Magazcitum

El magazine para los profesionales de la seguridad de TI

Los dispositivos móviles llegaron para quedarse

Buffer overflow (primera parte)

El reto de hoy: una cultura de cambios (Change Management)

Teléfonos inteligentes

Lo que estamos perdiendo de vista

AÑO 3, NÚMERO 2
ABR.-JUN. 2012
EJEMPLAR GRATUITO

http://gettag.mobi

Escanea este código con tu teléfono móvil o smartphone

FORTINET

Aquí paran las amenazas.

Cada día, Fortinet protege las redes de muchas de las más grandes y exitosas organizaciones en el mundo. Proporcionamos una protección completa de contenido para bloquear las amenazas ocultas. Nuestras tecnologías consolidadas combinan aplicaciones de control con políticas de bases de identidad. Aprenda cómo incrementar la seguridad, mejorar el rendimiento y la productividad con menores costos.

Servicios de Salud
Gobierno & Defensa
Educación

SEGURIDAD MULTI-AMENAZA

Proveedores de Seguridad
Servicios Financieros
Retail
Servicios Públicos

Visite www.fortinet.com para conocer cómo proteger su red hoy.

FORTINET

Protección de la Red en Tiempo Real

www.fortinet.com

FTNT NASDAQ LISTED

GRUPO DICE® TELECOMUNICACIONES

Roberto Corvera | Channel Account Manager | Fortinet
Office: +52 (55) 5524.8428 | Mobile: +(155) 1850.8154
Email: rcorvera@fortinet.com | Skype: roberto.corvera

AÑO 3, NÚMERO 2 ABRIL - JUNIO 2012

Magazcitum, revista trimestral de Scitum S.A. de C.V. Año 3, número 2, abril-junio de 2012. Editor responsable: Héctor Acevedo. Número de Certificado de Reserva otorgado por el Instituto de Derechos de Autor: 04-2010-071512010500-102. Número de certificado de Licitud de Título y Contenido: 14900, Exp.: CCPRI/3/TC/10/18827. Domicilio de la Publicación: Av. Paseo de la Reforma 373 piso 7, Col. Cuauhtémoc, delegación Cuauhtémoc, México DF 06500. Impreso en : Rouge & 21 S.A. de C.V. Av. Rómulo O'Farril # 520 int 5 Col. Olivar de los Padres México DF. Distribuida por Editorial Mexicana de Impresos y Revistas S.A. de C.V: Oaxaca 86-402 Col. Roma México DF. Magazcitum, revista especializada en temas de seguridad de la información para los profesionales del medio. Circula de manera controlada y gratuita entre los profesionales de la seguridad de la información. Tiene un tiraje de 5,000 ejemplares trimestrales.

Para cualquier asunto relacionado con esta publicación, favor de dirigirse a **contacto@magazcitum.com.mx**

contenido

8

» editorial

4

» opinión

5

» misión: crítica

20

misión: crítica

» conexiones

28

Los dispositivos móviles llegaron para quedarse

Héctor Acevedo
CISSP, CISA, CGEIT, ITIL y MCSE
hacevedoj@scitum.com.mx

En medio de las crisis y recesión de muchos países, el cómputo en la nube sigue ganando terreno, con todo que, como hemos mencionado constantemente, impone una serie de retos para lograr la operación de TI y la seguridad de la información.

Aunado a lo anterior resalta el hecho de que la venta de dispositivos móviles no se detiene, confirmando así las predicciones de los analistas. Día a día se agregan nuevos teléfonos inteligentes y tablets a la larga lista de equipos que requieren acceso a los datos personales y aplicaciones empresariales. Aunque llevamos varios años lidiando con el dilema de qué hacer con los dispositivos móviles comprados por los usuarios, hemos llegado al punto en que ya no es posible postergar el análisis y hay que tomar una posición al respecto. Conceptos como BYOD (*Bring Your Own Device*, "trae tu propio dispositivo") están en boca de todos y traen nuevos retos, cada vez más complejos, para lograr el equilibrio entre la facilidad de uso, la explotación de dichos dispositivos y una adecuada administración de la seguridad de la información.

Así pues, en esta edición de **Magazcitum** encontrarán una mezcla de artículos que hablan sobre los retos del cómputo en la nube y los dispositivos móviles, esperamos sean de su agrado.

Nuevamente agradezco sus visitas y comentarios en el sitio Web de la revista (**www.magazcitum.com.mx**), siempre es un placer saber qué opinan de los temas tratados por nuestros colaboradores.

Como siempre, muchas gracias por su atenta lectura.

Héctor Acevedo Juárez

Protegiendo y protegiéndonos de la computadora de mi abuelita

Omar Alcalá
CISSP, ISO-27001 y CCNA
oalcala@scitum.com.mx

La seguridad informática de hoy es muy diferente a la del año 2000. A principios del nuevo milenio, las fronteras que existían en las organizaciones estaban muy bien delimitadas, los datos eran trasladados en discos de 3½", CD y algunos incluso tenían quemadores de DVD; la mayoría los celulares eran equipos solo para llamadas telefónicas y mensajes de texto; un "ladrillo" llamado *BlackBerry* iniciaba su auge como oficina remota y las conexiones típicas en las casas eran de 256 Kbps con un incipiente y caro *DSL* asimétrico.

El panorama a once años del cambio de milenio, tomando el inicio en 2001, se ha transformado totalmente. Los seres humanos vivimos en una era diferente donde los datos viajan a velocidades cincuenta veces más rápido, se almacenan en cantidades impensables en la época del error *Y2K* y, sobre todo, en dispositivos más y más pequeños.

El exceso de información con el que vivimos hace que cualquier equipo en la red "deba" por defecto tener algún tipo de acceso a Internet y hoy es inimaginable una compañía que no tenga un servicio, propaganda o flujo de comunicación que viaje a través de redes públicas o privadas. Por otro lado, las computadoras caseras están conectadas a Internet desde el mismo momento en que son encendidas, algo comprensible para los que nos dedicamos a esta profesión pero muchas veces pasado por alto por la mayoría de la población.

Y todo esto, ¿qué tiene que ver con el título que ofrezco al lector? Mi objetivo inicial es sensibilizar en cómo ha cambiado el punto de vista de ubicación de la información y conectividad. Hace 10 años, era estática y con dificultad para moverse. Hoy la información viaja entre redes públicas y privadas, dispositivos y redes celulares con poco control. Mi artículo anterior versó sobre *DLP* y no es la intención en este de entrar en detalles respecto a la solución; ahora el foco es recalcar que las amenazas provienen de donde sea, lo cual brinda amplia ventaja a los atacantes.

Los ataques en los que quiero hacer hincapié son aquellos en los que se usan equipos personales "de quien sea" (literalmente hablando). Mucha gente ha oído hablar de los equipos zombies o las famosas botnets, sin embargo parece que en la industria se piensa en las *botnets/zombies* como equipos que se ubican en otra red y nunca se consideran en el equipo que está DENTRO de la red propia, pero lo cierto es que cualquiera, incluso "el equipo de mi abuelita", es susceptible de sufrir ataques que tomen el control de equipos personales, teléfonos inteligentes, etcétera.

Los ataques *APT* (*advanced persistent threat*) son sofisticados, perpetrados por gente experta y con un objetivo perfectamente identificado. Saben dónde atacar, por cuánto tiempo y son hábiles eliminando prácticamente cualquier traza que denote su "visita". Los equipos *zombies* o *botnets* son herramientas básicas para sus ataques a equipos estratégicos en las organizaciones.

Considero que la protección del equipo de cómputo personal es el área más difícil de asegurar y a la vez el punto más descuidado de cualquier infraestructura. Esto obedece a que el factor humano es el siguiente eslabón en la interacción, y es donde suele romperse la cadena de seguridad. Es probable que la mayoría de la gente implemente un antivirus como la única protección, o al menos la mejor, para las computadoras personales, lo cual dista mucho de la realidad.

Muchas instituciones, sobre todo las gubernamentales, piensan que la seguridad es un tema perimetral, pero bien sabemos que dentro de cada organización hay gente que requiere accesos especiales y por ello los dispositivos de seguridad como *firewalls* e IPS les permiten acceso privilegiado. Las posibilidades para un incidente de seguridad son infinitas: ¿Qué información puede capturar un equipo que recibe pagos de proveedores? ¿Qué nivel de criticidad puede tener una *laptop* con permisos para accesos a sistemas *SCADA*? ¿Cuánta información "sabe" la computadora de la asistente del *CEO* de cualquier compañía? Y solo la asistente, ¿cuánta información se mueve entre los diferentes dispositivos de los altos ejecutivos (los llamados nivel-C)?

En otras ocasiones he mencionado que muchos ataques no tienen por objetivo vulnerar sistemas de protección como *firewalls*, *IPS*, filtrado de contenido o *VPN* ¿Qué mejor que inducir al usuario a que "coopere" voluntaria o involuntariamente con la instalación de un pequeño programa que permita el control remoto de su equipo o que sea su equipo el que envíe la información necesaria para perpetrar un ataque mayor: contraseñas, navegación, acceso remoto, denegación de servicios, esa hoja de cálculo con información confidencial, etcétera?

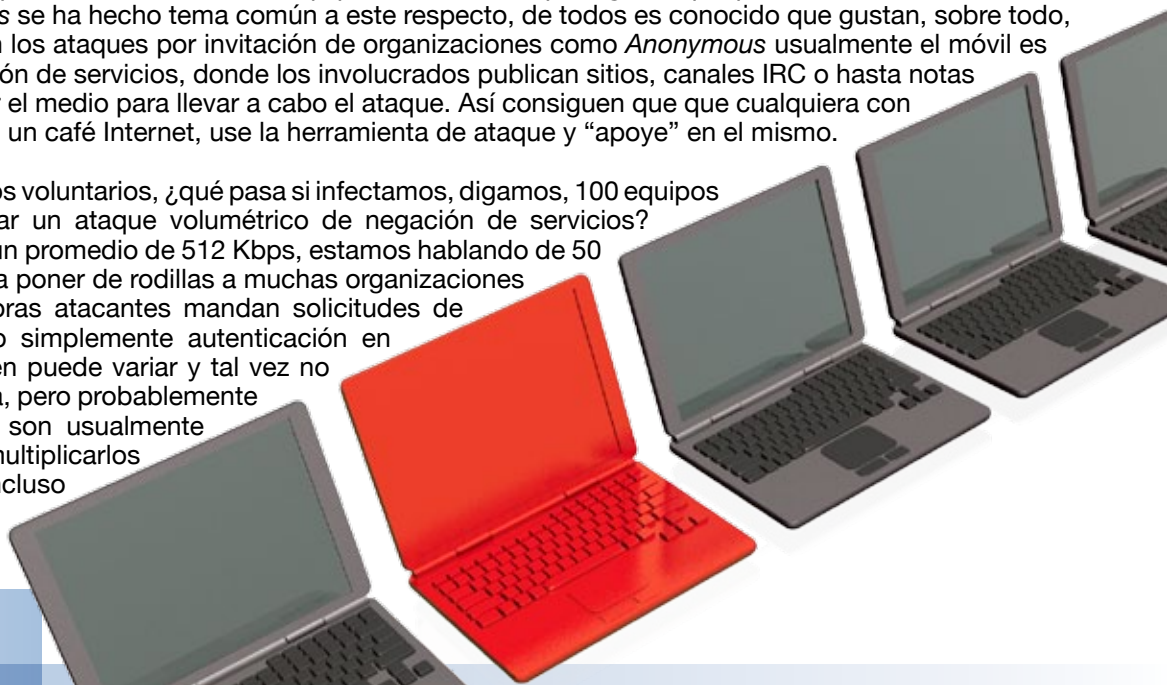
Peor todavía es común en el ámbito de seguridad generar políticas "permisivas" para usuarios VIP, y es exactamente este tipo de usuarios los que son objetivos frecuentes cuando de ataques persistentes se trata. Al parecer las políticas de seguridad no se alinean con la criticidad de la información que pretenden proteger.

Todo tiene sentido con la estadística que conocemos: 70% o más de los ataques provienen desde dentro de nuestras redes. Hoy más que nunca nuestras estaciones de trabajo se vuelven contra nosotros. No podemos considerar la seguridad completa si no tomamos a las estaciones de trabajo como equipos a proteger y creemos que un *firewall* y un *IPS* solucionarán todas las necesidades de seguridad de la organización.

