aux incidents pourrait rester en alerte pendant l'événement afin d'être immédiatement en mesure d'agir en cas d'incident et d'assurer la disponibilité, l'intégrité et la confidentialité de votre service et de vos données.

Il serait utile d'exiger de vos fournisseurs de services qu'ils effectuent des tests d'intrusion de tous les systèmes afin de tester leur exposition (extérieure) aux attaques.

Dans des cas rares et critiques, il est envisageable de contacter le CCB pour effectuer des tests d'intrusion occasionnels. Le CCB peut également vous aider à trouver des possibilités de financement concrètes pour réaliser des tests d'intrusion.

VIII. Questions

Si vous avez d'autres questions, n'hésitez pas à contacter le CCB : info@ccb.belgium.be

Les informations fournies :

- sont exclusivement à caractère général et n'entendent pas prendre en considération toutes les situations particulières ;
- ne sont pas nécessairement exhaustives, précises ou actualisées sur tous les points.

Éd. Responsable
Centre pour la Cybersécurité Belgique
M. De Bruycker, Directeur général
Rue de la Loi, 18
1000 Bruxelles

Dépôt légal
D/2023/14828/005

Photos © Adobe Stock