Consejos de ciberseguridad para las empresas de hoy

¿Su organización está al día en su estrategia de seguridad? Aquí le ofrecemos algunos consejos de expertos para asegurar la información empresarial.

La ciberseguridad, ¿le ocupa o le preocupa?

Seguramente ha visto en internet, en redes sociales o en las noticias, informes que resumen el estado actual de la ciberseguridad a nivel mundial. Sin duda, los informes pueden ser muy valiosos en cuanto a cifras, casos y datos duros de la cada vez más compleja escena de ciberataques a nivel mundial; el problema es que hay tantas versiones, formatos y cifras incluidas en dichos documentos que, sin la guía adecuada o la interpretación correcta, la información puede ser sacada del contexto real y traducirse en miedo o paranoia.

Cualquiera que sea la motivación que usted tenga para leer un informe (prevención, morbo, actualización, et cetera) y por muy valiosa que sea la información que contenga, le adelanto que de nada sirven las cifras ni el tiempo invertido en su lectura si, como profesionales de seguridad, no nos damos a la tarea de entender dichas amenazas en el contexto de lo que se conoce como ”riesgo digital” y su impacto para las organizaciones.

Para bien o para mal la (in)seguridad digital es una moda que llegó para quedarse y muchos datos sobre la sofisticación de los ataques cibernéticos seguirán ganando titulares en la prensa. Si bien es cierto que el tema es importante y que el *malware*, por ejemplo, crece de forma exponencial, más aún a partir de la dependencia que cualquier organización tiene en la tecnología para poder operar en la actualidad, de nada sirve estresarnos con historias de terror ocurridas a otras empresas si antes no entendemos nuestros propios ambientes de operación y nos ocupamos en controlar las puertas y ventanas abiertas en el plano digital, identificar los riesgos y determinar el verdadero impacto que un incidente podría tener para nosotros.

Por ello, no debemos confundirnos (ni dejar que nos confundan) y hay que tener claro que cuando los reportes hablan de amenazas digitales se refieren a esas instancias, ya sean manuales (ataques/hackeo dirigido) o automatizadas (virus, gusanos,

algunos ataques de negación de servicio, et cetera) que tienen como objetivo vulnerar nuestra seguridad y que son desarrolladas por personas o grupos para obtener información, o a final de cuentas y por encima de todo, un beneficio económico. Ahora bien, hay que entender que para que las amenazas se traduzcan en un riesgo real dependen del éxito que tengan encontrando y aprovechando las vulnerabilidades o debilidades (como malas configuraciones, fallas en la protección, falta de parches o actualizaciones de seguridad, et cetera) en nuestros activos de TI.

Así que mientras un informe bien puede mencionar que las amenazas han crecido, nosotros debemos preguntarnos cosas como: *¿Cuál es el riesgo que esto tiene para mi organización? ¿Sabemos cuáles son nuestros puntos débiles? ¿Qué protección tenemos?*

CÓMO APROVECHAR LA INFORMACIÓN SIN CAER EN LA PARANOIA

Independientemente de lo que diga un informe, reporte o *whitepaper*, es clave que entendamos que NUNCA controlaremos nosotros la motivación de los atacantes ni la forma en que tratan de afectarnos (amenazas). Tristemente y como en cualquier sociedad es obvio que los criminales aumentarán a medida que la sociedad se vuelva más digital, mientras exista una falta de conciencia de los usuarios y también la (in)capacidad de las autoridades para perseguir estos delitos así que no invierta energía ni tiempo en tratar de entender las motivaciones de los atacantes sino más bien enfóquese en aquello que está bajo su control.

Que si las vulnerabilidades crecieron en un 300% o 500% para ciertas plataformas, sistemas o redes sociales ... el hecho es que el mundo está lleno de vulnerabilidades y se generan en proporción del incremento de usuarios, servicios y tecnología. Ocúpese entonces en entender su ambiente de operación y poner esas vulnerabilidades en contexto de su realidad para tomar las acciones pertinentes. Habrá algunas que resulten más importantes que otras para su ambiente.