DDoS y la computadora de la abuelita

Con la negación de servicios distribuida (DDoS) el panorama es diferente pues normalmente los ataques vienen de fuera y los atacantes tienen a su disposición cada vez más equipos caseros mal protegidos que pueden usar como *zombies* para atacar a otros. *Anonymous* se ha hecho tema común a este respecto, de todos es conocido que gustan, sobre todo, de la negación de servicios. En los ataques por invitación de organizaciones como *Anonymous* usualmente el móvil es *hacktivismo* orientado a negación de servicios, donde los involucrados publican sitios, canales IRC o hasta notas en *Facebook* que invitan a usar el medio para llevar a cabo el ataque. Así consiguen que que cualquiera con una conexión *DSL* o incluso en un café Internet, use la herramienta de ataque y "apoye" en el mismo.

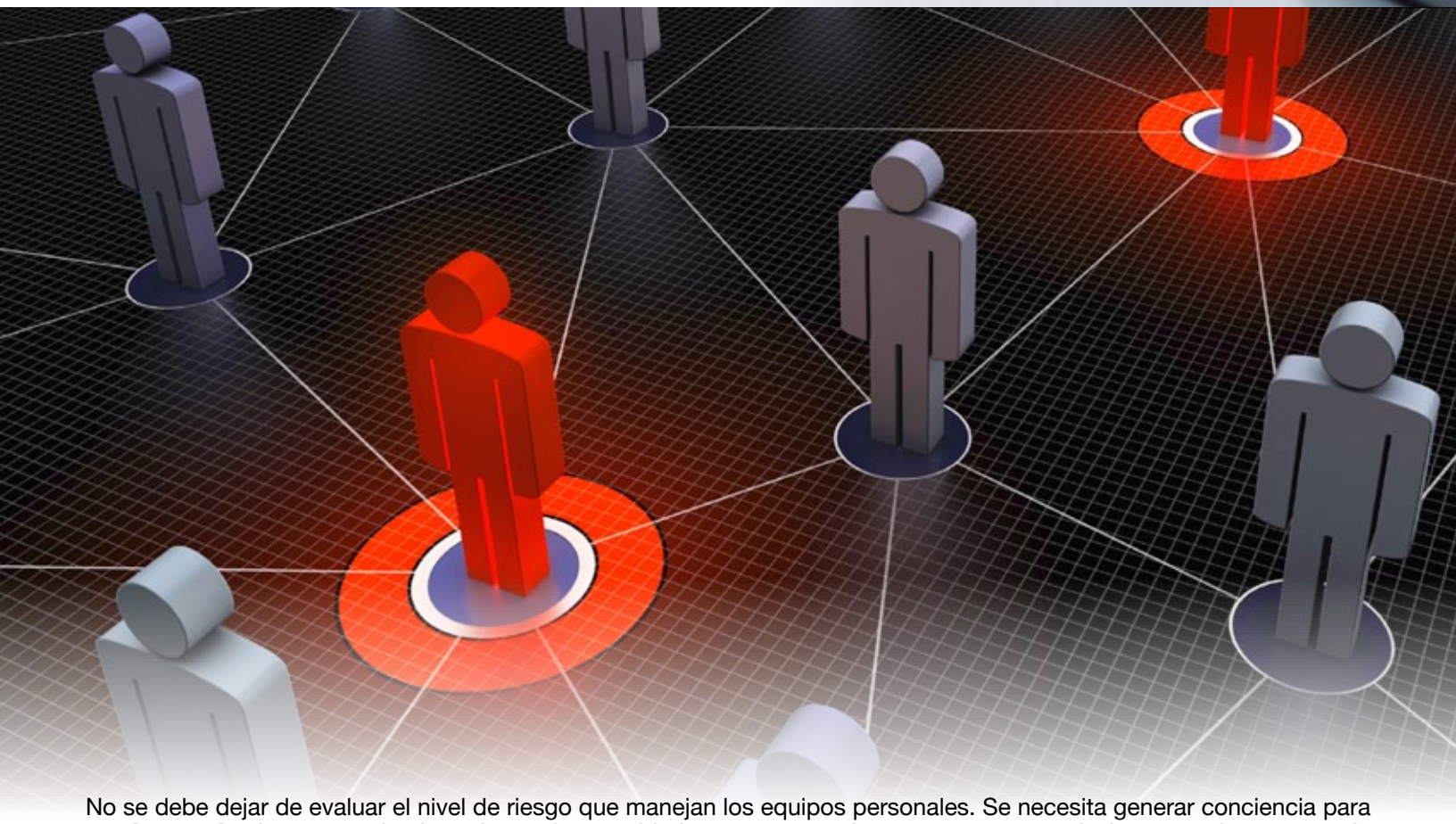
Pero si no se quiere confiar en los voluntarios, ¿qué pasa si infectamos, digamos, 100 equipos con conexión *DSL*, para enviar un ataque volumétrico de negación de servicios? Haciendo aritmética simple, a un promedio de 512 Kbps, estamos hablando de 50 Mbps de tráfico, suficiente para poner de rodillas a muchas organizaciones ¿Qué pasa si las computadoras atacantes mandan solicitudes de archivos como *PDF*, videos o simplemente autenticación en una base de datos? El volumen puede variar y tal vez no logre saturar el ancho de banda, pero probablemente sí la aplicación. Los ataques son usualmente sencillos, la idea es multiplicarlos por muchos y a veces incluso apalancarse con protocolos permisivos (ejemplo: ataque de amplificación de *DNS*).



¿Y cómo es que la computadora de la abuelita termina siendo parte de un ataque *APT* o de *DDoS*? Hay muchas maneras igualmente sencillas, por ejemplo, una liga de *Facebook* mostrando "un evento político", un malware instalado en una página comprometida, un disco pirata con malware incluido, un *USB* infectado, etcétera. Todo lo que requiere el atacante es esperar poco tiempo. En las organizaciones puede haber controles como *firewalls*, sistema para prevenir fuga de información, control de conexiones de equipos y muchos más pero, ¿en casa habrá algo? Muchas veces no.

¿Qué hacer?

El mensaje a las organizaciones es directo: no hay que perder de vista que las estaciones de trabajo deben ser consideradas en su justa dimensión. Así como se hace una segregación de funciones con empleados y servidores, también debe haberlo a nivel sistemas y equipos personales. Usualmente en las empresas se definen zonas desmilitarizadas (*DMZ* por sus siglas en inglés) para proteger servidores pero los usuarios suelen quedar en un mismo segmento. Basta que un empleado falle en el seguimiento de la política de seguridad para que un atacante "salte" entre equipos hasta llegar a uno relevante para el objetivo del ataque.



No se debe dejar de evaluar el nivel de riesgo que manejan los equipos personales. Se necesita generar conciencia para que los empleados se concienticen de que la seguridad es un tema serio y sepan que a partir de sus equipos se puede obtener información en detrimento de la organización. Hay que considerar especialmente a aquellos que tienen privilegios adicionales por requerimientos del negocio o de la operación, y segregarlos conforme sea necesario.

Un antivirus no basta; la estrategia de seguridad debe ir alineada con el riesgo al que están expuestos sus activos. No conviene tratar a todos los usuarios como iguales; los usuarios VIP deben tener políticas VIP, es ahí donde está la información relevante que los atacantes buscan y por ello deben ser especialmente cuidados. En este aspecto se percibe un cambio de paradigma, pero todavía falta mucho por hacer.

En el caso de la denegación de servicios, últimamente ha ido a la cabeza el tema de protección en la nube. Hoy los proveedores de servicios de Internet están tomando las medidas de seguridad para proteger a sus clientes, pero estas soluciones van desarrollándose e implementándose a medida que *Anonymous* o similares hacen de las suyas (*Anonymous* publicó en febrero de 2012 que todos los viernes estará atacando y no dice hasta cuándo dejará de hacerlo). Una buena protección requiere de un monitoreo eficiente y una detección a tiempo, lo que convierte al proveedor de Internet en un socio de negocios y en una extensión de la seguridad en temas de disponibilidad.

Otra manera de evitar una denegación de servicio es efectuar periódicamente un análisis de capacidad. No siempre es culpa de *Anonymous* o quien el lector mande: la capacidad de cómputo es parte integral de la disponibilidad y, como tal, deben existir medidas que la empresa implemente para que no sea su propia operación la que cause una denegación de servicios. En este mundo de las computadoras, cualquier detalle cuenta.

Para terminar, y a raíz de que recordé que en el mantenimiento de la certificación CISSP hay maneras de obtener puntos haciendo "altruismo en seguridad" ¿Por qué no considerar apoyar a la "abuelita" y brindarle un servicio de limpieza de su computadora cada año? De esta manera la protegemos y protegemos un poco nuestra propia empresa. Es muy probable que ISC² no tome estas acciones como puntos, pero no deberíamos dejar de hacerlo. La idea es ayudar a quienes no conocen, no quieren o no deben conocer de estos temas.

El cumplimiento en tiempo real genera confianza en tiempo real cuando las TI y el control trabajan como uno.

Cada segundo de cada día hay miles de eventos a través de la red. Las soluciones de Administración del Cumplimiento de Novell® monitorean continuamente esta actividad en búsqueda de inconsistencias, generando una vista holística en tiempo real de quién está accediendo qué y si están autorizados—todo mientras se integra con la infraestructura actual de tecnología. Así que en vez de documentar los riesgos después del suceso, puede confiar que el cumplimiento está activo, que la información está segura y que los costos de administración son reducidos. Obtenga cumplimiento en tiempo real y permita que Novell haga que las TI trabajen como una para su empresa.

Para mayor información contáctenos al (55) 5284 2700
o visite www.novell.com/compliance

Novell®
Making IT Work As One™

El reto de hoy: una cultura de cambios (Change Management)

Diana Cadena
MCP, MCSE: Security, RUP e ITILv3: OSA
dcadena@scitum.com.mx

Hoy en día las organizaciones que proveen servicios de TI están adoptando de manera creciente estándares y mejores prácticas como *ISO-27001, ITIL* y *Cobit* para la administración de sus servicios mediante procesos como los de gestión de cambios, manejo de incidentes o administración de configuraciones; y asignando funciones específicas para el rol que juega cada recurso, de tal manera que se minimice la interrupción de los servicios.

Cuando me refiero a la cultura del cambio, no solo incluyo el aspecto tecnológico (que veremos más adelante en este artículo) sino el humano, que se caracteriza de manera natural por su aversión al cambio, lo cual se traduce en una lucha constante en las organizaciones para la erradicación de hábitos improcedentes y hasta nocivos. Por eso es importante que quienes adopten las mejores prácticas de gestión de servicios de TI no solo se enfoquen en la implantación de una metodología de procesos hacia los servicios y en las tecnologías que desean alinear, sino que contemplen el factor humano. En muchas ocasiones este elemento puede ser un factor decisivo para el éxito o, en el peor de los casos, para el fracaso.

En el caos de TI existen muchos obstáculos para el cumplimiento de servicios que se vuelven un ciclo infinito de cambios tecnológicos, información, políticas, lineamientos, sistemas y personas. El ritmo vertiginoso en este entorno obstaculiza la solución y, como ya se dijo arriba, las cuestiones relacionadas con la gente son de las más difíciles: desde la alta dirección hasta aquellos operadores que son considerados (o autodenominados) amos y gestores de las herramientas tecnológicas a las cuales ningún otro ser mortal tiene acceso. Alinear a estas personas para bajarlas del pedestal en el que han vivido es un reto enorme pues, si bien la separación de funciones es una buena alternativa y constituye una excelente práctica para la gestión de los sistemas informáticos, debe establecerse adecuadamente para evitar incertidumbre y descontrol.

Antes que nada, es prioritario identificar el nivel de madurez en el que se encuentra el área u organización que se quiere alinear, con el fin de establecer un punto de partida. Frecuentemente se determinará que se tiene un nivel comúnmente conocido en el *argot* informático como “de apagado de incendios”, en el que existe poco o nulo control y hay un desconocimiento general sobre el impacto de la infraestructura en otras áreas y servicios de la empresa. Pueden existir huecos de seguridad pues la gestión de registros o eventos tal vez no son considerados como una fuente valiosa de información y por lo tanto el control de los cambios solo fluye en la incertidumbre. Este nivel de madurez INEXISTENTE termina siendo costoso ya que la posibilidad de obtener resultados positivos es casi nula.

