Fuga de datos a nivel mundial: El elevado costo de las amenazas internas

Resumen ejecutivo

Un estudio de seguridad a nivel mundial sobre la fuga de información reveló que la pérdida de datos debido a la conducta de los empleados es una amenaza más grande de lo que creen muchos profesionales de TI. Encargado por Cisco y realizado por InsightExpress, una compañía de investigación de mercado con sede en Estados Unidos, el estudio encuestó a más de 2000 empleados y profesionales de tecnología de la información en 10 países. Cisco seleccionó los países por sus culturas sociales y comerciales distintivas, a fin de comprender mejor si estos factores influyen en la fuga de información.

En manos de empleados desinformados, descuidados o descontentos, cada dispositivo que accede a la red o almacena datos se transforma en un riesgo potencial para la propiedad intelectual o la información confidencial de los clientes. Para acrecentar aun más el problema, en muchas empresas existe una dicotomía entre lo que creen los profesionales de TI y la realidad actual del entorno de seguridad. Los nuevos hallazgos muestran que las “amenazas internas” pueden causar mayores pérdidas financieras que los ataques provenientes del exterior.

- La preocupación principal del 33% de los profesionales de TI era la pérdida o robo de datos a través de dispositivos USB.
- El 39% de los profesionales de TI a nivel mundial estaba más preocupado por las amenazas provenientes de sus propios empleados que por la de los piratas informáticos externos.
- El 27% de los profesionales de TI admitió que no conocía las tendencias de la pérdida de información de los últimos años.

Mitigar la fuga de información desde fuentes internas es un desafío complicado. Las empresas deben aprovechar cada oportunidad que tengan para comprender mejor cómo la conducta y las intenciones de los empleados se relacionan con la seguridad, y para hacer de la seguridad una prioridad en cada aspecto de las operaciones comerciales.

Introducción

Aunque puede que aún haya piratas informáticos que planten virus y gusanos para interrumpir las operaciones comerciales, la mayoría se dedica a obtener ganancias. El robo de identidad, la venta de información tecnológica o financiera reservada a la competencia, el abuso de datos confidenciales de clientes y el uso indebido del nombre de una empresa o de marcas de productos son sólo algunas de las formas en que los piratas informáticos pueden lucrar al vulnerar la seguridad y obtener contenido confidencial.

La amenaza de ataques externos a la empresa es verdadera, y amerita que los profesionales de TI la tomen en serio y adopten medidas al respecto. Pero también se pierde gran cantidad de información producto de actividades internas. Al hablar de amenaza interna, generalmente se piensa en conductas maliciosas por parte de empleados tales como sabotaje, robo de datos o de dispositivos físicos, o filtración deliberada de información.

Sin embargo, las organizaciones deben comprender que la amenaza interna no proviene sólo de empleados deshonestos, sino más bien de cada empleado y de cada dispositivo que almacena información. Los empleados constituyen una amenaza interna si hablan por teléfono en voz alta sobre proyectos confidenciales en el

aeropuerto. Un equipo portátil con información empresarial puede convertirse en una amenaza interna si se pierde y lo encuentra una persona ajena a la empresa que tenga intenciones maliciosas.

Los primeros dos informes en esta serie se centraron en las conductas de los empleados que pueden mermar la seguridad de la información empresarial. En el presente informe se analizan con mayor profundidad algunas amenazas internas que afectan a la información, ya sea mediante conductas negligentes o maliciosas por parte de los empleados. Mitigar la gama completa de amenazas provenientes de los empleados es un desafío enorme que conlleva un costo sumamente elevado si no da resultado. Los profesionales de TI deben ser innovadores y persistentes al enfrentar las amenazas contra la seguridad que surgen con el avance de la era digital. Comprender la amenaza interna es un aspecto fundamental de este proceso.

La amenaza interna: empleados negligentes

Los primeros dos informes de esta serie, disponibles en http://www.cisco.com/go/dlp, se centraron en cómo las conductas involuntarias e imprudentes de los empleados y los profesionales de TI pueden comprometer la seguridad de la información. En el primer informe se analizó la pérdida de información desde la perspectiva de los empleados. El informe técnico Fuga de datos a nivel mundial: Riesgos y errores comunes de los empleados examinó la relación entre la conducta de los empleados y la pérdida de información, así como la percepción que tienen de ella los profesionales de TI. La encuesta reveló que empleados de todo el mundo exhiben conductas que ponen en riesgo la información personal y empresarial, que los profesionales de TI a menudo no están al tanto de dichas conductas y que prevenir la fuga de información es un desafío que abarca toda la empresa.

En el segundo informe se analizó la pérdida de información desde la perspectiva de los profesionales de TI. El informe técnico Fuga de datos a nivel mundial: La eficacia de las políticas de seguridad examinó cómo la creación, difusión y cumplimiento de las políticas de seguridad influyen en la fuga de información. El análisis reveló que la falta de políticas de seguridad y el incumplimiento de los empleados de dichas políticas son factores significativos en la pérdida de información. Al igual que en el primer conjunto de hallazgos, la encuesta reveló que los profesionales de TI carecían de información importante, en este caso sobre cuántos empleados realmente comprendían y acataban las políticas de seguridad. El informe concluyó que las empresas deben abordar el desafío doble de crear políticas de seguridad y hacer que los empleados las acaten.

Junto con los resultados del presente informe, estos hallazgos revelan que la ignorancia, la falta de diligencia y el desacato en el interior de la empresa constituyen una amenaza interna significativa para la información.

Ignorancia

A menudo los empleados exhiben sin darse cuenta conductas irresponsables que generan filtraciones de datos. En parte, este problema puede atribuirse a la falta de políticas empresariales o a la difusión inadecuada de las mismas a los empleados. En otros casos, los profesionales de TI suponen equivocadamente que los empleados exhibirán cierto grado de profesionalismo, conciencia de la seguridad y precauciones de sentido común.

- El 43% de los profesionales de TI afirmó que no educa a los empleados como es debido.
- El 19% de los profesionales de TI afirmó que no ha difundido las políticas de seguridad a los empleados como es debido.

Falta de diligencia

Entre los ejemplos comunes de conductas poco diligentes de los empleados con respecto a la seguridad de la información se incluye hablar en voz alta sobre información confidencial en lugares públicos, no cerrar sesiones en equipos portátiles, dejar contraseñas a la vista o desprotegidas y acceder a sitios web no autorizados. Una amenaza especialmente significativa proviene de empleados que pierden dispositivos empresariales tales como

equipos portátiles, teléfonos móviles y discos duros portátiles, o cuando estos dispositivos son robados por no haberlos protegido correctamente. De estos dispositivos, la pérdida de discos duros portátiles era la principal preocupación entre los profesionales de TI. Ahora con los nuevos dispositivos extraíbles de 64 GB que permiten copiar todo un disco duro en un aparato del tamaño de un paquete de chicle, es mucho más fácil acceder, mover o perder propiedad intelectual o datos de los clientes.

- El nueve por ciento de los empleados informó que ha perdido o le han robado dispositivos empresariales.
- De los empleados que informaron sobre la pérdida o el robo de dispositivos empresariales, al 26% le sucedió más de un incidente el año anterior.
- La principal preocupación a nivel mundial entre los profesionales de TI con respecto a la fuga de datos era el uso de dispositivos USB, con un 33%. La segunda preocupación en importancia era el correo electrónico; con el 25% de todos los profesionales de TI.
- Cuando se les preguntó por qué sus empleados eran menos diligentes al momento de salvaguardar la propiedad intelectual, el 48% de los profesionales de TI respondió que los empleados manejaban más información que nunca, y el 43% señaló que existe una creciente apatía hacia la seguridad debido al acelerado paso del trabajo.

La amenaza interna: empleados descontentos

Un empleado descontento o que procura beneficios financieros mediante el uso ilícito de recursos empresariales se convierte en una amenaza interna que agrega una nueva y peligrosa dimensión al desafío de prevenir la pérdida de información.

Un empleado descontento que se ha transformado en una amenaza interna contradice la percepción común de que las principales amenazas contra la seguridad provienen desde el exterior de la empresa. Un empleado deshonesto y motivado por la codicia puede aprovechar su condición y llevar a cabo actividades que causen una mayor pérdida financiera que las amenazas externas.

