07/12/2011

www.enisa.europa.eu

Colmater les brèches dans la lutte contre les cyber-menaces L'Agence de l'UE publie un rapport sur la détection proactive des incidents de cyber-sécurité en vue de rendre les "pompiers numériques" plus efficaces

L'Agence publie aujourd'hui un rapport qui identifie 16 brèches dans la détection des incidents de sécurité réseau. Ce rapport révèle que tous les outils disponibles ne sont pas utilisés assez largement par les "pompiers numériques", à savoir les Équipes d'intervention en cas d'urgence informatique (CERT), pour lutter efficacement contre les cyber-menaces. Pour cette raison, l'Agence a publié 35 recommandations adressées aux fournisseurs de données, aux utilisateurs de données et à l'échelle nationale/de l'UE pour colmater ces brèches.

L'étude a déterminé que les CERT n'utilisent actuellement pas toutes les sources externes possibles à leur disposition de manière optimale. De même, de nombreuses CERT ne collectent pas, ni ne partagent, les données d'incidents liés à d'autres circonscriptions avec les autres CERT. Cela est préoccupant, car l'échange d'informations est essentiel pour combattre efficacement les logiciels malveillants et les activités malicieuses, ce qui est extrêmement important dans la lutte contre les cyber-menaces transfrontalières.

Les brèches Les 16 brèches dans la détection des incidents ont été examinées de manière approfondie. Les principales lacunes sur le plan technique incluent une qualité insuffisante des données (faux positifs dans les donnés fournies, imponctualité des livraisons), ainsi que l'absence d'outils, de ressources, de compétences et de formats standards. Le problème juridique le plus important implique les règlementations relatives à la confidentialité et les lois sur la protection des données personnelles qui obstruent l'échange d'informations.

"*Les responsables des CERT nationales/gouvernementales devraient tirer parti de ce rapport pour colmater les brèches identifiées, en utilisant davantage de sources externes d'informations liées aux incidents, ainsi que des outils internes additionnels pour recueillir des informations*", a déclaré le Directeur Exécutif de l'Agence, le Professeur Udo Helmbrecht.

35 recommandations pour colmater les brèches. **Pour les fournisseurs de données**, les principales recommandations consistent en de meilleurs moyens d'atteindre les CERT, un meilleur format des données, une meilleure distribution ainsi que l'amélioration de la qualité des données. **Pour les utilisateurs de données,** elles comprennent des activités additionnelles des CERT afin de vérifier la qualité des fils de données, ainsi que des déploiements spécifiques

de nouvelles technologies recommandées. Enfin, **à l'échelle nationale et de l'UE**, un équilibrage des besoins en sécurité et en protection de la confidentialité est nécessaire, au même titre que la facilitation de l'adoption de formats communs, l'intégration de données statistiques sur les incidents et une recherche sur les rapports de fuites de données.

Informations contextuelles : la détection proactive des incidents consiste en la découverte d'activités malicieuses avant que les plaintes et les rapports d'incidents les concernant ne soient reçus. En tant que tel, il s'agit de la pierre angulaire d'un portefeuille efficace de services de CERT. Elle peut considérablement améliorer l'efficacité d'une CERT dans ses opérations, renforçant ainsi sa capacité de gestion des incidents, l'un des principaux services des CERT nationales/gouvernementales.

Pour consulter l'intégralité du rapport

Informations contextuelles : Agenda numérique pour l'Europe, action 38

Pour toute demande d'interview, veuillez contacter : Ulf Bergstrom, Porte-parole de l'ENISA, press@enisa.europa.eu, Portable : +30-6948-460-143, ou Agris Belasovs ou Andrea Dufkova, CERT-Relations@enisa.europa.eu.

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

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