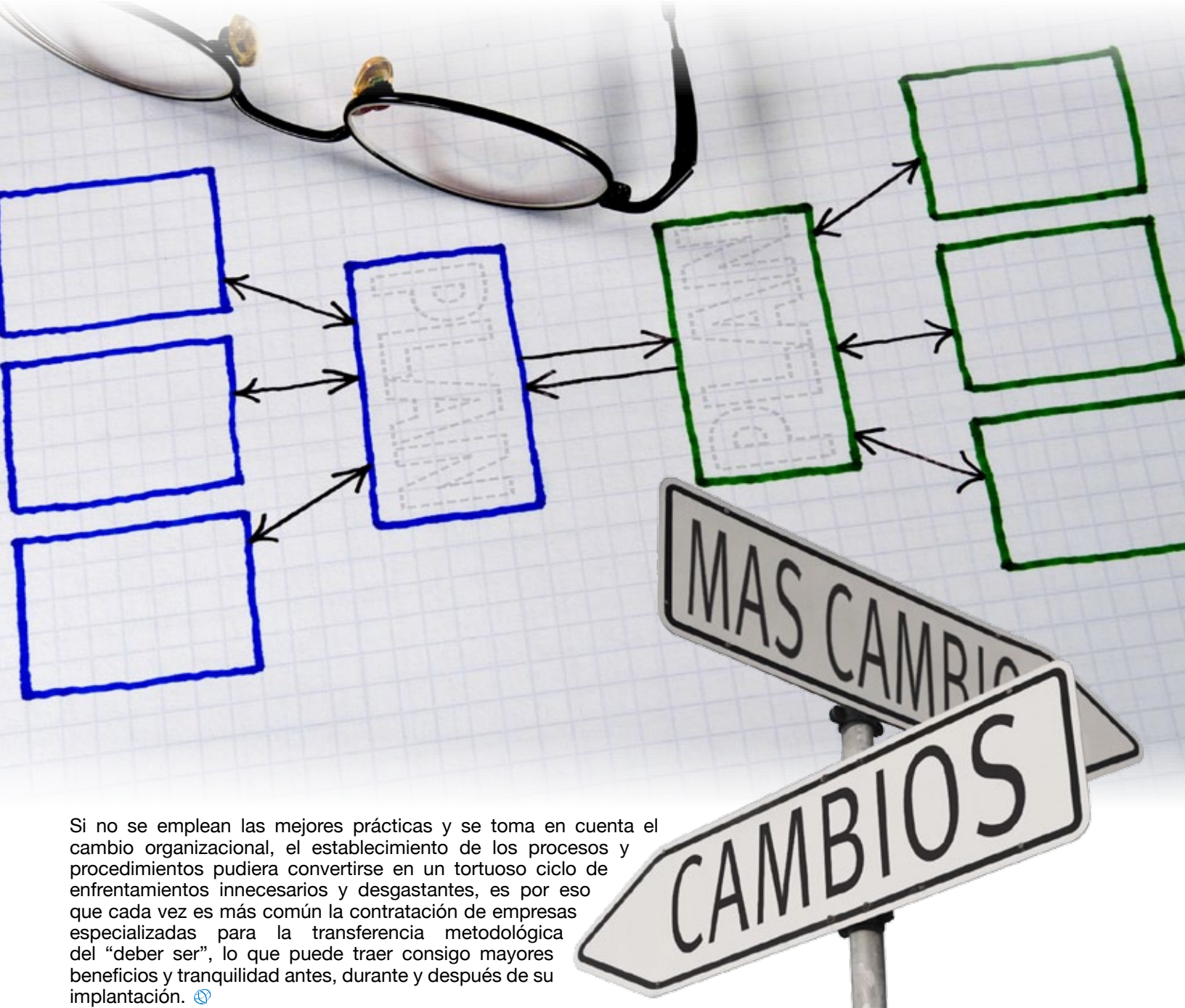
Si se ha sentido familiarizado con alguna de estas situaciones, no se preocupe, nunca es tarde para comenzar a cambiar y eso quiere decir que ha surgido el reconocimiento de la necesidad de la implementación de procesos.

Para detectar en qué posición se encuentra una organización o área de TI en cuanto a sus procesos, hay una clasificación de niveles de madurez –inicial, gestionado, establecido, predecible y optimizado- y es a través de evaluaciones predefinidas y utilizando una serie de criterios objetivos como se identifican los puntos débiles y oportunidades (*ITIL* es muy bueno para esta tarea). Una vez detectado el grado de madurez, se estará en el punto de partida para definir hacia dónde ir en el corto, mediano y largo plazo.

El cambio cultural es una herramienta básica para establecer un adecuado proceso de administración de cambios, ya que este proceso es el instrumento utilizado para saber qué adecuaciones están siendo introducidas de manera controlada y coordinada a uno o más elementos de configuración de la infraestructura tecnológica. Ahora bien, para definir la infraestructura a administrar es indispensable alcanzar un contexto claro de qué elementos formarán parte del alcance de la administración de cambios y definir la matriz de asignación de responsabilidades RACI (*Responsible, Accountable, Consulted, Informed*) para asegurar que cada uno de los elementos de dicho alcance esté asignado al equipo que participa en el proceso de administración de control de cambios. Escoger al equipo de trabajo no siempre es posible pero es lo ideal en términos de asignación de responsabilidades de acuerdo a las habilidades tecnológicas de cada persona.

El proceso de administración de cambios es complejo por naturaleza debido a que su estructura se relaciona con muchos otros procesos de *ITIL* y la implantación de una metodología de procesos para el dominio de Change Management es de los más arduos y laboriosos en sembrar, aunque también se convierte en uno de los más fructíferos.

"Una mala planeación es aquella que no admite modificaciones"



Si no se emplean las mejores prácticas y se toma en cuenta el cambio organizacional, el establecimiento de los procesos y procedimientos pudiera convertirse en un tortuoso ciclo de enfrentamientos innecesarios y desgastantes, es por eso que cada vez es más común la contratación de empresas especializadas para la transferencia metodológica del "deber ser", lo que puede traer consigo mayores beneficios y tranquilidad antes, durante y después de su implantación.

Buffer overflow (primera parte)

Gastón Olguín
golguin@scitum.com.mx

Más de uno habrá oído hablar del desbordamiento de pila (*buffer overflow* en inglés), un error a la hora de desarrollar *software* que puede ser aprovechado para que un programa realice funciones u operaciones para las cuales no fue programado. Este tipo de vulnerabilidad es esencial para llevar a cabo las pruebas de penetración.

Antes de hacer el salto cuántico y empezar a desbordar pilas a diestra y siniestra, es necesario entender conceptos que quizá no se relacionen a primera vista con el tema de seguridad, sino con cuestiones de programación y de cómo la computadora gestiona la memoria. Ya que se haya entendido esto, se podrá comprender cómo es que se produce un desbordamiento de pila, qué lo ocasiona y cómo es que se toma ventaja de él. Claro, siempre es factible saltar conceptos y obviarlos, tomarlos como si fueran dogmas de fe para simplemente realizar pruebas de seguridad corriendo herramientas automatizadas y esperar que funcionen. Sin embargo, resulta importante, en nuestro esfuerzo de difusión, expandir el panorama.

¿Qué pasa cuando las herramientas no funcionan?, ¿solo levantamos los hombros y decimos “no funcionó”? ¡No! Lo que debemos hacer es verlo de esta manera: sabemos que en la computadora hay una aplicación que es vulnerable, pero que por alguna razón la herramienta que tiene el *script* que explota la vulnerabilidad no funcionó. Tenemos en nuestro poder la información necesaria que puede ayudar (tipo de sistema operativo, la aplicación, el puerto a la escucha, etcétera); tomemos todo esto, un poco de procesamiento de nuestro cerebro y desarrollemos el script que permita tomar ventaja de la vulnerabilidad que, al final de cuentas, sabemos existe y que simplemente debemos pensar y hallar la manera de explotar.

Para llegar a ese punto primero se requiere entender los conceptos implicados y no solo saber cómo correr una herramienta. Es eso, y no otra cosa, lo que separa a un hacker de un simple mortal que sabe como teclear comandos.

Variables, el poder de variar

Cuando se elabora un programa puede surgir la necesidad de esperar por datos que sean proporcionados desde una fuente externa, para lograrlo se hace uso de algo que en el argot de programación se conoce como “variable”. Una variable de programación, al igual que una variable en una función matemática, puede tomar cualquier valor. Tomemos justamente el ejemplo matemático para entenderlo y pensemos en la función: $y = x + 5$.

Supongamos ahora que deseamos hacer un programa que nos diga cuánto vale “y” una vez que determinemos el valor de “x”. Dicho programa diría algo como: “Hola, tengo un severo problema y necesito de tu ayuda. Debo saber el valor de “y” que resulta de la función “x + 5” pero yo no sé cuánto vale “x” ¿Podrías indicarlo?”

Así pues, sabemos que un programa puede recibir información de una fuente ajena al programa (el usuario, en el caso de nuestro ejemplo) y que esa información será almacenada en variables, pero, ¿cómo se hace esto? Sencillo, el programa, al ser ejecutado toma espacio de memoria, de todo ese espacio que tomó deja una parte pequeña de memoria para los valores que desconoce (las variables) y que está a la espera de que alguna fuente externa se los proporcione.

Arreglos

Dentro de la programación existen varios tipos de variables. Están las que llegan a almacenar valores llamados enteros, las que llegan a almacenar valores flotantes o las que almacenan solo un carácter alfanumérico, entre otras. Pero hay un tipo de variable a la que le debemos prestar especial atención: los arreglos.

¿Qué es un arreglo? Imaginemos un largo estante, tan largo como lo deseemos, que tiene cajones y dentro de cada uno podemos guardar lo que sea, lo que queramos, y a ese estante le asignamos un nombre con el cual lo identificamos fácil y rápidamente. Un arreglo es algo similar, es un gran estante que llevará un nombre y que usaremos para guardar valores ya sea de tipo entero, flotante, caracteres, etcétera. Cuando necesitemos un valor en específico solo bastará ir al “cajón” indicado del estante y tomarlo.

La manera en que un programa maneja un arreglo que no ha sido inicializado (es decir, que no tiene valores) es similar a la manera que maneja las variables, les deja un espacio de memoria, pero esta vez la deja de manera continua: si el arreglo es de cinco elementos dejará el espacio para cinco variables, si es de diez, dejará diez espacios, de acuerdo a lo que haya sido definido por el programador.

El error que se comete al momento de programar

Imaginemos que es necesario hacer una aplicación que guarde cinco números proporcionados de manera externa. Existen dos opciones, una es declarar cinco variables o hacer uso de un arreglo que conste de cinco elementos. Después de una no tan difícil deliberación decidimos usar el arreglo y corremos la aplicación para probarla. Llegamos al punto en donde el programa solicita introducir los cinco datos y empezamos a proporcionar uno por uno hasta llegar al quinto dato, llegado este punto lo normal sería que ya no se pudieran introducir más datos, sin embargo el programa permite un sexto dato, es decir, meter más datos de los que debería guardar. Es justo ahí donde hemos cometido un error al momento de desarrollar el programa, que más que un error es un descuido, ya que no se tomaron las debidas precauciones para evitar introducir más datos de los que el programa puede manejar de acuerdo con su diseño y es esto justamente la esencia de la vulnerabilidad llamada desbordamiento de *buffer*.

Cuando un programa nos permite introducir más datos de los que espera y puede manejar, sucede que existe la posibilidad de escribir en zonas de memoria donde se ubica información que ayuda al control y flujo del programa. Ahora entonces, la pregunta lógica es ¿Qué es y cómo funciona esa zona de memoria que controla la ejecución del programa?

El *stack*

La cosa es muy simple, un programa que es inicializado necesita tomar un espacio de memoria que usará para, llegado el momento, poner en ese espacio el valor de las variables que no fueron declaradas desde el código del programa y que será conocido una vez que el programa esté corriendo. Este espacio de memoria se conoce con el nombre de *stack*, o "pila" si se prefiere la traducción al español.

¿Y cómo funciona el *stack*?, para ilustrar este concepto hay un sinfín de objetos con los cuales se pude ejemplificar, pero tomemos uno de mis favoritos, los libros. Imaginemos un libro sobre una mesa, y sobre ese libro ponemos otro, y sobre ese libro otro más, y así hasta que tenemos una columna de cincuenta libros. Si eventualmente necesitamos tomar el primero, aquel que está justo entre la mesa y los cuarenta y nueve restantes, no podremos hacerlo sin antes quitar los que están encima de este. De hecho, no podemos tomar el libro cuarenta y nueve sin antes haberle quitado de encima el libro cincuenta. Entonces, para llegar al de hasta abajo tengo que retirar el libro cincuenta, luego el cuarenta y nueve, luego el cuarenta y ocho, y así hasta llegar al primero.

El *stack* es algo muy similar, es una gran columna (virtual) de memoria donde se almacenará información, ya sea de control o de variables, y, a diferencia del ejemplo de los libros, no es que exista la posición uno, la dos o la tres; lo que existe es una dirección de memoria para cada elemento.

