Nouveau guide de l'ENISA: Informations décisionnelles en réponse à un incident de sécurité

L'ENISA publie un guide de bonnes pratiques sur les Informations décisionnelles en réponse à un incident de sécurité, dans le but de fournir une bonne image des défis que les Equipes de réponse d'urgence informatique (Computer Emergency Response Team, CERT) nationaux et autres organisations de sécurité rencontrent quand ils essaient de générer des résultats utilisables issus de larges sommes de données.

L'étude donne un large aperçu du paysage actuel d'échange de l'information dans une optique de production d'informations pratiques, il identifie les outils et standards existants, met en lumière les meilleures pratiques et écarts existants et fournit des recommandations à des fins d'amélioration.

La principale partie du rapport décrit comment l'information décisionnelle est obtenue, utilisée et partagée de manière systématique. Le modèle conceptuel proposé, qui forme la structure de l'étude, introduit un pipeline de traitement généralisé de l'information en cinq étapes : collecte, préparation, stockage, analyse et distribution. Le but du modèle est de faciliter la manière avec laquelle les CERT traitent l'information, avec le but de rationaliser le processus de gestion des incidents.

Le Directeur Exécutif de l'ENISA Udo Helmbrecht a commenté: « Les CERT sont en première ligne de notre cyber-défense. Comme leur travail quotidien est basé sur le traitement de quantités de données croissantes, le défi est d'en tirer le meilleur et de générer un résultat utilisable. L'information décisionnelle est identifiée comme un élément fondamental de la réponse à un incident. Cette étude est la première tentative de fournir un guide de référence sur le sujet pour les CERT. L'ENISA salue cette opportunité de soutenir davantage le travail dans ce domaine, avec un travail de notification, de recherche et le développement de futurs outils. ».

Les écarts souvent observés dans les processus CERT afin de gérer de l'information décisionnelle sont ici étudiés, et une série de recommandations générales est fournie pour les organisations dotées de responsabilités d'informations et de dissémination. Une conclusion globale montre que les échanges d'informations n'ont pas encore atteint maturité, et que l'environnement de partage va devoir se développer davantage avant que les bénéfices de ces échanges soient pleinement réalisés.

Le travail inclus trois études de cas qui couvrent les aspects divers de l'information décisionnelle gérée par les CERT. Ces scénarios capturent les processus opérationnels de vraies équipes CERT et les caractéristiques réelles des outils utilisés, indiquant comment ils peuvent être appliqués afin d'améliorer la capacité des équipes CERT à produire, partager et utiliser l'information décisionnelle.

Inventaire pour partage d'information

L'étude est accompagnée par un inventaire intitulé Standards et outils pour l'échange et le traitement de l'information décisionnelle qui peut être appliqué à des activités d'échange de l'information. Il explore les relations entre les différents standards en fournissant une meilleure compréhension des protocoles sous-jacents.

Dans la première partie, l'inventaire couvre un total de cinquante-trois différents standards de partage de l'information, un mélange de formats, protocoles, approches techniques et cadres

d'utilisation communs. Ils sont divisés en sept catégories basées sur l'étendue du standard.

Dans la seconde partie, l'inventaire consiste en seize outils d'échange d'information et de plateformes pertinents pour les échanges et le traitement de l'information décisionnelle. Ce sont principalement des solutions en open source qui sont disponibles pour les CERT.

Un exercice pratique : utiliser des indicateurs pour améliorer les capacités de défense et l'information décisionnelle

Dans le cadre du projet, un nouveau scenario d'exercice pratique a été créé comme exercice pour les membres des équipes de réponse aux incidents et pour les autres professionnels de la sécurité des technologies de l'information responsables des réponses aux incidents de sécurité.

Le but de cet exercice est d'enseigner comment créer et déployer des indicateurs de compromis utilisant une plateforme Recherche collaborative en menaces (Collaborative Research into Threats, CRIT). En outre, il démontre comment démultiplier les CRIT afin de visualiser les relations au sein des différents éléments d'une campagne, comment extraire des indicateurs de données d'accidents, développer des actions d'atténuation, et traquer ces actions. L'exercice a été créé pour une approche plus structurée dans la gestion des indicateurs, pour finalement arriver à être mieux équipé pour sécuriser les réseaux.

Pour les rapports entiers :

- Informations décisionnelles en réponse à un incident de sécurité
- Standards et outils pour l'échange et le traitement de l'information décisionnelle
- Utilisation d'indicateurs pour améliorer les capacities de défense et l'information décisionnelle

Notes aux éditeurs:

https://www.enisa.europa.eu/activities/cert/support/awa

https://www.enisa.europa.eu/activities/cert/support/proactive-detection

Pour toute demande d'interviews:

Cosmin Ciobanu, NIS Expert, **Email:** Cosmin.Ciobanu@enisa.europa.eu, **Tél:** (+30) 2814 409663