

## Protegiendo la empresa de los ex-empleados enojados

Un alto ejecutivo de la empresa deja la compañía, se lleva su porta retratos con fotos de la familia, su juego de lapicera y lápiz dorados y las contraseñas de varios cientos de empleados.

Una de las vendedoras de mayor experiencia de la firma oye un rumor respecto de que es seguro que será despedida. Y lo es, pero antes de recibir su carta de despido al comenzar el próximo trimestre, se las arregla para descargar en su cuenta de Gmail una larga lista de los clientes clase A+ y sus historiales de compras y pagos.

Si está pensando &ldquo;En mi compañía jamás&rdquo; ó &ldquo;Mis empleados no&rdquo;, piénselo de nuevo. Escenarios como los descritos arriba están sucediendo todos los días, dicen los expertos, y aún los profesionales más capaces y confiables pueden verse forzados al robo de información y otros crímenes de computación frente a las agobiantes presiones económicas y los inminentes despidos.

Estadísticas recientes lo confirman. En un estudio de finales de 2008 realizado por la firma de seguridad de TI Cyber-Ark Software Inc. El 56% de los trabajadores de servicios financieros de Nueva York, Londres y Amsterdam admitió que estaban preocupados por los despidos.

Preparándose para lo peor, más de la mitad dijo que ya había descargado información corporativa competitiva que planeaban usar para obtener su próximo trabajo.

En los EEUU el porcentaje fue un poquito más alto, con un 58% de los trabajadores de Wall Street diciendo que ya lo habían hecho. Y 71% de todos los trabajadores dijeron que definitivamente se llevarían información con ellos si se enfrentaran con la posibilidad de un despido el día de mañana.

&ldquo;Cuando la gente está desesperada por pagar el techo que tiene sobre su cabeza o por llevar comida a su mesa, es capaz de hacer cosas que normalmente no haría, lo cual es el porque el crimen aumenta cuando sufre la economía,&rdquo; dice David Griffeth, vice presidente de integración de línea de negocios e informes del RBS Citizens Bank. &ldquo;Eso no deja de pasar porque uno tenga una licenciatura o una maestría. Es un miedo común basado en la necesidad. Uno tiene un distinto nivel de comodidad con el crimen que comete.&rdquo;

### Oferta y demanda

&ldquo;Tiene sentido que el robo [de información] esté en aumento cuando la demanda es baja y la oferta es alta. En este momento, hay una gran cantidad de oferta de empleados, y si una persona puede hacerse más atractiva que otra frente a un potencial nuevo empleador, esto será una gran tentación.&rdquo; dice Keith Jones, un investigador digital forense y socio de Jones Dykstra & Associates, una consultora de seguridad informática de Columbia, Md.

Entretanto, la legión de trabajadores despedidos continua creciendo. En los últimos meses, Citigroup, SAP, Sun Microsystems, IBM, Sprint y Microsoft han anunciado despidos, que se suman a las decenas de miles de personas que ya están desempleadas, muchos de los cuales son técnicos expertos y tiene acceso a sistemas clave de computación, a información corporativa altamente sensible, o a ambos.

Lo que es sorprendente, y potencialmente letal para la seguridad corporativa, es cuantos trabajadores que se fueron conservan ese acceso mediante las llamadas cuentas huérfanas, mucho tiempo después de haber sido despedidos. Cuatro de cada diez empresas no tienen ni idea de si sus cuentas de usuarios permanecen activas después que un empleado se va, según afirma un estudio de 850 ejecutivos de seguridad, TI y de recursos humanos hecho por Symark International Inc. , una compañía de programas de seguridad.

Además, 30% de los ejecutivos informaron que no hay un proceso establecido para ubicar y deshabilitar las cuentas huérfanas. Otra estadística lamentable: 38% de ellos no tiene forma de determinar si un empleado actual o ex-empleado está usando o ha usado una cuenta huérfana para acceder a información.

La amenaza más común es aquella en la cual el empleado toma propiedad intelectual, incluyendo planes estratégicos o datos de clientes, antes o apenas después que se fueron, dice Jonathan Penn, un analista de Forrester Research Inc.

Y las cosas pueden volverse más inciertas aún cuando el personal de TI es despedido. A menudo, estos son empleados con &ldquo;las llaves del reino,&rdquo; dice Jones.

Destaca que Roger Duronio, un antiguo empleado de TI en UBS Paine Webber que fue condenado y sentenciado a ocho años en prisión por plantar una bomba lógica en el software, pudo realizar tal vasto daño a la compañía porque &ldquo;tenía acceso a todas partes.&rdquo; (Una bomba lógica es un código de programa que dispara funciones maliciosas bajo ciertas condiciones predeterminadas; por ejemplo, uno podría fijar el borrado de todas las cuentas de clientes en una fecha específica.)

