27/08/2012
EPR010/2012

www.enisa.europa.eu

La agencia de la UE ENISA analiza la legislación sobre seguridad cibernética y las lagunas en su implementación; incidentes no detectados o que no fueron comunicados

En un nuevo informe la agencia de "seguridad cibernética" de la UE, ENISA, toma una instantánea sobre la actual y futura legislación comunitaria en materia de medidas de seguridad y denuncia de incidentes. El análisis pone de relieve importantes pasos hacia delante, y también identifica lagunas en la implementación nacional y el hecho de que la mayoría de los incidentes no son reportados.

Los incidentes cibernéticos tienen un impacto significativo en la sociedad. He aquí cinco ejemplos bien conocidos:

- En 2012, millones de contraseñas de redes de negocios fueron expuestas
- En 2011, la tormenta Dagmar destruyó millones de enlaces de comunicación escandinavos
- En 2011, un fallo en un de centro de datos británico interrumpió millones de comunicaciones empresariales en todo el mundo
- En 2011, una autoridad de certificación fue violada desvelando comunicaciones de millones de usuarios
- En 2010, un proveedor de telecomunicaciones chino pirateó el 15% del tráfico mundial de Internet durante 20 minutos

Cada vez más, millones de ciudadanos y empresas se han visto afectados seriamente. Pero la mayoría de los incidentes no son reportados o ni siquiera detectados. El doctor Marnix Dekker y Karsberg Chris, co-autores del informe, afirman que: *"Los incidentes cibernéticos son los más comúnmente mantenidos en secreto cuando se descubren, dejando a los clientes y a los responsables políticos en la oscuridad acerca de la frecuencia, el impacto y las raíces del problema."*

El nuevo informe "Cyber Incident Reporting in the EU" proporciona una visión general de la legislación existente y prevista (ver gráfico adjunto), que cubre las cláusulas de notificación obligatoria de incidentes en el artículo 13 a del paquete Telecom, el artículo 4 de la Directiva sobre privacidad electrónica, el artículo 15 sobre la propuesta de regulación de la identificación electrónica, y los artículos 30, 31, 32 de la reforma de Protección de Datos. El estudio muestra los factores comunes y las diferencias entre los artículos y mira hacia adelante a la estrategia de seguridad cibernética de la UE. El documento también identifica áreas que mejorar. Por ejemplo, sólo uno de los incidentes mencionados anteriormente estaba dentro del alcance del mandato de los reguladores nacionales, lo que indica que hay lagunas en la regulación. Por lo tanto, el intercambio de informes de incidentes en la UE debe mejorar.

Se ha progresado mucho recientemente: un grupo de trabajo de ENISA para los reguladores nacionales ha desarrollado tanto un conjunto común de medidas de seguridad así como un formato de reporte de incidentes. Esto permitirá una aplicación más uniforme del artículo 13a. ENISA acaba de recibir informes de los reguladores acerca de 51 grandes incidentes, que describen el impacto, causas, medidas adoptadas y lecciones aprendidas. Este material se utiliza como recurso para la estrategia europea de seguridad

cibernética European cyber security strategy y la European cyber security exercise. El director ejecutivo de ENISA, el profesor Udo Helmbrecht, comentó: *"El reporte de incidentes es esencial para obtener una imagen real de seguridad cibernética. La estrategia de seguridad cibernética de la UE es un paso importante y uno de sus objetivos es ampliar el alcance de la declaración de provisiones, como el artículo 13 a, más allá del sector de las telecomunicaciones."*

Informes: European Cyber Security Strategy y Art 13a working group documents

Entrevistas: Ulf Bergstrom, Portavoz, ENISA, press@enisa.europa.eu, Teléfono:+ 30 6948 460 143, or Dr Marnix Dekker, ENISA, marnix.dekker@enisa.europa.eu

Traducción. La versión original en inglés es el documento auténtico.
www.enisa.europa.eu