El final de la inocencia: el estado global de la seguridad de la Información

Autor: Scott Berinato, Reach Executive Editor sberinato@cxo.com

http://www.csoonline.com/read/100107/fea_innocence.html

Traducción para Segu-Info: Alejandra Stolk y Fernando Spettoli

Revisión: Lic. Cristian Borghello, CISSP

Fecha Publicación: 23 de febrero de 2008

*Hace cinco años, cuando el CIO, CSO y PricewaterhouseCoopers realizaron en colaboración la primera encuesta de seguridad de información llamada **"El estado global de la seguridad de información"**, muy pocas personas sabían que tan grave era el problema. Ahora todos saben, sólo que no saben como arreglarlo.*

El conocimiento de la problemática de la naturaleza de la seguridad de información está alcanzando su nivel más alto. De cada de dólar gastado, aproximadamente 15 centavos van a seguridad. El personal de seguridad de información está siendo empleado a una tasa más rápida. Sin embargo, sorpresivamente, la seguridad empresarial no está mejorando.

Por quinto año consecutivo, CIO, CSO y PricewaterhouseCoopers (PWC) presentan los resultados y análisis de la encuesta "El estado global de la seguridad de información", la encuesta anual de seguridad de información más larga y completa.

La primera pregunta que hay que hacerse es: ¿Te sientes ansioso?

Te estás sintiendo inquieto por saber que no hay razón por la cual tu empresa podría ser la próxima TJX? ¿Sientes la angustia de saber que las plagas modernas - Los correos SPAM, las botnets y los rootkits — seguirán llegándote no importa cuánto esfuerzo y dinero se gasten tratando de frenarlas? ¿Sientes la piel de gallina que proviene de saber cuánto no conoces?

Si, lo estás sintiendo.

Lo estás sintiendo porque lo estás viendo. De acuerdo con los resultados de la encuesta en el 2007, una complejo conjunto de 7200 encuestados provenientes de 6 continentes indica que los problemas de seguridad de información se ven más claros que nunca. Estás viéndolos porque se han creado herramientas para ello. Por ejemplo:

Añadiste procesos. Hace tres años, sólo el 37% de las compañías reportaron una estrategia general en seguridad. Este año, el 57% lo hizo. También, prácticamente cuatro de cada cinco empresas realizaron un análisis de riesgo, al menos de periódicamente.

Has aplicado tecnología. Nueve de cada diez encuestados dijeron que utilizaban cortafuegos, monitorizan usuarios y mantienen una infraestructura de detección de intrusos. Este número se acercó al 98% cuando las respuestas se limitaron a empresas grandes (con beneficios mayores de un billón de dólares). El

cifrado está un su cima de todos los tiempos, con un 72% de uso en alguna de sus formas (comparado con 48% el año pasado).

Has contratado personal. El número de CISOs y CSOs (Jefe de seguridad de información y Oficiales de Seguridad) empleados continua en ascenso. El número de trabajadores de seguridad información por compañía ha llagado un tipo de 100, normalmente dado por un aumento en la tercerización y en el uso de empleados contratados.

Has desarrollado una infraestructura para el entendimiento. Lo estás viendo, y por eso lo estás sintiendo. Estás experimentando un cambio de un poco de ignorancia de las graves fallas en la seguridad informática a un gran deprimente conocimiento de ellas.

La conciencia puede estar en un máximo histórico, pero la conciencia no equivale a la mejora, y la conciencia no trae la felicidad. La triste realidad es que los avances realizados hasta la fecha no nos han hecho cruzar el umbral de ver los problemas a la reparación de los mismos.

"No hemos llegado al siguiente nivel de madurez," dice Mark Lobel, un director de PWC's en servicios de asesoría. "Nosotros tenemos la tecnología pero aún no tenemos nuestras manos en lo que es importante y en aquello que debemos estar monitorizando y protegiendo. Dónde está la herramienta capaz de decirnos: "Epa, los números de tarjetas de crédito están cruzando el cortafuegos" y ¿No es allí dónde está el asunto que realmente afecta el impacto real en nuestros negocios?"

Lee más sobre lo que la conciencia no has llevado y otras revelaciones en la encuesta: "El estado global de la seguridad de información 2007".

"Ya veo", dijo un hombre ciego.

Hace cinco años, 36 % de los encuestados en "El estado global de la seguridad de información" reportaron que no habían sufrido incidentes de seguridad. Este año, el número ha bajado a 22%.

