

Panorama

El verde colorea el último avance contra los estafadores en la Red

IZENPE REÚNE EN BILBAO A LAS PRINCIPALES AUTORIDADES DE SEGURIDAD EN INTERNET PARA ESTUDIAR OPCIONES CONTRA EL 'PHISHING'

SANTOS GUTIÉRREZ

Quién no ha recibido un 'e-mail' que parece de una entidad bancaria advirtiéndole que actualice urgentemente sus datos. Da igual si usted tiene una cuenta allí o no, alguno de los miles de destinatarios del mensaje la tendrá y mordeará el anzuelo. Al pinchar en el enlace que aparece en el correo enviado, se abrirá una página web idéntica a la del banco o caja presuntamente remitente. El usuario introduce sus datos y sus claves como de costumbre, y ya está, su información ha sido clonada para futuros -y fraudulentos- usos. Esta es una de las herramientas preferidas por los estafadores 'on-line' para hacerse con sus preciados detalles bancarios, una práctica conocida como 'phishing'. Los delincuentes copian meticulosamente los sitios de Internet legi-

timos, para que los incautos usuarios les proporcionen sus confidencias.

En el último año se han duplicado los ataques de 'phishing', y España es el país desde el que se envió la mayor cantidad de correos electrónicos con esta finalidad en 2007, según un informe elaborado por un equipo de investigación de IBM. Desde este contexto trabaja CABForum, una organización compuesta por entidades de certificación y navegadores de Internet, que vuelca sus esfuerzos por reforzar las carencias de seguridad en la red, como esta modalidad de estafa. Por tal razón, la empresa de certificación y firma digital de las administraciones vascas, Izenpe, ha invitado a representantes de Microsoft, Google, Firefox, Opera, Verisign, Entrust o Red Hat para participar, esta pa-



Íñigo Barreira

sada semana en Bilbao, por primera vez en un taller relacionado con este tipo de amenaza.

En esta ocasión han dilucidado sobre una clase de certificado de servidor seguro (SSL) -ese pequeño candado que aparece en la parte inferior derecha de nuestras pantallas, y que nos confirma que la página se encuentra encriptada-, con el atributo de la validación extendida (EV, por sus siglas en inglés) que «ofrece la novedad de mos-

trar la identidad del titular de la página visitada», señala Íñigo Barreira, responsable de Seguridad y Proyectos de Izenpe, quien añade que «de esta manera la persona que visite esa página está segura de que es de quien dice ser, y no es de otra persona como sucede con el phishing». La forma de identificar estos sitios de seguridad 'reforzada' es mediante el color que se muestra en la barra de navegación -donde se coloca la dirección web-. «Si el 'browser' colorea de verde la barra del navegación, es porque la página cuenta con SSL EV, y es segura», apunta Barreira.

Entornos más seguros

Los servidores seguros son principalmente utilizados en páginas de operaciones financieras o trámites administrativos, es decir, sitios donde se intercambian datos sensibles con riesgo de ser interceptados, y por ello se recurre a la codificación del entorno para añadir seguridad. Izenpe será la primera entidad de certificación en España que ofrecerá la tecnología de certificados de validación extendida, la cual es soportada por

«prácticamente todos los navegadores», según afirma Barreira, pero advierte de que «sólo funciona en las versiones actualizadas».

Los SSL EV requieren un procedimiento de obtención complejos, y de hecho, las propias entidades de certificación tienen que superar una evaluación específica y obligatoria para poder emitirlos. Para obtener un SSL basta comprarlo en línea a través de cualquier autoridad certificadora. Dar el paso a la validación extendida son palabras mayores. «Los requisitos para emitir estos certificados son más complejos, y están basados en la identificación del titular de la página web. El solicitante tiene que personarse en la entidad y acreditar su identidad y condición», explica el responsable de Izenpe. Para ello, el interesado «tiene que presentar el registro mercantil, poder notarial, y todos los documentos necesarios para dar fe de su cualidad. Con los SSL sólo basta dar la denominación del dominio, puesto que la identidad no se comprueba», advierte Barreira.

Son herramientas que están a disposición de «cualquier empresa o entidad que tenga un dominio colgado en Internet», indica el experto, pero aclara que «los certificados sirven exclusivamente para identificar, por lo que las operaciones realizadas dentro de la página son de la única responsabilidad del sitio».

al candidato ideal se le distingue enseguida

En infoempleo.com encontrarás la herramienta más poderosa para elegir al candidato que tu empresa necesita.
→ infoempleo.com

→ infoempleo.com

tu red profesional