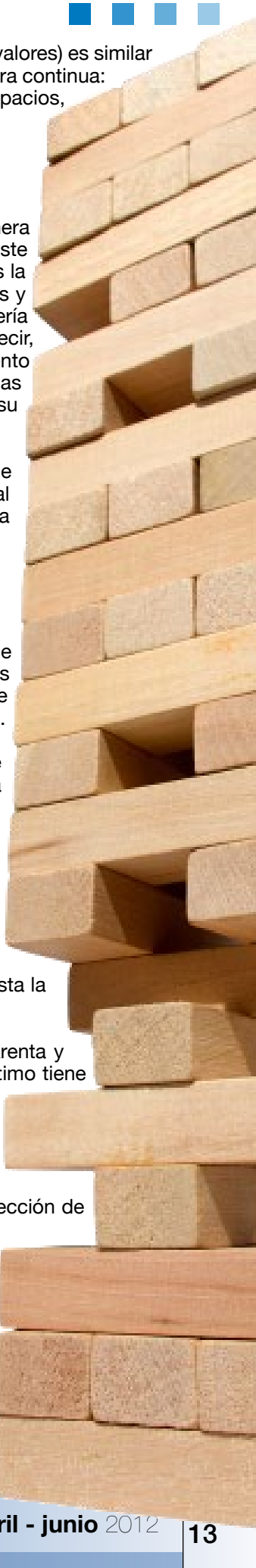
En el ejemplo se señaló que si quería llegar al primer libro, deberían quitarse uno por uno los cuarenta y nueve libros que estaban arriba. Este concepto de ir quitando uno por uno empezando desde el último tiene un nombre y se llama LIFO (*last in, first out*), que quiere decir que el último que entra será el primero en salir.

El *stack* es una sección de memoria que suele utilizar el concepto LIFO (aunque no todos los *stack* operan así) para introducir datos que pueden ser de control y flujo del programa o el valor de variables que no fueron declaradas en el código del programa. Ahora, ¿cómo sabe la computadora en qué sección de memoria debe introducir información? La respuesta tiene un acrónimo y es SP.

SP es el acrónimo para *Stack Pointer* y su función, como lo dice su nombre, es apuntar a una dirección de memoria de la pila, de hecho la del último elemento. Es importante entender que el SP siempre se encontrará apuntando al último elemento, porque justamente así es como se determinan dos operaciones que se utilizan para manipular datos en la pila: *push* para introducirle datos y *pop* para sacar.

Por ahora dejemos el asunto, en la siguiente entrega veremos cómo operan *push*/*pop*, cómo se construye una función en el *stack* una vez que un programa ha sido ejecutado, y qué sucede cuando se hace un desbordamiento de pila.

Continuará…



Teléfonos inteligentes
Lo que estamos perdiendo de vista

Claudio Polanco Olguín
CISSP, PMP, CRISC e ITIL
cpolanco@scitum.com.mx

En el año de 1997 Scott Adams publicó "*The Dilbert Future*", un libro en el que con su estilo satírico de criticar la sociedad y la forma en que se desarrolla la tecnología, elaboró varias predicciones, algunas de ellas completamente proféticas. Una que llama la atención y viene al caso con el presente artículo es la siguiente: "*En el futuro las computadoras de red se comprarán y utilizarán con el mismo entusiasmo que los aparatos para ejercitarse en el hogar*"[1], refiriéndose a "*Network Computer*" como a una computadora diseñada para solo interactuar con Internet[2]. Se podría decir que estas son, en concepto, el equivalente de las actuales *tablets* y los teléfonos inteligentes. Efectivamente, hoy en día el número de dispositivos móviles tiende a ser mucho mayor que los dispositivos tradicionales.

Con esto en mente, me propongo generar en el lector la necesidad de ver este tipo de dispositivos no como simples medios de comunicación portátil o juguetes electrónicos sofisticados, sino como activos que se integran a las empresas fuera de los planes estratégicos de tecnología, solo por iniciativa de ejecutivos o empleados impulsados por el deseo de contar siempre con el último gadget y que se convierten en un reto organizacional que implica resolver la complejidad de su gestión desde el punto de vista de la seguridad. Para lograrlo, iniciaré revisando información de las tendencias de crecimiento de estos dispositivos y explicando por qué es necesario estudiarlas por tipo de plataforma. Continuaré con una muy breve explicación de los riesgos asociados a las principales alternativas tecnológicas dependiendo de sus orígenes, para después analizar la complejidad de determinar los límites de responsabilidad sobre la información y uso de dichos dispositivos desde el punto de vista corporativo y, por último, propondré algunas líneas de acción básicas que los responsables de la seguridad de la información pueden impulsar como primer paso para mitigar los riesgos actuales.

La probabilidad de ocurrencia de un acontecimiento contra la seguridad aumenta proporcionalmente al tamaño del universo de elementos que participan en dicho acontecimiento, en otras palabras, cuando la superficie de ataque se incrementa, también se incrementa la probabilidad de que sea atacada. Por ello, reconocer cómo se ha incrementado el número de dispositivos nos subraya la posibilidad de que un evento de este tipo se desencadene. Una idea de la dimensión del riesgo la encontramos en el estudio del "INEGI: Usuarios de telefonía móvil por países seleccionados, 1998 a 2009", que muestra que en 2009 ya existían 774 teléfonos móviles por cada 1,000 habitantes. En el mismo estudio se observa que en Asia y EE.UU. existe una proporción de 1.4 teléfonos móviles por habitante. Pese a que no ha sido publicado un estudio más reciente, se percibe que estas no son cifras que tienden a estancarse o a descender, por el contrario, el número de dispositivos móviles que cuentan con funciones avanzadas es mayor y aumenta día a día como refiere Winn Schwartau, especialista en seguridad informática, quien estima que para 2020 existirán 20 mil millones de equipos móviles comunicados a través de Internet y que serán los principales blancos de ataques informáticos[3].

En cuanto al tipo de dispositivos, según *AC Nielsen*, firma especializada en estudios de mercado, 38% de los teléfonos móviles que se compran en Estados Unidos son *smartphones*[4] e IDC (*International Data Corporation*) pronostica que para 2014 40% de los activos informáticos de las empresas serán teléfonos inteligentes[5]. Como último dato estadístico relevante apunto que la participación actual de teléfonos inteligentes, en el universo de los dispositivos conectados a la red de telefonía en Estados Unidos es de 70%, según datos de *Millenial Medias*[6].

Ilustración: Silverio Ortega

Source: Millennial Media, 11/11. Smartphone data does not include what could be considered Smartphones running proprietary Operating Systems, e.g. Samsung Instinct, LG Vu. Millennial Media defines a Connected Device as a handheld device that can access the mobile web, but is not a mobile phone. Examples include Apple iPod Touch, Sony PSP, NintendoDS, iPad, etc.

Conexiones móviles de datos por tipo de aparato

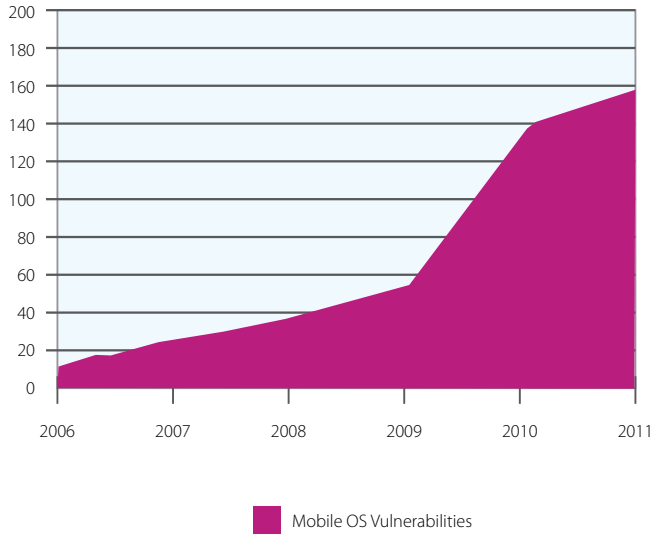
Pese a esta tendencia, no se aprecia una preocupación real en las organizaciones por incorporar prácticas y políticas de seguridad para estos dispositivos. El problema aumenta por la variedad de plataformas sobre las que operan los teléfonos celulares tanto en *hardware* como *software*, que al ser diseñadas y construidas con diferentes prácticas de seguridad, hacen muy complicado contar con herramientas para proteger oportunamente toda la gama de dispositivos móviles.

«Efectivamente, hoy en día el número de dispositivos móviles tiende a ser mucho mayor que los dispositivos tradicionales»

Para facilitar el análisis, es conveniente agrupar en subconjuntos o categorías con base en alguna característica predominante. Se podría pensar en el fabricante o en el *carrier* que provee los servicios, sin embargo estos argumentos no permitirían hacer una generalización ya que presentan una importante correlación geográfica que sesgaría el análisis. Otras características que se antojan probables para agrupar son la arquitectura de procesadores y las funciones de interacción con el usuario, pero el análisis se haría muy extenso debido a la diversidad de los dispositivos. Agrupar por el sistema operativo arroja un número de subgrupos muy manejable para analizar, con una importante ventaja adicional: esta característica se encuentra íntimamente relacionada con las brechas de seguridad, como muestran Kimber Spradlin y Tom Cross -especialistas de IBM- en las siguientes dos gráficas. En ellas observamos la tendencia en aumento de las vulnerabilidades en los sistemas operativos y, en consecuencia, en el número de técnicas de ataque para hacer uso de ellas.

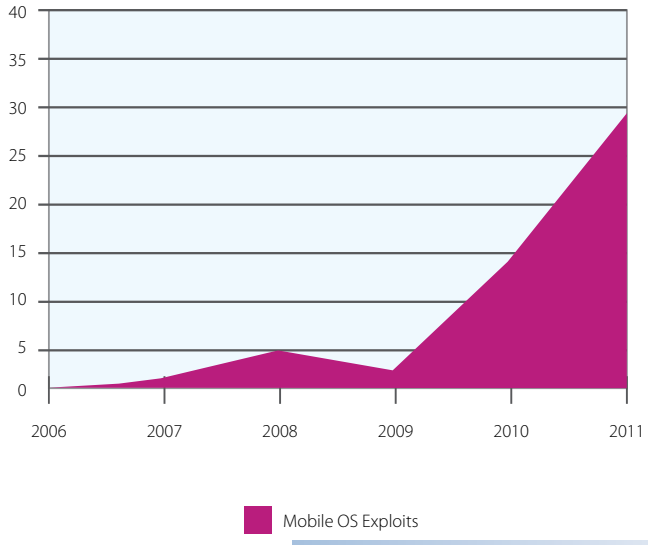
Vulnerabilities in Mobile Operating Systems

Total Mobile Operating System Vulnerabilities
2006 - 2011 (Projected)



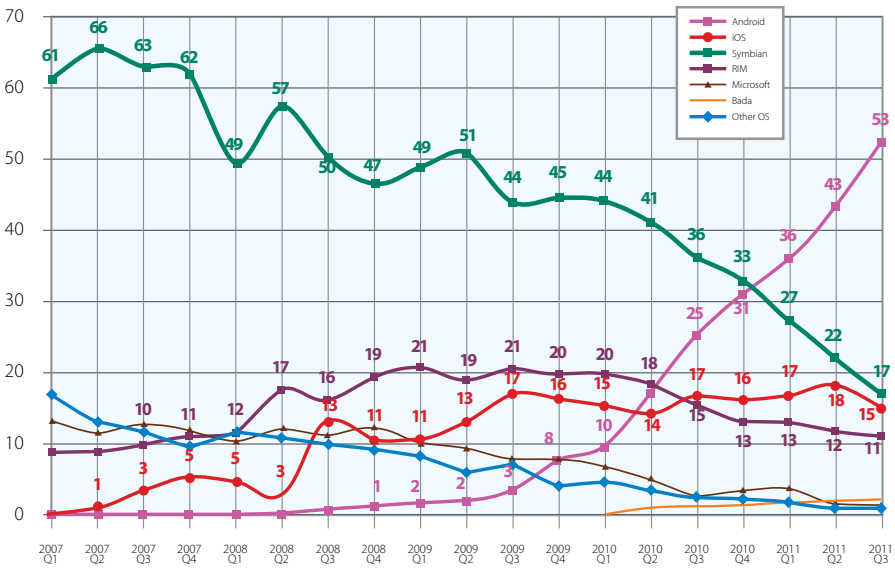
Exploits that target Mobile vulnerabilities

Mobile Operating System Exploits
2006 - 2011 (Projected)



Para identificar la importancia relativa de cada plataforma en el universo instalado, Gartner publica un estudio trimestral que permite conocer los datos de participación de cada uno de los sistemas operativos: el "*Gartner Smartphone Marketshare*", que *Milominderbinder2* ha compartido en Wikipedia[7] en la forma del siguiente diagrama:

World-wide Smartphone Mobile OS Marketshare %



Entrando en materia del origen de las vulnerabilidades que los teléfonos inteligentes han heredado del sistema operativo que utilizan, se observa que *Android*, el nuevo sistema dominante en el mercado, está basado en un entorno *Java* lo que permite, mediante el uso del *sand box*, aislar las capacidades aplicativas del *hardware*, lo cual es benéfico para empatar a distintos fabricantes de *software* independientemente del modelo de teléfono. Otra ventaja es que se pueden realizar decompilaciones del *software* para tener acceso a registros básicos del sistema lo cual representa una importante brecha de seguridad.