Muchos informes se enfocan en el crecimiento de amenazas pero hablan poco del riesgo. En este sentido, para el lector es clave tener esto presente y comprender que es imposible reducir el riesgo al 100%, ya sea por razones operativas, humanas,

funcionales o tecnológicas así que dependiendo del grado de exposición y lo crítico de una situación se deberá asumir una postura ante el riesgo y determinar si es posible mitigarlo de alguna forma, evitarlo, transferirlo o aceptarlo. Si bien las cifras y datos de los reportes ayudan, la decisión debe basarse en el costo en tiempo o recursos que implique reducirlo vs. lo que puede costar no hacer nada. Siempre asegúrese de documentar el impacto que cualquier decisión tendrá en la rentabilidad y competitividad de su empresa.

Que si hackearon a Sony, Target, algún auto, et cetera ... Si bien los reportes incluyen ejemplos de compañías afectadas (y estoy seguro que la suya no quisiera aparecer en la lista), más que compararse con otros o sembrar miedo entre los directivos de su organización, aproveche los informes para conocer el entorno, explore la tecnología en el mercado y apóyese en su proveedor de seguridad. Es inaceptable que cualquier profesional o proveedor de servicios o tecnología de seguridad se justifique solamente usando a otros, hablando de amenazas o promoviendo tecnología de moda, sin antes entender quién es su organización, qué se debe proteger, y los riesgos que enfrenta lo que sin duda resultará en un planteamiento más profesional.

Con esta reflexión no pretendo minimizar la gran labor que hacen los investigadores para generar reportes que nos ayuden a entender la problemática de los ciberataques, sino más bien invitar a los profesionales a usar la información existente de forma responsable en nuestra labor.

Ocúpese de entender su ambiente de operación y poner las vulnerabilidades descubiertas en contexto con su realidad para tomar las acciones pertinentes.

Hace tiempo que soy detractor de las campañas de terror para generar conciencia en seguridad digital pues habiendo desarrollado funciones de ingeniería, consultoría, ventas y desarrollo de negocios en la industria de la seguridad estoy convencido que las historias de terror en los informes dejaron de ser efectivas sin un contexto adecuado y sin el análisis de cada caso.

Soy un fiel creyente de que a las personas se les activa a través de la motivación y no del estrés pero cuando leo y/o escucho aún a ciertos colegas en la industria usar datos de informes fatalistas o historias trágicas para generar ventas sin conocer a la organización en cuestión, lo respeto pero no lo comparto pues considero que, como profesionales de TI y responsables de proteger a nuestras organizaciones, debemos exigir más y mejor información de acuerdo a la naturaleza de lo que queremos proteger pero, sobre todo, asegurarnos de estar haciendo una correcta inversión de tiempo para conocer los riesgos que tenemos en casa y cómo mitigarlo. —*Gilberto Vicente*

Consideraciones para aplicar la seguridad ofensiva

La omnipresencia de los ataques cibernéticos hoy en día tiene a más empresas considerando seriamente una estrategia de seguridad ofensiva. Pero la definición fluida de ciberdefensa activa, las cuestiones éticas y jurídicas que la rodean, y una serie de otras variables tienen a muchos debatiendo sobre si tal respuesta es realmente práctica y eficaz para impedir a los piratas informáticos. Además, hay muchos riesgos asociados con tácticas ofensivas como el "hackeo reversivo", incluyendo posibles contraataques, daños colaterales y más.

Debido a los costos, las consecuencias y las incógnitas de la ciberseguridad ofensiva, los participantes del chat de gestión de riesgos #GRCChat de nuestra publicación hermana SearchCompliance estuvieron de acuerdo en que probablemente no debería ser considerada como una primera instancia, pero tiene su lugar en las empresas.

Los editores y seguidores de Twitter ofrecieron ejemplos de métodos eficaces de seguridad ofensiva, así como consejos sobre cómo las organizaciones deben evaluar su entorno antes de decidirse a practicar la ciberdefensa activa.

¿CUÁLES SON ALGUNOS EJEMPLOS DE CIBERDEFENSA ACTIVA EFICAZ?

Ben Cole, editor de *SearchCompliance,* señaló algunas formas de defensa activa que permiten una organización atraer a los atacantes en su red—con documentos ficticios, por ejemplo—y luego monitorear su actividad. Cole comentó que las estrategias de defensa activa incluyen registrar los movimientos de los hackers para evitar que éstos se beneficien de los datos robados.

