Estafas Business Email Compromise

BCSC_ALERTA_ESTAFAS_BEC

www.basquecybersecurity.eus

BASQUE CYBERSECURITY CENTRE

GRUPO spri TALDEA

EUSKO JAURLARITZA
GOBIERNO VASCO
EKONOMIAREN GARAPEN ETA AZPIEGITURA SAILA
DEPARTAMENTO DE DESARROLLO ECONÓMICO E INFRAESTRUCTURAS

Septiembre 2018

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se facilita a título meramente informativo y orientativo. En ningún caso el Basque Cybersecurity Centre será o podrá ser responsable solidaria o subsidiariamente, de cualesquiera responsabilidades, daños, pérdidas y costos sufridos o incurridos, directos o indirectos, fortuitos o extraordinarios que pudieran derivarse del uso de la información que en el mismo se contiene.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

1. SOBRE EL BCSC

El BASQUE CYBERSECURITY CENTRE (en adelante, BCSC), es una iniciativa que se enmarca en la Agencia Vasca de Desarrollo Empresarial (en adelante Grupo SPRI), sociedad dependiente del Departamento de desarrollo Económico e Infraestructuras del Gobierno Vasco. El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

El BCSC es un instrumento del Gobierno Vasco para elevar la cultura de ciberseguridad en la sociedad vasca y aspira a erigirse como punto de encuentro entre oferentes y demandantes de servicios especializados, generando con ello una oportunidad para la innovación, potenciando la competitividad de las empresas y facilitando que la ciudadanía desarrolle hábitos para una actividad digital más segura.

Para alcanzar sus objetivos, el BCSC se define como una iniciativa transversal que desde su inicio involucra a cuatro Departamentos del Gobierno Vasco, el ya antes citado de Desarrollo Económico e Infraestructuras, el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación. La actividad incluye proyectos de investigación, iniciativas de emprendimiento y colaboración coordinada con otros agentes competentes a nivel estatal e internacional. No en vano se trabaja en estrecha colaboración con agentes de la Red Vasca de Ciencia Tecnología e Innovación que forman parte de su Comité Permanente.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución proyectos de colaboración entre actores complementarios en los ámbitos de la innovación tecnológica, de la investigación y de la transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

El BCSC ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CSIRT, por sus siglas en inglés “Computer Security Incident Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar su capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca.

2. RESUMEN EJECUTIVO

Los ataques **Business Email Compromise (BEC)**, les cuestan a las empresas una **pérdida media de 120.000 euros**. Se estima que este tipo de ataques continuarán creciendo (lo han hecho ya un 1.300% desde 2015), evolucionando y, en la actualidad, ya afectan a **empresas de todos los tamaños**. Este año, de acuerdo con las estimaciones de Trend Micro, las pérdidas provocadas rondarán los **8.000 millones de euros**.

En general, la estrategia de los ciberdelincuentes es obtener beneficio económico con el mínimo riesgo posible y el mayor retorno de la inversión. En este sentido, cada vez se centran más en este tipo de estafas que explicamos a continuación.

2.1. ¿Qué son?

Los ataques de tipo Business Email Compromise son un tipo de estafas que consisten en suplantar la identidad de una persona vía email para engañar a otra con el fin de que realice una transferencia económica a una cuenta controlada por el estafador. A diferencia de los ataques de phishing tradicionales, los ataques Busines Email Compromise son dirigidos, **diseñados para cada víctima** y emulan correos electrónicos totalmente profesionales.

La mayoría de las ocasiones los ciberdelincuentes estudian las últimas noticias de las empresas e investigan las redes sociales de los empleados para hacer que el ataque, el señuelo, sea lo más convincente posible. Este nivel de personalización es lo que ayuda a que este tipo de estafas por correo electrónico **superen los filtros de spam y otras protecciones**. Además de conseguir **grandes sumas de dinero**, también utilizan este método de ataque para **obtener información confidencial** de la empresa que puede acarrear a la organización serios problemas, no solo económicos sino también de reputación.

2.2. Tipos de ataques

Este tipo de ataques toman usualmente una de estas cuatro formas:

- **Fraude del CEO**. Los ciberdelincuentes envían un email que parece proceder de uno de los responsables de la empresa a un empleado que tenga capacidad para realizar transferencias, dándole instrucciones para que envíe fondos a una cuenta que en realidad se encuentra bajo el control de los ciberdelincuentes.
- **Estafa de factura falsa**. Los ciberdelincuentes, tras comprometer la cuenta de un usuario, buscan en el correo de este hasta dar con una factura que venza pronto para después contactar con el departamento financiero y pedirles que cambien la cuenta de pago por una diferente.
- **Suplantación del Abogado**. El ciberdelincuente se hace pasar por el bufete de abogados de una empresa y solicita una transferencia de fondos para resolver un litigio o pagar una factura vencida.

- **Robo de datos**. Es la única versión de este tipo de estafas cuyo objetivo no es una transferencia de fondos directa, son los ataques que buscan el robo de datos mediante el compromiso de la cuenta de correo electrónico de un ejecutivo para solicitar que se le envíe información confidencial.

2.3. Situación en Euskadi

Desde el **Centro Vasco de Ciberseguridad,** en colaboración con la **Sección de Delitos Informáticos de la Ertzaintza,** hemos identificado recientemente diferentes campañas de este tipo de estafas orientadas a empresas vascas y nos han reportado varios casos en los que empresas de la región se han visto afectadas, por lo que es muy importante ser conscientes de la existencia de este tipo de estafas y conocer cómo funcionan y cómo prevenirlas.

2.4. Prevención

Para hacer frente a este tipo de amenazas es fundamental la **concienciación a los empleados** con el fin de que sean capaces de identificar solicitudes fuera de lo común y que presten especial atención a los emails que solicitan cambios relacionados con el destino de facturas o cuentas bancarias.

Por otra parte, se recomienda que las organizaciones requieran a los empleados **validar la solicitud de transferencias electrónicas** a través de otros medios como por ejemplo por teléfono, con el fin de eludir un posible email falso, e **implementar medidas técnicas** como pueden ser SPF, DKIM o DMARC **y medidas de seguridad robustas** para acceder al correo.