Journalisation et surveillance de la sécurité de réseau

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Décembre 2022 | ITSAP.80.085

Les réseaux constituent l'infrastructure dorsale qui soutient les systèmes de technologie de l'information (TI), les technologies opérationnelles (TO) et les systèmes de contrôle industriels (SCI). Il est important pour les organisations et les gouvernements de pouvoir compter sur une infrastructure réseau sécuritaire, car celle-ci offre une protection essentielle contre les violations, les intrusions et autres cybermenaces. La journalisation et la surveillance sont des mesures qui aideront votre organisation à identifier des indicateurs de compromission, à prendre des mesures correctives en temps opportun et à atténuer les répercussions lorsque se produit un incident lié à la sécurité. Le présent document offre des directives de haut niveau pour procéder à la journalisation et à la surveillance de réseaux.

En quoi consistent la journalisation et la surveillance de la sécurité de réseau?

La journalisation est le processus de collecte de données qui représentent des activités, des événements, des conditions d'erreur spécifiques, ou l'état général d'un système d'information ou d'un réseau. L'objectif de ce processus est de saisir des données pertinentes pour la sécurité afin de permettre aux administrateurs de système de mieux comprendre le comportement des systèmes pour ainsi soutenir les enquêtes sur des effractions possibles ou réelles.

La surveillance est le processus d'observation des données recueillies de diverses sources, y compris des dispositifs réseau, des serveurs, des applications, des bases de données et d'autres composants de l'infrastructure de TI, afin de repérer des changements et des anomalies. La surveillance a comme objectif de chercher des indices d'attaques connues, des changements inhabituels de comportement du système ou des activités non autorisées en lien avec la sécurité. La surveillance doit être effectuée par des analystes de la sécurité ou par une équipe de sécurité, et non pas par les administrateurs de système qui établissent et configurent les systèmes.

Gestion des informations et des événements de sécurité (GIES)

Une plateforme de GIES est un type d'outil fréquemment utilisé pour la journalisation et la surveillance. Elle centralise les données provenant d'utilisateurs, de dispositifs de réseau, d'applications et de points d'extrémité. Voici quelques-unes de ces capacités de base:

- La surveillance et l'analyse des événements historiques et en temps réel.
- La normalisation ou le reformatage des données de journal dans un format standard pour faciliter l'analyse.
- La facilitation de la corrélation et de l'analyse des enregistrements de vérification (p. ex., la mise en parallèle des événements avec des résultats d'analyse des vulnérabilités).
- La détection d'incidents de sécurité et l'envoi de notifications et d'alertes aux utilisateurs lorsque des menaces (réelles ou potentielles) sont repérées.
- L'absorption d'information dynamique concernant les indicateurs de compromission et le signalement de ces indicateurs s'ils sont détectés sur le réseau.
- L'archivage des journaux, ce qui est avantageux lors de la détection d'incident, de l'intervention et de la reprise après l'incident.

Quels sont les avantages de la journalisation et de la surveillance d'un réseau?

Les activités de journalisation et de surveillance peuvent aider votre organisation à détecter des menaces internes et externes et à atténuer les vulnérabilités du réseau avant que celles-ci ne soient exploitées par des auteurs de menace. D'autres avantages de la journalisation et de la surveillance:

- Surveiller la conformité d'utilisation des dispositifs par rapport aux politiques organisationnelles.
- Faciliter la prise de décisions axée sur les risques avec une surveillance en temps quasi réel.
- Découvrir de possibles failles de sécurité, vulnérabilités et erreurs de configuration au sein d'un réseau.
- Détecter des dispositifs indésirables ou non autorisés dans le réseau.
- Détecter des incidents de sécurité à partir de l'analyse de données de journal, ce qui peut aider à cerner la source et l'étendue de la compromission au cours des enquêtes effectuées sur les incidents de sécurité.
- Faciliter l'évaluation de la santé générale de votre infrastructure de réseau.

Fournisseurs de services infonuagiques (FSI) et surveillance de réseau

Si votre organisation souscrit à un service infonuagique, vous devez savoir et comprendre comment le FSI s'y prend pour vous protéger, vous et vos biens précieux. Certaines des questions à poser sont les suivantes:

- Quel genre de surveillance est effectué?
- Quel est le degré de surveillance (p. ex., la fréquence de l'examen et de l'évaluation des données de journal)?
- Quelles certifications le FSI détient-il (p. ex., AICPA SOC 2 Type 2)?
- Où les données de journal d'un abonné sont-elles stockées?
- Quelles sont les données de journal auxquelles les abonnés ont accès?
- Quelle est la politique en matière de rétention et de destruction de données de journal?

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

Journalisation et surveillance de la sécurité de réseau

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Décembre 2022 | ITSAP.80.085

Les renseignements recueillis dans le cadre d'activités de journalisation et de surveillance sont d'une grande utilité, car elles permettent à votre organisation de prendre des décisions éclairées et efficaces basées sur les risques. En mettant en œuvre les pratiques exemplaires suivantes, vous pouvez solidifier la posture de cybersécurité de votre organisation, minimiser les risques qui pourraient perturber vos activités, et éviter à vos clients des dérangements inutiles.

Pratiques exemplaires en matière de journalisation et de surveillance de la sécurité de réseau

- ☐ Élaborez un plan de surveillance qui définit les risques auxquels s'expose votre organisation, identifie les biens et les événements importants à journaliser et à surveiller, et précise les politiques en matière de rétention de journal de l'organisation ainsi que les processus, les procédures et les outils de surveillance.
- ☐ Appliquez une stratégie de journalisation pour recueillir les données de toutes les sources nécessaires. Cherchez à centraliser et à regrouper les données de journal à l'aide d'un outil de GIES. Cela permettra de faciliter les opérations de sécurité et de réseau pour effectuer l'analyse de données et prendre des mesures correctives immédiates.
- ☐ Veillez à ce que les données de journal au repos soient protégées par cryptographie pour empêcher qu'elles soient falsifiées.
- ☐ Établissez une base de référence pour les habitudes de trafic sur le réseau et les indicateurs de rendement. Vous aurez ainsi un point de référence pour détecter un comportement anormal.
- ☐ Surveillez les tentatives de connexion sortante à partir de réseaux internes et déterminez s'il y a des signes d'hôte compromis.
- ☐ Soyez à l'affût de transferts de données non autorisés sortant du système pour détecter une exfiltration de données indiquant une possible intrusion ou compromission.
- ☐ Mettez en œuvre des mesures pour prévenir les maliciels, comme un logiciel antivirus et des listes d'applications autorisées. Pour obtenir plus de renseignements, consultez Les outils de sécurité préventive (ITSAP.00.058) et Les 10 mesures de sécurité des TI: No 10, Mettre en place une liste d'applications autorisées - ITSM.10.095.
- ☐ Déployez des agents de surveillance à la périphérie de réseau, comme des limites extérieures, pour détecter des connexions provenant de sources inconnues.
- ☐ Lorsque la situation le permet, automatisez la collecte de journaux et l'analyse de données. Utilisez des outils qui peuvent analyser des journaux et déclencher automatiquement des alertes pour des événements pertinents.
- ☐ Utilisez des outils et des technologies pour assurer une collecte et une analyse de données efficaces. Le document Special Publication (SP) 800-137, Appendix D (en anglais seulement) du National Institute of Standards and Technology (NIST) fournit des renseignements sur divers outils et diverses technologies pour la collecte, l'agrégation et l'analyse de données, comme les outils de GIES, les systèmes de détection d'intrusion et les systèmes de prévention d'intrusion.
- ☐ Élaborez un plan d'intervention en cas d'incident et des politiques connexes. Pour obtenir plus de renseignements, consultez Élaborer un plan d'intervention en cas d'incident (ITSAP.40.003).
- ☐ Établissez un centre des opérations de sécurité (COS) ou abonnez-vous à un service COS. Un COS a recours à des gens, à des processus et à la technologie pour surveiller en permanence les menaces de cybersécurité pour votre infrastructure de réseau, les repérer, les atténuer et enquêter sur elles.
- ☐ Faites une sauvegarde des configurations de dispositifs dans un endroit centralisé et sécuritaire.
- ☐ Surveillez les configurations de tous les dispositifs connectés au réseau. Soyez à l'affût de tout changement apporté à la configuration du système par rapport à une référence connue.
- ☐ Limitez le nombre d'administrateurs de système autorisés à apporter des changements à l'infrastructure. Assurez-vous que chacun possède son propre compte protégé par une phrase de passe ou un mot de passe robuste et l'authentification multifacteur, dans la mesure du possible. Par exemple, vous pourriez choisir de suivre le processus de gestion du changement de la bibliothèque d'infrastructure des TI.
- ☐ Surveillez en permanence les composants de l'infrastructure de réseau, comme les dispositifs, les serveurs, les applications, les bases de données, les routeurs et les coupe-feu. Recueillez des renseignements sur l'état des dispositifs, leur conformité à la politique établie et des événements relatifs aux dispositifs liés à l'utilisateur, à l'authentification et aux activités de connexion en particulier.
- ☐ Surveillez les activités liées aux comptes d'utilisateur et à l'accès d'usager (p. ex., création, suppression, désactivation, changements de mot de passe, blocages, échecs de connexion et élévation des privilèges).
- ☐ Vérifiez les obligations juridiques et les politiques connexes concernant les renseignements personnels qui pourraient se trouver sur un réseau, et adaptez les activités de surveillance en conséquence. Par exemple, n'effectuez pas une inspection poussée ou d'autres surveillances intrusives sur des sites Web bancaires ou consacrés à la santé.
- ☐ Effectuez régulièrement des contrôles de sécurité de réseau. Les précieux renseignements obtenus à la suite du contrôle vous permettront d'ajuster vos pratiques de journalisation et de surveillance en conséquence. Pour obtenir plus de renseignements, consultez Vérification de la sécurité des réseaux (ITSAP.80.086).

SCI/TO et la surveillance de réseau

Les exploitants de SCI et de systèmes TO doivent faire preuve de prudence en utilisant des outils automatisés d'inventaire et détection des vulnérabilités, car ceux-ci peuvent faire des balayages de manière intensive. Ces outils peuvent provoquer un comportement erratique des dispositifs, entraîner l'arrêt ou une panne de ceux-ci, leur redémarrage ou la nécessité d'y aller d'une intervention manuelle pour revenir à un état opérationnel. Tenez compte des facteurs suivants lors de la sélection de technologies pour surveiller vos SCI et vos systèmes de TO:

- Assurez-vous que la technologie choisie est axée sur des SCI et comprenne les communications SCI, comme les capacités d'inspection approfondie des paquets.
- Assurez-vous également que la technologie prend en charge les SCI, par exemple qu'elle garde les profils pour des protocoles de communications de données comme modbus ou bus de terrain.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada