Nouveau guide de l'ENISA sur les bonnes pratiques en matière de divulgation des vulnérabilités

L'ENISA publie un guide des bonnes pratiques sur la divulgation de vulnérabilité présentant un panorama des défis posés aux chercheurs en sécurité, aux vendeurs et aux autres acteurs impliqués et confrontés à ce problème lors de la divulgation des vulnérabilités de matériel/logiciel. L'étude offre un aperçu de la complexité de la situation concernant la divulgation des vulnérabilités en faisant le bilan de la situation actuelle, en identifiant les défis et les bonnes pratiques, et en proposant des recommandations concrètes d'amélioration.

La principale partie du rapport présente les principaux concepts liés à la divulgation de la vulnérabilité, ainsi que des chiffres sur le nombre de vulnérabilités dévoilées dans les treize (13) dernières années. Le rapport présente ensuite les acteurs clés impliqués dans le processus de divulgation des vulnérabilités et leur rôle, ainsi que quatre (4) études de cas de vulnérabilités divulguées.

Udo Helmbrecht, Directeur exécutif de l'ENISA, a déclaré : « De nos jours, la divulgation de la vulnérabilité implique toute une série d'interdépendances complexes ne pouvant être abordées qu'en coordonnant toutes les parties concernées par ce processus ». Cette étude constitue la première tentative de fournir un guide de référence sur le sujet de la divulgation de vulnérabilités. L'ENISA soutient volontiers d'autres travaux dans ce domaine en encourageant les bonnes pratiques, en sensibilisant davantage, et en accroissant la recherche et le développement sur ce sujet complexe ».

Les failles liées à la divulgation de vulnérabilité concernent généralement des aspects juridiques, le manque de sensibilisation des acteurs, et la différence de niveaux de maturité parmi les vendeurs et les chercheurs. Les principales recommandations d'amélioration sont :

- La communauté doit encourager l'amélioration de la maturité du vendeur.
- Internationalisation par l'apprentissage stratégique, c'est-à-dire qu'Internet nécessite une approche plus transnationale sur le sujet de la divulgation de vulnérabilité ; les expériences réussies doivent être prises en compte.
- Introduction d'un tiers neutre ou renforcement des centres de coordination existants.
- Les décideurs politiques européens et les États membres doivent améliorer le cadre légal relatif à la divulgation
- Les vendeurs doivent favoriser la mise en confiance, la transparence et l'ouverture.
- L'ENISA peut soutenir et conseiller sur l'amélioration de la situation de la divulgation de vulnérabilité au sein de la communauté et de la Commission européenne.

Par ailleurs, le rapport fournit un « modèle de politique de divulgation de vulnérabilité » comprenant toutes les étapes et le calendrier de la procédure pouvant être suivie pour mettre en œuvre une politique relative à la divulgation de la vulnérabilité.

La conclusion générale est que même si l'on relève de nombreux éléments positifs dans ce domaine, il existe encore une marge d'amélioration. Identifier ces potentiels permettra d'établir un cadre légal approprié mais aussi

davantage de confiance et de transparence entre les parties impliquées.

Pour lire le rapport complet
Pour des informations techniques : Cosmin Ciobanu, expert SRI, **e-mail :** Cosmin.Ciobanu@enisa.europa.eu, **tél. :** +30 2814 409663
Pour plus d'informations sur ce sujet et pour tout contact presse, veuillez contacter **press@enisa.europa.eu**, **tél**. +30 2814 409576