ESTAFAS POR INTERNET A EMPRESAS DE ARABA/ GIPUZKOA /BIZKAIA

La Sección Central de Delitos en Tecnologías de la Información de la Ertzaintza se ha puesto en contacto con CÁMARA DE GIPUZKOA porque viene detectando desde hace unos meses ataques informáticos y estafas por Internet dirigidos contra empresas vascas que pueden llegar a ocasionar (en algún caso ya lo han hecho), un gran perjuicio económico y organizativo.

Los métodos que están siendo más utilizados son el **secuestro de datos** (conocido como ransomware y las **suplantaciones de identidad**.

En el primer caso, el ataque suele producirse al **abrir o descargar correos electrónicos con una apariencia más o menos oficial** (ejemplo último envío suplantando al Operador español servicio postal y paquetería Correos) que desencadenan todo el proceso, logrando el acceso remoto al ordenador de las víctimas.

Facilitan o influyen en este ataque:

- Un servicio del sistema operativo mal securizado porque no existen políticas de seguridad implantadas en la organización: contraseñas robustas, firewall, programa antivirus, copias de seguridad actualizadas, etc.
- Agujeros de seguridad en sistemas operativos no actualizados, o que ya no tienen soporte por parte del fabricante (por ejemplo Microsoft ya no da soporte a los sistemas operativos: Windows Xp y Windows Server 2003).
- Troyanos y virus informáticos.
- Empleando la técnica conocida como ingeniería social con el fin de engañar a un empleado, utilizando habitualmente el correo electrónico.

A- Modalidad de ataque haciendo ilegibles los datos almacenados por la empresa:

Esta técnica es conocida como ransomware , es un tipo de programa informático que restringe el acceso a determinadas partes o ficheros del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizándolo y coaccionando al usuario a pagar el rescate.

La ultima variante de este tipo se denomina TorrentLocker, que apareció a finales de agosto de 2014, este programa cifra o encripta ficheros de Microsoft Office, LibreOffice, archivos pdf, fotos, copias de seguridad, planos de autocad, ficheros comprimidos zip y rar, etc., haciéndolos ilegibles. El cifrado no se limita a los ficheros contenidos en la maquina infectada, además, se extiende a todas las carpetas de red a las que tiene acceso el usuario, a los ficheros sincronizados en Dropbox, a las copias de seguridad almacenadas en un disco duro externo usb conectado al ordenador ... etc. La clave para descifrar los ficheros se guarda en un servidor y se mantiene durante un número de días, pidiendo al usuario de la máquina que pague un rescate a través de métodos de pago por Internet, difíciles de rastrear, antes de que se borre y se pierda para siempre la posibilidad de rescatar los ficheros.

Según aconseja la Ertzaintza, para evitar este tipo de ataque debemos seguir las siguientes buenas prácticas:

1. Implantar una política de copias de seguridad con frecuencia diaria (o como mínimo semanal) en soportes extraíbles como cintas de backup o dvds, en todo caso que no estén conectadas al servidor principal. Desde estas copias se pueden restaurar los ficheros afectados por el cifrado, o incluso restaurar todo el sistema.
2. Se considera igualmente imprescindible que todo servicio que permita el acceso remoto a los equipos de una empresa cuente con una seguridad extrema, con una clave de acceso no fácilmente adivinable, así como prestar atención frecuente (preferentemente diaria) a las vulnerabilidades publicadas que hayan podido surgir en las aplicaciones, por ejemplo la web del instituto nacional de ciberseguridad: https://www.incibe.es
3. Tener instalado y actualizado en todos los equipos informáticos de la empresa un programa antivirus que evite este tipo de ataques.
4. Tener actualizados todos los sistemas operativos y programas de la empresa para evitar la entrada de troyanos que explotan las vulnerabilidades de software.
5. Dar formación a los usuarios sobre el uso correcto y seguro del correo electrónico, ya que es esta la vía más habitual de infección de este tipo de virus.
6. La Ertzaintza recuerda a los administradores de equipos de las empresas que es fundamental tener activadas auditorías de seguridad que permitan los sistemas operativos empleados detectar lo antes posible cuando se está sufriendo un ataque (los llamados logs).

Todas estas y más prácticas las podéis encontrar siguiendo el siguiente enlace:
https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/Decalogo_buenas_practicas_seguridad_Departamento_Informatica

Para aquellas empresas que tengan sus sistemas infectados o comprometidos con este tipo de virus ramsomware recomiendo la siguiente pagina web:
http://www.bleepingcomputer.com/virus-removal/torrentlocker-cryptolocker-ransomware-information

También se pueden descargar herramientas de eliminación de este tipo de malware, aquí incluyo un vinculo que explica como eliminar el torrentlocker y desencriptar los ficheros cifrados:
http://www.im-infected.com/trojan/remove-torrentlocker-virus-removal.html

B- Modalidad de ataque a través de la suplantación de identidad.

El atacante se informa sobre las transacciones de negocio que realiza la empresa, vulnerando servicios de correo electrónico o equipos concretos. Se envía luego en nombre de la empresa víctima o de un proveedor un correo electrónico, haciéndose pasar por alguien vinculado al negocio desde una dirección de e-mail similar a las utilizadas por éstos o desde una dirección de la empresa previamente comprometida. Una vez establecida una relación de confianza, el atacante solicita con cualquier excusa una transferencia bancaria a una cuenta diferente a la habitual, consumándose así la estafa y siendo el seguimiento del dinero desviado extraordinariamente complejo.

Según nos ha trasladado la Ertzaintza, este tipo de estafa se podría evitar no realizando ni admitiendo ninguna operación relacionada con pagos o con cobros a través de correos electrónicos sin que exista un protocolo de confirmación telefónica o bien una forma de transmisión segura de esos datos con clientes y proveedores (por ejemplo, cifrado-descifrado con contraseñas por otro canal).

Es de sumo interés que la generalidad de las empresas conozcáis estos peligros y la forma de solventarlos, dado que no existe en la CAV un Centro de Respuesta y Prevención de Incidentes Tecnológicos (Ciberseguridad) que preste servicio público a Administraciones y empresas.

Siguiendo las indicaciones recibidas de la Ertzaintza, te recomendamos encarecidamente que prestes especial atención a la realización de auditorías periódicas de seguridad, que efectúes copias de seguridad de la información de la empresa en soporte externo, que conciencies a empleados y directivos respecto a los peligros de internet y que implantes protocolos de seguridad sobre los interlocutores en las relaciones de negocio que impliquen pagos y cobros separando canales de comunicación.

En el caso de que necesites más información o para que puedas comunicar este tipo de incidentes y recibir recomendaciones, la Ertzaintza, ha habilitado los siguientes correos electrónicos:

delitosinformaticos@ertzaintza.net
delituinformatikoak@ertzaintza.net

Confiando en que esta comunicación contribuya a que tu empresa quede a salvo de estas prácticas delictivas, que vienen incrementándose de forma preocupante, recibe un cordial saludo.