

## LOS "HACKERS", LOS FEDERALES Y EL FUTURO DEL COMERCIO ELECTRÓNICO

"La gran guerra del Ciberespacio", los delitos que se cometen a nivel informático pueden llevar a los supuestos delincuentes, en algunos casos, hasta la cárcel. Esta delincuencia a llegado hasta la casa blanca y por ello el FBI se encarga de conseguir órdenes de registro, inicia procesos judiciales y confisca ordenadores, para frenar los llamados "delitos informáticos".

Podríamos citar como faltas o ataques, (no delitos) a cambiar la página de entrada de un servidor del Senado o mantener fuera de combate a la web del FBI durante una semana. Estos ataques han afectado en los Estados Unidos, en el periodo de una semana; al Departamento de Energía, al FBI, al Senado, al Departamento del Interior, incluso a la propia Casa Blanca, y el FBI logró detener a 6 personas que fueron acusadas de CRIMEN INFORMÁTICO.

Pero el tema va más allá, la exagerada reacción del gobierno a éstos ataques viene provocada porque los hackers usan determinadas herramientas que pueden causar daños físicos y económicos a un país. Sin ir más lejos, hace dos años Clinton fue informado de que Irak estaba probablemente detrás de una serie de ataques informáticos sobre servidores web del gobierno estadounidense, justo en medio de uno de los periódicos pulsos militares entre los dos países.

Todo esto conlleva unas consecuencias y de este modo el FBI, decidió que los proveedores de todo el mundo deberían guardar obligatoriamente los datos de su tráfico, para así poder seguir a los cibercriminales hasta sus casas. Por otro lado las aduanas luchan contra la pornografía infantil, y también querría ver un mayor control de la navegación. Ahora bien, tienen algo en común, y es que ninguno de ellos quiere que los internautas utilicen sistemas de cifrado de la información. Y eso está reñido tanto con las normas Europeas de privacidad, como con el futuro desarrollo del comercio electrónico. SIN CIFRADO NO PUEDE HABER COMERCIO SEGURO.

EUROPA-EE UU: amor, guerra, comercio y espionaje.

Sobre la discrepancia de ¿quién va a tener la última palabra en Internet? EEUU tiene varias proposiciones sobre las cuales Europa discrepa: por ejemplo, que no se usen métodos de cifrado potentes, o que la protección de datos privados la definan las propias compañías comerciales de Internet, o les gustaría que los proveedores de acceso guarden los datos de tráfico en la Red.

La Comisión Europea quiere que todos los comerciantes de la Red cumplan con sus estándares de privacidad, mucho más elevados que los de EEUU. Otra discrepancia es la del cifrado. EEUU quiere recuperar las claves cifradas y descifrar los mensajes. Pero las empresas Europeas no están muy convencidas, ya que; un informe encargado por el parlamento Europeo les ha puesto tras la pista de Echelon, una red de espionaje dirigida por los EEUU que rutinariamente intercepta comunicaciones de interés

militar y comercial, y cede la informacion a instituciones y empresas.

Desde mi punto de vista, los ataques informáticos no son nada positivo y debería encontrarse la forma para detenerlo, pero considero que la omisión de los mensajes cifrados no es la solución más apropiada aunque sí la más fácil para dar con los cibercriminales, pero la más desagradable para el comercio electrónico, ya que si no está garantizada la privacidad, ¿quién va a participar en este comercio, pudiendo escoger otro modo de comerciar en el que los participantes no corren ningún riesgo?