BALUARTE
newsletter de seguridad

TECNOLOGIA: SEGURIDAD INFORMATICA

Espionaje Corporativo: más extraño que en la ficción

Por Keith Blogg

¿Qué tienen en común el gigante de la industria química Procter and Gamble, la compañía líder en IT, Oracle y el ex cónsul general francés en Houston, Texas?

La respuesta es que todos ellos han estado involucrados en una de las más grandes industrias del nuevo milenio: el espionaje corporativo.

Sus casos ponen al descubierto a una industria global que en un año le ha quitado a las compañías estadounidenses su información privilegiada y su propiedad intelectual por un valor de U$S 59 billones (£34 billones), según una encuesta de la American Society of Industrial Security (Sociedad Americana de Seguridad Industrial) y PriceWaterhouseCoopers, publicada en el año 2002. Un cálculo estimativo indica que las cifras actuales ascienden a 100 billones de dólares.

Este estudio del área, que ha tomado en cuenta las experiencias de 138 compañías pertenecientes al ranking Fortune 1000, demostró que el 40% de los empleados

El espionaje es una actividad en rápido desarrollo y suele ser realizado por los propios empleados.

sospecha o efectivamente sabe del robo de información privilegiada en sus compañías e informó que la mitad de aquellos que habían sido afectados mencionaron que el blanco del espionaje fueron una serie de proyectos de investigación y desarrollo, con una pérdida promedio de U$S 405.000 (£231,000) por cada uno de estos robos; la cifra no tuvo en cuenta la ventaja competitiva perdida.

Una asombrosa estadística muestra que el 90% de las computadoras conectadas a Internet están infectadas con spyware.

Se trata de un software instalado en una computadora sin que su dueño lo sepa con el fin de recopilar información y retransmitirla a terceros. La cantidad de intentos de robo de datos confidenciales ha aumentado en un 50% en un año de acuerdo con el estudio antes mencionado, y aproximadamente el 45% de las compañías han tenido episodios de acceso no autorizado a datos corporativos por parte de individuos que en razón de su cargo tienen acceso a esta información confidencial (llamados insiders).

Recopilación de Información de Inteligencia

En Europa, la alarma suscitada por las actividades de la red de espionaje electrónica Echelon, controlada principalmente por los EE.UU., que incluye el espionaje industrial entre sus prácticas de recopilación de datos de inteligencia, ha llevado al Parlamento Europeo a solicitar que la encriptación de los correos electrónicos se convierta en norma y a intentar lograr una mayor cooperación entre compañías europeas y los servicios de contraespionaje. En su informe, el Parlamento Europeo denunció que Echelon fue capaz de interceptar mensajes de telecomunicaciones por satélite, correos electrónicos y faxes internacionales. El año pasado, en Gran Bretaña, el servicio de contrainteligencia M15 expresó su “profunda preocupación” por la infiltración de espías chinos en los negocios británicos y asimismo declaró que el espionaje es realmente desenfrenado y que ello es una de las serias consecuencias de la economía globalizada.

En la batalla por la protección de secretos comerciales, el éxito de un nuevo emprendimiento no es solamente lo que está en juego sino también el futuro mismo de la compañía.

En muchas compañías, la brecha entre ganadores y perdedores es tan delgada como unas pocas semanas o aún unos pocos días solamente, ya que es posible que años de investigación puedan perderse en el robo de un proyecto o de formulaciones o que meses de tratativas para lograr una fusión o una adquisición sean tirados por la borda debido a que la competencia ha robado la cifra final de la oferta.

Contrariamente a lo que ocurre con los bienes tangibles, que se pueden ver si han sido robados, es posible que por años se le haya estado sustrayendo a una compañía su propiedad intelectual o su ventaja competitiva y que nadie se de cuenta.

La competencia puede sacar ventajas en el mercado constantemente, ya sea haciendo una oferta más baja en una licitación o simplemente desarrollando innovaciones más económicas o más rápidamente. Sus secretos corporativos en manos de la competencia significan conocimiento que puede volverse en su contra.

Todo aquello que pueda traerle beneficios a su compañía y colocarla en una posición de ventaja sobre sus competidores es el blanco natural de la industria del espionaje. Ello varía desde el código fuente de una computadora, un software pronto a lanzarse hasta su propiedad intelectual, sus planes de marketing, secretos corporativos, documentación de investigaciones, etcétera.

El espionaje corporativo no se limita, por supuesto, a los actores globales y a una inversión técnica masiva. Es posible que los espías profesionales descubran el perfil de una pequeña compañía obteniendo sus conversaciones privadas, documentos desechados, memos, proyectos y desechos de material de viajes.

El enlace más débil

Allen H. Beiner, consultor en sabotaje electrónico del FBI, afirma que el enlace más débil con respecto a la protección de datos comerciales vitales es el trabajador mismo. "Podemos colocar firewalls (cortafuegos) en cada una de las computadoras pero en realidad todo depende de la persona", agrega el consultor. Según datos de un cálculo estimativo, dos tercios del total del espionaje corporativo en los EE.UU. es desarrollado por los propios empleados.

En algunas ocasiones, los empleados venden secretos corporativos con fines de lucro. En otros casos, pueden hacerlo por venganza. Un empleado disconforme es capaz de enviar sus secretos corporativos directo a la competencia.

