Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense, de la protection de la population et des sports DDPS

Office fédéral de la cybersécurité OFCS

20 juin 2024

Conférence de haut niveau sur la paix en Ukraine : premier bilan de l'OFCS sur les travaux du réseau de suivi de la cybersituation

La conférence de haut niveau sur la paix en Ukraine s'est déroulée les 15 et 16 juin 2024 au Bürgenstock avec la participation de délégations de près de cent États. Des attaques informatiques contre la conférence et les infrastructures en Suisse étaient déjà attendues avant la tenue de cet événement. Plusieurs cyberattaques ont effectivement eu lieu, mais elles ont toutes été identifiées à temps et rapidement contrées. Dans le présent rapport, l'Office fédéral de la cybersécurité (OFCS) dresse un premier bilan de l'engagement du réseau de suivi de la cybersituation.

1. Objectifs et mission

Les objectifs prioritaires au niveau de la cyberdéfense étaient les suivants :

1. **Garantir la liberté de mouvement et la disponibilité en tout temps** des moyens de communication des forces de sécurité et d'intervention ;

2. **Assurer la confidentialité, l'intégrité et la disponibilité des ressources informatiques** de tous les participants à la conférence et des partenaires du réseau de suivi de la cybersituation ;

3. **Garantir une circulation efficace des informations** là où elles apportent une utilité opérationnelle maximale ;

4. Établir une compréhension **claire des rôles** et adopter des **mesures uniformes** entre les partenaires.

En plus de sa mission de protection, l'OFCS a assuré la coordination générale de la préparation, de la mise en œuvre et du suivi. Le réseau de suivi de la cybersituation comprenait près d'une centaine de spécialistes des autorités nationales et cantonales ainsi que des organisations du secteur privé. Chaque organisation a rempli sa mission et a partagé les informations nécessaires avec ses partenaires. La mission a été accomplie et les objectifs atteints.

2. Réseau de suivi de la cybersituation et centre de suivi de la cybersituation

Le jeudi 12 juin 2024, l'OFCS a mis en service, en collaboration avec la police cantonale lucernoise et dans les locaux de cette dernière, le centre de suivi de la cybersituation pour l'engagement lors de la conférence de haut niveau sur la paix en Ukraine. Des travaux de planification et de prévention avaient eu lieu en amont pendant des semaines. Ceux-ci comprenaient notamment des mesures de sensibilisation aux cibles potentielles et la réduction de la vulnérabilité (*Attack Surface Management*) des infrastructures critiques et des organisations impliquées.

Grâce au grand engagement de toutes les parties concernées et à une bonne préparation, la coopération a fonctionné en permanence et sans accroc. Le large soutien dont a bénéficié le réseau de suivi de la cybersituation a considérablement contribué à renforcer la cyberrésilience avant la conférence et à réagir rapidement et efficacement aux cyberattaques qui ont tenté de la perturber.

Parallèlement, la communication destinée au public a été assurée sous la direction de l'OFCS. L'objectif était d'informer tous les partenaires de manière aussi transparente, correcte et rapide que possible sur les incidents les concernant. Cela a nécessité de préparer en permanence des informations actuelles provenant du suivi coordonné de la situation et de se synchroniser avec les organisations partenaires.

3. Événements dans le cyberespace en raison de la conférence

Plusieurs événements se sont produits dans le cyberespace en Suisse peu avant, pendant et peu après la conférence. Les événements suivants méritent notamment d'être mentionnés :

- **Attaques par saturation contre des sites web d'autorités et d'organisations :**
  Le jeudi 13 juin 2024, l'OFCS et ses partenaires ont détecté des attaques par saturation (dites attaques *DDoS*), dont il a été démontré qu'elles avaient été menées par un groupe de hacktivistes pro-russes appelé « NoName057(16) ». Ces cyberattaques étaient dirigées contre les sites web publics de 22 autorités et organisations suisses au total. Dans l'ensemble, les attaques par saturation se sont situées dans la plage attendue et n'ont entraîné que des perturbations mineures des infrastructures informatiques. À aucun moment, les systèmes informatiques et les données de la conférence ou des organisations impliquées dans son déroulement n'ont été menacés.

