The Institute of Internal Auditors

TONE at the TOP®

Edición 70 | Noviembre/Diciembre 2014

Proporcionando información concisa en asuntos de gobernabilidad a la alta dirección, consejos de administración y comités de auditoría.

Cyberseguridad: Están adentro. ¿Ahora qué?

Casi diariamente vemos reportajes en los noticieros sobre piratas informáticos o "hackers" quebrantando las seguridades de los servidores y robando información de grandes corporaciones. La mayoría de las compañías responden al ataque similarmente: Se anuncian planes a un público ya alarmado para rectificar la situación y protección de sus clientes.

Luego pasa otra vez, entrando en un ciclo vicioso de ataques y defensas, ataques y defensas; moviéndose de compañía en compañía (y algunas veces de vuelta) como un comprador en un "Viernes Negro" buscando el mejor descuento.

Pero la cruel realidad es que para varias organizaciones — tal vez la mayoría— ya no es un tema de cuándo romperán las seguridades de su sistema. Probablemente ya son víctimas de un ciberataque, sólo que aún no ha sido descubierto. El virus y otros programas fraudulentos pueden tener detonantes, plantados mucho antes de que las "bombas" exploten.

En un estudio realizado por Verizon Enterprise Solutions que reunió información de 50 organizaciones globales, los investigadores encontraron que para los cibercriminales solo les toma días para infiltrar los sistemas más sofisticados de defensa, pero pueden demorar meses en ser detectados. De la misma manera, MarketWatch recientemente reportó que una encuesta realizada por la firma de seguridad Trustwave encontró que, a las compañías les toma un promedio de 114 días detectar y contener un robo de información.

Claramente, algo se debe hacer para disminuir ese tiempo.

La pregunta es, ¿cuál es la mejor línea de defensa — u ofensa? El asesor legal de sólo un tercio de 1000 compañías de Fortune dice que ellos sienten que sus organizaciones están preparadas para prevenir un ciberataque significativo. Eso deja un tremendo espacio para que ocurra el desastre.

Las juntas directivas tienen la clave

"Por mucho tiempo se asumía que (entre la mayoría de juntas directivas corporativas y ejecutivas) el director de seguridad tenía todo a la mano" dijo Christopher Novak, gerente principal de respuesta investigativa en Verizon. "En el último año, hemos visto que quieran o no estar involucrados, miembros de la alta gerencia y de la junta directiva están siendo obligados a participar."

La encuesta de Seguridad y Privacidad de TI de Protiviti en el 2014 encontró que la participación de la Junta directiva es un punto diferenciador clave en la fortaleza de los perfiles de seguridad de TI. Aun así, menos del 15% de las respuestas de la encuesta el Pulso de la Profesión del 2014 del

Audit Executive Center del The Institute of Internal Auditors dijo que sus juntas directivas participaron activamente en la preparación de ciberseguridad.

¿Cómo pueden prepararse los miembros de la junta directiva para involucrarse? En primer lugar, entendiendo los múltiples enfoques que recomiendan los expertos para gestionar los riesgos cibernéticos. Estos incluyen: protección perimetral con monitoreo interno y un proceso (ya probado) para detectar intrusiones; cerrarlos rápidamente y la comunicación con las partes interesadas de manera oportuna y razonada.

"Puerta Principal" Medidas

Una buena primera línea de defensa incluye pruebas de infiltración controlada, en donde una organización paga a un consultor para que intente introducirse en los sistemas protegidos.

"Dominique Vicenti" directora ejecutiva de auditoría en Nordstrom llama a esto "construir un Fort Knox", pero es una estrategia de protección de perímetro que ella también advierte puede crear una falsa sensación de seguridad.

¿Por qué? Porque, mientras los administradores del riesgo están cuidando la puerta principal, los cibercriminales están furtivamente engañando a un empleado o inclusive a un ejecutivo para que les proporcione su clave— mediante un virus enviado por email, el cual es abierto sin darse cuenta del peligro oculto.