¿Esto se debe a que han ocurrido más incidentes? Nosotros no lo pensamos así. Nosotros creemos que simplemente las empresas tienen hoy en día mayor conciencia de los incidentes que siempre han sufrido, pero hasta hace muy poco no tenían visibilidad. Esos inexplicables sucesos en los que cae la red hoy en día son conocidos por incidentes de seguridad. Posiblemente, una masiva cantidad de SPAM no era considerada un incidente de seguridad, pero ahora que este puede traer consigo malware, si lo es. La conciencia es mayor y por ello las empresas pasaron los últimos cinco años construyendo una infraestructura que les brinda mayor visibilidad en su postura de seguridad.

La infraestructura está en su lugar

El despliegue de personas, procesos y tecnología sigue aumentando de manera constante, a veces de manera dramática. Sin embargo, entre las empresas que aún no tienen estas tecnologías operando, la prioridad por añadirlas es realmente baja, indicando que muchas de las personas que creen que las necesitan ya las tienen.

	2006	2007	Prioridad para 2008
Gente: Tú tienes un...			
CSO	21%	28%	13%
CISO	22%	32%	17%
CPO	16%	22%	14%
Procesos: Tú tienes...			
Una estrategia general de seguridad	37%	57%	13%
Una línea base para clientes/ socios	25%	42%	10%
Sistemas de centralizados de identidades	34%	44%	11%
Tecnología: Tú tienes operando...			
Cortafuegos	77%	93%	15%
Cifrado	43%	72%	25%
IDS / Antivirus / otros detectores *	57%	90%	28%
Respaldo de datos	78%	82%	14%
Seguridad de usuarios / gestión de identidad *	73%	89%	33%
IPS/ filtros	44%	83%	22%
Seguridad de Internet *	31%	70%	14%

* Antes del 2007, estas categorías no estaban consolidadas. El porcentaje está listado en su máximo dado para una de las subcategorias que ahora conforman la nueva categoría.

Nosotros hemos visto al enemigo, eres tú.

Este año fue la primera vez en que los "empleados" le ganaron a los "hackers". Claro... en la pregunta de quien es probablemente la fuente de un incidente de seguridad. Los ejecutivos en el campo de la seguridad, con mayor visibilidad en los incidentes, son quienes más nombraron a los empleados como una fuente de incidentes.

Probables fuentes de incidentes

El reconocimiento del riesgo interno es un signo de que se ha elevado la conciencia, esto viene dado prácticamente por la gran cantidad de controles que se han puesto en los últimos cinco años.

¿Quien nos atacó?	2006	2007	2007 Sólo ejecutivos de seguridad
Empleado/ Ex-empleado	51%	69%	84%
Hacker	54%	41%	40%

¿Se han vuelto los empleados más maliciosos? ¿Están más de moda y son más productivos los trabajos internos de lo que eran antes? Probablemente no. La mayoría de los expertos en seguridad te dirán que los ataques internos son relativamente constantes y son usualmente más grandes y frecuentes de los que la víctima sospecha. Ninguno de nosotros quiere pensar que contratamos personal poco confiable.

Esta espina que asigna la responsabilidad de los ataques a los empleados, es probablemente la razón por la cual la empresas reportaban cero incidentes, una reflexión de conciencia que indica la habilidad de los gerentes por reconocer lo que siempre estuvo allí pero que previamente no podían determinar.

“Lo que está sucediendo es que estamos haciendo un mejor trabajo archivando y entendiendo situaciones,” dice Ron Woerner, un ex-gerente de seguridad de información de la empresa ConAgra Foods, el ingeniero de seguridad, ahora consultor de TD Ameritrade. “Por un tiempo, pienso, la ignorancia nos brindó felicidad. Ahora, con la tecnología en su lugar, nosotros nos estamos dando cuenta que tenemos los mismos problemas".

A continuación se muestra cómo la construcción de una infraestructura de seguridad puede llevar a determinar que más empleados sean nombrados como culpables de los incidentes de seguridad. Un CISO es contratado. Él tiene las herramientas para investigar las anomalías de la red interna y la autoridad para pedir a los dirigentes de la unidad de negocios que le proporcionen la información para una investigación.

Su despliegue de herramientas para el seguimiento de las actividades de los usuarios le ayuda a identificar las amenazas internas de abuso de información privilegiada. Después se centraliza la gestión de la información de seguridad de software que automáticamente detecta un comportamiento anómalo de red.

