¿Es vulnerable la banca online?

jueves, 10 de agosto de 2006

La Comisión de Seguridad de la Asociación de Internautas publicó el pasado mes de junio publicar un extenso informe, elaborado tras varios meses de investigación por Hugo Vázquez (Director Técnico de PENTEST, Consultores de Seguridad Telemática) y certficado por el esCERT, en el que se hace una completa revisión sobre la seguridad de la banca online en España. --ACTUALIDAD -- Un fallo de seguridad hace vulnerables tres millones de cuentas del HSBC.

Tras la lectura del informe podemos pensar que aun queda mucho trabajo en la banca online. Pero tampoco podemos olvidar los nuevos métodos empleados por las entidades bancarias, en este informe se aportan también ideas para un futuro mas seguro. Estas son sus principales conclusiones:

No se ha realizado un estudio en detalle para otro tipo de sistemas de autentificación de banca on-line, debido a la falta de un “estándar” para el resto de sistemas de autentificación de firma.

La conclusión mas inmediata que se desprende del presente informe es que los sistemas de firma de banca online, ya sea basados en "tokens" físicos, teclados virtuales, u otros, actualmente distan mucho de poder considerarse como soluciones robustas pues prácticamente todos adolecen del mismo fallo: que su seguridad se implementa -en gran medida- a través de un protocolo, http, que jamás se diseñó para ser seguro, sino solo funcional.

Hasta que llegue el día en que los mecanismos de verificación de la identidad del usuario de una aplicación web sean “robustos”, la banca on-line estará expuesta a toda serie de riesgos. ¿Se pueden eliminar completamente dichos riesgos? No es probable, pero si que se pueden reducir en gran medida mediante la realización de pruebas periódicas especializadas sobre los sistemas de seguridad empleados.

Si nos fijamos en la evolución de las metodologías de evaluación de la seguridad en los sistemas de información, observamos una tendencia a analizar cada vez con menor detalle las distintas tecnologías de protección. Ello es así porque a veces se confía ciegamente, en ciertos mecanismos clásicos, sin tener en cuenta que tan importante es un estudio de las particularidades de cada escenario concreto, como el del diseño en general y su específica implementación, y esto sea cual sea su origen y los “Argumentos de Autoridad” que lo defiendan.

Informe 1ª parte del informe

Informe 2ª parte del informe

Informe 3ª parte del informe

Informe 4ª parte del informe

Informe 5ª parte del informe

Hugo Vázquez Caramés
Director Técnico de PENTEST

Nota:

”La empresa española “PENTEST” tal vez sea una de las mejores del entorno europeo en la realización de Tests de Intrusión. Empresa que basa su éxito en la recluta para cada tipo de proyecto de los mejores “Pen-Testers" existentes en la problemática a auditar. Una vez seleccionados, forma un equipo de auditores o "Tiger Team" que pone al servicio del cliente. Normalmente los "Tiger Team" de “PENTEST” no solo son los mejores, sino también los más motivados pues trabajan a partir de la propia libertad de sus conocimientos y experiencia y de la que concede Pentest para el desarrollo de su función profesional.

Se abre el debate: ¿Podemos prevenir posibles ataques de fraude de phishing bancario?

nomasfraude.es http://www.nomasfraude.es/

Asociación de Internautas