Cybersécurité : les Five Eyes redoutent une offensive russe

Face à l'élévation du risque cyber en plein conflit Russie-Ukraine, l'alliance de renseignement dite des Five Eyes – États-Unis, Canada, Australie, Nouvelle-Zélande, Royaume-Uni – peaufine sa communication officielle. Les agences* de cybersécurité concernées exhortent les organisations en charge d'infrastructures critiques, alliées et partenaires, à se préparer à des attaques opérées par des entités parrainées par l'État russe ou ses sympathisants.

« L'invasion russe de l'Ukraine pourrait exposer des organisations aussi bien dans la région que dans le reste du monde à une augmentation de la cyberactivité malveillante », indique une alerte de sécurité conjointe. « Cette activité pourrait répondre [aux sanctions] économiques sans précédent imposées à la Russie, et au soutien matériel apporté (à l'Ukraine) par les Etats-Unis, leurs alliés et leurs partenaires », ajoutent les auteurs de l'alerte.

Dans leur alerte, les entités concernées fournissent des détails techniques concernant l'activité présumée d'une douzaine de groupe de pirates informatiques et cybercriminels,parrainées par l'État russe ou privés, susceptibles de mener ces attaques cyber.

Protégez mieux vos infrastructures critiques

Dans ce contexte, les autorités de cybersécurité recommandent à leurs alliés et partenaires en charge d'infrastructures essentielles de :

– Patcher tous les systèmes. Appliquer en priorité des correctifs aux vulnérabilités exploitées connues.
– Utiliser l'authentification multifacteur.
– Sécuriser et surveiller le protocole RDP (Remote Desktop Protocol) et « d'autres services à risque ».
– Sensibiliser et former les utilisateurs finaux.

L'alerte émanant des Five Eyes fait suite à d'autres avertissements de sécurité émanant de l'administration Biden et du Bureau fédéral d'enquête (FBI) depuis le lancement de l'offensive militaire russe contre l'Ukraine, le 24 février dernier.

En France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a elle aussi réaffirmé l'importance du « renforcement de la vigilance cyber » des organisations.

Un bulletin, alimenté et « mis à jour régulièrement » par l'ANSSI, centralise et diffuse « les éléments d'intérêt cyber en lien avec le contexte actuel pour favoriser le renforcement du niveau de protection de l'ensemble des entités françaises. »

* CISA (Etats-Unis), CCCS (Canada), ACSC (Australie), NCSC NZ (Nouvelle Zélande), NCSC UK (Royaume-Uni).

(crédit photo © Shutterstock)