Entonces, tal vez se añade un proceso periódico de evaluación de riesgos (otra tendencia en aumento, de acuerdo a la encuesta) y de pronto se dá cuenta de que está encontrando vulnerabilidades desconocidas. Se agrega un servicio de denuncias anónimas de incidentes de seguridad a través de una dirección de correo o línea telefónica. Con todo esto y mucho más en su lugar, la empresa ha aumentado sus probabilidades de detección de incidentes de seguridad.

Pero tenemos una extraña paradoja. Sin importar la masiva construcción de gente, procesos y tecnología durante los últimos cinco años, y menos empresas reportando cero incidentes, 40% de los encuestados no sabían cuántos incidentes habían sufrido, lo que muestra un incremento pues el año pasado eran el 29%.

La tasa de "No sabe" para el tipo de incidente y el principal método utilizado para atacar también se aceleró.

Lo que usted no sabe… podrían llenar volúmenes

Yo Dunno (I don't know)

Cada vez más, los que participan en la seguridad de la información responden "No sé" cuando se le preguntó por el número y la naturaleza de los incidentes de seguridad.

	2006	2007	2007 CSO/CISO
Número de incidentes	29%	40%	29%
Tipo de ataque	26%	45%	32%
Método principalmente usado	26%	33%	20%

No augura nada bueno que después de años de la compra y la instalación de sistemas y procesos para mejorar la seguridad, cerca de la mitad de los encuestados no tienen una pista sobre lo que estaba pasando en sus propias empresas. Pero cuando cerca de una tercera parte de organizaciones de la sociedad civil y CISOs, quien, presumiblemente, debería tener la visión de la mayoría de los incidentes de seguridad, dice que no sabe cuántos incidentes que han sufrido o la forma en que estos se produjeron incidentes, eso es aún peor.

La verdad es que sistemas, procesos, herramientas, equipos y programas informáticos, e incluso el conocimiento y la comprensión de éstos sólo nos lleva hasta allí. Como Woerner dice, "cuando ganas visibilidad, te das cuenta que no se pueden ver todos los posibles problemas. Puede que veas que tal vez se gastó el dinero en asegurar las cosas que no eran. Ves que un buen empleado con buenas intenciones que quiere llevarse el trabajo a casa puede convertirse en un incidente de seguridad cuando pierde su computadora portátil o pone los datos en su ordenador personal. Hay tanto por ahí, que es abrumador."

Woerner y otros creen que la disciplina de la seguridad hasta ahora se ha concentrado en tecnología -cortafuegos, manejo de identidades, detección de intrusos- en lugar de análisis de riesgos y obtención dinámica de inteligencia.

Si la mayoría de las inversiones se han concentrado en tecnología, la mayoría del retorno proviene de allí también. Las herramientas realizan su trabajo. Ellas te dirán lo que está pasando y bloquearán la mayoría de los ataques bien conocidos y documentados. Pero la tecnología es en gran medida reactiva. Proporciona alarmas e informes de anomalías post ataque o comportamientos extraños.

En la detección de intrusos, por ejemplo, no es terriblemente eficaz una herramienta que necesita comprender la naturaleza de las vulnerabilidades antes de que afecten a usted. Todas las cajas de IDS lo que conocen son conjuntos de reglas y si éstas se han roto. Piense en un sensor de romper el vidrio de una ventana en un museo. Esta pieza de la tecnología es muy eficaz en una indicación de que alguien rompió la ventana, no hace nada para explicar cómo y por qué una pintura fue robada, ni puede ayudar a evitar que la próxima ventana de sea rota y las pinturas sigan siendo arrebatadas.

Además, incluso un rápido vistazo a las tendencias de seguridad demuestra que los adversarios, ya se trate de empleados descontentos o de los piratas informáticos, tienen instrumentos mucho más sofisticados de los que se han puesto en marcha para detenerlos. Técnicas antiforenses. La distribución masiva de malware a través de sitios web comprometidos. Botnets. Keyloggers. Las empresas pueden haber pasado los últimos cinco años con la construcción de su infraestructura de seguridad, pero también lo han hecho los chicos malos.

La conciencia incluye un nuevo nivel de comprensión de lo poco que sabemos acerca de cómo funcionan los chicos malos. Al igual que en las carreras armamentistas son "los malos" quienes llevan la delantera.

Porque tienes que cambiar de estrategia

¿Qué podemos hacer al respecto? La inversión en seguridad debe redirigirse de la gran carga en tecnología hacia la operación táctica, análisis de riesgo y la filosofía de mitigación.

Los ejecutivos de la información y seguridad, por ejemplo, deberán invertir en la investigación en materia de seguridad y el personal técnico que puede capturar y diseccionar malware, y deben ir a las profundidades de Internet para encontrar las últimas tendencias. Docenas de empresas de seguridad hacen esto precisamente y ofrecen sus suscripciones servicios de investigación.