Las entrevistas de trabajo también constituyen otra fuente de espionaje más "discreta" para las compañías inescrupulosas. Preguntas tales como "¿Cuáles han sido tus tareas?" o "¿Cuál es el próximo paso de tu compañía?" son formuladas con el sólo fin de conocer los secretos profesionales del rival.

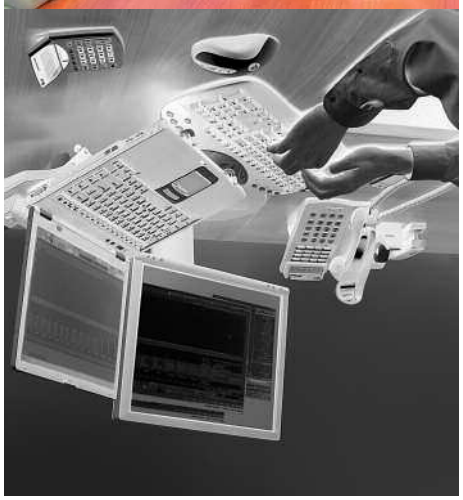
A menudo, los empleados roban simplemente por las suculentas recompensas que se les ofrecen. Este año, dos personas, una de ellas empleada de Samsung Electronics, fueron arrestadas en Corea del Sur por intentar robar tecnología de fabricación de telefonía celular valuada en U$S 1.3 billones (£ 0.75 billones) de la compañía en la que trabajaban y venderla a otra compañía en Kazajstán.

El caso puso de manifiesto el alza del índice de filtración de tecnología a través del espionaje. De acuerdo con datos brindados por el Servicio de Inteligencia de Corea, la cantidad total de casos en el año 2003 fue de seis, por un valor de U$S 13.9 billones (£8 billones), aumentando a 26 casos en el año 2004 por un valor aproximado de U$S 32.9 billones (£19 billones) y finalmente de 29 casos el año pasado por un valor de U$S 35.5 billones (£20 billones).

El valor de la basura

En el caso Procter and Gamble, un ex experto en inteligencia de Vietnam, John Nolan, encabezó una operación encubierta que tenía como fin descubrir los secretos de las exitosas marcas comerciales de productos capilares Salon Selective y Finesse, pertenecientes a su rival Unilever.

La operación, que incluyó "dumpster diving" ("buceo en la basura") –práctica que consiste en revisar los cestos de basura en busca de información– fue encubierta por los propios ejecutivos senior de P&G, quienes no sólo no sancionaron la operación sino que se dirigieron a sus rivales y les confesaron todo. Como resultado, tres empleados fueron despedidos.



Oracle también utilizó la práctica de "dumpster diving" para intentar obtener los secretos corporativos de su más grande rival, Microsoft. Apodado "Garbagegate" (por la combinación de "garbage": basura, y "gate" en alusión al escándalo "Watergate"), los ataques fueron declarados legítimos por su CEO Larry Ellison.

Posteriormente, se descubrió que uno de los integrantes de otro de los grupos dedicados a la recolección de residuos en el hogar de un ejecutivo estadounidense en Houston era el cónsul general de Francia. Este funcionario se defendió asegurando que estaba recolectando basura para rellenar un hueco en su jardín pero el FBI estaba convencido de que el hueco que quería rellenar era en beneficio de la capacidad de defensa de Francia.

Las técnicas que utilizan los espías corporativos evolucionan constantemente. Sin embargo, algunas son sorprendentemente simples. En Sudáfrica, escondidos en salones de conferencias, se han encontrado teléfonos celulares cuyo sistema había sido modificado esperando su activación remota. Es decir, se modificaron para que no sonaran al recibir una llamada sino que simplemente se prendan y transmitan todo lo que oigan a través de un micrófono sensitivo.

Este año una pareja israelí fue arrestada por haber desarrollado una pieza de software maliciosa –conocida como "Troyano"– que infecta el sistema de la computadora y permite que personas ajenas tengan acceso a documentos confidenciales, hojas de cálculo, correos electrónicos, y asimismo las claves y los nombres de usuario contenidos en las computadoras.

Entonces, ¿qué se puede hacer al respecto? Además de la protección técnica de aquellos datos guardados en una computadora es necesario desarrollar un programa de capacitación en cuestiones de seguridad para los empleados.

"Los empleados deben ser la principal línea de defensa de la compañía", sugiere el especialista en seguridad de información Capt Raghu Rahman, CEO de Mahindra Special Services Group. "Un empleado atento y capacitado es más eficiente que cualquier sofisticado sistema de seguridad y además presentan la ventaja de estar disponibles a un menor costo", agrega.

"En segundo lugar, debe considerarse la seguridad de la información y no la seguridad de IT, y ello debe formar parte de las principales responsabilidades del área de administración de la compañía. Implica un cambio cultural, especialmente en el subcontinente Indio, en donde los elementos privacidad y protección de datos han estado tradicionalmente ausentes".

Fuente: Web de G4S, www.g4slatam.com

BALUARTE

newsletter de seguridad

www.BaluarteOnline.com.ar
Rodríguez Peña 55 PB • 4383-8300