A través de deslices, en lugar de atacar las murallas es como frecuentemente los hackers pueden infiltrarse sin ser detectados, robando secretos comerciales, inteligencia de defensa o información de la cuenta del cliente, algunas veces por meses o años antes de ser capturados o que desaparezcan en el olvido.

Planes de respuesta rápida

Más allá de las vulnerabilidades que permiten una infiltración, "las empresas que son destrozadas ante el público son aquellas que no respondieron bien" una vez que los ladrones entraron, dijo Glyn Smith directora ejecutiva de auditoría en Sabre Holdings. Los expertos dicen que toda organización necesita un plan de respuesta documentado y ensayos regulares que son parte de una estrategia integral de gestión de crisis.

Para calmar las preocupaciones de la junta directiva, la gerencia debería presentar un plan que incluya los roles de los directivos.

Smith dice que es como una jugada de futbol, la que necesita ser entrenada a la perfección antes de que cualquier entrenador la considere aplicar en un juego real. "Si ellos nunca han practicado esa jugada, si el capitán nunca ha pasado la pelota en el calor de la batalla, no les va a ir muy bien," dijo Smith.

Comunicación y Colaboración

En adición a la comunicación "hacia abajo" y "hacia arriba" dentro de una organización, Novak recomienda que las organizaciones trabajen juntas en sus industrias para compartir información y proteger sus puntos débiles entre ellas.

"Si algún grupo está dirigiendo su ataque a una compañía en su industria, existe la posibilidad de que también estén dirigiendo ataques a su compañía," dice. Los hackers "trabajan juntos. Las organizaciones necesitan trabajar juntas para cerrar esa brecha entre el compromiso y la detección."

¿Ahora qué?

Un informe reciente realizado por The IIA Research Foundation e ISACA, titulado "Seguridad Cibernética: Lo que la Junta Directiva necesita preguntarse" citó un informe sobre los riesgos cibernéticos publicados por la National Association of Corporate Directors (NACD) en conjunto con American International Group (AIG) y la Internet Security Alliance (ISA). El NACD ofrece cinco principios de supervisión que los miembros de las juntas directivas corporativas deben realizar para mantenerse al tanto de las preocupaciones de seguridad cibernética y planificar un escudo protector superior. Estos principios son:

1 Trate la ciberseguridad como un tema de gestión de riesgos en toda la empresa, no solo una preocupación de TI.

2 Entienda las implicaciones legales de los riesgos cibernéticos y su relación con las potenciales vulnerabilidades de la compañía.

3 Pulse la experiencia de la organización en ciberseguridad y otorgue a los temas de gestión de riesgos cibernéticos el tiempo suficiente y regular en la agenda de la reunión de la junta directiva.

4 Fije la expectativa de que la gerencia establecerá un marco de gestión en toda la empresa, con suficiente dotación de personal y presupuesto.

5 Identifique los riesgos a evitar, aceptar, mitigar o transferir mediante seguros y asegure deliberaciones con la gerencia sobre planes específicos asociados con cada enfoque.

Una Lista de Preguntas para Directores

- ¿Cuándo fue nuestra última evaluación en ciber-vulnerabilidad?
- ¿Qué aprendimos de ella?
- Si estamos siendo atacados, ¿Cómo íbamos a saber?
- ¿Cómo reaccionaríamos?
- ¿Tenemos un plan de respuesta por escrito?
- ¿Esto incluye una estrategia de comunicación?
- ¿Hemos ensayado el plan como parte de nuestra gestión de crisis y actividades de respuesta?

Encuesta Rápida

1. Un ataque cibernético está en marcha. ¿Qué tan preparada está su organización para responder? (Escala de 1 a 5, siendo 1 "muy preparada" y 5 "nada preparada").
2. ¿Tiene su organización un equipo de respuesta rápida en el lugar para controlar los daños y remediación?

Visite **www.theiia.org/goto/quickpoll** para contestar las preguntas y ver cómo otros están respondiendo.

Cuidado con el Virus

¿Por qué romper, cuando tienes una llave o acceso a través de una puerta trasera abierta, o una ventana abierta? Los hackers han desarrollado carteristas electrónicos cualificados. Probablemente ya ha escuchado hablar de "phishing", un tipo de estafa que involucra un email falso que, en algunas formas, infecta los computadores de los empleados con un software malicioso que al presionar las teclas del teclado captura contraseñas.