- **Tentatives d'intrusion numérique dans les systèmes informatiques des cantons NW/OW :**
  Les services informatiques des cantons de Nidwald (NW) et d'Obwald (OW) ont signalé des tentatives d'intrusion numérique dans leurs systèmes de messagerie électronique. Une analyse de l'OFCS a montré qu'il s'agissait de tentatives d'intrusion opportunistes sans rapport avec la conférence. Elles ont toutes échoué. L'informatique cantonale a identifié avec l'OFCS des mesures de durcissement et les a immédiatement mises en œuvre.

- **Attaque de phishing (hameçonnage) contre des collaborateurs de la centrale d'appels sanitaires urgents de Lucerne (LU) :**
  Peu avant la conférence, une cyberattaque présumée a eu lieu contre des employés de la centrale d'appels sanitaires urgents du canton de Lucerne. Des inconnus auraient tenté d'obtenir les données d'accès de collaborateurs et collaboratrices au

moyen d'e-mails falsifiés (appelés *phishing e-mails*). La cyberattaque a été identifiée comme telle par des employés et signalée au réseau de suivi de la cybersituation. Grâce à la réaction rapide des collaboratrices et collaborateurs, la cyberattaque a pu être contrée à temps.

- **Un faux pas pendant la retransmission en direct du DFAE entraîne des rumeurs de cyberattaques :**
  Après la retransmission en direct d'un discours de la présidente de la Confédération Viola Amherd et du président ukrainien Zelensky, des collaboratrices et collaborateurs du service d'interprétation ont oublié de couper leur micro.
  Lors de la discussion qui s'en est suivie, ces derniers ont fait état dans le flux en direct du DFAE de « problèmes techniques » pendant la traduction, l'un d'entre eux faisant remarquer qu'il avait en effet mis en garde contre les cyberattaques avant la conférence. Cette mésaventure a entraîné plusieurs demandes de la part des médias auprès de l'OFCS et du Département fédéral des affaires étrangères (DFAE), ainsi que des articles sur de possibles cyberattaques (russes) dans certains médias suisses. Les problèmes techniques évoqués n'étaient toutefois pas liés à une cyberattaque.

- **Panne de courant dans la ville de Berne :**
  Une panne de courant survenue dimanche matin dans la ville de Berne a alimenté les rumeurs d'une possible cyberattaque. La panne de courant a entraîné le basculement sur le réseau électrique de secours de certaines autorités fédérales ainsi que d'autres organisations sises à Berne. Après clarification avec les exploitants de réseau et les entreprises d'électricité, il a été possible d'exclure qu'une cyberattaque ait été à l'origine de la panne de courant.

- **Vandalisme numérique :**
  Une personne inconnue a commis des actes de vandalisme numérique sur un portail accessible au public, ce qui a entraîné la détérioration momentanée d'un système d'intervention. Le portail est supporté et exploité par une association suisse.
  L'incident a été rapidement identifié et les données « dégradées » ont pu être retirées sans délai du système d'intervention. La sécurité des systèmes d'intervention ou de leurs données n'a jamais été menacée.

D'autres cyberattaques présumées ont été lancées contre le dispositif de sécurité de la conférence. Des mesures ont été prises rapidement. Aucune information supplémentaire n'est communiquée à l'heure actuelle sur ces attaques. Grâce aux mesures prises, ces attaques n'ont toutefois jamais pu mettre en danger la sécurité ou le déroulement de la conférence.

4. Généralités

L'OFCS a mis fin à l'engagement du réseau de suivi de la cybersituation le dimanche 16 juin 2024. Le 20 juin 2024, l'OFSC constate encore quelques attaques DDoS sur des cibles en Suisse. La situation devrait se normaliser dans les jours à venir.