Otra táctica que puede confundir a los piratas informáticos, de acuerdo con Cole y el usuario de Twitter Mark Underwood, es colocar los archivos *beacon* (archivos que fungen como una especie de

faro para llamar la atención de los atacantes) en lugares que les puedan interesar. Cuando los atacantes accedan a los archivos, activarán una alerta. "Engañe a los hackers para que roben una pieza específica de datos, usen un beacon, o faro, para registrar los datos y cómo son utilizados", comentó Cole.

Underwood agregó que los archivos de firma, o beacons, sirven para los hackers descuidados o en servidores que alojan grandes volúmenes de datos.

Además de los archivos señuelo, otras estrategias engañosas que pueden confundir atacantes incluyen la creación de tarros de miel (*honey pots*), o ambientes y sistemas falsos.

La editora senior Rachel Lebeaux señaló que algunas empresas contratan hackers para penetrar sus propios sistemas y redes para buscar vulnerabilidades, una práctica conocida como pen testing. Estas personas a veces se llaman hackers de sombrero blanco o hackers éticos. Underwood agregó que el pen test es subutilizado, generalmente; a lo que el usuario @Forvalaka41 coincidió y expresó que el pen testing tradicional se basa en la vieja escuela, carece de tecnología y buscan únicamente direcciones de red de la lista negra o fallos de firewall como causas probables.

Tal vez una de las razones de que las pruebas de penetración sean infrautilizadas es porque muchas empresas no destinan fondos suficientes para ello, según comentó Dave Shackleford, fundador y consultor principal de Voodoo Security a nuestro sitio hermano SearchSecurity. "Solamente quieren lograr que se haga, y ello deja muchas aberturas, por desgracia."

La evaluación de riesgos puede ayudar a decidir qué información es vulnerable y atractiva para los atacantes, así como a determinar dónde se necesita una defensa activa y hackeo reversivo.

¿Cómo pueden las empresas determinar de manera proactiva qué vulnerabilidades están mejor dirigidas?

Sería poco realista, por no hablar de casi imposible, que las organizaciones apliquen controles de

seguridad para todos los sistemas, procesos, datos o usuarios, que es donde las evaluaciones de riesgo entran en juego. Como ilustra Cole, estas evaluaciones no sólo arrojan luz sobre qué riesgos están asociados con qué sistemas, sino que también proporcionan orientación sobre la mejor forma de proteger esos activos.

"La evaluación de riesgos puede ayudar a decidir en dónde enfocar los recursos corporativos, pero se debe decidir qué información es vulnerable y atractiva para los atacantes. También puede ayudar a determinar qué tipo de vulnerabilidades de datos necesitan prevención temprana para una defensa activa y hackeo reversivo."

¿Otro aspecto clave de una evaluación eficaz del riesgo? Debe ofrecer una idea de hasta qué punto se verá afectada una organización, sobre si un sistema específico o activos de datos deben estar disponibles, tal como señaló el participante Dan Sanders.

El participante Forvalaka41 sugirió que las amenazas conocidas—las detectadas por la infraestructura de seguridad, en contraposición a las amenazas desconocidas, que se mostrarán como patrones anormales en los datos del sistema—no son buenos candidatos para un enfoque ciberdefensa activa, pues ya será tarde para un enfoque proactivo.

Forvlaka41 también cuestionó la efectividad en cuanto a costos sobre la búsqueda de ciberdefensa activa en comparación con la inversión en ingeniería de seguridad, el software y la construcción de sistemas con un menor número de vulnerabilidades: "Es difícil cuantificar el costo-beneficio; de manera similar al desarrollo de fuente abierta, los ajustes del kernel, et cetera"

Underwood, por su parte, señaló que así como muchos expertos en seguridad, los capitalistas de riesgo suelen ser recelosos de la ciberdefensa activa. Señaló el enfoque de seguridad adaptable de la nueva empresa de seguridad de Illumio como un ejemplo de que los inversionistas favorecen un método de seguridad menos ofensivo.