"Tenemos que empezar a abordar el elemento humano de la seguridad de la información, no sólo el tecnológico", dice Woerner. Sólo entonces las empresas dejarán de ser las bolsas de golpear. Solo en ese momento podrán devolver a golpe.

IT ataca de nuevo

Hablando de volver, la encuesta de seguridad del 2007 muestra una tendencia que debemos remarcar (algunos hasta podrían decir que es problemática).

El departamento de IT quiere controlar la seguridad nuevamente.

En el primero año de participación en la encuesta (ver www.cio.com/article/29841), CIO, CSO y PWC notaron que mientras más segura se sentía una compañía en seguridad, menos probabilidades había de que el área de IT SEC le hubiera reportado al área de IT. Estas compañías además invirtieron más en seguridad.

La razón por la cual CIO's y CSO's siempre defendieron la separación de IT y de Seguridad es el clásico problema del zorro en la casa de la gallina. El inconveniente se da cuando el CIO controla, por ejemplo, un proyecto dedicado a la innovación del uso de IT y la seguridad del ese proyecto, lo que atrasaría al proyecto y encima le agregaría costos. Con esto se daría un serio conflicto de intereses. En la encuesta del 2003, un CISO dijo que el conflicto era demasiado grande para superarlo. Que le CISO tenga que reportar a IT, sería un fracaso.

Y cada año a partir de ese momento, la tendencia fue que la función de seguridad fuera ganando autonomía. Se fueron creando más posiciones ejecutivas en seguridad. El poder de toma de decisión se fue pasando al área de seguridad y

alejando de IT. Y más grupos en seguridad reportaron sus tareas a otras áreas distintas de IT, incluyendo el departamento de legales, el departamento de riesgos y el más significativo, el CEO. Esta tendencia es aún más pronunciada en las grandes compañías.

Pero en el 2007, esta tendencia no disminuyó, sino que se volteó por completo. Más aún, este cambio fue más pronunciado en las grandes compañías. Por ejemplo, los encuestados eligieron entre 12 posibles tareas que el CISO podría reportar. Esas 12 tareas fueron divididas en 3 categorías:

1. IT (CIO, CTO)

2. Neutral (Directorio, CEO, CFO, COO, legales)

3. Seguridad (auditoria, CPO, CSO, riesgos, comité de seguridad)

Para permitirles a los encuestados seleccionar más de una de éstas respuestas, se crearon las "compartidas" (porcentaje de los encuestados con alguna injerencia en el reporte a una de las 3 categorías).

Aquí están los resultados:

Reportando a IT

Los encuestados tienen alguna relación reportando a los siguientes grupos

	2006	2007	2007(>$1B Ingresos)
IT	41%	53%	60%
Neutral	76%	79%	68%
Security	44%	46%	48%

Un 12 % de crecimiento en el número de ejecutivos de seguridad reportando a IT es enormemente significativo. Y cuando se refiere a las grandes compañías, es un crecimiento de un 19%. Cabe destacar también que las grandes compañías muestran unos pocos ejecutivos en seguridad de la información reportando a posiciones neutrales.

M. Eric Johnson, un economista que se especializa en asuntos de seguridad de la información en la Universidad Dartmouth dice "De hecho, analizamos los organigramas, y las líneas sólidas de relaciones están volviendo a IT y al CIO. Los CISO's tienen en su mayoría relaciones de líneas punteadas, pero IT está dominando las estructuras de reporte y los presupuestos."

Más aún, la tendencia es más pronunciada cuando sigues la ruta del dinero.

Otra prueba de una función de seguridad evolucionada es en convergencia con la seguridad física, habitualmente bajo un CSO. Esto tiene sentido para la eficiencia operacional y porque las amenazas están convergiendo cada vez más. El control de acceso es un clásico ejemplo. Combinando los accesos al edificio y los accesos a la red en un único sistema, ahorras dinero, mejoras la eficiencia y creas una única visión ante ambas amenazas, la física (ingresos ilegítimos) y la digital (acceso ilegítimo a la red).

Y durante cuatro años, la convergencia de seguridad física y de IT se incrementó constantemente. Hasta éste año.

La Seguridad Física y de Información convergen, luego divergen.

