

La ciberdelincuencia, amenaza para el hospital

Un 80 por ciento del robo de información digital es cometido por los propios trabajadores de las empresas. En el ámbito sanitario esta amenaza cobra mucha importancia, dada la especial protección de los datos de los pacientes. Además de las medidas de seguridad, es necesario poder identificar al ciberdelincuente y asegurar las pruebas ante un posible proceso judicial. Para luchar contra el fraude en entornos digitales se debe actuar a *priori*, complementando la seguridad, y a *posteriori*, encontrando la prueba electrónica.

Gonzalo de Santiago 28/11/2008

La evolución de la ciberdelincuencia obliga a los hospitales y centros de atención primaria a tomar buena nota y a reforzar sus medidas de seguridad, ya que los ataques cada vez son más elaborados. Los datos personales de los pacientes tienen una alta protección, como regula la Ley de Protección de Datos, y los centros no sólo deben asegurar que esa información es segura, sino también poder averiguar quién es el culpable en caso de fraude o robo de dicha información.

Un 80 por ciento de los delitos cibernéticos son cometidos por los propios empleados de las empresas. El fin puede ser el dinero, el espionaje industrial o el chantaje de trabajadores que no están a gusto. Los hospitales prevén medidas de protección, pero cuando el incidente ya ha existido dentro del sistema informático, deben poder ser capaces de recabar las pruebas para un eventual proceso judicial.

Cybex, empresa especializada en investigación del fraude empresarial y económico en entornos virtuales, así como en servicios forenses digitales, complementa la seguridad informática dedicándose a la prueba electrónica. "Nosotros descubrimos al ciberdelincuente, eliminamos su anonimato", afirma Ana Rubio, directora de Desarrollo de Negocios de la empresa.

Luchar contra el fraude

Es importante contar con una política de seguridad conocida por todos los trabajadores, así como un sistema controlado de acceso a las diferentes bases de datos, previniendo la salida ilegal o la pérdida de datos confidenciales o sensibles, pero también es necesario actuar una vez que se ha cometido un fraude cibernético.

Cybex no es una empresa de seguridad informática, sino que complementa esa seguridad dedicándose a la prueba electrónica, es decir, reconstruye los incidentes ocurridos en un entorno digital que puede ser delincuencia cibernética. "Investigamos lo que ha ocurrido dentro de las entrañas del sistema informático o dentro de la memoria de cualquier dispositivo electrónico". Además, en el caso de que finalmente se acuda a juicio se utiliza la actividad forense informática para "obtener y preservar las pruebas para poder utilizarlas luego en juicios con el proceso denominado cadena de custodia, que asegura que esa prueba es admitida".

Se trata de una garantía procesal que asegura que el elemento que pretende hacerse valer como prueba en juicio, sea efectivamente aquél que fue recaudado y que su integridad no ha sido alterada en el proceso penal.

Los últimos estudios han dejado constancia de que la ciberdelincuencia ha evolucionado de forma notable en los últimos años. De los hackers tradicionales, la amenaza ha pasado a bandas de delincuentes que utilizan la más alta tecnología a su alcance para llevar a cabo ciberdelitos sistemáticos y profesionales. Por ello, conocer sus procedimientos y técnicas resulta fundamental para mantener los sistemas informáticos a buen recaudo y bien protegidos.

Matías Bevilacqua, director tecnológico de Cybex, se refiere a los problemas concretos de la sanidad. A su juicio, es un sector complicado por la importancia de los datos que custodia, lo que obliga a prestar una especial atención a la ciberdelincuencia. Su empresa utiliza los conocimientos que adquiere en su investigación para prevenir el fraude en entornos digitales.

Casos anuales

Según Bevilacqua, esta empresa gestiona una media de entre 20 y 30 incidentes anuales "y las trampas del ciberdelincuente suelen repetirse, por lo que esos conocimientos que se van adquiriendo se ofrecen en el servicio de preparación forense". El objetivo es revisar los sistemas de información, pero no sólo la parte tecnológica, sino también todo el cuerpo normativo que regula cómo se actúa con esa información.

Por ejemplo, un hospital dispone de tres opciones para dar de baja como usuario del sistema informático a un médico que ya no trabaja en el centro: borrar el usuario del sistema, cambiar la contraseña o deshabilitar el usuario.

Desde el punto de vista del centro, los tres procedimientos pueden ser válidos teniendo en cuenta

la seguridad, porque centra su objetivo en que el médico ya no pueda entrar en el sistema. "Desde nuestro punto de vista esos tres sistemas son distintos y sólo uno es válido para investigar luego un posible fraude y asegurar las pruebas para un posible juicio".

En opinión del especialista, casi nunca se diseñan estos sistemas pensando que un día habrá un fraude, sino desde la seguridad. "La trazabilidad es un subproducto de la seguridad y no se le suele dar importancia cuando sí que la tiene porque luego sirve para investigar un posible fraude".

Cuando el enemigo está en casa

El centro médico de la Universidad de California en Los Ángeles (UCLA) despidió al menos a 13 trabajadores y suspendió a otros seis por fisgonear en la historia clínica de la estrella de pop Britney Spears durante una reciente hospitalización en la unidad psiquiátrica. Además, otros seis médicos se enfrentaron a medidas disciplinarias por mirar a hurtadillas archivos informáticos de la popular paciente. Este caso ilustra el peligro al que se enfrentan los hospitales por acciones de sus propios trabajadores.

Preguntados sobre estos abusos por parte de algunos trabajadores y sobre la violación del derecho de confidencialidad de la enferma, los directivos del hospital afirmaron que no es la primera vez que se habían tomado medidas contra trabajadores del centro por mirar historias de pacientes. Varios de ellos fueron sorprendidos entrometiéndose en los archivos después de que la cantante diera a luz a su primer hijo en septiembre de 2005, en el centro médico de UCLA-Santa Mónica, y algunos fueron despedidos.

Otro caso al que se puede enfrentar un centro son los empleados descontentos que buscan dañar la imagen del hospital y utilizan sus perfiles informáticos para hacerlo.

Clases de ciberdelitos y consecuencias

Existen muchas formas de realizar un ciberataque; como el robo de datos confidenciales, el corte de acceso de la compañía a internet, la denegación del servicio o ataques a los PC, que se vuelven muy inestables. Estos ataques pueden además generar enormes pérdidas económicas en las empresas. Sin embargo, el coste provocado por los ataques de ciberdelincuencia es difícil de calcular, pues no sólo se limita al término monetario sino que también hay que tener en cuenta las pérdidas por daños a la imagen de la compañía o las pérdidas de información confidencial, entre otros aspectos.

Diario Médico