—Francesca Sales

Reporte de brechas y seguridad: mejores prácticas

He visto dos enfoques por separado, adoptados recientemente para la remediación de una violación de datos. Por un lado, el gerente general de Target al momento de la brecha fue muy franco y la compañía se comunicó activamente con los clientes afectados desde que se descubrió la infracción. Por otro lado, la CEO de Neiman Marcus, Karen Katz, esperó varios días para emitir una declaración pública después de que se confirmaron los rumores de una brecha en su empresa. En general, ¿cómo usted, como CISO, asesoraría a un director general respecto a manejar una brecha públicamente? ¿Hay algo que aprender de estos dos ejemplos?

Hay varios factores que contribuyen a la rapidez con la que una empresa puede reportar una violación de datos que hay que tener en cuenta al comparar estos dos incidentes. Las circunstancias de cada violación de datos son únicas, por lo que no es justo comparar o examinar las respuestas de una empresa sin el conocimiento de primera mano de cada incidente. Neiman Marcus pudo no haber tenido toda la información necesaria para salir al público, por ejemplo. La exactitud de lo que se informa al público es tan importante como la puntualidad del informe.

Puede llevar mucho tiempo identificar el punto de entrada y el número de registros o dispositivos que se han comprometido. Aplicar la ley puede requerir una demora en la notificación hasta que se tenga más información también sobre los autores.

La desafortunada realidad de hoy en día es que hay una buena probabilidad de que ocurra una brecha de datos. Es ingenuo para una organización operar con el modo de pensar que sus sistemas son impenetrables y de que todos sus datos están siempre completamente protegidos, porque es un entorno de riesgo en constante cambio. Las organizaciones mejor preparadas han aceptado esta nueva realidad y han desarrollado planes de

respuesta formales ante incidentes para cuando se produzca una violación de datos.

Un plan de respuesta a incidentes bien pensado es fundamental para la capacidad de una organización de navegar a través de todas las acciones requeridas durante un incidente de seguridad. El plan de respuesta a incidentes debe guiar a la organización a través de cada fase de la respuesta a una violación de datos, incluyendo el descubrimiento, la investigación, la mitigación, la comunicación y el procesamiento. Debe tener roles definidos para cada miembro del equipo de respuesta a incidentes, incluyendo la supervisión, las relaciones públicas, las finanzas y los equipos técnicos. Estos roles permitirán a la organización responder lo más rápido y preciso posible, dada la gran variedad de posibles incidentes de violación de datos.

Hay demasiados factores que juegan en la rapidez con que una organización comunica una violación de datos al público para hacer comparaciones entre las respuestas. Las organizaciones mejor preparadas utilizan un plan de respuesta a incidentes como su libro de jugadas durante una investigación de violación de datos. Prefiero juzgar a una organización por lo bien que su plan de respuesta a incidentes la ayudó a través del incidente que por el tiempo que toma para reportar el incidente. Las organizaciones que merecen un examen más detallado son las que están haciendo caso omiso de la realidad del entorno de las amenazas modernas y no cuentan con ningún plan de respuesta a incidentes. —*Joseph Granneman*

Varios factores determinan la rapidez con la que una empresa puede reportar una violación de datos. La exactitud de lo que se informa al público es tan importante como la puntualidad del informe.

Cinco pasos para asegurar los datos empresariales

El Día Internacional de la Protección de Datos tiene como objetivo sensibilizar a los consumidores y las empresas de la importancia de salvaguardar los datos, respetando la privacidad y creando confianza.

El 28 de enero fue elegido porque ese día, en 1981, el Consejo de Europa aprobó el Convenio 108 sobre la protección de los datos personales de los individuos, la raíz de toda la legislación sobre privacidad y protección de datos.

"De acuerdo con la Alianza Nacional para la Ciberseguridad, el 50% de los ataques cibernéticos dirigidos están apuntados a empresas con menos de 2,500 empleados" expresó Jennifer Burl, gerente senior de marketing de producto y soluciones de Iron Mountain.

Burl agregó que hay cinco pasos—desglosados a continuación—que las empresas pueden tomar para mantener los datos seguros y protegidos, y así evitar problemas legales y de reglamentación.

PASO 1: CONOZCA DÓNDE RESIDEN SUS DATOS

"No puede completar su plan de seguridad hasta que usted sepa exactamente lo que está protegiendo y dónde se almacena", dijo Burl.

La mayoría de las empresas almacenan datos en múltiples tipos de medios: discos locales, sistemas de respaldo basados en disco, en cintas fuera de las instalaciones y en la nube. Cada tecnología y formato requiere su propio tipo de protección.

