

L'Agence européenne de cybersécurité ENISA appelle dans un nouveau rapport « Detect, SHARE, Protect » à améliorer le système de partage des données et à renforcer l'interopérabilité entre les « brigades d'incendie numériques » afin d'atténuer les conséquences d'attaques informatiques.

L'Agence européenne ENISA publie un nouveau rapport « Detect, SHARE, Protection: Improving Threat Data Exchange among CERTs » (« Détecter, PARTAGER, protéger : *Améliorer l'échange de données sur les menaces informatiques entre les CERT* ») présentant des méthodes afin de simplifier et d'optimiser l'échange de données sur les menaces entre les « brigades d'incendie numériques » (les équipes d'intervention en cas d'urgence informatique - CERT). L'Agence parvient à la conclusion que l'amélioration de l'échange d'information doit s'appuyer sur les solutions et les efforts de standardisation existants en matière de formats d'échange de données, afin de rendre ces derniers interopérables.

Malgré une coopération fructueuse, les CERT se heurtent encore à des obstacles entravant la fluidité des échanges d'informations en matière de sécurité. Les principaux problèmes concernant le partage efficace des informations sont de nature légale et technique. Ils sont également dus au manque d'intérêt de la part des acteurs de la cybersécurité à partager ces informations.

Le [directeur exécutif](#) de l'ENISA, le professeur Udo Helmbrecht commente : « *La complexité grandissante des attaques informatiques nécessite un échange d'informations plus efficace et au-delà des frontières entre les équipes d'interventions en cas d'urgence informatique. S'il est efficace, l'échange d'information permet d'économiser du temps et des efforts lors des interventions et des analyses post mortem. Cela renforce également les synergies et permet aux CERT de s'aligner sur les meilleures pratiques* ».

La détection locale, accompagnée de l'échange d'informations fondé sur la confiance, permet de **prévenir** les attaques informatiques **à l'échelle mondiale**. Elle est par conséquent très utile pour réussir à identifier et, dans un deuxième temps, à neutraliser un incident, si celui-ci a déjà été détecté par les CERT et si cette information est ensuite partagée. Par ailleurs, des avancées majeures ont récemment été réalisées grâce à la mise en place de CERT au niveau national/gouvernemental en Europe, visant à coordonner les réponses aux attaques informatiques. Celles-ci ayant souvent lieu à l'échelle mondiale, il est essentiel que les interventions soient coordonnées non seulement à l'intérieur des frontières nationales, mais également au niveau international. C'est pourquoi **un échange d'informations sûr et efficace rapportant de tels d'incidents** doit être mis en place. Le rapport recense les outils et les normes en cours d'élaboration qui devraient aider les CERT à partager, de manière efficace, les informations stratégiques sur les incidents. L'ENISA a défini une série de recommandations pour le réseau CERT et pour les autres acteurs de la sécurité visant à mettre en place de meilleures pratiques en matière d'échange de données :

2013/11/20

EPR/152013

www.enisa.europa.eu

- Faciliter l'adoption, l'interopérabilité et l'amélioration des fonctionnalités des outils essentiels pour la communauté CERT
- Promouvoir la stabilité et la continuité du flux d'informations concernant les incidents, lequel est souvent modifié sans notification préalable
- Promouvoir l'utilisation de normes pour l'échange de données
- Améliorer la fonctionnalité des outils existants dans les domaines suivants :
 - Interopérabilité
 - Analyse automatique de corrélation des incidents
 - Amélioration des services de renseignements concernant les menaces
 - Analyses et visualisation avancées pour un très grand nombre d'incidents

L'Union européenne, avec l'ENISA, soutient les CERT nationales/gouvernementales dans leurs efforts pour faciliter l'échange d'informations sur les incidents. En 2014, l'ENISA s'emploiera activement à soutenir des projets communautaires aidant les CERT à collaborer de manière plus efficace.

Voir le rapport complet ; « [Detect, SHARE, Protect](#) »

Pour toute demande d'interview, veuillez consulter Ulf Bergström, porte-parole, ulf.bergstrom@enisa.europa.eu, téléphone portable : + 30 6948 460 143, ou notre expert Romain Bourgue, cert-relations@enisa.europa.eu

Veillez noter: traduction. La version anglaise est la seule version officielle

www.enisa.europa.eu/media/enisa-en-francais/

www.enisa.europa.eu

ENISA is a Centre of Expertise in Network and Information Security in Europe

Securing Europe's Information Society

The European Union Agency for Network and Information Security