Vérification de la sécurité des réseaux

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Décembre 2022 | ITSAP.00.086

La **vérification de la sécurité des réseaux** est un processus qui consiste à examiner de façon indépendante l'information relative aux contrôles de technologies de l'information (TI), aux systèmes de sécurité et aux politiques et procédures d'atténuation des risques de votre organisation. La vérification a pour objectif de relever les menaces, les lacunes et les compromissions, et de s'assurer qu'une organisation respecte les exigences réglementaires (par exemple, les contrôles au niveau du système et au niveau organisationnel [SOC pour *System and Organization Controls*], la norme North American Electric Reliability Corporate Critical Infrastructure Protection [NERC CIP] et la norme de sécurité des données de l'industrie des cartes de paiement [PCI DSS pour *Payment Card Industry Data Security Standard*]). Elle devrait être effectuée par des professionnels et professionnelles des TI qui ont l'expérience nécessaire en sécurité et en gestion des réseaux, et qui ne sont pas responsables d'assurer la gestion de réseaux ou de systèmes sujets à la vérification.

Quels avantages la vérification de la sécurité des réseaux procure-t-elle?

La vérification de sécurité est une activité importante qui permet à votre organisation de comprendre dans quelle mesure ses contrôles de sécurité sont efficaces face aux menaces liées à la cybersécurité. Procéder à une vérification régulière de la sécurité des réseaux procure les principaux avantages suivants:

- Renforcer les politiques et les pratiques organisationnelles faibles.
- S'assurer que les dispositifs ont été utilisés conformément aux politiques organisationnelles.
- Faciliter l'évaluation des politiques et des processus par rapport aux normes réglementaires et de conformité obligatoires.
- Faciliter l'évaluation de l'intégrité globale de l'infrastructure de vos réseaux.
- Relever les inefficacités des réseaux et les problèmes liés au matériel et aux logiciels.
- Découvrir les possibles lacunes de sécurité, vulnérabilités et erreurs de configuration dans un réseau.
- Détecter les dispositifs indésirables ou non autorisés sur le réseau.
- Aider à identifier la source et l'étendue d'une compromission dans le cadre des enquêtes liées à des incidents de sécurité.
- Permettre une prise de décisions efficace basée sur le risque.

Fournisseurs de services infonuagiques (FSI) et vérification des réseaux

Si votre organisation souscrit à un service infonuagique, il convient de demander au FSI comment il assurera votre protection et celle de vos données précieuses. Voici quelques exemples de questions que vous pourriez poser:

- À quelle fréquence la vérification est-elle effectuée et par qui?
- Quel type de vérification est effectué?
- Quelle est la politique en matière de conservation et de destruction des données de journal?
- Le FSI fait-il l'objet d'une vérification et par qui?
- Les rapports des vérifications sont-ils mis à la disposition des abonnés?
- Les abonnés peuvent-ils vérifier le service?
- Quelles sont les données de journal accessibles aux abonnés?

Pratiques exemplaires en matière de vérification de la sécurité des réseaux

L'information recueillie dans le cadre d'une vérification de sécurité vous permet de mieux comprendre les problèmes qui pourraient peser sur votre infrastructure réseau. Les pratiques exemplaires suivantes vous permettront de corriger ces problèmes avant qu'ils ne provoquent des interruptions ou n'aient une incidence sur vos activités.

- ☐ Procédez à l'inventaire régulier de tous les dispositifs s'exécutant sur le réseau. Faites le suivi des détails comme le nom des hôtes, les addresses IP, les numéros de série, les paramètres de configuration et les versions du code.
- ☐ Utilisez des outils pour effectuer l'inventaire du réseau, évaluer les configurations des dispositifs et analyser les performances du réseau.
- ☐ Dressez la liste des dispositifs qui sont pris en charge par le fournisseur (logiciels et matériel), désuets ou nécessitant un remplacement ou une mise à niveau.
- ☐ Procédez à l'analyse des vulnérabilités sur vos réseaux pour détecter les problèmes de sécurité connus et relever les lacunes.
- ☐ Assurez-vous que les correctifs de sécurité ont été appliqués à tous les composants du réseau. Pour de plus amples renseignements, prière de consulter le document Les 10 mesures de sécurité des TI N°2 – Appliquer des correctifs aux applications et aux systèmes d'exploitation (ITSM.10.096).
- ☐ Mettez en place un système de journalisation robuste pour assurer la collecte des données depuis toutes les sources nécessaires sur votre réseau. Idéalement, les données de journal sont exportées sur un serveur de journaux centralisé et sont protégées (en transit et au repos). Pour de plus amples renseignements, prière de consulter le document Journalisation et surveillance de la sécurité de réseau (ITSAP.00.085).
- ☐ Évaluez les connexions aux autres réseaux, en particulier ceux qui ne sont pas approuvés (comme Internet), pour veiller à ce qu'elles soient approuvées et que les protections périphériques appropriées soient bien en place.
- ☐ Évaluez les politiques et processus internes, notamment l'accès physique, la gestion des configurations, la mise à niveau des réseaux, le traitement des incidents et les procédures de reprise après sinistre.
- ☐ Évaluez les pratiques en matière de gestion des mots de passe et de chiffrement.
- ☐ Évaluez les comptes utilisateur et de groupe pour les autorisations et les niveaux d'accès appropriés. Pour de plus amples renseignements, prière de consulter le document Les 10 mesures de sécurité des TI: N°3 Gestion et contrôle des privilèges administratifs (ITSM.10.094).
- ☐ Analysez les stratégies de sauvegarde et de récupération des données. Assurez-vous de tester la stratégie adoptée. Pour de plus amples renseignements, prière de consulter le document Sauvegarder et récupérer vos données (ITSAP.40.002).
- ☐ Vérifiez votre politique Prenez vos appareils personnels (PAP) pour vous assurer que les dispositifs personnels n'exposent pas le réseau aux auteurs de menace. Pour de plus amples renseignements, prière de consulter le document Sécurité des appareils des utilisateurs finaux pour les modèles de déploiement Prenez vos appareils personnels (PAP) (ITSM.70.003).
- ☐ Vérifiez la consommation de bande passante de votre réseau pour comprendre l'utilisation que vous en faites et mieux gérer le flux du trafic.
- ☐ Procédez à une vérification régulière de la sécurité de votre réseau et communiquez les observations et les recommandations aux intervenants concernés au sein de l'organisation.
- ☐ Synchronisez tous les dispositifs réseau à un serveur de temps central pour veiller à ce que les journaux de vérification enregistrés utilisent la même source de temps. Configurez un minimum de trois serveurs de temps pour faciliter la maintenance et le dépannage .

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada