

e-penteo

Spam, malware y cibercrimen: impacto en la empresa.

Manuel Ángel Méndez, Analista Asociado. Penteo.

Atrás han quedado los años en los que la recuperación de desastres, la continuidad de negocio o el spam masivo eran los principales problemas de seguridad a combatir dentro de las organizaciones. Siguen siendo relevantes, pero menos. El 2010 marcó un punto de inflexión: el spam, *phishing* y fraude interno cayeron drásticamente en volumen y, con ellos, el impacto económico para las compañías. Las amenazas se han vuelto más sofisticadas y dispersas: malware en emails y redes sociales, vulnerabilidades de nuevos equipos y sistemas operativos, pérdida de portátiles, filtración de datos en aplicaciones web, fallos de sistemas alojados en modelos de cloud computing...

Si hace unas semanas hablábamos de seguridad en entornos móviles, hoy queremos profundizar un poco más en estos temas que cada vez son más críticos para el CIO.

Continuidad de negocio, recuperación de desastres, cumplimiento de regulaciones... ¿Recuerdan estas prioridades? Hasta hace poco eran las principales palancas del gasto en seguridad informática empresarial. Hoy siguen ahí, no han desaparecido, pero ya no suponen el principal foco de amenazas para las compañías. Hace cuatro años, por ejemplo, el 70% de organizaciones consideraba la recuperación de desastres y la continuidad de negocio como el principal componente de su presupuesto de seguridad. Hoy solo son el 40% de organizaciones.¹

¹ Fuente: 2011 Global state of Information Security, PwC.

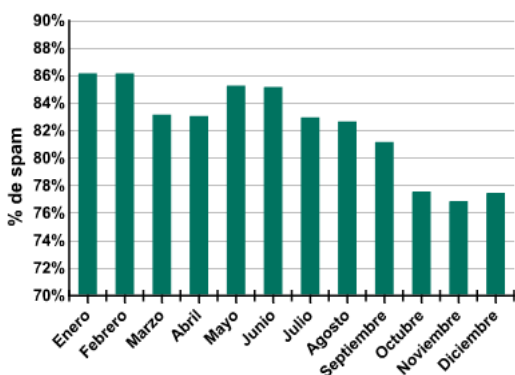
¿Qué ha cambiado? ¿Cuáles son las palancas del gasto corporativo en seguridad informática hoy en día? Tres palabras resaltan por encima de todas: **protección de datos**. La pérdida, filtración o robo de datos corporativos es ahora una de las amenazas que más pérdidas económicas causan a las empresas. Además, la evolución de los peligros tradicionales, como el spam y el phishing masivo, hacia nuevas tácticas y canales, hace que el panorama de seguridad sea hoy más complejo que nunca. Estas son algunas de las tendencias clave:

_Menos spam, más sofisticado. Es un hecho que todas las compañías de seguridad han constatado en los últimos meses: los niveles de spam se han reducido drásticamente en los últimos meses. Según Symantec el spam cayó un 55% en los cinco últimos meses; según Hispasec, un 75%. Kaspersky Labs apunta a que ha pasado de suponer un 86% del total de los correos electrónicos a un 78% a comienzos de año, uno de los niveles más bajos en mucho tiempo (ver Gráfico 1). El phishing, o la suplantación de la identidad de una empresa, alcanzó cotas mínimas: constituyó el 0,35% del total de mensajes de correo en 2010, según Kaspersky Labs.²

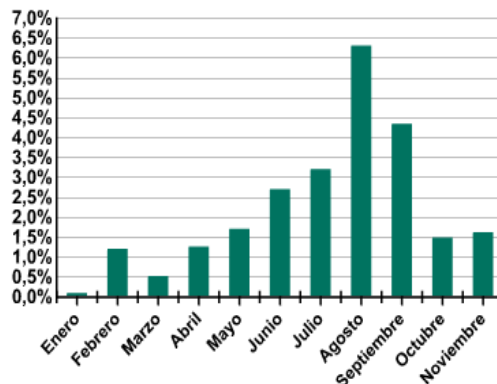
La explicación apunta a dos motivos fundamentales: **a)** el cierre de múltiples botnets en varios países, como la clausura del botnet Bredolab el pasado octubre, que según la policía holandesa contaba con 30 millones de equipos conectados en todo el mundo, y **b)** el desplazamiento del spam tradicional en el correo electrónico hacia nuevos canales de propagación como las redes sociales y móviles y el incremento de otras amenazas como el *malware*.

Para las compañías son buenas y malas noticias a la vez. Lo bueno: el coste asociado a la gestión del spam (menor productividad de empleados, renovación de soluciones anti-spam...) decrece. Lo malo: el spam no desaparece ni desaparecerá, sino que poco a poco abandona su carácter ‘masivo’ para pasar a ser más selectivo y eficaz utilizando nuevos canales de propagación. Por ejemplo, en el 2010 los ficheros maliciosos adjuntos a correos de spam estuvieron presentes en un 2,2% del total de mensajes, un nivel 2,6 veces superior al de 2009 (ver Gráfico 2).

G. 1: % de spam en el tráfico de correo, 2010



G. 2: % de spam con adjuntos maliciosos, 2010



_Malware, el problema continúa. Un reto más serio al que se enfrentan ahora las compañías es hacer frente a sofisticados programas de malware diseñados para sustraer información interna corporativa. En el 2010, la firma de seguridad Sophos

² Fuente: Kaspersky Security Bulletin, 2010.

analizó 95.000 diferentes programas de malware cada día, casi el doble que en 2009. Según uno de sus informes, un 40% de usuarios corporativos recibió mensajes con malware o se vio afectado por programas maliciosos en la Red.³

Gran parte de estos problemas se generan por el uso que los empleados hacen de Internet en el trabajo. El 59% de las empresas se muestran preocupados porque creen que el uso que los empleados hacen de las redes sociales en horas de trabajo puede suponer una seria amenaza de seguridad.⁴ Un 40% de compañías, según Cisco, ha decidido simplemente prohibir el acceso a redes sociales en el trabajo. España es un caso curioso: es uno de los países de Europa donde los empleados dedican más tiempo en horas de trabajo a utilizar redes sociales, 30 minutos. Eso sí, un tiempo que no necesariamente es empleado en redes de ocio.

En busca de datos corporativos, el nuevo cibercrimen. Es una de las tendencias que debería preocupar más a las empresas: los costes de la pérdida, robo o filtración de datos corporativos cuestan cada año más a las compañías. Symantec y Ponemon Institute señalan que la pérdida de datos corporativos costó una media de 7,2 millones de dólares a cada gran empresa en EE UU en el 2010, un 7% más que el año anterior.⁵ Es decir, unos 214 dólares por dato comprometido. En este coste se incluye todo: pérdida de negocio por clientes que se dan de baja a raíz del problema, costes legales (defensa, regulación), análisis de incidencias, auditoría, comunicación...

Entre las principales causas que explican la filtración de datos corporativos destacan la negligencia de los empleados (generalmente por desconocimiento, pero también intencionada), ataques internos o externos intencionados y fallos en los sistemas TIC de la empresa. Entre ellos, los ataques externos intencionados a través de malware son los que más rápido crecen y los más costosos para las organizaciones.

Hacia dónde evoluciona el cibercrimen corporativo

Si algo muestran los datos es que las amenazas tradicionales (spam y phishing masivos...) pierden fuerza y efectividad frente a una combinación de viejos peligros y nuevos canales: spam con adjuntos maliciosos, malware distribuido en redes sociales, phishing personalizado para contactos y empresas determinados, virus en dispositivos móviles (smartphones, tablets...).

Algunas de las nuevas amenazas que están empezando a afectar a las operaciones de las empresas son:

Filtrado de datos corporativos en redes sociales. Cada vez más cibercriminales utilizan las redes sociales para recabar información precisa sobre los perfiles e intereses concretos de empleados clave en una organización. Esta información se emplea para producir malware que reciben los empleados por email u otras vías con el fin de obtener datos confidenciales de la empresa o producir fraude financiero. Más del 80% de los responsables de seguridad de las compañías, según Deloitte, consideran estas técnicas de ingeniería social como muy peligrosas.⁶ Otros peligros asociados a la

³ Fuente: Sophos, Security threat report, 2010

⁴ Fuente: Cisco 2010 Annual Security Report

⁵ Fuente: 2010, Annual Study: US Cost of data breach. Symantec y Ponemon Institute.

⁶ Fuente: The future of security: evolve or die, 2011. Deloitte.

actividad de los empleados en redes sociales son el robo de identidad o el acceso a vulnerabilidades de red por parte de externos. El problema es que la gran mayoría de compañías, más de un 60% según PwC, no han tomado medidas concretas para protegerse de estas amenazas.

_Malware en nuevos equipos y sistemas. Windows, poco a poco, está dejando de ser el único canal de ataque utilizado por cibercriminales. A medida que la industria informática gira del PC hacia otros dispositivos (móviles, tabletas...) y software (aplicaciones web y sistemas operativos en crecimiento – iOS, Android, Windows Phone...), estos comienzan a ser el foco de ataques. Nuevamente, la tendencia ya no apunta a amenazas masivas sobre una plataforma mayoritaria como Windows, sino a ataques a usuarios y compañías concretas sobre nuevos equipos y sistemas.

_Cloud computing, ¿dónde están mis datos? Detrás del *boom* del cloud computing del que hablan los proveedores tecnológicos se esconden serios retos de seguridad informática que no pueden ser ignorados. ¿Dónde residen los datos?, ¿cuál es el nivel de encriptación de las comunicaciones?, ¿qué herramientas y procesos se utilizan en caso de filtrado de datos?, ¿qué empleados del proveedor tienen acceso a qué información en cada momento?, ¿qué tipo de auditorías se realizan para asegurar la integridad de los datos?... Todas estas preguntas, y su correspondiente reflejo en cláusulas contractuales, quedan sin responder en muchas de las propuestas actuales de cloud computing de los proveedores, tanto a nivel de aplicaciones como infraestructura.

Cómo reaccionar ante las nuevas amenazas

Casi cada año surgen nuevas amenazas de seguridad que ponen en peligro los datos y sistemas de las compañías. Ese es en realidad el objetivo de los cibercriminales: dar con vulnerabilidades no cubiertas y explotarlas en busca de retorno financiero. ¿Cómo evitarlo? Hay tres consejos clave, entre otros, que las empresas pueden seguir:

_Educar al empleado en entender los riesgos. La mayoría de las ocasiones en las que datos corporativos acaban en manos de cibercriminales se deben a negligencias internas no intencionadas: mal uso de passwords, irresponsabilidad en el uso de portátiles y móviles corporativos, abuso de redes sociales y webs de ocio en horas de trabajo... El porcentaje del presupuesto de seguridad TIC destinado a educar al empleado para evitar riesgos innecesarios es ínfimo, cuando no inexistente. Aspectos tan sencillos como establecer reglas en el uso de portátiles y móviles fuera de la oficina o formar al empleado en la gestión de su email, documentos adjuntos y uso de redes sociales puede evitar muchos dolores de cabeza.

_Revisar y actualizar políticas y tecnologías de protección. La estrategia de seguridad, el presupuesto y las herramientas de protección utilizadas en la empresa deben evolucionar al mismo ritmo que las amenazas. Todavía muchas empresas no tienen sólidos procesos de control de inventario de dispositivos (USBs, móviles, portátiles...) o seguros que protejan en caso de robo de datos o uso negligente de información corporativa que acabe en pérdida de negocio. Muchas tampoco utilizan tecnologías de encriptación de discos y equipos móviles, soluciones de prevención de pérdida de datos (DLP), software avanzado de gestión de identidades y acceso a la información o anti-malware. Actualizar periódicamente la estrategia y herramientas de seguridad es fundamental.

_El CIO debe estar a los mandos. Un signo preocupante para el CIO es que el responsable de seguridad informática, el llamado Chief Security Office (CSO) o directivo equivalente, ha ido progresivamente dejando de reportar al CIO para reportar a las unidades de negocio, bien el CEO, el CFO, el COO o el comité de dirección. Un dato: en el 2007, según PwC, el CSO reportaba al CIO en

casi el 40% de grandes compañías mundiales. Hoy esto solo ocurre en el 23% de las organizaciones. En la mayoría, casi el 70%, el CSO reporta al CEO o al comité de dirección.⁷ ¿Por qué? La seguridad de la información y los datos ha ido adquiriendo un componente cada vez más alineado con el negocio pero la figura del CIO no ha evolucionado a la misma velocidad. Una situación que el CIO no se puede permitir si quiere aspirar a un rol estratégico dentro de la organización.

Manuel Ángel Méndez es licenciado en Economía por la Universidad de Oviedo y cuenta con estudios en Microeconomía Avanzada en la London School of Economics y Economía Internacional en la Universidad de Maastricht (Holanda). Manuel posee amplia experiencia en asesoría y análisis tecnológico para grandes empresas en España y Reino Unido, habiendo dirigido durante 5 años el departamento Europeo de análisis de gasto tecnológico en Forrester Research en Londres. En la actualidad escribe para las secciones de tecnología de El País y Cinco Días y es analista asociado en Penteo ICT Analyst.

Penteo

Madrid
Velázquez 114
28006 Madrid

Barcelona
Córcega 282
08008 Barcelona

T.: +34 902 154 550
www.penteo.com

⁷ Fuente: 2011 Global state of Information Security, PwC.