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

Mesures de cyberrésilience dans le contexte de grands événements et conférences internationales

De grands événements ou des conférences internationales, comme le Eurovision Song Contest (ESC), ont des répercussions sur la situation en matière de cybermenace. Le risque que des acteurs en profitent pour lancer des cyberattaques contre ces manifestations, ou des organisations ou des personnes qui y participent, est plus élevé. Alors que les motivations et les objectifs des cyberattaques sont très variables, les mesures de protection de base restent les mêmes : il suffit de les appliquer pour prévenir déjà quantité de cyberincidents potentiels.

Ce document donne un aperçu des recommandations de base pour protéger ce qui entoure les grands événements et les conférences internationales. Connues depuis des années, nombre d'entre elles sont désormais considérées comme les meilleures pratiques (« *best practices* ») dans ce domaine. L'Office fédéral de la cybersécurité (OFCS) conseille d'appliquer ces mesures indépendamment du niveau de menace dans le cyberespace et de lui annoncer toute activité suspecte au moyen du formulaire d'annonce[1].

Ce document ne traite pas des besoins de protection spécifiques des organisations directement impliquées. Ainsi, ces organisations doivent tenir compte des dangers et des exigences qui leur sont propres en plus des mesures décrites ici.

Mesures prioritaires :

Les mesures suivantes se révèlent particulièrement efficaces pour minimiser les cyberrisques et augmenter la cyberrésilience.

- **Sécurisation des accès à distance**
  Il importe de sécuriser systématiquement les accès à distance (VPN, RDP, Citrix, etc.) et tous les autres accès aux ressources internes (messagerie électronique, Sharepoint, etc.) avec un second facteur (double authentification). Il en va de même pour les accès des fournisseurs, des partenaires contractuels, etc.
- **Gestion des correctifs et du cycle de vie**
  Il importe de sécuriser au fur et à mesure tous les systèmes en installant systématiquement les mises à jour (« *update* »). Il faut installer dans les 24 heures les mises à jour qui visent à corriger les failles de sécurité critiques d'un système accessible sur internet. Il faut désactiver les logiciels et les systèmes qui ne sont plus actualisés par le fabricant (obsolètes) ou les placer dans une zone cloisonnée, séparée du restant du réseau.
- **Sauvegardes hors ligne**
  Il faut effectuer régulièrement des copies de sauvegarde des données. Vous pouvez recourir à la méthode de rotation de la sauvegarde des données (principe des générations : sauvegardes quotidiennes, hebdomadaires et mensuelles, avec au moins deux générations). Après la sauvegarde, il faut s'assurer que le support est déconnecté de l'ordinateur et du réseau, et le conserver en lieu sûr. Vous pouvez aussi recourir au système de stockage WORM.

[1] https://www.report.ncsc.admin.ch/fr

Recommandations supplémentaires

Les mesures mentionnées précédemment réduisent déjà considérablement les cyberrisques. Nous vous recommandons dans la mesure du possible de les renforcer par les mesures complémentaires suivantes.

- **Contact en cas d'incident de sécurité**
  Il est fortement recommandé de définir un responsable de la sécurité en cas d'incident. Ainsi, l'OFCS ou les autorités de poursuite pénale peuvent le contacter rapidement au besoin. Il est recommandé d'utiliser la norme security.txt[2] pour publier ce contact de sécurité.
- **Gestion de la continuité des activités**
  Il est utile de réfléchir aux activités essentielles de l'entreprise, à leurs dépendances informatiques et à leur poursuite en cas de panne, au moins en mode dégradé. Il faut aussi contrôler régulièrement si les processus d'urgence et de crise sont à jour. Au minimum, il faut déterminer qui informe qui et qui peut prendre quelle décision.
- **Protection contre les attaques par déni de service (DDoS)**
  Il faut protéger les applications web, les plateformes ou les systèmes exposés sur internet qui sont indispensables aux activités de l'entreprise avec une solution anti-DDoS. Demandez les solutions possibles à votre hébergeur ou à votre fournisseur d'accès internet.
- **Recours à un EDR ou un XDR pour détecter les anomalies**
  Utilisez un EDR (« *Endpoint Detection and Response* ») ou un XDR (« *eXtended Detection and Response* ») sur tous les clients et serveurs pour détecter et bloquer les activités suspectes.
- **Accès limité aux systèmes exposés**
  Contrôlez les accès aux systèmes, applications et plateformes exposés sur internet et limitez-les autant que possible. Il est utile de recourir au blocage géographique ou à une liste de permissions (« *allowlist* ») des adresses ou réseaux IP.
- **Contrôle des fichiers journaux pertinents pour la sécurité**
  Contrôlez régulièrement les fichiers journaux (« *logs* ») importants pour la sécurité, comme ceux des logiciels antivirus, des EDR/XDR, des services proxy web ou des VPN, pour détecter au plus vite toute activité suspecte. Il est important de vérifier immédiatement tout message d'alerte d'un logiciel de sécurité et prendre les contre-mesures qui s'imposent.

Vous trouverez d'autres mesures techniques et organisationnelles dans notre aide-mémoire pour les PME : https://www.ncsc.admin.ch/it-sicherheit-fuer-kmus-fr

[2] https://www.ncsc.admin.ch/securitytxt-fr