LISTE D'APPLICATIONS AUTORISÉES

FEVRIER 2022 **ITSAP.10.095**

Mettre en place une liste d'applications autorisées est l'une des 10 meilleures mesures de sécurité des TI que nous vous suggérons de mettre en œuvre. Une liste d'applications autorisées permet de sélectionner et d'approuver des applications et des composants d'application spécifiques (p. ex. des programmes exécutables, des bibliothèques de logiciels, des fichiers de configuration) à exécuter dans des systèmes organisationnels. Les listes d'applications autorisées vous permettent d'éviter le téléchargement d'applications malveillantes qui pourraient infecter votre serveur. Il s'agit de l'une des techniques les plus efficaces pour lutter contre les rançongiciels.

Utiliser une liste d'applications autorisées vous permet de décider quelles applications sont exécutées dans vos systèmes. Une liste d'applications autorisées est une solution efficace pour prévenir l'installation et l'exécution de logiciels non autorisés (p. ex. maliciels) par les utilisateurs sur leurs appareils de travail. Seules les applications qui ont été examinées, testées et approuvées peuvent être exécutées.

Votre organisation peut également utiliser une liste d'applications autorisées à d'autres fins que le contrôle de l'accès aux applications. Par exemple :

- **Inventaire des logiciels** : Pour conserver un inventaire des applications et des versions d'applications installées sur chaque hôte afin que votre organisation puisse identifier les applications non autorisées.
- **Protection des points d'extrémité** : Pour exécuter le code de hachage et le comparer aux fichiers dans votre système.

COMMENT FONCTIONNE UNE LISTE D'APPLICATIONS AUTORISÉES

Il s'agit pour votre organisation de créer une liste des applications dont l'utilisation est autorisée dans les lieux de travail ou qui proviennent d'un fournisseur digne de confiance. Lorsqu'une application est lancée, elle est comparée à la liste d'applications autorisées. L'application est autorisée seulement si elle se trouve sur cette liste. Vous pouvez définir la liste d'applications autorisées en sélectionnant de nombreux attributs de fichier et de dossier (p. ex. les chemins d'accès, les noms de fichiers, la taille des fichiers, la signature numérique ou l'éditeur, ou encore l'empreinte numérique).

Pour une sécurité optimale, n'oubliez pas de mettre à jour votre liste d'applications autorisées lorsque vous appliquez des correctifs de sécurité ou lorsque vous installez une mise à jour d'une application. Certaines listes d'applications autorisées se mettent automatiquement à jour pour refléter ces changements.

Nous vous recommandons d'utiliser le mode observation lorsque vous commencez à utiliser une liste d'applications autorisées. En mode observation, vous pouvez voir tout ce qui s'exécute dans votre réseau et ce mode expose toutes les activités inhabituelles afin de réduire au minimum les risques de compromission du serveur.

Vous devriez définir et mettre en œuvre des stratégies liées aux listes d'applications autorisées dans l'ensemble de votre organisation.

LISTES D'APPLICATIONS AUTORISÉES DES FOURNISSEURS DE SERVICES

Si vous travaillez avec un fournisseur de services infonuagiques (FSI) ou un fournisseur de services gérés (FSG), tenez compte de la sensibilité de vos données lorsque vient le temps de définir et de contrôler l'accès aux données.

SÉRIE SENSIBILISATION

No de cat. D97-1/10-095-2022F-PDF
ISBN 978-0-660-42181-0

ÉLÉMENTS À CONSIDÉRER

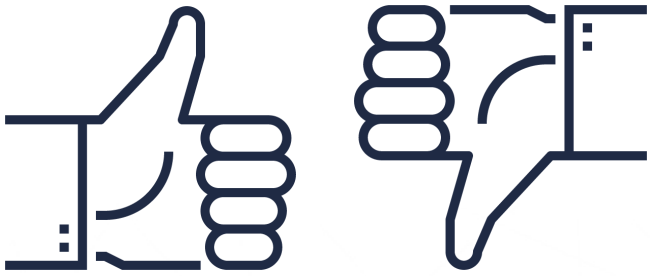
Pensez aux astuces suivantes lorsque viendra le temps de créer une liste d'applications autorisées pour votre organisation :

- Évaluez vos besoins opérationnels et vos besoins en matière de sécurité afin de sélectionner les applications qui appuieront vos objectifs opérationnels.
- Faites l'examen des réseaux et systèmes de votre organisation pour vous assurer de mettre en œuvre une solution compatible.
- Déterminez quelles ressources sont nécessaires pour mettre en œuvre et gérer une liste d'applications autorisées (p. ex. administrateur, personnel de soutien).
- Déterminez si vos hôtes (p. ex. ordinateurs de bureau, ordinateurs portables, serveurs) disposent de systèmes d'exploitation avec des listes d'applications autorisées intégrées et si ces technologies conviennent à votre environnement.
- Mettez à jour votre liste d'applications autorisées chaque fois que vos applications sont mises à jour ou que vous apportez des correctifs de sécurité, ou lorsque vous commencez ou cessez l'utilisation d'un logiciel.
- Les listes d'applications autorisées doivent être configurées pour autoriser uniquement les scripts signés et approuvés là où des scripts sont requis.

COMMENT SÉLECTIONNER UN FOURNISSEUR

Utilisez des applications de fournisseurs qui font preuve de diligence raisonnable et qui ont mis en place des contrôles de sécurité pour s'assurer que leurs produits sont sûrs.

Si vous choisissez d'utiliser une technologie de liste d'autorisation provenant du commerce, assurez-vous de sélectionner un fournisseur réputé. Assurez-vous de configurer le produit pour satisfaire aux besoins de votre organisation.



COMMENT TESTER VOTRE LISTE D'APPLICATIONS AUTORISÉES

Pour juger de son efficacité, testez votre liste d'applications autorisées en mode observation avant de la mettre en œuvre. Les tests devraient comprendre ce qui suit :

- Fonctionnalité de base (p. ex. les applications de la liste peuvent-elles être exécutées?)
- Capacités de gestion des administrateurs (p. ex. les administrateurs peuvent-ils mettre à jour les applications ou y appliquer des correctifs de sécurité?)
- Journalisation et alertes (p. ex. les modifications sont-elles enregistrées?)
- Rendement (p. ex. quel est le rendement lors de l'utilisation normale et de pointe?)
- Sécurité (p. ex. est-ce que la solution comporte des vulnérabilités qui pourraient être exploitées?)

Lorsque vous serez satisfait des résultats en mode observation, vous pourrez effectuer la transition pour passer au mode exécution et contrôler l'exécution sur votre réseau des applications se trouvant sur votre liste d'applications autorisées.

À RETENIR

Mettre en œuvre une liste d'applications autorisées n'est pas le seul élément nécessaire pour améliorer la cybersécurité de votre organisation.
Pour une protection optimale de votre organisation contre les cybermenaces, consultez et mettez en œuvre toutes les mesures recommandées dans *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information* (ITSM.10.089).

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.