Conseils en matière de cybersécurité en cas de niveaux de menace élevés

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

JUILLET 2022 | ITSAP.10.101

Les niveaux de menace auxquels votre organisation est confrontée sont fluides et changent souvent en fonction de facteurs tels que les événements mondiaux et les taux de cybercriminalité. En suivant les conseils ci-dessous, en plus des pratiques de base en matière de cybersécurité, votre organisation peut renforcer sa posture de cybersécurité, améliorer sa résilience et être mieux protégée en cas de niveaux de menaces élevés.

Comprendre les risques

Il est impératif de comprendre vos risques de cybersécurité de base par rapport aux risques auxquels votre organisation est confrontée dans un contexte de niveaux élevés de menaces connues. Votre organisation doit effectuer une évaluation pour déterminer ses risques de base, ainsi qu'une évaluation supplémentaire pour cerner et atténuer les risques en cas de niveau de menace élevé. Vous devez également élaborer un plan d'action présentant des instructions détaillées à votre équipe sur la façon d'agir rapidement lorsque votre organisation est confrontée à des niveaux de menace élevés. Comprendre les risques vous permettra de mieux protéger vos réseaux, systèmes, données, clients et opérations commerciales.

Trouver l'équilibre

When your organization needs to ramp up its cyber security posture in response to a heightened threat level, it can be hard to strike a balance between enhanced security and operational requirements. You also need to consider the cost of ramping up your cyber security posture and the implications increased spending can have on your organization's ability to perform core business functions.

Passer à l'action

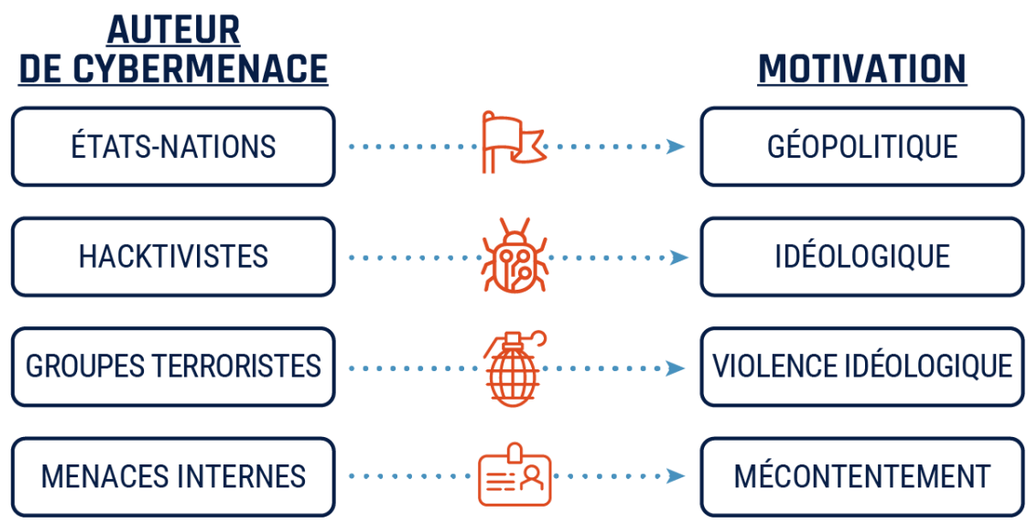
Lorsque les cybermenaces envers votre organisation sont plus élevées que la normale, il est important de mettre en place un plan d'action pour faire facilement passer votre organisation vers un état d'alerte renforcée. Votre plan d'action doit :

- prioriser les mesures de sécurité qui doivent être prises immédiatement
- expliquer comment les défenses déjà en place seront renforcées
- fournir un échéancier ou des objectifs de mise en œuvre de chaque élément

Votre plan doit être approuvé par le plus haut niveau d'autorité de votre organisation pour s'assurer que le processus d'approbation ne fasse pas obstacle à l'activation de votre plan et pour permettre à votre organisation de passer à une posture défensive renforcée. Vous trouverez plus bas une liste de vérification des mesures de sécurité à prendre en cas de niveau de menace élevé.

Les auteurs de cybermenaces et leurs motivations

Les auteurs de cybermenaces sont des États, des groupes ou des personnes qui cherchent à profiter des vulnérabilités, d'une sensibilisation insuffisante à la cybersécurité et des progrès technologiques pour obtenir un accès non autorisé aux systèmes d'information ou encore porter préjudice aux données, aux dispositifs, aux systèmes et aux réseaux des victimes. On peut catégoriser les auteurs de cybermenaces selon leur motivation et, dans une certaine mesure, selon leur degré de sophistication. Les auteurs de menaces cherchent à obtenir accès aux dispositifs, à la puissance de traitement, aux ressources informatiques et à l'information pour toutes sortes de raison. Or, chaque type d'auteurs de cybermenaces est animé par une motivation principale.



Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ
JUILLET 2022 | ITSAP.10.101

Comment réagir à des niveaux de menace élevés

Mesures de sécurité en cas de menace élevée

Les mesures suivantes vous permettront d'améliorer la posture de cybersécurité de votre organisation dans un contexte de menace élevée :

- ☐ Examiner les systèmes de surveillance, de journalisation et de détection existants pour s'assurer qu'ils fonctionnent correctement
- ☐ Améliorer la surveillance du réseau si nécessaire (p. ex. les terminaux)
- ☐ Prioriser l'examen des services réseau essentiels et des journaux de systèmes exposés à Internet
- ☐ Changer les mots de passe sur vos réseaux et demander aux utilisateurs de changer leurs mots de passe
- ☐ Remettre à plus tard (si possible) les changements ou les mises en œuvre de systèmes, jusqu'à ce que le niveau de menace baisse
- ☐ Effectuer des exercices pour tester vos plans de réponse aux incidents et de continuité des activités afin de vous assurer que vous pouvez réagir et récupérer rapidement et efficacement en cas de cyberincident
- ☐ Signaler les incidents de cybersécurité par l'entremise de Mon cyberportail
- ☐ Désactiver tous les ports et services non essentiels
- ☐ Mettre les systèmes essentiels hors ligne si possible pour empêcher les auteurs de menace d'y accéder
- ☐ Surveiller, inspecter et isoler le trafic des zones de troubles géopolitiques connus
- ☐ Améliorer la surveillance de la menace interne et mettre en œuvre une règle de « deux personnes » lors de l'exécution de fonctions administratives essentielles pour vous protéger contre les tactiques de piratage psychologique d'auteurs de menace dotés de moyens très sophistiqués
- ☐ Passer en revue tous les comptes d'accès privilégiés et redéfinir les niveaux d'accès ou les supprimer entièrement
- ☐ Mettre en œuvre l'authentification multifacteur pour tous les accès à distance aux réseaux de votre organisation
- ☐ Déployer une solution de système de prévention des intrusions sur l'hôte (HIPS pour *Host-Based Intrusion Prevention System*) afin de protéger vos systèmes contre les activités malveillantes connues ou inconnues

Signaler les incidents de cybersécurité

Un élément essentiel de votre plan en cas d'incident consiste à signaler tout cybercrime aux organismes d'application de la loi (c.-à-d. au service de police local ou au Centre antifraude du Canada) et en ligne au Centre canadien pour la cybersécurité dans Mon Cyberportail.

Infrastructures essentielles (IE) et cibles de grande valeur

- ☐ Isoler les éléments et les services des IE d'Internet en cas de menace imminente
- ☐ Utiliser les postes de travail à accès privilégié pour séparer les tâches et les comptes sensibles
- ☐ Mettre en œuvre des zones de sécurité de réseau pour contrôler les accès et les flux de données de manière à en limiter l'accès à seulement quelques composants et utilisateurs autorisés
- ☐ Mettre à l'essai les contrôles manuels pour garantir que les fonctions essentielles demeurent opérationnelles si votre réseau devenait indisponible ou non fiable
- ☐ Identifier, séparer et surveiller vos réseaux de technologie de l'information (IT) et de technologie opérationnelle (OT)
- ☐ Tester les systèmes de contrôle industriel (SCI) et les TO pour s'assurer que les fonctions essentielles demeurent opérationnelles pendant une panne

Outils du Centre pour la cybersécurité

Le Centre canadien pour la cybersécurité met à votre disposition un ensemble d'outils et de services afin d'aider les secteurs des infrastructures essentielles à améliorer leur posture de cybersécurité. Les responsables des secteurs des infrastructures essentielles peuvent demander accès à ces outils et services à notre centre d'appel, puis ils devront effectuer un processus d'inscription. Les services suivants sont offerts :

- Renseignement sur les menaces
- Alertes sur les cybermenaces et les vulnérabilités (et mesures d'atténuation)
  - Résumés hebdomadaires des incidents
  - Publication régulière de notes d'informations sur les menaces
  - Notifications de vulnérabilités
- Accès à notre plateforme d'analyse de maliciels
- Accès à des données en temps réel sur les indicateurs de compromission
- Accès aux modèles et aux évaluations sur la cybersécurité
- Personne-ressource du Centre pour la cybersécurité

Les organisations qui ne sont pas responsables d'éléments des infrastructures essentielles peuvent s'abonner à des alertes, des flashs et des évaluations sur la cybersécurité en communiquant avec notre centre d'appel.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada