Qué es y cómo funciona el CERT: contribuyendo a un ecosistema más ciberseguro

En el Basque CyberSecurity Centre (BCSC), el CERT, acrónimo de *Computer Emergency Response Team*, es nuestro equipo encargado de gestionar los servicios de prevención, detección y respuesta de incidentes de ciberseguridad con impacto en las empresas y ciudadanía de Euskadi.

Precisamente la prevención de situaciones de riesgo para la ciberseguridad es una parte muy importante del trabajo que realizamos, al tiempo que ofrecer una respuesta contundente que ayude a evitar que otras personas, empresas u organizaciones sufran situaciones parecidas. En este sentido, nuestro trabajo tiene **cuatro destinatarios principales**:

- **Empresas y agrupaciones empresariales**. Cada vez son más habituales los incidentes de ciberseguridad sufridos por las empresas vascas cuyas consecuencias se manifiestan en pérdidas económicas, de reputación y, en definitiva, de competitividad. Por eso, el trabajo del CERT se centra en gran parte en tomar medidas globales para mitigar el impacto potencial de las ciberamenazas para evitar que afecten a las empresas vascas.
- **La ciudadanía**. La tecnología avanza a una velocidad de vértigo; la mayoría de las veces, mucho más rápido de lo que la sociedad es capaz de asumir. Es imprescindible que la ciudadanía conozca los riesgos que entraña vivir en un entorno hiperconectado para adoptar las medidas necesarias que contribuyan a minimizarlos. Para conseguirlo utilizamos dos herramientas: la formación y la información. La sensibilización es una parte muy importante de la labor que realizamos para ayudar a la sociedad a identificar dichos "*ciberriesgos*", prevenir y actuar de una manera responsable en materia de ciberseguridad.
- **Administraciones públicas**. Apoyamos a las instituciones públicas vascas a través de proyectos concretos de actuación, ya sea a través de la formación, de campañas de concienciación o a través del análisis de su infraestructura. Así mismo, realizamos una monitorización de la superficie de exposición de organizaciones públicas ya que conforman uno de los grupos más sensibles a sufrir los efectos de un ciberataque porque sus consecuencias tienen impacto sobre el conjunto de la ciudadanía.
- **Profesionales de la ciberseguridad**. No solo proporcionamos y publicamos información actualizada sobre vulnerabilidades, alertas sobre incidentes de seguridad o avisos técnicos imprescindibles en la actividad diaria de los profesionales de la ciberseguridad de nuestro ecosistema empresarial, sino que además miramos al medio o largo plazo apoyando también la formación y desarrollo del nuevo talento en el ámbito de la ciberseguridad.

¿Qué tipo de trabajo realizamos en el CERT?

El trabajo que realizamos en el CERT es muy amplio, **estando totalmente enfocado a mejorar el nivel de protección de la sociedad vasca en su conjunto, y en especial en el ámbito empresarial**. Para conseguirlo llevamos a cabo diferentes acciones, algunas de las cuales se indican a continuación:

- **Takedown de campañas de malware y phishing**. tomamos las medidas técnicas oportunas para desmantelar las campañas de phishing y malware con impacto potencial en Euskadi.
- **Divulgación responsable de vulnerabilidades**. Las vulnerabilidades son prácticamente inevitables, por lo que otra de las tareas que realizamos consiste en divulgar de forma responsable esas debilidades en el software o los sistemas que sufren las diferentes organizaciones para evitar que a ese daño se le añadan otras consecuencias adicionales. Creemos que la investigación y la divulgación sobre ciberseguridad responsable nos ayudan a mejorar constantemente. Una vez recibida una notificación de vulnerabilidad, la divulgación responsable consiste en realizar un análisis inicial para confirmarla, notificar a las entidades afectadas para que éstas realicen un análisis profundo del fallo y aplicar las medidas oportunas para solucionarlo.
- **Análisis e informes técnicos de ciberamenazas**. La ciberdelincuencia forma parte de un universo técnico muy complejo que requiere los análisis y conocimientos adecuados para poder combatirla. Estos análisis culminan con la elaboración de informes que ayudan a comprender cómo hacer frente a este tipo de amenazas.
- **Intercambio de información sobre ciberamenazas**. El intercambio de información es vital para combatir la ciberdelincuencia, especialmente entre agencias especializadas. En nuestro CERT estamos comprometidos con el intercambio de información que permita conseguir una sociedad más segura.
- **Monitorización de la superficie de exposición de Euskadi**. Para poder asegurar la ciberseguridad es necesario llevar a cabo una vigilancia permanente de cara a identificar riesgos que puedan derivar en incidentes de ciberseguridad y poder tomar medidas tempranas para prevenirlo.

Como ves, llevamos a cabo una labor muy intensa para investigar y rastrear las amenazas e incidentes de ciberseguridad que se producen en Euskadi. Os animamos a que nos ayudéis en nuestra labor, reportando cualquier ciberataque sufrido a través de nuestro buzón incidencias@bcsc.eus o en el teléfono gratuito 900 104 891. Es parte de nuestro servicio de asesoramiento frente a incidentes y estamos juntos en esta lucha para mitigar las amenazas que puedan afectar a la ciudadanía o a nuestras empresas.