2012/12/17

EPR24/2012

www.enisa.europa.eu

Especial: La Agencia europea ENISA publica el Informe de situación 2012 sobre las capacidades básicas de los equipos de respuesta a emergencias informáticas

La Agencia europea de ciberseguridad ENISA ha publicado dos nuevos informes: 1. El Informe de situación 2012 sobre los equipos de respuesta a emergencias informáticas (CERT, por sus siglas en inglés), que ofrece una visión general del estado de la cuestión en cuanto a las capacidades de los CERT nacionales/gubernamentales (CERT n/g) e identifica la diversidad de capacidades entre los distintos Estados miembros como un reto crucial. 2. El informe de acompañamiento sobre las recomendaciones actualizadas para los CERT n/g, que aborda las carencias y deficiencias por resolver.

Varios documentos comunitarios (Agenda Digital para Europa/Estrategia de Seguridad Interior de la UE/Comunicación PICI) resaltaban la necesidad en Europa de una red de CERT n/g operativa para finales de 2012. **El Informe de situación 2012 muestra que el principal obstáculo para la cooperación y la respuesta a incidentes transfronterizas es la diversidad de capacidades entre Estados miembros. Algunos equipos no cuentan con un «grado de madurez adecuado» en comparación con los equipos de otros Estados miembros. El informe se centra en cuatro capacidades básicas:**

Pasajes de las principales conclusiones acerca de los CERT n/g.

1. Mandato y estrategia:

-La mayoría de los CERT n/g tienen unas funciones y un mandato claros, aunque su forma y su contenido varía mucho de un país a otro.

-Se requiere un enorme trabajo para lograr la inclusión adecuada de los CERT n/g en las estrategias de ciberseguridad nacionales; actualmente, menos del 50% de los Estados miembros cuentan con estrategias de este tipo.

2. Cartera de servicios:

El alcance de la asistencia depende del tipo de destinatario: los destinatarios principales (p. ej. organismos gubernamentales) son los que se benefician de la cartera de servicios completa. Las valiosas competencias en ciberseguridad de los CERT n/g también están muy solicitadas por cuerpos policiales y otros actores.

3. Capacidad operativa:

Más del 80% emplean a 6–8 trabajadores a jornada completa, lo que se considera el mínimo necesario para ofrecer unos servicios aceptables. No obstante, en equipos más pequeños, los empleados desempeñan funciones múltiples, lo cual constituye una barrera para la especialización. En particular, los CERT n/g encuentran dificultades a la hora de contratar a forenses digitales y especialistas en técnica retroactiva.

4. Capacidad de cooperación:

Dado que la respuesta a ciberincidentes a gran escala requiere una gestión tanto nacional como internacional, los CERT n/g presentan una buena implantación en estructuras internacionales (FIRST, TF-CSIRT, EGC, Trusted Introducer, APWG o los talleres de ENISA).

El profesor Udo Helmbrecht, **Director Ejecutivo de ENISA**, afirmó: «*Estos dos informes muestran que, si bien se han realizado grandes avances en Europa recientemente, se requiere un mayor esfuerzo para salvar las diferencias entre los niveles de madurez de los CERT. Se identificaron los siguientes retos: la necesidad de clarificación de las funciones y responsabilidades de los CERT gubernamentales, la falta de financiación y la ausencia de recursos como expertos altamente especializados en tecnología de la información, derecho, y relaciones públicas. Estos retos deben resolverse desde varios frentes: legisladores, equipos CERT, socios de cooperación y organizaciones internacionales».*

Informes completos:

Informe de situación sobre los CERT 2012

Recomendaciones actualizadas 2012

Entrevistas: Ulf Bergstrom, Portavoz, press@enisa.europa.eu, móvil: +30 6948 460 143, o Andrea Dufkova, Experta, opsec@enisa.europa.eu

n oficial es la ingleesa.

www.enisa.europa.eu