PASO 2: PONGA EN PRÁCTICA UNA POLÍTICA DE "CONOCIMIENTO SEGÚN NECESIDAD"

Para minimizar el riesgo del error humano (o curiosidad), cree políticas que limiten el acceso a los conjuntos de datos particulares.

Designe el acceso basado en descripciones herméticas de puestos. También asegúrese de automatizar las entradas de acceso al registro para que

nadie que ha tenido acceso a un conjunto de datos en particular pase inadvertido.

PASO 3: REFUERCE LA SEGURIDAD DE SU RED

"Su red está casi seguramente protegida por un firewall y un software antivirus. Pero es necesario asegurarse de que esas herramientas están actualizadas y son lo suficientemente amplias como para hacer el trabajo", dijo Burl.

Diariamente se lanzan nuevas definiciones de malware, y el software antivirus tiene que seguirles el ritmo.

La filosofía de traiga su propio dispositivo está aquí para quedarse, y su equipo de TI debe extender su paraguas de seguridad sobre los teléfonos inteligentes y las tabletas que los empleados utilizan para fines de negocios.

PASO 4: MONITOREE E INFORME SOBRE EL CICLO DE VIDA DE SUS DATOS

Cree un plan de gestión del ciclo de vida de los datos para garantizar la destrucción segura de los datos antiguos y obsoletos de la empresa.

Como parte de este proceso, las empresas deben:

- Identificar los datos que debe proteger, y por cuánto tiempo;
- Construir una estrategia de respaldo múltiple que incluya respaldos en cinta fuera de línea y fuera de las instalaciones;
- Predecir las consecuencias de un ataque exitoso, luego resguardar las vulnerabilidades reveladas en este ejercicio;
- Tomar los archivos de papel en cuenta, ya que también pueden ser robados;
- Inventariar todo el hardware que podría albergar datos antiguos y disponer de forma segura de copiadoras, sistemas de correo de voz obsoletas e incluso viejas máquinas de fax.

PASO 5: EDUQUE A TODO EL MUNDO

"La seguridad de los datos se trata, en última instancia, de la gente", dijo Burl. "Cada empleado

debe entender los riesgos y consecuencias de las violaciones de datos y saber cómo prevenirlas, especialmente con el aumento de los ataques de ingeniería social".

"Hable con sus empleados acerca de las vulnerabilidades, como enlaces web de malware hábilmente disfrazados en mensajes de correo electrónico no solicitados. Anímelos a hablar si sus computadoras empiezan a funcionar de forma extraña".

Construya una cultura de seguridad en la cual todo el mundo entienda el valor crítico de sus datos de negocio y la necesidad de su protección. "Porque cuando se piensa en ello, todos los días son días de protección de datos", dijo Burl.

—Warwick Ashford

Seguridad de datos corporativos en apps móviles

Las aplicaciones móviles no pueden desempeñarse bien a menos que hayan sido construidas sobre una base sólida como una roca. Pero las medidas prácticas de seguridad para las aplicaciones móviles, tales como una buena gestión de dispositivos móviles y el cifrado de datos almacenados, pueden mitigar los riesgos de la entrega de aplicaciones móviles.

Después de todo, las aplicaciones móviles solo pueden ser tan seguras como la base sobre la cual están construidas: los dispositivos móviles y los sistemas operativos en los que se ejecutan. Así que es imperativo entender los riesgos inherentes asociados con los dispositivos móviles, las medidas de seguridad nativas integras en los sistemas operativos móviles y las mejores prácticas para mitigar los riesgos de seguridad de las aplicaciones móviles.

Los *smartphones* y tabletas perdidos o robados suponen un riesgo significativo. El robo de teléfonos está creciendo, y representó el 14% de los principales crímenes en la ciudad de Nueva York el año pasado, así como 38% de los robos en Washington, D.C. Las empresas están en lo correcto al estar preocupadas, ya que el análisis forense de los dispositivos revendidos puede generalmente recuperar algunos de los datos del usuario anterior. Si no se aplica ninguna seguridad, un dispositivo perdido o robado puede llevar fácilmente a una brecha en los datos de negocios almacenados, que incluyen mensajes de correo electrónico, contactos, registros de los clientes, contraseñas y más.