El acceso legítimo a la red del que gozan y tener en custodia dispositivos como equipos portátiles y agendas PDA facilita que empleados desleales filtren información empresarial.
Algunos empleados simplemente se quedan con los dispositivos empresariales cuando dejan el empleo. Esta conducta, además de costosa, representa un peligro para la empresa ya que añade una nueva vía por la que puede perderse información.

Incluso si sólo el 5% de los empleados se queda con dispositivos, esto equivaldría a 50 empleados en una empresa con 1000 trabajadores, o 500 en una con 10.000. Las organizaciones de mayor tamaño presentan un mayor riesgo financiero y de pérdida de información.

- Un alarmante 11% de los empleados respondió que ellos u otros colegas accedieron a información no autorizada y lucraron con ella, o robaron computadoras (Tabla 1).
- Entre las razones de los empleados para quedarse con dispositivos empresariales al dejar el empleo se incluyeron que los necesitaban para fines personales (60%), para vengarse de la empresa y porque pensaron que el empleador antiguo no se enteraría.
- El 20% de los profesionales de TI afirmó que los empleados descontentos constituían su principal preocupación en cuanto a las amenazas internas.

Tabla 1. Robo o acceso ilegal a información de la empresa y otros recursos

	Usuarios finales										
	Total (n=1009)	EE.UU. (n=100)	BRA (n=101)	REINO UNIDO (n=104)	FRA (n=100)	ALE (n=101)	ITA (n=101)	CHN (n=100)	JPN (n=101)	IND (n=100)	AUS (n=101)
Conoció a alguien en el trabajo que ha accedido a la computadora de otra persona para buscar información personal o empresarial no autorizada	**6%**	3%	7%	4%	14%	4%	3%	8%	0%	10%	6%
Accedió a la computadora de otra persona para buscar información personal o empresarial no autorizada	**5%**	1%	7%	3%	12%	2%	5%	11%	1%	4%	0%
Conoció a alguien en el trabajo que ha robado computadoras u otros equipos que contenían información de la empresa	**3%**	1%	3%	2%	4%	2%	8%	3%	0%	6%	0%
Conoció a alguien en el trabajo que ha vendido información empresarial a terceros	**3%**	0%	5%	1%	3%	3%	1%	5%	3%	4%	1%
Robó computadoras u otros equipos que contenían información de la empresa	**1%**	0%	0%	0%	1%	0%	2%	0%	0%	3%	0%
Vendió información empresarial a terceros	**1%**	0%	2%	0%	0%	2%	2%	0%	1%	2%	0%
Ninguna de las anteriores	**89%**	96%	85%	93%	79%	93%	87%	82%	96%	84%	94%

Conciencia limitada de TI

Toda amenaza interna es significativa, pero el impacto potencial puede ser mayor cuando existe una dicotomía entre la percepción que tienen los profesionales de TI con respecto a la conducta de los empleados y las acciones de los usuarios. El veintisiete por ciento de los profesionales de TI admitió que no conocía las tendencias de los incidentes de pérdida de información en los últimos años.

El contraste entre la conducta de los empleados y la percepción de los profesionales de TI se hace más evidente en las proyecciones a futuro. El cincuenta por ciento de los profesionales de TI cree que los incidentes de fuga de información no disminuirán en los siguientes 12 meses. Eso deja a un sorprendente 43 por ciento que cree que sus datos estarán más seguros durante el próximo año, a pesar de que la encuesta reveló que los empleados tienden a menospreciar las políticas y exhiben conductas que ponen los datos empresariales en riesgo.

El costo de la pérdida de información

Al considerar el costo de la pérdida de información, el aspecto más sencillo de medir es el costo de capital que implica reponer los equipos perdidos o robados. Estos costos varían según lo avanzado de los equipos y el

tamaño de las empresas. Para las empresas más pequeñas, el costo de reemplazar un teléfono celular o un equipo portátil probablemente sea más significativo que para una empresa más grande que tenga un mayor presupuesto para tecnología.