Aquí están un par de ciberataques que probablemente no ha escuchado antes:

Ataque con Arpón: emails personalizados dirigidos para capturar contraseñas de ejecutivos. Basado en el supuesto de que los ejecutivos tienen altos permisos de seguridad, los hackers perfeccionarán sus mensajes de correo electrónico utilizando información obtenida de los perfiles de redes sociales, informes de prensa, y otras fuentes de acceso público para elaborar un correo electrónico que parece ser una comunicación legítima de alguna organización, o tema de interés de la víctima. Una vez que el email ha sido abierto, funciona como cualquier otro ataque de phishing.

Ataque de Agujeros: Ataques indirectos, en los que el virus auto instalable y spyware se colocan en sitios web con baja seguridad, tales como aquellos que sirven para servicios básicos, clubes de campo e iglesias, pero que son frecuentados por ejecutivos de compañías de alta seguridad. Nuevamente, el objetivo es tener acceso a la computadora de un ejecutivo - en este caso, al permanecer en espera en un servidor de baja seguridad hasta que el ejecutivo inicia sesión y sin saber instala programas de rastreo de presión en las teclas que le permitirá al hacker capturar contraseñas para información protegida.

Fuente: Christopher Novak, Verizon Enterprise Solutions

Sobre El IIA

El Instituto de Auditores Internos Inc. (IIA) es una asociación profesional mundial con 180.000 miembros en 190 países. El IIA sirve como defensor de la profesión de auditoría interna, pionero de las normas internacionales y principal investigador y educador. **www.globaliia.org**

Suscripciones a disposición

Visite **www.globaliia.org/Tone-at-the-Top** o llame al: +1-407-937-1111 para solicitar su suscripción gratuita.

Comentarios de los Lectores

Envíe sus preguntas / comentarios a **tone@theiia.org.**

Contenido del Consejo Consultivo

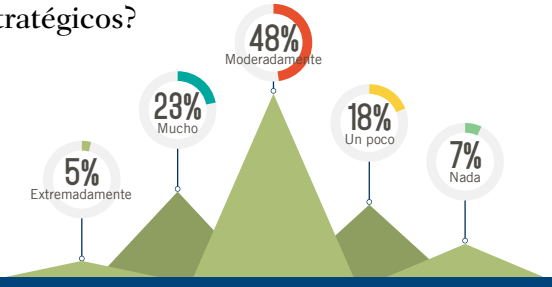
Con décadas de experiencia en la alta dirección y consejo de administración, los siguientes apreciados profesionales proporcionan orientación sobre el contenido de esta publicación:

Martin M. Coyne II
Michele J. Hooper
Nancy A. Eckl
Kenton J. Sicchitano

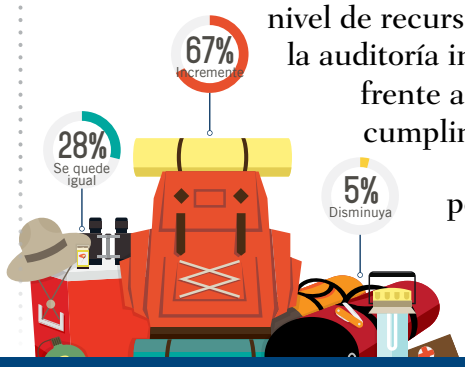
The Institute of Internal Auditors | TONE at the TOP®

Resultados de la Encuesta Rápida:

¿Qué tan seguro está usted de que su organización equilibra eficazmente las demandas de cumplimiento con otros riesgos estratégicos?



¿En los próximos 3 años, espera que el nivel de recursos requeridos por la auditoría interna para hacer frente a las exigencias de cumplimiento: aumente, disminuya o permanezca igual?



Basados en 352 respuestas. Fuente: The Institute of Internal Auditors Encuesta *Tone at the Top* Agosto/Septiembre 2014.

El presente documento fue traducido por el IIA ECUADOR el 28/11/2014.