El segundo competidor, iOS, que es utilizado en *iPhone* e *iPad* está desarrollado en plataforma Linux. Este sistema operativo realiza un proceso de compilación de manera nativa que integra al objeto información de la configuración del equipo por lo que puede ser rastreado para realizar ataques. Finalmente RIM, utilizado por BlackBerry, presenta un mejor enfoque de la seguridad, pero lo hace poco versátil y poco vistoso, que parecieran ser unas de las razones por las cuales ha perdido una jugosa participación en el mercado.

Sin importar la plataforma, los teléfonos inteligentes tienen capacidades de "*dual homing*", lo que significa que pueden trabajar simultáneamente con dos distintas redes y esto posibilita a un atacante a utilizar estos dispositivos como un back door o puente entre ellas para tener acceso a la red empresarial.

El universo de vulnerabilidades aumenta con la creciente oferta de aplicaciones que se pueden descargar ya sea de manera gratuita o con costo. Derivado de la presión por una fuerte competencia que acorta los tiempos de liberación, muchas aplicaciones son creadas y puestas al alcance del consumidor sin haber realizado suficientes pruebas de seguridad, que garanticen que estas no contienen código malicioso, comúnmente enfocado a obtener acceso no permitido a los recursos del propio teléfono y, en su caso, a las redes en que el dispositivo se encuentra operando. Entre las deficiencias en el desarrollo de aplicaciones se reconoce que los ataques más comunes son por inyección de SQL y robo de sesiones; baste decir, para ver la extensión del riesgo, que McAfee desde hace dos años identificó la existencia de *botnets* en dispositivos móviles[8].

Revisando el factor humano, los mismos usuarios, al buscar un mejor desempeño o nuevas funcionalidades, pueden estar tentados a aplicar técnicas de *JailBreaking*[9], para obtener más recursos y permisos para ejecutar las aplicaciones creando severas brechas en la seguridad de la operación del equipo.

Una vez reconocida la criticidad que el problema representa para la seguridad corporativa, así como las tendencias de participación de mercado de las principales plataformas, es primordial ocuparse de cómo mitigar el impacto a los riesgos asociados a estos dispositivos.

Para minimizar la posibilidad de ser víctima de un ataque, la seguridad debe plantearse en distintas capas:

- **Estratégica**. Definir las condiciones de uso y seleccionar la tecnología adecuada para las necesidades de la organización.
- **Organizativo.** Determinar quiénes deben tener este tipo de activo y qué políticas debe regir su uso, así como proveer de un proceso continuo de concientización de los riesgos de seguridad.
- **Gestión de activos.** Normar dónde se encuentran y bajo la responsabilidad de quién, y qué aplicaciones y usos están permitidos.
- **Operación.** Aplicar configuraciones en los teléfonos para el endurecimiento de las directrices de seguridad, incluyendo el posible encriptado de datos y conversaciones.

Protege

al activo más importante de tu empresa,

tu información

Seguridad IT mantiene segura la información y aplicaciones de tu empresa, con el respaldo de la infraestructura más sólida de Latinoamérica.

- Control de acceso a la información.
- Sistema de prevención de intrusos.
- Filtrado de contenido Web.
- Filtrado de correo electrónico.
- Cifrado de datos.
- Seguridad administrada a través del Security Operation Center (SOC).

TELMEX IT

Scitum

Tú pones la imaginación,
nosotros la tecnología.

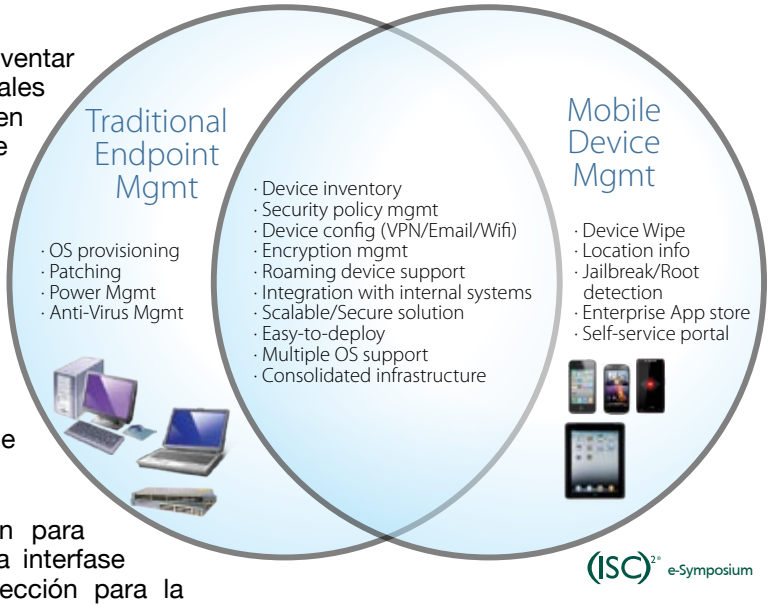
telecom | it | consulting

01 800 835 6391
telmex.com/it

TELMEX
está contigo

En relación al establecimiento de políticas de uso para estos dispositivos, tal vez el mayor reto es definir las responsabilidades del usuario. En los Estados Unidos, donde los temas legales suelen ser revisados con mayor detenimiento, han encontrado problemas para definir los límites dependiendo de la propiedad del equipo y pago de los servicios de conexión. Por ejemplo, aplicar políticas estrictas para el control, monitoreo y uso es posible cuando ambos pagos son realizados por la empresa (tanto el *hardware* como el servicio de comunicación); sin embargo, cuando el modelo de pago implica una erogación del mismo empleado para tener un teléfono donde almacena o realiza transacciones con la empresa, entonces es legalmente complicado responsabilizar al empleado por el posible mal uso del aparato, sea hecho con dolo o no. Pese a la complejidad legal, es necesario que el usuario esté consciente de los problemas de seguridad relacionados a su dispositivo móvil y que la compañía presente una postura formal y dicte sanciones en cuanto al mal uso de la información y recursos de la empresa.

Para trabajar sobre la gestión de los activos no es necesario inventar controles nuevos, pero sí enfocar las necesidades puntuales para este tipo de dispositivos. Kimber Spradlin comparte en la siguiente imagen[10] una comparación entre el universo de acciones para una PC normal, "*Traditional Endpoint*", y un teléfono inteligente, "*Mobile Device*"; como se aprecia, muchas de estas prácticas ya son realizadas por la organización, amén de que propone algunas específicas a incluir para la gestión de móviles:



En cuanto al endurecimiento de la seguridad en los dispositivos, acciones sencillas son convenientes para disminuir el riesgo de un ataque. Algunas de ellas son:

- **Manejo de contraseña.** Habilitar esta función para impedir el acceso lógico al dispositivo desde la interfase de usuario. Esta es la acción básica de protección para la información que el equipo contiene.
- **Protección automática de teclado**. En conjunto con la acción anterior, en caso de que el equipo permanezca sin ser utilizado, evitará el acceso a extraños, especialmente si se deja olvidado.
- **Protección de datos.** Borrar la información de manera preventiva cuando el equipo se encuentre comprometido; aunque es una opción drástica, garantiza que no se comprometa la confidencialidad. Se debe acompañar de respaldos periódicos con cifrado de datos.
- **Manejo adecuado de conexiones.** Evitar el uso de *Bluetooth*, así como habilitar las notificaciones de redes *WiFi*. Si esto se combina con concientización respecto a los riesgos de los *back doors*, disminuirán la posibilidad de ataques por las facilidades de *dual homing*.

Conclusión

Se debe reconocer que los teléfonos inteligentes, sin importar como hayan llegado a la empresa, deben ser tratados y administrados con un enfoque integral y consistente con las políticas y el modelo de seguridad de cada organización. Se deben reconocer en las políticas y en el modelo de seguridad las necesidades de movilidad de los empleados desde el punto de vista estratégico, lo que apoya en reducir la complejidad por el número de plataformas al restringir los modelos y funciones que estos pueden soportar. Con pocos cambios, las políticas y procesos para la administración de los activos pueden adecuarse para incluir las terminales móviles, una gestión adecuada del *software* que se instala también es de mucha ayuda. Finalmente, no está de más insistir en que si algo debe permanecer en mente, es que estos equipos ya son parte de la operación diaria de las personas y empresas, por lo que no es recomendable obviar ni minimizar su impacto.

[1]Adams, Scott; *The Dilbert Future*, Ed. Harper Business, 1997.
[2]Adams, Scott; *The Dilbert Future*, Ed. Harper Business, 1997.
[3]Schwartau Winn; *CyberWar* 4G a/k/a *The Coming Smart Phone Wars*, ISC2 e-symposyum October 27, 2011
[4]http://blog.nielsen.com/nielsenwire/?p=28237
[5]IDC ; *World Wide Business Use Smarthphone* 2010-2014
[6]Millenial Media´s; November 2011 Mobile Mix Report
[7]http://en.wikipedia.org/wiki/Mobile_operating_system#cite_note-Gartner_2011_Q3-3
[8]Schwartau Winn; CyberWar 4G a/k/a *The Coming Smart Phone Wars*, ISC2 e-symposyum October 27, 2011
[9]El *JailBreaking* es un proceso que realizan los usuarios para, mediante *kernels* modificados, para tener acceso completo al sistema operativo del equipo, principalmente al sistema de archivos y a la ejecución de línea de comando. Aunque es un término que en principio solo se aplica a equipos corriendo bajo la plataforma iOS, su uso se ha extendido a otras plataformas, refiriéndose al aumento de privilegios del modo usuario.
[10]Spradlin Kimber, Cross Tom; 2011 Mobile Threat Landscape, ISC2 e-symposyum October 27, 2011

¿puedo hacer que la seguridad deje de ser un "NO" por default, al "conocer (KNOW)" lo que protejo en primera instancia?

con **ca**, usted puede

Gracias a nuestra capacidad única para conocer todos los entornos.

Decirle "no" al acceso no autorizado es importante. Pero "conocer" es mucho más importante.

Identidades. Accesos. Información. Cumplimiento.

Para obtener una solución segura, emplee el poder de conocer para que su negocio sea más ágil.

Visite security.com y ponga a trabajar todo el poder de conocer.

agility
made possible™

ca technologies

misión: crítica

Los nuevos dispo

¿Quién ganará?

Ulises Castillo

M. en C., CISSP, CISM y CISA
ucastillo@scitum.com.mx

Cada vez con mayor intensidad los usuarios en todo el mundo están presionando a sus organizaciones para que les permitan utilizar sus propios teléfonos inteligentes y *tablets* para acceder a datos y aplicaciones corporativas. La respuesta ha sido muy variada, unas lo autorizan e incluso apoyan financieramente a los empleados, mientras que otras lo prohíben rotundamente. Las que adoptan la segunda posición (de restricción) argumentan los riesgos de seguridad como la principal razón de su negativa. En este artículo analizaré el fenómeno que genéricamente se ha llamado BYOD (por las siglas en inglés de *Bring Your Own Device*, que se traduce como "trae tu propio dispositivo") así como los argumentos a favor y en contra, para terminar con algunas recomendaciones concretas al personal encargado de la seguridad.