Un costo más significativo para todas las empresas es el gasto operativo relacionado con el robo de equipos. Cuando se roba un dispositivo, un profesional de TI debe resolver el problema ordenando y configurando un nuevo aparato, dedicando a ello tiempo valioso que podría haberse utilizado para otros fines. Los costos operativos aumentan aún más cuando los datos o dispositivos perdidos o robados se utilizan para causar daños maliciosos que el personal de TI debe corregir gastando tiempo valioso.

Los gastos de capital y operativos son indicadores mensurables del costo por la pérdida de información. Aunque estos costos sean dolorosos, no son nada en comparación con una faceta de la pérdida que no puede medirse en términos presupuestarios. Dicha faceta es el uso de datos confidenciales para socavar la reputación de una empresa, la integridad de la marca o la confianza de los clientes. Estos factores pueden alterar el panorama competitivo.

No es sencillo asignar un valor monetario a la pérdida de información que se utiliza para fines maliciosos. ¿Cuánto le cuesta a una organización perder su ventaja competitiva debido al robo de códigos fuente o a la divulgación prematura de planes de fusión y adquisición? ¿Cuánto vale su marca? La pérdida de información de tarjetas de crédito de clientes conlleva el doble impacto de la sanción legal correspondiente y la pérdida de confianza por parte de los clientes. La información es un recurso de valor incalculable que debe protegerse.

Mejores prácticas para combatir las amenazas internas

Uno de los desafíos más grandes que los profesionales de TI enfrentan es la omnipresencia de las amenazas internas. Los empleados filtran información en forma verbal, física y a través de la red. Exhiben conductas que ponen en riesgo los datos empresariales por motivos técnicos, culturales, monetarios, requisitos laborales, personales y maliciosos. Esto es mucho terreno que cubrir y los profesionales de TI no lo pueden hacer solos. Prevenir la fuga de información es un desafío que incumbe a toda la empresa. Los profesionales de TI, ejecutivos y empleados de todos los niveles de responsabilidad deben trabajar en forma mancomunada para proteger los recursos de información críticos. Esto requiere una estrategia integral que abarque diferentes prácticas culturales y comerciales, y se centre en la educación y la responsabilidad.

- Fomente una cultura consciente de la seguridad en la que la protección de la información sea una parte normal y natural del trabajo de cada empleado, y no una tarea adicional percibida como una carga o en conflicto con otros objetivos.
- Proporcione las herramientas y la educación que los empleados necesitan para mantener la información segura, comenzando por la capacitación de empleados nuevos y luego mediante reforzamiento verbal en vez de por correos electrónicos que pueden perderse o ser ignorados.
- Evalúe la conducta de los empleados y los riesgos asociados basándose en factores tales como el país y el panorama de amenazas. Luego de acuerdo con dicha evaluación, diseñe planes de educación sobre amenazas, capacitación en seguridad y procesos comerciales.
- Analice continuamente los riesgos de cada interacción entre usuarios y redes, puntos terminales, aplicaciones, datos y, por supuesto, otros usuarios para siempre tener presente el entorno de amenazas.
- Formule, divulgue y haga cumplir políticas de seguridad sensatas. Simplifique el cumplimiento creando un número limitado de políticas de seguridad fáciles de comprender que estén integradas en los procesos comerciales y concuerden con los requisitos laborales.
- Proporcione un liderazgo claro mediante el compromiso y el ejemplo de la plana ejecutiva, para que los empleados vean que los ejecutivos están comprometidos y se hacen responsables.
- Fije expectativas en relación con la seguridad.

Cómo detener la fuga de información

Las culturas empresariales varían en distintas partes del mundo y no hay una sola forma correcta de proteger la información. Pero la amenaza interna es un problema generalizado con costosas consecuencias. Las amenazas internas deben enfrentarse con la misma energía que los ataques externos. Al igual que las amenazas externas, enfrentar la amenaza interna requiere una estrategia integral que incluye educación, políticas y tecnología. Las empresas que toman medidas adicionales para abordar los problemas inherentes a sus culturas empresariales propias y para comunicarse a nivel personal con los empleados estarán mejor posicionadas para establecer y poner en práctica estrategias de seguridad sostenibles.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Impreso en EE.UU. C11-506224-00 11/08