2012/12/17

EPR24/2012
www.enisa.europa.eu

Focus sur le rapport d'étape 2012 sur les capacités des CERT (Computer Emergency Response Teams) publié par l'Agence européenne ENISA

L'agence de cyber sécurité européenne, ENISA a publié deux nouveaux rapports: 1. Le Rapport 2012 État des CERT qui fournit un état d'avancement des capacités des CERT nationales / gouvernementales » (n / g CERT) qui démontre que le principal défi réside dans la diversité des capacités des États membres en Europe. 2. Le rapport ci-joint mis à jour sur les recommandations pour combler les lacunes restantes pour les CERT.

La nécessité d'un réseau fonctionnel de n / g CERT en Europe d'ici la fin de l'année 2012 a été établi par plusieurs documents de l'UE (Agenda numérique pour l'Europe / Stratégie de sécurité intérieure de l'UE / la communication de la CIIP). Le Rapport d'étape 2012 indique que le principal obstacle à la coopération transfrontalière et de réponse aux incidents est la disparité des capacités dans les États membres. Certaines équipes n'ont pas un «niveau suffisant de maturité» par rapport aux équipes d'autres États membres. Quatre capacités de base constituent le point central du rapport:

Extraits des principales conclusions de n / g CERT :

1. Mandat et stratégie:

- La plupart des CERT ont un rôle et un mandat clairs, mais les détails et la forme varient considérablement au sein de l'UE.

- Beaucoup de travail reste à accomplir en ce qui concerne la prise en compte correcte par les n / g CERT nationaux de cyber stratégies de sécurité; actuellement, moins de 50% des États membres ont mis en place de telles stratégies.

2. Portefeuille de services:

Le champ d'application de l'aide dépend du type de clients: Les organismes gouvernementaux reçoivent la gamme complète des services. L'expertise précieuse en cyber sécurité de n / g CERT est également très recherchée par les services policiers et judiciaires et d'autres intervenants.

3. Capacité opérationnelle:

Plus de 80% des CERT emploient 6-8 personnes à temps plein, ce qui est le niveau minimum nécessaire pour des services complets. Toutefois, dans les petites équipes, le personnel a de multiples rôles, ce qui constitue un obstacle à la spécialisation. En particulier, certains CERT font état de difficultés à recruter des criminalistes numériques et des spécialistes d'ingénierie inverse.

4. Capacité de coopération:

Les cyber incidents à grande échelle nécessitent à la fois une coopération nationale et internationale de gestion de crise. Les CERT sont bien ancrées dans des structures internationales telles que (FIRST, TF-CSIRT, EGC, Trusted introducteur, APWG ou les ateliers ENISA).

Le directeur exécutif de l'ENISA, le Professeur Udo Helmbrecht, a déclaré: *«Ces deux rapports montrent que si de grands progrès ont été réalisés en Europe récemment, d'autres travaux sont nécessaires pour combler les différents niveaux de maturité des CERT. Les défis identifiés: les questions de la clarté des rôles et des responsabilités gouvernementales pour les CERT, le manque de financement et le manque de ressources hautement qualifiées en IT, experts juridiques et RP doivent aussi être abordés. Ces défis doivent être résolus par de nombreux acteurs: les législateurs, les équipes CERT, les partenaires de coopération et les organisations internationales».*

Pour les rapports complets:

Rapport d'étape 2012 pour les CERT

Mise à jour des recommandations 2012

Pour toute demande d'interviews,

Ulf Bergstrom, Porte-parole, press@enisa.europa.eu, mobile: +30 6948 460 143,

ou Andrea Dufkova, Expert, opsec@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