Más aún, los dispositivos móviles perdidos permiten la intrusión a redes y servicios corporativos. Un *smartphone* configurado con acceso al correo electrónico corporativo, Wi-Fi o red privada virtual, puede ser una puerta trasera abierta hacia sistemas de otro modo seguros, evitando la seguridad del perímetro. Si bien lo mismo puede decirse

de las laptops, los usuarios pierden *smartphones* y tabletas mucho más seguido. Casi siempre contienen contraseñas guardadas, y es menos probable que verifiquen la identidad del usuario con una autenticación de dos factores.

Estos riesgos en la seguridad de las aplicaciones móviles y la red están exacerbados por el malware móvil. De acuerdo con Nielsen, el *smartphone* promedio en los Estados Unidos tiene 41 aplicaciones descargadas por el usuario. Si bien la mayoría de aplicaciones viene de sitios de buena reputación, como la App Store de Apple o la Play Store de Google, el malware móvil está creciendo rápidamente, especialmente para el sistema operativo de fuente abierta Android. Incluso apps legítimas muchas veces tienen acceso a datos sensibles y servicios tales como contactos y ubicación. Un dispositivo ejecutando una app maliciosa o demasiado inquisitiva, combinada con acceso a datos, redes o servicios corporativos, supone un gran riesgo de negocios.

De hecho, el malware se extiende explotando vulnerabilidades del sistema operativo móvil y las aplicaciones. Los ecosistemas móviles están muy por detrás de la infraestructura establecida de parches para los sistemas de escritorio y laptops. Cuando los escritores de parches encuentran un nuevo bug de Android para explotar, una forma de arreglarlo debe ir a través de Google, luego a través de los fabricantes de dispositivos y luego a través de los operadores de redes celulares antes de ser ofrecida a los usuarios móviles. Como resultado, el área de TI en la empresa tiene poca visión hacia dentro y ningún control efectivo sobre la gestión de vulnerabilidad en la seguridad de las aplicaciones móviles.

Finalmente, quizás el mayor riesgo de todos es la mano humana que sostiene un teléfono inteligente o tableta. Los usuarios finales a menudo ignoran actualizaciones sugeridas, advertencias de permisos y avisos de contraseñas. De acuerdo con la Corporación de Defensa de la Información, 71% de los directores de seguridad dijeron que los dispositivos móviles han contribuido a los incidentes en seguridad, generalmente debido al descuido de empleados que carecen de conciencia de seguridad. El comportamiento del usuario supone un riesgo incluso mayor dada la tendencia poco asegurada y de uso mixto de traer sus propios dispositivos.

—Lisa Phifer

Siete consejos de seguridad para las empresas

Las amenazas de seguridad a empresas han aumentado exponencialmente en tamaño, alcance y sofisticación. En una época en que la computación en la nube, el movimiento BYOD (Bring Your Own Device) y los medios sociales están cambiando las reglas del juego para las empresas, se han intensificado los desafíos en términos de seguridad para directores de TI (CIO) y directores de seguridad (CSO) como nunca antes. La seguridad tradicional actual ha probado ser ineficiente frente al avance y la persistencia de ataques a redes corporativas por medio de internet, que van desde robo de datos, hasta ataques para robo de contraseñas, violación de datos y ataques cuidadosamente planificados de 'negación de servicio'.

La información de seguridad en dicho tipo de entornos requiere una estrategia de seguridad integrada y alineada con el negocio, con el objetivo de construir una base sólida para obtener una postura de seguridad sólida. Un abordaje proactivo, en términos de seguridad, está en la habilidad de la organización para mitigar efectivamente los riesgos futuros de su entorno.

Aunque ninguna organización está inmune a ataques, estos son algunos consejos que podrían seguir para protegerse mejor:

1. Desarrollar una estrategia de seguridad completa: Una estrategia de seguridad exhaustiva debe alinear objetivos de seguridad y medidas con estrategias empresariales y metas. Dicho abordaje disminuye los costos totales, proporcionando a los técnicos, ingenieros y profesionales de seguridad una hoja de ruta que guíe las operaciones críticas.

