# Les cyberrisques mondiaux s'intensifient à la suite de la guerre en Ukraine

Selon les experts, les cyberattaques russes contre l'Ukraine pourraient se propager dans le monde entier, et toutes les organisations doivent se préparer immédiatement.

## Aperçu

- L'assaut militaire de la Russie contre l'Ukraine comporte une importante composante cybernétique, notamment des attaques par déni de service distribué (DDoS), des rançongiciels et des logiciels malveillants destructeurs qui effacent les données.
- La propagation de rançongiciels leurres et de logiciels malveillants destructeurs qui effacent les données utilisés pour attaquer l'Ukraine reste possible alors que l'escalade se poursuit.
- Les gouvernements et les experts en cybersécurité lancent cette mise en garde : « Chaque organisation, grande ou petite, doit être prête à répondre à une cyberactivité perturbatrice. »

## Rester informés

Alors que les entreprises du monde entier continuent de surveiller l'évolution de la situation en Russie et en Ukraine et d'évaluer le potentiel d'escalade des cyberattaques, il est essentiel de demeurer informés. Alors que les informations et les conseils évoluent rapidement, la Cybersecurity and Infrastructure Security Agency (« CISA ») des États-Unis et le Centre canadien pour la cybersécurité (« Cybercentre ») demeurent deux des sources les plus crédibles de renseignements opportuns et exploitables.

**Sources des bulletins sur les renseignements et les menaces :**

**CISA**

- Boucliers levés - https://www.cisa.gov/shields-up
- Avis sur les cybermenaces en Russie - https://www.cisa.gov/uscert/russia

**Cybercentre**

- Rapports et évaluations - https://cyber.gc.ca/fr/rapports-evaluations
- Alertes et avis - https://cyber.gc.ca/fr/alertes-avis

En plus de la cyberpréparation, les organisations de toutes tailles sont également encouragées à rester conscientes des opérations d'influence étrangère qui tentent d'utiliser des tactiques de

mésinformation, de désinformation et de malinformation (MDM) afin de perturber et saper les intérêts démocratiques.

**Sensibilisation à la mésinformation, désinformation et malinformation :**

- https://www.cisa.gov/sites/default/files/publications/cisa_insight_mitigating_foreign_influence_508.pdf

## Orientation

À l'heure actuelle, les directives de la CISA reposent sur la position suivante : « Bien qu'il n'y ait pas de cybermenaces précises ou crédibles… à l'heure actuelle, l'attaque non provoquée de la Russie contre l'Ukraine, qui a impliqué des cyberattaques contre le gouvernement ukrainien et les organisations d'infrastructures critiques, peut avoir un impact sur les entités, tant à l'intérieur qu'à l'extérieur de la région, en particulier à la suite des sanctions ».

**Pour toutes les organisations :**

- Réduire la probabilité d'une cyberintrusion dommageable
- Prendre des mesures pour détecter rapidement une intrusion potentielle
- S'assurer que l'organisation est prête à réagir en cas d'intrusion
- Maximiser la résilience de l'organisation face à un cyberincident destructeur

**Pour les chefs d'entreprise et les PDG :**

- Habiliter les responsables de la sécurité de l'information
- Abaisser les seuils de signalement des incidents
- Participer à un test de réponse des plans de contingence
- Se concentrer sur la continuité des activités critiques de l'entreprise
- Planifier un scénario du pire cas potentiel

**Mesures que les individus peuvent prendre pour se protéger**

- Mettre en œuvre l'authentification multifacteur (MFA) sur tous les comptes
- Mettre à jour les logiciels et activer les mises à jour automatiques
- Bien réfléchir avant de cliquer sur un lien hypertexte ou d'ouvrir une pièce jointe non sollicitée
- Utiliser des mots de passe forts et/ou un gestionnaire de mots de passe

Pour obtenir des descriptions complètes de chaque point du bulletin énuméré ci-dessus, visitez la page Shields Up.

## Services et outils de cybersécurité gratuits

CISA a compilé une liste d'outils et de services de cybersécurité disponibles gratuitement pour aider les organisations à faire progresser leurs capacités de sécurité. Ce référentiel actif comprend des services de cybersécurité fournis par CISA, des outils de code ouvert largement utilisés et des outils et services gratuits proposés par des organisations des secteurs privé et public de la communauté de la cybersécurité.

- https://www.cisa.gov/free-cybersecurity-services-and-tools

Si vous avez besoin d'aide pour gérer ce risque complexe, le groupe de résilience organisationnelle au sein de la division des services de gestion de risques de HUB fournit des services consultatifs pour vous aider à vous préparer et à gérer un large éventail de risques de cybersécurité, de fraude et de menace à la continuité.  Le moment est peut-être également propice pour évaluer et comprendre vos options de transfert de risque par le biais de couvertures de cyberassurance.

## Nous sommes HUB

Lorsque vous vous associez à nous, vous êtes au centre d'un vaste réseau d'experts. Nous vous conseillons sur la façon d'identifier, de quantifier et de réduire les risques en toute confiance grâce à des solutions sur mesure, afin que vous puissiez protéger ce qui compte le plus : votre personnel, vos biens et votre rentabilité.

En savoir plus sur **hubriskservices.com**