Seguridad de la Información y Física, están separadas

	Porcentaje	Ingreso $1B o más
2003	71%	NA
2004	50%	NA
2005	47%	NA
2006	25%	36%
2007	46%	55%

Seguridad Física y de la Información, que reportan al mismo jefe ejecutivo

	Porcentaje	Ingresos $1B o más
2003	11%	NA
2004	26%	22%
2005	31%	24%
2006	40%	33%
2007	34%	27%

Encuestados que no integran la Seguridad Física con la de la Información: 69%

De éstos, el porcentaje de aquellos sin planes de integrarlas: 80%

¿Quién está a cargo?

Las señales de ejercer mayor control e influencia de IT están en todos los resultados de las encuestas. Por ejemplo, cuando se consultó que lineamientos de seguridad seguían las compañías, los encuestados, entre el 60% y hasta el 90%, respondieron seguir lineamientos como el ITIL, en vez de algunos específicos en seguridad como SAS 70 y varios estándares ISO de seguridad.

¿Qué está ocurriendo aquí? Johnson tiene una teoría: "Seguridad parece estar siguiendo una trayectoria similar a la de Quality hace 20 o 30 años atrás, sólo que con seguridad está ocurriendo mucho más rápido. Durante el momento de Quality, todos crearon VP's de Quality. Pero 10 años más tarde, la posición había desaparecido"

En ese caso, Johnson dice que se puede haber debido en parte a que la calidad pasó a estar arraigada, siendo un valor corporativo, y no necesitaba ser un área ejecutiva separada. Pero las evidencias en la encuesta sugieren que la seguridad no es ni arraigada ni valorada. Aún no es claro para las compañías donde

poner la seguridad, lo que explicaría las tantas cantidades de líneas punteadas en los organigramas.

Esto nos lleva a otra teoría: Políticas organizacionales. ¿Qué ocurriría si al separar Seguridad de IT, creasen controles en el desarrollo de software? (nada malo desde el punto de vista de la seguridad) Y ¿qué si la poca conciencia en seguridad que se muestra en la encuesta nos enseña el riesgo que existe en los típicos departamentos de IT con sus prácticas inseguras?

Una manera de responder para IT, sería tratar de socavar la seguridad. Mantener al enemigo cerca. Empujar la función de nuevo hacia donde puede ser mejor controlada.

"Lo que escucho de los CIO", dice Johnson, "es que al final del día, de cualquier manera ellos son los responsables por las fallas. Ellos están siempre implicados, esté la seguridad separada o no." Por qué no querría el CIO controlar algo por lo que es en última instancia responsable?

Por otro lado, quizás la seguridad nunca estuvo tan separada como pareció. Las compañías crearon las posiciones del tipo CISO, pero nunca le dieron autonomía. "Continuamente veo a la gente de seguridad en el papel del caído", dice Woerner de TD Ameritrade. "Quizás, en realidad esa separación fue subconscientemente, crear un grupo para recibir los golpes".

Woerner también cree que la tendencia de que el presupuesto de seguridad se maneje en el departamento de IT puede ser un resultado directo de auditar una seguridad que se enfoque principalmente en la infraestructura. Esto es, cuando los auditores buscan debilidades en la seguridad de la información, recomiendan parches tecnológicos. Y luego IT compra la tecnología necesaria para resolver el problema. Entonces, por qué debería IT cargar con los gastos de otro departamento?

Cualquiera fuera el motivo, la tendencia está molestando a algunos profesionales en seguridad, especialmente cuando están llevando adelante un rol más central en las crisis corporativas y en la sociedad en general.

El estado de la seguridad en Internet se está erosionando velozmente. La confianza en las transacciones online se está evaporando y requerirá de un fuerte liderazgo en seguridad para reconstruir dicha confianza. Para que Internet siga manteniendo el liderazgo en el comercio y en la productividad, se ha vuelto más necesario invertir en más seguridad.

Pero justo cuando las mejores y más brillantes mentes en seguridad se necesitan más, se los está valorando menos.

METHODOLOGY: The "Global State of Information Security 2007" survey, a worldwide study by CIO, CSO and PricewaterhouseCoopers, was conducted online from March 6, 2007, through May 4, 2007.

Readers of CIO and CSO and clients of PricewaterhouseCoopers from around the globe were invited via e-mail to take the survey. The results shown in this report are based on the responses of 7,200 CEOs, CFOs, CIOs, CSOs, VPs and directors of IT and IS, and security and IT professionals from more than 100 countries.

Thirty-six (33) percent of the respondents were from North America, followed by Europe (28%), Asia (23%), South America (12%) and the Middle East and South Africa (2%). The margin of error for this study is +/- 1%.

Reach Executive Editor *Scott Berinato* at sberinato@cxo.com.

Dated: October 01, 2007