2. Establecer la mentalidad de que la seguridad debe ser prioridad: Mantener capacidades superiores de monitoreo de seguridad, conciencia y generación de informes de seguridad dentro de un marco de seguridad cibernética holística, para

proteger los datos empresariales y las redes de amenazas internas y externas. Se trata de una visión operativa común y en tiempo real a través de todos los aspectos de las operaciones de seguridad, que permitirán que las organizaciones implementen y lleven a cabo acciones de seguridad de TI que proteja la información.

3. Implementar análisis de datos para proteger información confidencial: Esto es esencial para reconocer la realidad del volumen de datos que necesitan protección y establecer maneras automatizadas para analizar y monitorear grandes volúmenes de datos.

4. Gestionar identidades y autorizaciones: Administrar de manera centralizada la identidad digital de los usuarios y las autorizaciones para proporcionar el más alto nivel de garantía de identidad y reducir errores críticos de los empleados con mensajes continuos e implementación de políticas.

5. Aprovechar las capacidades integradas de los dispositivos móviles: Dispositivos móviles como teléfonos inteligentes y tabletas permiten autenticación avanzada por medio de técnicas biométricas de reconocimiento de voz, firma y reconocimiento facial. Las organizaciones pueden usar estas tecnologías emergentes para avanzar a la par con las preferencias del cliente, garantizando al mismo tiempo los más altos niveles de protección.

6. Evaluación y reevaluación continua: El monitoreo y la evaluación continua deben ser parte integral del programa de seguridad empresarial. Es esencial llevar a cabo evaluaciones de riesgos, ejecutando escaneos de vulnerabilidad periódicamente y programando auditorías para obtener visibilidad continua de las brechas de seguridad y de las actividades de remediación.

7. Aislar y ocultar dispositivos terminales: Al garantizar los sistemas de toda la empresa, se reduce el riesgo de vulnerabilidad, previniendo que se propaguen por la red y la empresa. Las comunidades de interés basadas en software proporcionan una manera ágil, simple y rentable de proteger comunicaciones de datos de misión crítica en terminales que sean invisibles a todos, excepto para aquellos a los que se han pre identificado como parte de una 'comunidad segura'.— *Francisco Farrera*

WARWICK ASHFORD *es editor de seguridad en Computer Weekly. Llegó al periodismo de TI después de tres años como desarrollador de cursos y escritor técnico para una organización de capacitación en TI.*

FRANCISCO FARRERA *es director de servicios profesionales para la unidad de negocio de consultoría tecnológica y soluciones de integración (TCIS) en Unisys México.*

JOSEPH GRANNEMAN *es experto en gestión de seguridad de la información de SearchSecurity. Tiene más de 20 años de experiencia en tecnología, principalmente enfocado en tecnologías de la información para el sector salud.*

LISA PHIFER *es dueña de Core Competence, firma de consultoría especializada en el uso seguro de las tecnologías emergentes con enfoque en la seguridad móvil, de redes y software.*

FRANCESCA SALES *es editor para los sitios SearchCIO y SearchCompliance. Durante sus estudios universitarios fue colaboradora del The Huntington News.*

GILBERTO VICENTE *es profesional de TI y seguridad informática con más de 15 años de experiencia, con un fuerte enfoque en la promoción de tecnologías y desarrollo de negocios para los mercados de México y América Latina.*

TechTarget

Consejos de ciberseguridad para las empresas de hoy
es una publicación de SearchDataCenter.Es

Rich Castagna | *Vicepresidente editorial*

Lizzette Pérez Arbesú | *Editora ejecutiva*

Melisa Osores | *Editora adjunta*

Linda Koury | *Director de diseño online*

Anita Koury | *Diseñador gráfico*

Joseph Hebert | *Editor de producción*

Bill Crowley | *Publisher*
BCrowley@techtarget.com

TechTarget
275 Grove Street, Newton, MA 02466
www.techtarget.com

Acerca de TechTarget: TechTarget publica contenidos para profesionales de tecnología de información. Más de 100 sitios web focalizados permiten un rápido acceso a un vasto repositorio de noticias, consejos y análisis sobre tecnologías, productos y procesos cruciales para su trabajo. Nuestros eventos virtuales y presenciales le proporcionan acceso directo a los comentarios y consejos de expertos independientes. A través de IT Knowledge Exchange, nuestra comunidad social, usted puede obtener asesoría y compartir soluciones con colegas y expertos.

COVER ART: FOTOLIA