Listes d'applications autorisées

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Avril 2024 | 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'établir les applications et les composants d'applications (p. ex. programmes exécutables, bibliothèques de logiciels, fichiers de configuration) qui sont autorisés à s'exécuter sur des systèmes organisationnels.

Pourquoi utiliser des listes d'applications autorisées

Utiliser des listes d'applications autorisées vous permet de décider quelles applications sont installées et exécutées dans vos systèmes. Les listes d'applications autorisées empêchent les utilisateurs de télécharger des applications malveillantes qui pourraient infecter vos serveurs. Seules les applications qui ont été examinées, testées et approuvées peuvent être exécutées. Les listes d'applications autorisées sont l'une des techniques les plus efficaces pour lutter contre les rançongiciels.

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

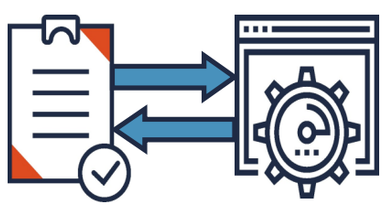
- **Inventaire des logiciels :** Pour conserver un inventaire des applications et des versions d'applications installées sur chaque hôte de sorte que votre organisation puisse identifier les applications non autorisées;
- **Surveillance de l'intégrité des fichiers :** Pour surveiller les tentatives de changements liées aux fichiers d'application et les signaler.
- **Intervention en cas d'incident :** Pour utiliser la liste d'applications autorisées de manière à vérifier la présence de fichiers malveillants sur d'autres hôtes.
- **Protection des points de terminaison :** Exécutez le code de hachage et comparez-le aux fichiers dans votre système.

Comment fonctionne les listes d'applications autorisées

Votre organisation crée 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.

Votre liste d'autorisation peut être basée sur les différents attributs des fichiers et dossiers, comme :

- chemin, nom et taille du fichier
- signature numérique
- éditeur
- valeur de hachage



Nous vous recommandons d'utiliser plusieurs attributs pour définir vos listes d'applications autorisées.

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.

Centre de la sécurité des télécommunications Canada | Communications Security Establishment Canada

Canada

No de cat. D97-1/10-095-2024F-PDF ISBN 978-0-660-69993-6

Listes d'applications autorisées

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ
Avril 2024 | ITSAP.10.095

Listes d'applications autorisées des fournisseurs de services

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

Créer une liste d'applications autorisées efficace

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. personnel administratif et 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.
- Configurez vos listes d'applications autorisées pour autoriser uniquement les scripts signés et approuvés là où des scripts sont requis.

Sélectionner un fournisseur d'application digne de confiance

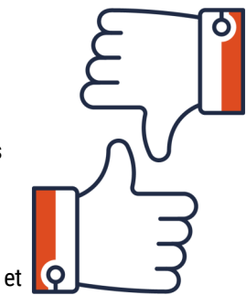
Utilisez des applications de fournisseurs qui ont mis en place des contrôles de sécurité pour s'assurer que leurs produits sont sûrs.

Si vous choisissez d'utiliser une technologie de liste d'autorisation commerciale prête à l'emploi, assurez-vous de sélectionner un fournisseur réputé. Assurez-vous de configurer le produit pour satisfaire aux besoins de votre organisation.

Tester la liste d'autorisation 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
  - Les applications de la liste d'autorisation peuvent-elles s'exécuter?
  - Les applications exclues sont-elles bloquées?
- Capacités de gestion des administrateurs et administratrices : Les administratrices ou administrateurs peuvent-ils mettre à jour ou corriger des applications?
- Journalisation et alertes : Les changements sont-ils journalisés?
- Performance : Quelles sont les performances durant une utilisation normale et maximale?
- Sécurité : 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.

Pour en savoir plus

Mettre en œuvre une liste d'applications autorisées n'est qu'un seul des nombreux éléments nécessaires pour améliorer la cybersécurité de votre organisation.

Pour en savoir plus sur les listes d'applications autorisées, consultez Les 10 mesures de sécurité des TI : no 10, Mettre en place une liste d'applications autorisées (ITSM.10.095).

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.10.189).

Centre de la sécurité des télécommunications Canada | Communications Security Establishment Canada

Canada

No de cat. D97-1/10-095-2024F-PDF ISBN 978-0-660-69993-6