El caso de Chanchis

Chanchis, empleada en una empresa financiera, está francamente molesta el día de hoy. Hace unos días, y después de ahorrar algunas quincenas, compró su nuevo *iPad*. Muy orgullosa llegó a su casa y empezó a bajar algunas aplicaciones de Internet. Le habían recomendado dos que le podrían servir para el trabajo: una para llevar anotaciones y otra para coordinación de proyectos. Al día siguiente llegó a su lugar de trabajo, configuró su nuevo dispositivo para conectarse a la red corporativa y empezó a jugar (perdón, a trabajar) con sus nuevas aplicaciones, comprobando lo fácil y útiles que resultan. Pero hoy, cuando acudió al área de sistemas pues no podía imprimir desde la red, Cuco, el encargado de seguridad, le dijo que no estaba permitido usar ese tipo de dispositivos en la red corporativa y le enseñó una nueva política al respecto (que, por supuesto, Chanchis no conocía). Ella argumentó que con el *iPad* sería más productiva para la empresa y que, incluso, estaba pensando ya no ocupar su PC de escritorio con lo cual la organización podría tener un ahorro, pero todo fue en vano. Cuco se limitaba a repetir "la política es muy clara. No se puede conectar a la red ningún dispositivo que no esté específicamente autorizado".

El escenario anterior resume las dos posturas que cada día se enfrentan más y más: por un lado los usuarios que quieren ser más productivos usando dispositivos más amigables y versátiles. Por el otro, los responsables de seguridad y de infraestructura que saben los riesgos de permitir la entrada a la red de dispositivos tan "abiertos" como las *tablets* y los teléfonos inteligentes.

A esta necesidad o deseo de los usuarios para utilizar sus propios dispositivos en el trabajo y acceder desde ahí a la red corporativa (con la información y aplicaciones que requieren para realizar sus funciones) se le ha llamado BYOD. Esta tendencia, cada vez más fuerte, es -de acuerdo a varios especialistas- una parte de un fenómeno más global llamado "*consumerización*" (anglicismo que no me gusta usar y que es una mala traducción de la palabra inglesa *consumerization*) y que tiene que ver con el poder creciente de los clientes para decidir no solo a quién le comprarán los bienes y servicios que desean, sino también el poderlos particularizar a sus necesidades.

Un ejemplo: Pedro está en un supermercado y quiere comprar un determinado vino, pero en vez de poner la botella en su carrito de compras simplemente la gira para que se vea el código de barras. A continuación lee dicho código con su teléfono celular y consulta por Internet el precio en tiendas similares, así comprueba que el mejor precio lo tiene una tienda cercana que, adicionalmente, tiene servicio a domicilio. Eso es un ejemplo del poder que actualmente tiene un cliente, y por lo cual las tiendas tradicionales están francamente preocupadas.

ositivos **vs.** la seguridad

Regresando al tema que nos ocupa, analicemos los argumentos que más comúnmente esgrimen los usuarios a favor de la utilización de sus dispositivos en la empresa:

» **Facilidad y comodidad de uso**. Estos dispositivos tienen interfases más amigables, son más portátiles y tienen una gran variedad de aplicaciones, muchas de ellas gratuitas, lo que causa que los usuarios prefieran estos dispositivos en vez de una computadora tradicional.

» **Ahorro**. Como lo establecen varios estudios[1], la mayoría de los usuarios están dispuestos a comprar sus propios dispositivos, por lo cual la organización para la que trabajan podría tener un ahorro al dejar de adquirir computadoras de escritorio o laptops.

» **Libertad de elección**. Uno de los elementos que más atraen a los empleados es poder elegir sus dispositivos en vez de adaptarse al que la organización les asigne. Parece que esta es la razón por la que, como hemos dicho, muchos prefieren pagar por sus propios dispositivos y usarlos para su trabajo.

En contrapunto de los argumentos de los usuarios, las áreas de sistemas tienen los propios:

1. **Dificultad de control**. Para muchas empresas los nuevos dispositivos son cosas parecidas a las PC y, por tanto, están tratando de aplicar el mismo modelo de control que han usado para ellas: mantener un inventario actualizado que incluya la configuración de cada dispositivo, validar que solo se usen aplicaciones autorizadas por la organización, administrar direccionamiento IP, acceso a servicios y aplicaciones corporativas. Bajo este paradigma de control, encuentran que la tarea resulta sumamente complicada, si no imposible.
2. **Falta de estandarización y mayores costos de soporte**. Asociado con el punto anterior, el personal de soporte, regularmente ya sobrepasado por la cantidad de trabajo y requerimientos de los usuarios, ahora que tiene que conocer y hasta dominar diversos sistemas operativos y los trucos de cada tipo de dispositivo. Por ejemplo, si se trata de teléfonos inteligentes, deberá conocer al menos tres ambientes: *iPhone, Blackberry* y *Android*. Además, cuando los usuarios tienen la libertad de instalar cualquier tipo de aplicación, las necesidades de soporte pueden crecer exponencialmente.
3. **Inseguridad creciente**. Desde hace un par de años los reportes especializados de seguridad han documentado las cada vez mayores amenazas que tienen estos dispositivos. Los eventos recientes sobre ataques específicos lo han confirmado[2] y se prevé que debido al número creciente de usuarios de estos dispositivos, y a la poca seguridad que típicamente manejan, mucho del *malware* esté dirigido a ellos y ya no tanto a las PC convencionales.

Como vemos, ambas posturas tienen muchos argumentos lógicos y válidos, aunque encontrados ¿Qué hacer entonces? Esta discusión sobre libertad vs orden ha hecho que algunas personas desempolven viejas historias de los anales de la informática y recuerden lo que pasó con allá a principios de los años 80. En aquel entonces los usuarios querían más libertad, manejar su información y usar aplicaciones más rápidas. Sus quejas giraban en torno a lo tardado que resultaba el desarrollo de sistemas, la complicación de generar reportes en forma más dinámica y no tener acceso directo a su información.

misión: crítica

Las computadoras personales que surgieron a finales de los años 70 y tomaron fuerza con la primera IBM PC (1981), vinieron a resolver algunos de estos problemas. Nacieron diversas herramientas, como procesadores de texto y hojas de cálculo, para que los usuarios manejaran su propia información o desarrollaran sus propios programas; productos como *dBase*, *Turbo-Pascal* o *SQL-Windows* fueron representativos de esa época. Además, las redes locales que se popularizan a mediados de la década de los años 80 les permitían compartir información y recursos de una manera sencilla.

¿Pero cómo respondieron los informáticos? En aquellos años, la mayoría de las personas de sistemas utilizaban computadoras mayores, *mainframes* o minicomputadoras con terminales tontas, por lo que veían a las PC como algo extraño y se mostraban reacios a adoptarlas masivamente. Acostumbrados a tener una fuerte centralización, no mostraban mucho interés en las posibilidades que estas nuevas opciones tecnológicas y herramientas les ofrecían. La respuesta no se hizo esperar: los usuarios compraban sus PC e incluso las conectaban en red sin permiso del área de sistemas, creaban sus primeras hojas de cálculo o desarrollaban sus primeras aplicaciones usando bases de datos.

¿Y qué resultó? Las áreas de sistemas –de una forma u otra- tuvieron que aceptar esta nueva realidad y sumarse a ella, a la vez que cambiaban su paradigma y creaban nuevos roles y formas de trabajo para este mundo que era bastante diferente. Junto con estos roles y funciones, también surgió la necesidad de crear formas de organizar el desorden que se había creado. Había que contestar preguntas muy distintas: ¿Quién debería llevar el control de las PC, incluyendo las marcas y modelos que se comprarían, qué tipos de configuración se permitirían o con qué software se le entregarían a los usuarios? ¿Quién debería desarrollar las nuevas aplicaciones y con qué herramientas? ¿Qué tipo de red, topología y tipo de cableado utilizar? ¿Cómo administrar las direcciones IP? Y otras muchas preguntas por el estilo.

¿Y en los últimos años? Sumada a la explosión de las PC y las redes locales ha venido la de Internet y la conectividad IP. Esto ha creado un sinfín de aplicaciones y servicios para beneficio de las organizaciones y de los usuarios, pero también ha creado un número creciente de vulnerabilidades y amenazas, que han hecho de la seguridad informática un tema del que cada vez es más necesario conocer. Junto con estrategias y enfoques más amplios, han surgido distintas herramientas y soluciones tecnológicas para administrar los riesgos en la infraestructura de TI.

Pero ¿Qué tiene que ver todo lo anterior con el BYOD? Pues que la historia se repetirá en lo fundamental si los que estamos a cargo de la seguridad y de TI no cambiamos de paradigma. En otras palabras, tenemos que pensar en cómo balancear entre libertad y control, entre el uso libre, indiscriminado e inseguro de los dispositivos de los usuarios en la empresa, y el control y seguridad de nuestra información. Nota importante: observe que no hablo del control sobre los dispositivos, sino del control y seguridad sobre la información de la organización.

Si no cambiamos de paradigma, de todas formas van a ganar los usuarios y después tendremos que “limpiar el desorden”, ¿o de verdad creemos que podemos ir en contra de las modas, de la facilidad de uso, de la versatilidad de las aplicaciones que esos nuevos dispositivos tienen? ¿Qué va a hacer usted cuando el propio director de la empresa le diga: “¡Cuco, no me vengas con esos cuentos de los riesgos. Quiero usar mi *iPad* en la oficina, tú ve cómo le pones seguridad pero déjame trabajar con lo que soy más productivo!”

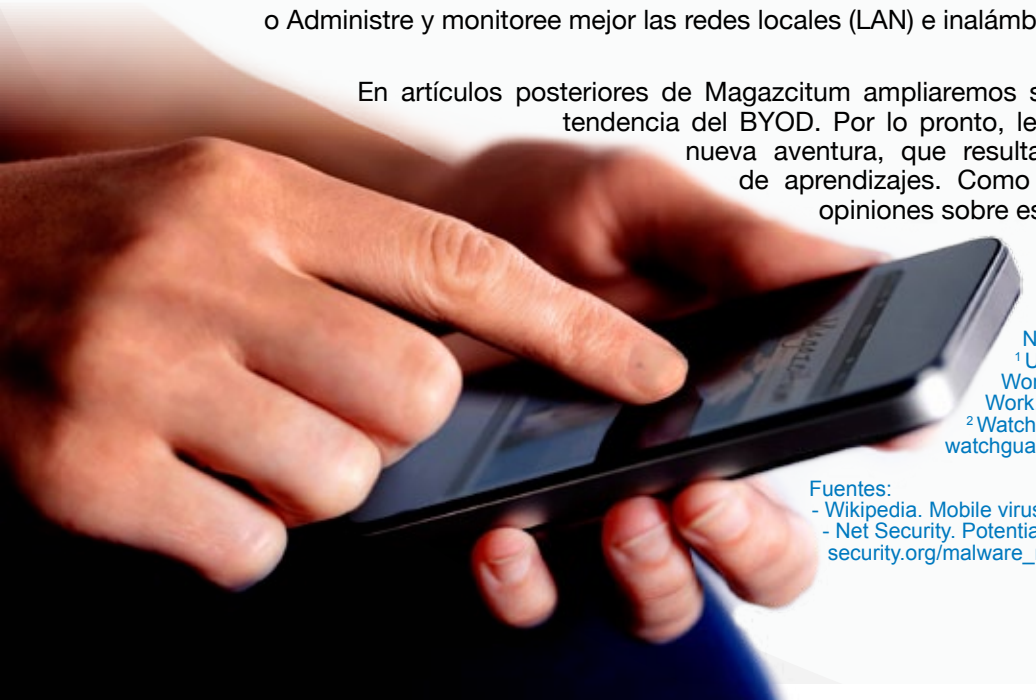
Algunas empresas en Estados Unidos y en el mundo han optado por autorizar el uso de estos dispositivos, aunque el nivel de aceptación no siempre es el mismo. Por ejemplo, de acuerdo al reporte de Ovum en Europa, 50% de las empresas estudiadas ya permiten que sus empleados utilicen el correo electrónico desde sus dispositivos personales, aunque solo un porcentaje pequeño de la misma muestra (6%) les da acceso completo a aplicaciones y datos de la red corporativa.

Por otro lado, dentro de las que lo permiten, hay algunas que le dan la libertad al empleado para que elija marca y modelo del dispositivo, siempre y cuando el empleado lo adquiera con sus recursos. Curiosamente esta medida ha sido bien recibida pues los empleados prefieren pagar por sus dispositivos a cambio de tener la libertad de escoger el que desean.

Permítame ahora darle algunas recomendaciones para sobrevivir mejor en este nuevo torbellino que se avecina con el BYOD:

» Empiece a revisar las soluciones de seguridad específicas que están surgiendo en el mercado, compárelas, analice a fondo los supuestos casos de éxito y considere que a veces los proveedores tienden a exagerar las bondades de sus productos o no explican bien las implicaciones de utilizarlos. Aquí le presento algunas preguntas que es bueno contestar:
  - o ¿Quién provee la solución? Algunas podrán venir de los proveedores de red, de proveedores de antivirus, de los propios proveedores de dispositivos o de las empresas de telefonía móvil. De acuerdo al tipo de proveedor puede esperar ciertas características tecnológicas y del servicio, así como ciertos enfoques. Por ejemplo, si es un proveedor de redes su interés es que TODO lo que usted compre sean dispositivos de esa marca.
  - o ¿Las soluciones son transparentes para los usuarios? En otras palabras, ¿qué tan visible es la solución para el usuario?, ¿este pierde funcionalidades o le resulta incómodo utilizarla? Si la solución es intrusiva su implementación será más difícil, a menos que usted trabaje en una organización tipo militar. Por ejemplo están surgiendo algunas que, utilizando tecnología de virtualización, le permiten manejar los dispositivos en dos modalidades: modo personal y modo corporativo. De esta forma, el usuario no perderá ninguna funcionalidad cuando utiliza su dispositivo para uso personal, pero tendrá ciertas restricciones cuando su función sea dentro de la red corporativa.
  - o ¿Qué tan amigable y completa es su capacidad de gestión y de seguridad? Es conveniente entender a fondo qué implicará la gestión de los dispositivos, tanto para el usuario como para el administrador, y a qué nivel se podrá establecer la seguridad. Algunos fabricantes de redes, por ejemplo, han lanzado recientemente productos con niveles de granularidad muy interesantes para ser aplicados a los dispositivos. Uno de ellos usa un enfoque "Aristotélico" al contestar a las preguntas: ¿Quién? ¿Qué? ¿Cuándo? ¿Dónde? ¿Cómo? Por ejemplo, hay que permitir que Chanchis (¿Quién?) pueda acceder al módulo de consultas del sistema ERP de la empresa (¿Qué?) todos los días y horas hábiles (¿Cuándo?) si está dentro de la red corporativa (¿Dónde?) con cualquier tipo de dispositivo (¿Cómo?).
  - o ¿Ante qué escenarios de riesgo me protege? Cada propuesta tecnológica contempla diversos escenarios de riesgo. Si los entiende bien tendrá una herramienta adicional de comparación. Por ejemplo, hace unas semanas le hice una pregunta a un proveedor, refiriéndome a la posibilidad de que un usuario avanzado (¿*hacker*?) pudiera saltarse el mecanismo de autenticación de su solución BYOD, y la respuesta honesta que recibí fue: "sí, eso es posible. Si quieres una autenticación a prueba de balas, tendrás que utilizar certificados digitales junto con nuestra solución".

» Mientras, vaya adelantando con otras labores que serán necesarias antes del BYOD.
  - o Controle sus PC e impresoras. Si –hoy por hoy- no tiene un buen control sobre sus computadoras personales (laptops y de escritorio) entonces el caos aumentará al agregar los dispositivos móviles. En lugar de pensar mucho en cómo podrá frenar al BYOD, le sugiero que empiece a inventariar sus equipos actuales (PC, laptops, impresoras, escáner, etc.) y a definir políticas de uso e implementar controles para reforzarlas. Ejemplos de controles son: instalar un antivirus en las PC y gestionarlo permanentemente, bloquear los puertos USB de todos o algunos equipos (ojo, este control hay que evaluarlo con mucha calma), homogeneizar versiones del sistema operativo, definir configuraciones seguras de los equipos y aplicarlas (lo que se denomina aseguramiento o "hardening" de configuraciones).
  - o Administre y monitoree mejor las redes locales (LAN) e inalámbricas de la empresa.



En artículos posteriores de Magazcitum ampliaremos sobre diversos aspectos de esta nueva tendencia del BYOD. Por lo pronto, le deseo la mejor de las suertes en esta nueva aventura, que resultará –creo yo- muy interesante y llena de aprendizajes. Como siempre, me encantaría escuchar sus opiniones sobre este tema.

Notas:
[1] Uno de los estudios es el de Tony Bradley en PC World: Pros and Cons of Bringing Your Own Device to Work.
[2] Watchgard Security Predictions 2012 [http://www.watchguard.com/predictions/index.asp]

Fuentes:
- Wikipedia. Mobile virus. [http://en.wikipedia.org/wiki/Mobile_virus]
- Net Security. Potential first Android bootkit spotted [http://www.net-security.org/malware_news.php?id=2051]

Ilustración: Silverio Ortega

El arte de incorporar la seguridad a los controles de acceso (primera parte)

Esteban San Román
CISSP, CISA y CEH
esanroman@scitum.com.mx

Cuenta la leyenda que para realizar sus actividades cotidianas los usuarios requieren acceso a una red donde comparten recursos como impresoras, digitalizadores o servidores de archivos; necesitan hacer uso de servicios de *groupware* como el correo electrónico y requieren de aplicaciones de negocio como un ERP (*Enterprise Resource Planning*) o un sistema de CRM (*Customer Relationship Management*). Seguramente para cada uno de esos sistemas hará falta su respectiva contraseña de acceso y, por si eso no fuera suficiente, las organizaciones se están viendo obligadas a trabajar más estrechamente con redes sociales como *Facebook, Twitter y Linkedin*, todas con contraseñas de acceso.

En la comunidad de TI estamos habituados a trabajar con contraseñas para cualquier sistema, muchos de nosotros tenemos varias cuentas de correo: la corporativa, la de nuestro(s) correo(s) personales, la de mensajería instantánea, la clave de acceso a un servidor universitario que solo mantenemos para "evocar viejos tiempos", los NIP de las tarjetas bancarias, claves para entrar al portal bancario o de algún fabricante y hasta para entrar a los sitios de organizaciones que respaldan nuestras certificaciones.

Como se puede notar, hemos ido complicando nuestra existencia al grado de que podemos manejar por persona cuando menos una docena de accesos diferentes, y para todos esos accesos nos solicitan construir contraseñas de al menos ocho caracteres, que incluyan caracteres alfanuméricos, mayúsculas y minúsculas, que haya por lo menos un caracter especial y además que no se reciclen.

Agregue a lo anterior que de acuerdo a las mejores prácticas, las políticas de contraseñas de acceso obligan a renovarlas cada treinta días en promedio, multiplique eso por el tamaño de la organización y el resultado es que se ha gestado un grave problema para el que aún no encontramos la solución.

Para complicar más las cosas hay que tomar en cuenta aspectos culturales, sociales y laborales. Por ejemplo, uno de mis clientes comenta que además de todo lo anterior, tiene que tomar en cuenta que él debe negociar con su sindicato porque entre sus prerrogativas está la de "salvaguardar los derechos" de sus trabajadores, lo cual lleva a tener estrictamente prohibido hacer cualquier sugerencia de seguridad que complique o atente contra su labor cotidiana.

¿Cuántos usuarios se preocupan por proteger adecuadamente sus accesos? ¿Cuántos más tienen las posibilidades de blindar realmente sus cuentas de acceso? Solemos ser predecibles, las contraseñas tienden a seguir un patrón y en muchos casos también a replicarse en varios sistemas, de manera que si uno de esos es interceptado, el usuario y la información que este maneja queda a merced de un potencial atacante no solo en el sistema inicial sino también en algunos otros.

Hay infinidad de artículos que se dedican al tema de ingeniería social, de ataques de "hombre en medio", de *phishing* o de uso de *sniffers* para husmear el tráfico en la red, con el fin de interceptar las claves de acceso de los usuarios. El resto de este artículo lo dedicaré a plantear las soluciones que hoy están disponibles para apoyar a una mejor administración de identidades desde el punto de vista de la seguridad de cómputo.

Ilustración: Silverio Ortega

Lo básico: identificación, autenticación, autorización y "*accountability*".

El proceso de acceso comienza con la "identificación" del usuario, que se realiza a través de una cuenta que le asigna el administrador del sistema y que usualmente se construye con la inicial del nombre del usuario y el apellido, al estilo *jperez*, pero pueden existir otras convenciones que la hagan menos predecible, combinando números, letras mayúsculas y minúsculas, algo similar a la manera en que solemos formar una contraseña, por ejemplo *MX03rj26*.

Controlar el acceso a los sistemas se ha vuelto una tarea compleja para los usuarios finales y un dolor de cabeza permanente para los administradores.

Una vez identificado el usuario, los sistemas piden que el mismo pruebe que es quien dice ser. A esta parte del proceso se le conoce como "autenticación" y la idea es contar con mecanismos de seguridad robustos para avalar el acceso; estos mecanismos suelen incluir *tokens*, tarjetas inteligentes o el apoyo de algún sistema biométrico.

La siguiente etapa, "autorización", se presenta una vez que el usuario tiene acceso a los sistemas y consiste en cotejar contra una matriz de usuarios y permisos si existen privilegios suficientes para el acceso a ciertos recursos y cuál es el nivel de autorización sobre los mismos.

Finalmente, derivado de todo el manejo que se efectúe sobre los recursos, los sistemas deben recabar, a través de un proceso llamado "*accountability*" (rendición de cuentas en español), toda la actividad que realiza el usuario: apertura, modificación, borrado de archivos, etcétera. Dicha actividad queda registrada en una bitácora o registro de auditoría.

Contraseñas (***passwords*** y ***passphrases***)

Los sistemas que requieren contraseñas (*passwords*) han evolucionado con el paso de los años, pasando de sistemas que aceptaban cualquier longitud, como por ejemplo "123", a sistemas que requieren de una longitud mínima con combinaciones de números, letras y caracteres especiales. Para facilitar el uso de contraseñas complejas, una alternativa en años recientes ha sido la incorporación de contraseñas compuestas a partir de varias palabras o *passphrases* que el usuario puede asociar con mayor facilidad y que a la vez complican el trabajo de quien quiere obtener acceso ilícito a sus cuentas.

Acceso de una sola vez (***single-sign-on***)

Al principio de este artículo planteé que conforme aumenta el número de sistemas a los que requiere acceder el usuario, es más complicado mantener una cultura de protección de contraseñas pues se tiende a replicar los accesos. Existen usuarios que guardan todas sus contraseñas en un archivo de su computadora que puede dañarse o ser copiado sin su conocimiento. En la práctica es muy difícil tener al mismo tiempo varias contraseñas complejas y es aún más difícil reemplazarlas cada treinta días como suelen dictar las mejores prácticas.

Por lo anterior surgieron las soluciones de acceso de una sola vez, que permiten el acceso a varios sistemas con un mismo proceso de autenticación, de manera que el esfuerzo de administración se realice en un solo lugar. Un ejemplo de esto es Kerberos.

Kerberos

Es un popular sistema de autenticación de una sola vez que fue diseñado por el MIT a mitad de los ochenta para autenticar dos servidores a través de criptografía simétrica y un tercer servidor en el que ambos confiaran. Kerberos funciona de forma muy parecida a los parques temáticos de diversiones donde el usuario tiene un acceso principal y una vez dentro tiene que obtener boletos (*tickets*) para hacer uso de diferentes recursos (una impresora de calidad, un escáner, un servidor de archivos, etcétera). Los boletos se asignan en función de los privilegios asignados al usuario en cuestión y tanto los usuarios como los servicios dentro del parque confían unos en otros porque hay una taquilla general (el tercero) en la que ambos confían.

Federación de identidades.

La federación de identidades es una forma de fomentar la interacción de diferentes entidades dentro del comercio electrónico en beneficio de los consumidores; por ejemplo, cuando una persona está planeando sus vacaciones y entra al portal de un proveedor de servicios, este, a su vez, está realizando las conexiones a otros sistemas para armar un propuesta completa: el portal bancario para realizar la transferencia, la línea aérea, el hotel, una agencia de renta de automóviles y sitios para comprar boletos de las diferentes atracciones del destino turístico. Con estas opciones los costos de operación bajan y se pueden armar ofrecimientos integrales donde todos ganan.

Biometría

Cuando se habla de esta disciplina queda la idea de que aún tiene mucho de ciencia ficción, pero hoy están disponibles varias modalidades que enumero a continuación:

» **Huella digital** - Reconoce puntos únicos dentro de la digitalización de las huellas digitales. Muchos piensan que la imagen de la huella digital es fácilmente replicable pero en los dispositivos de hoy se manejan algoritmos matemáticos muy elaborados y se requiere la presencia del usuario para que el sistema intente siquiera autenticarlo.

» **Escaneo de retina** - Inspecciona la distribución de los vasos sanguíneos del globo ocular para hacer el reconocimiento del individuo. Este también es un método con un alto nivel de aceptación.

» **Escaneo de iris** - Funciona mediante la identificación de patrones únicos dentro de la composición del iris, que es una característica única de cada persona.

