De : Gaillard Joëlle pour le compte de Info DGAIC
Cc : DGAIC_PREF_Préfets; DGAIC_PREF_resp de bureau; comite@avsm.ch; ucv_ucv.ch; presidence@asccgv.ch
Objet : Situation en Ukraine | Mesures préventives contre les cyberattaques
Date : jeudi, 24 mars 2022 14:23:39
Pièces jointes : image002.png
image005.png

DGNSI

Sécurité de l'information et Cybersécurité

Mercredi 23 mars 2022

Mesdames, Messieurs,

Suite au déclenchement de la crise en Ukraine, de potentiels risques liés à l'informatique et à la cybersécurité apparaissent.

De par sa prise de position dans ce conflit, la Suisse et le Canton de Vaud se trouvent dans une position jugée hostile à la Russie, et des représailles sous forme de cyberattaques ne peuvent malheureusement pas être exclues.

Afin de se préparer au mieux contre de potentielles cyberattaques, le Canton de Vaud émet les recommandations suivantes :

1. **Mise en place de protection anti-DDOS**

   Les attaques DDOS (attaque distribuée par déni de service) pourraient être utilisées contre des organisations, entreprises ou administrations vaudoises afin de paralyser les activités opérationnelles.

2. **Renforcement de la protection contre les rançongiciels**

   Cette menace n'est pas directement liée à la situation en Ukraine, mais peut être amplifiée par cette dernière. Afin de vous prémunir contre une attaque de rançongiciels, nous vous recommandons de mettre en place les mesures suivantes :

   - Assurez-vous d'avoir des sauvegardes hors ligne à jour et de votre capacité à les restaurer.
   - Formez vos collaborateurs à la bonne gestion des courriers électroniques. L'e-mail est souvent le canal d'entrée de ce type d'attaque, il est primordial que votre personnel sache reconnaître ces tentatives.
   - Renforcez votre protection e-mail en bloquant la réception de courriels contenant des fichiers dangereux sur votre passerelle de messagerie. Bloquez toutes les pièces jointes contenant des macros (par ex. les fichiers Word, Excel ou PowerPoint contenant des macros) ainsi que les fichiers exécutables (extensions .exe, .bat., .cmd, etc.).
   - Utilisez une solution anti-malware afin qu'une attaque par rançongiciel soit détectée au plus tôt. Ces logiciels peuvent être déployés facilement sur les postes de travail, ainsi que sur les serveurs.
   - Ayez connaissance de la procédure à suivre en cas d'attaque :
     - https://www.vd.ch/fileadmin/user_upload/organisation/dinf/dsi/ussi/ConseilsCyberattaque.pdf
     - https://www.skppsc.ch/fr/sujets/internet/piratage-logicielsmalveillants/
     - https://www.ncsc.admin.ch/ncsc/fr/home/cyberbedrohungen/ransomware.html

3. **Evaluation et surveillance des dépendances informatiques**

   Il se pourrait que la Russie utilise les fournisseurs de solutions informatiques pour propager des

logiciels malveillants et attaquer leurs utilisateurs. Vérifiez et surveillez les dépendances potentielles que vous pourriez avoir sur des solutions provenant d'entreprises russes, biélorusses ou ukrainiennes.

Ces logiciels pourraient être détournés de leurs utilisations premières à des fins de cyberattaques ou de cyber espionnage. L'Allemagne a récemment mis en garde contre l'utilisation des solutions antivirus Kaspersky (https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html)

4. **Mise en place d'un blocage géographique de connexion (geofencing)**

   Si votre infrastructure le permet, coupez les flux entrants et sortants vers les IP russes, biélorusses ou ukrainiennes.

   Ces sources pourraient être utilisées pour lancer ou véhiculer des attaques informatiques depuis ces pays.

   Cette mesure peut cependant être contournée par l'utilisation de VPN ou de services informatiques commerciaux se trouvant dans d'autres pays.

En vous remerciant pour l'attention que vous porterez à ce message, nous vous prions de recevoir, Mesdames, Messieurs, nos cordiales salutations.

Direction générale du numérique
et des systèmes d'information

Centre opérationnel de sécurité (SOC)

Avenue de Longemalle 1, CH-1020 Renens
Tél: +41 21 338 10 38 – soc@vd.ch

canton de vaud