20/01/2011

www.enisa.europa.eu

Nouveau guide sur la gestion des incidents liés à la sécurité informatique pour soutenir la lutte contre les attaques informatiques

L'agence européenne chargée de la sécurité informatique, l'ENISA (European Network and Information Security Agency) a publié un nouveau guide des bonnes pratiques, d'informations pratiques et de directives pour la gestion des incidents liés à la sécurité du réseau et de l'information par les Équipes d'intervention en cas d'urgence informatique (Computer Emergency Response Team; CERT).

Les rapports récents sur les attaques informatiques en 2010 ont révélé que le besoin et l'utilisation du rapport de l'agence sur la manière de lutter contre les attaques informatiques sont plus actuels et réels que jamais. Le Guide de bonnes pratiques sur la gestion des incidents cible le processus de traitement des incidents. Le traitement des incidents est le service principal réalisé par la plupart des CERT. Cela implique la détection et l'enregistrement des incidents, suivi par ce que l'on nomme le «triage» (classification, définition des priorités et attribution des incidents), la résolution des incidents et l'analyse a posteriori.

Les autres sujets traités dans le guide incluent:
- les bases d'un CERT,
- ses missions,
- sa circonscription et son autorité,
- le cadre organisationnel,
- les rôles au sein d'un CERT,
- les flux de travail,
- les politiques internes,
- la coopération avec des parties externes,
- l'externalisation, et
- la manière de présenter le travail à la direction.

Contexte politique. L'ENISA a préconisé la mise en place d'un CERT par tous les États membres et la Commission européenne a récemment (le 22/11/2010) proposé une Stratégie de Sécurité Interne pour l'Union Européenne, ce qui comprend par exemple qu'il faudrait procéder à la mise en place d'une Équipe d'intervention en cas d'urgence informatique dans tous les États membres afin de constituer un réseau dans toute l'Europe d'ici à 2012, ainsi qu'un réseau pour les institutions européennes. Le Directeur Exécutif de l'agence, le Dr. Udo Helmbrecht, a déclaré:
«*Ce guide est un outil très utile pour soutenir la proposition de la Commission du 30/09/10 visant à renforcer les défenses de l'Europe contre les attaques informatiques.*»

Le Guide des bonnes pratiques sur la gestion des incidents fait suite au guide de 'mise-en-place- CERT' de l'ENISA. Ce nouveau guide facilite les efforts de l'ENISA pour renforcer les

pouvoirs des CERT nationaux/gouvernementaux, les «pompiers numériques», qui jouent l'un des rôles majeurs dans la protection des infrastructures critiques de l'information (CIIP) au niveau des États membres.

Le public ciblé par ce guide est le personnel technique et la direction des institutions gouvernementales et autres, dirigeant une Équipe d'intervention en cas d'urgence informatique (CERT) afin de protéger leur structure informatique. Cependant, n'importe quel groupe ou équipe qui traite les incidents de sécurité des réseaux et de l'information peuvent suivre ce guide et en tirer parti.

Pour lire le rapport complet: http://www.enisa.europa.eu/act/cert/support/incident-management

Pour tout entretien: Ulf Bergstrom, Porte-parole, ENISA, press@enisa.europa.eu, Mobile: +30-6948-460143, ou Agris Belasovs, cert-relations@enisa.europa.eu.

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