Los administradores de sistemas y usuarios con cuentas de acceso privilegiadas, tales como quienes conocen la contraseña de 'root', pueden representar una gran amenaza, dice Sally Hudson, una analista de investigación de mercado de IDC. &ldquo;Quienes tienen acceso a contraseñas privilegiadas poseen el poder de cambiar datos del sistema, el acceso y configuración de los usuarios. También tienen la capacidad de sabotear fácilmente operaciones críticas de toda la organización,&rdquo; dice ella.

Más allá de estas vulnerabilidades, hay medidas que las compañías pueden tomar para limitar el daño potencial, especialmente cuando llevan a cabo despidos.

Haga su tarea, las estrategias de salida y medidas de seguridad varían dependiendo del rol del empleado. Los ejecutivos y gerente que están a cargo del despido de personal no deben asumir que el deshabilitar el acceso a la computadora es simplemente cuestión de desenchufar un cable.

&ldquo;Antes de despedir, mire detalladamente las clases de personas&rdquo; recomienda Jones. &ldquo;Si son de ventas, RRHH o de finanzas o son empleado de alta categoría, puede demorar más [deshabilitar sus accesos] porque tienen accesos más amplios a los sistemas,&rdquo; respecto al que tienen otros empleados.

Involucre a TI en la planificación de los despidos tan temprano como sea posible en el proceso. &ldquo;Es importante para TI estar estrechamente sincronizado con RRHH,&rdquo; dice Ken van Wyk, un especialista de seguridad de la información y consultor en Alexandria, Va. &ldquo;Pero la gente de TI necesita comprender cuán sensibles son sus roles y debe haber tolerancia cero respecto de hacer correr rumores. Si una persona de TI le dice a la gente que van a ser despedidos, entonces esa persona de TI también debe ser incluida en la nómina de despidos.

Asegúrese de tener instaladas las políticas y programas de seguridad apropiados un tiempo antes de los despidos, recomienda Hudson de IDC. Entre otras cosas, debería asegurarse que está usando sistemas que aseguran el contenido, impiden la pérdida de datos y manejan las amenazas. Tales sistemas incluyen a los cortafuegos, las herramientas de filtrado de spam y contenidos y de antivirus.

También debe contar con una infraestructura de manejo seguro de identidad y acceso. Conocida también como IAM, este tipo de instalación &ldquo;controla el quién, qué, donde, cuando y porque de las actividades del usuarios a lo largo de toda la empresa,&rdquo; explica Hudson. Teniendo la capacidad de monitorizar y evaluar como son usados los permisos de acceso es crítico para alcanzar los mandatos de gobierno e identificar el abuso en los sistemas.

Compartimentar el acceso a los sistemas según los roles de los empleados. Este es un principio de diseño seguro de sistemas que las compañías deberían implementar al comienzo de todo esfuerzo de desarrollo de software. &ldquo;El control de acceso significa ajustar mucho mas en la capa de lógica de negocios,&rdquo; explica van Wyk.

Pero demasiado a menudo las compañías olvidan esta estapa &ldquo;porque requiere mucho tiempo y pensar a lo largo del siseño del software,&rdquo; dice. En ausencia de un diseño seguro inicial, la siguiente mejor medida es implementa un software que registre los accesos del usuario al sistema y las acciones que lleva a cabo mientras usa las distintas aplicaciones de negocio, dice van Wyk.

Casi todas las aplicaciones de negocios tienen algún nivel de seguridad con identificación de usuario y contraseña, y entonces, cuando uno está adentro, está adentro,&rdquo; dice. Pero con un sistema de seguimiento, cuando un usuarios ingresa en una base de datos, todo lo que este hace allí es registrado, y potencialmente informado a las fuerzas del orden, explica van Wyk.

Despida en buenos términos, pero planifique para malos momentos. Jones recomienda que incluso si un despido sucede tranquilamente sin aparentes contrariedades por parte del empleado, una compañía debe recoger igualmente evidencia de su propia debida diligencia en caso de alguna futura investigación.

Esto es porque las compañías que experimentan cualquier tipo de brechas de seguridad, incluyendo robo de información por parte de empleados despedidos, deben ser capaces de mostrar que tomaron todas las precauciones posibles y medidas para proteger esa información.

Específicamente, Jones dice que las compañías deben tomar imágenes forenses de las notebooks de los empleados que se van, de modo que estén disponibles en caso que se lleve a cabo una investigación. (Una imagen forense es una copia del disco rígido de la computadora).

&ldquo;Usualmente, cuando algo malo sucede, no sucede enseguida,&rdquo; explica Jones. De hecho, puede demorar seis, 12 o incluso 24 meses antes de que salga a la luz. Si, hay un gasto adicional por tomar la imagen, dice, pero debe contrastar eso con el costo potencial de un litigio.

Traducido para blog Segu-info por Raúl Batista - Autor: Julia King

Fuente: <http://blog.segu-info.com.ar/2009/03/protegiendo-la-empresa-de-los-ex.html>