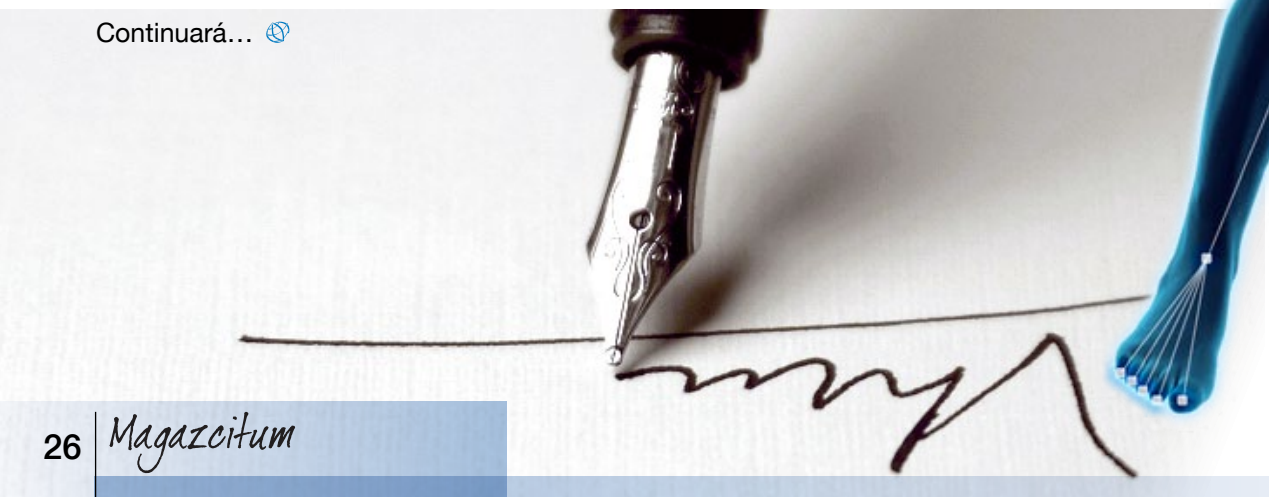
» **Escaneo de la voz humana** - Estos sistemas registran y comparan las frecuencias únicas que emite cada ser humano con su voz y que no pueden ser replicadas ni por el mejor imitador.

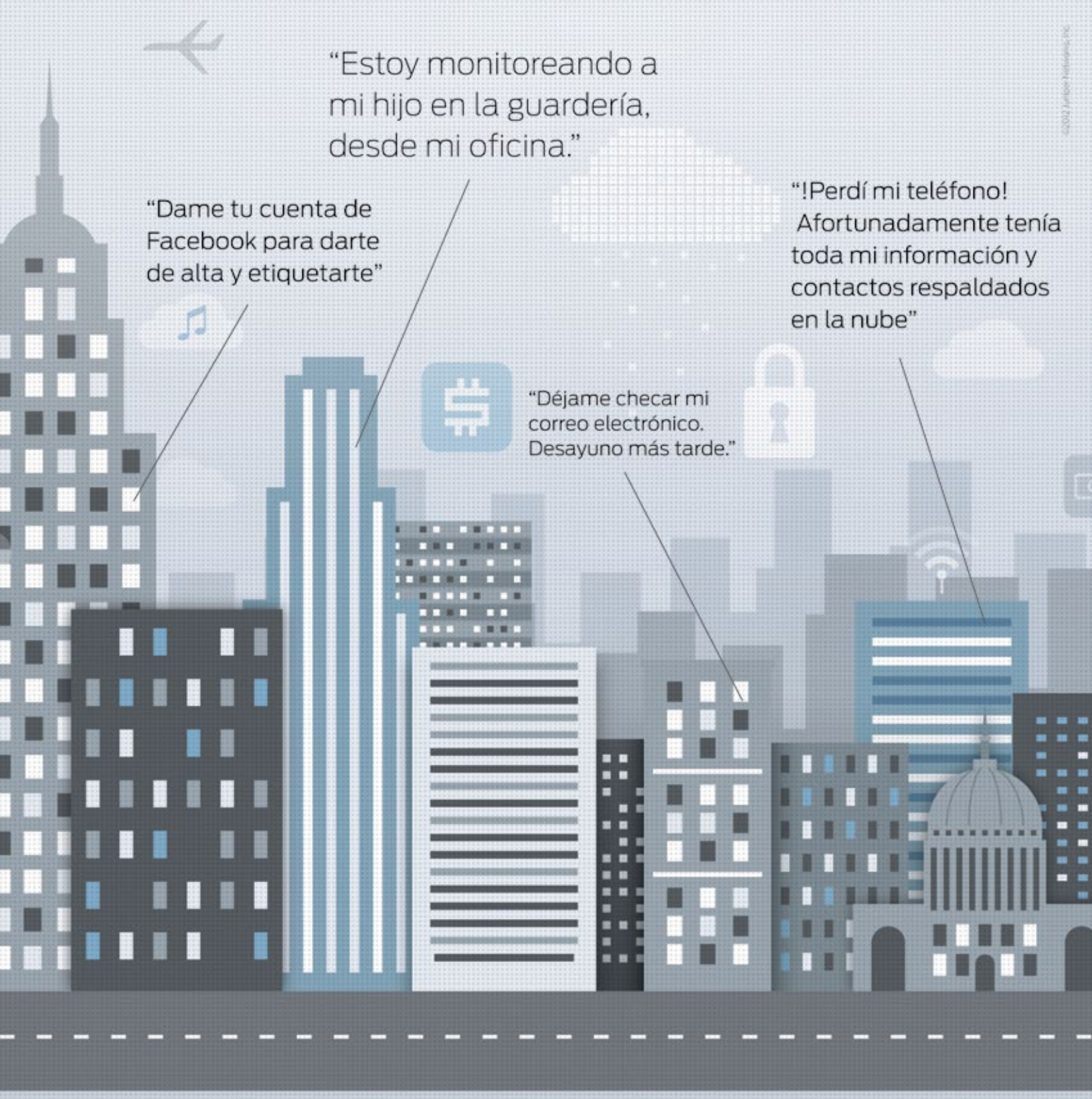
» **Comportamiento en la escritura** - Una forma reciente de reconocer al usuario es la que se realiza a través de la identificación de la presión que se hace al escribir y también la forma en que hacen ciertos trazos.

» **Comportamiento por movimientos** - Los usuarios pueden autenticarse pasando por tapetes que identifican características únicas como la amplitud de la apertura de sus pasos.

En mi siguiente colaboración continuaré revisando algunas soluciones adicionales que apoyan el control de acceso. Entre ellas escribiré sobre la administración de identidades, las bóvedas de contraseñas y el estándar *OpenID* para autenticación descentralizada de usuarios.

Continuará…





AHORA QUE TODO EL MUNDO HABLA DE TECNOLOGÍA, QUIZÁ ES EL MOMENTO DE EMPEZAR A HABLAR DE LA RED.

Desde habilitar servicios de próxima generación hasta contar con una nube más segura, "La Nueva Red" permite que la innovación suceda todos los días para empresas de todo el mundo. Descubre en **juniper.net** lo que "La Nueva Red" puede hacer por tus empleados, tus clientes y por lo que es más importante para tí.

"La nueva red" significa negocios.

JUNIPER NETWORKS

Contacto: **Vladimir Lopez Araiza;** valopez@juniper.net; +52 1 55 43444266

En el pensar de...

Eduardo P. Sánchez Díaz
CISSP, CISM, GCIH, GWAPT, CEH y CHFI
epsanchez@scitum.com.mx

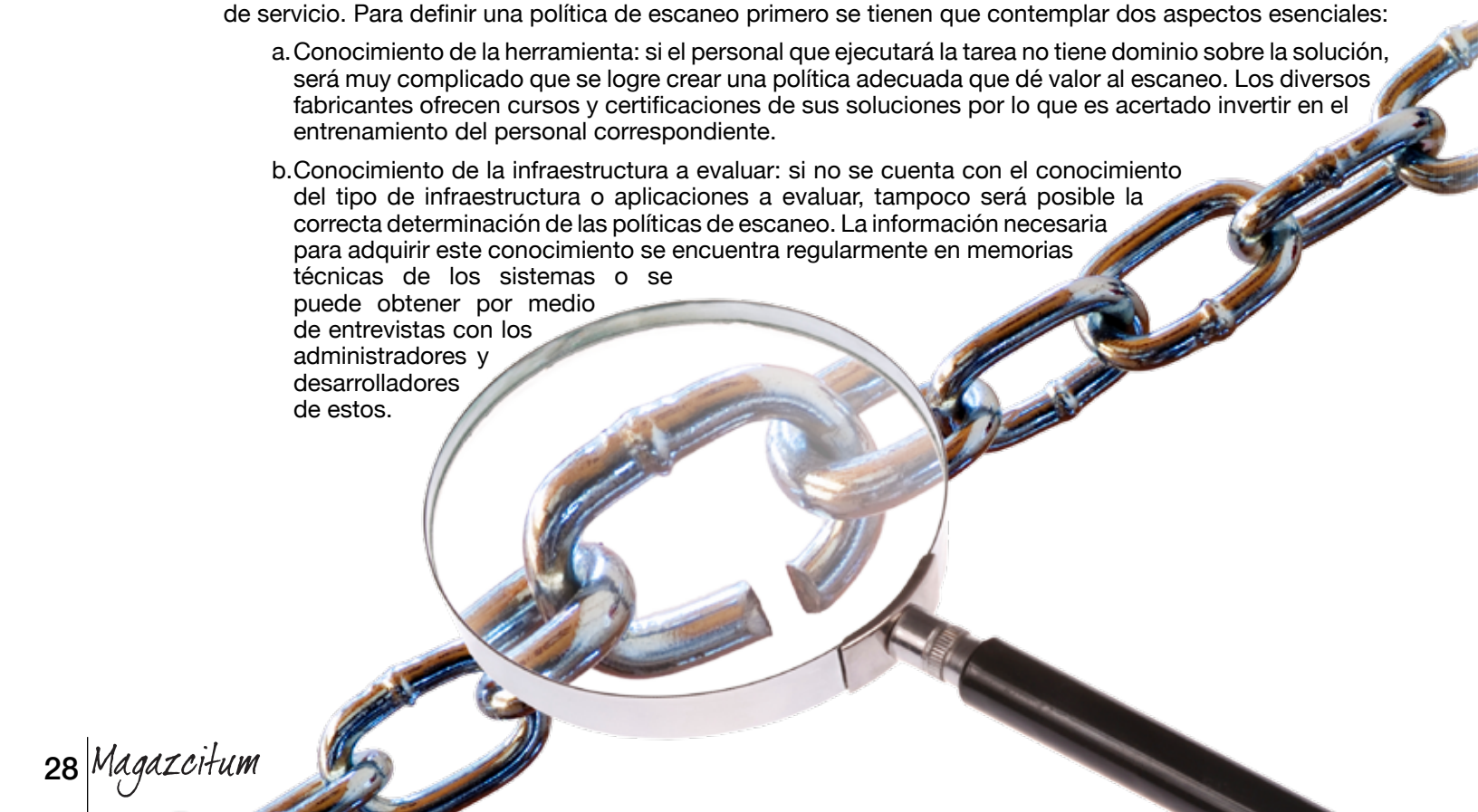
Retomando el valor de un análisis de vulnerabilidades

Cuando se habla de análisis de vulnerabilidades, también denominado AV, regularmente se asocia a la ejecución de una herramienta automatizada que detecta vulnerabilidades conocidas y cuando alguien me pregunta ¿Mi infraestructura necesitará un análisis de vulnerabilidades?, siempre trato que entre ambos tomemos en cuenta algunas consideraciones.

Un análisis de vulnerabilidades es más que la ejecución de una herramienta automatizada, es parte fundamental del proceso de administración de vulnerabilidades y no debe verse como un ente aislado; pero ¿Qué pasa si en mi organización no existe un proceso formal de administración de vulnerabilidades? En este caso hay que entender primeramente cuáles son las necesidades en la organización para requerir un estudio de este estilo, lo cual es importante para poder obtener el máximo beneficio.

Las necesidades pueden surgir del cumplimiento de alguna regulación o tal vez de la liberación a producción de infraestructura y aplicaciones, sin embargo en muchas ocasiones sigue siendo complicado lograr visualizar nuestra verdadera necesidad. Al contratar a un proveedor para que realice el servicio, o incluso si compramos una herramienta para realizarlo de forma interna, frecuentemente nos sentimos frustrados porque el resultado no es lo que esperábamos. Para evitar estas situaciones, quiero mencionar algunos puntos que, desde mi perspectiva, es recomendable examinar:

1. Una herramienta automatizada contiene un conjunto de pruebas definidas. A estos conjuntos se les conoce como perfiles o políticas de escaneo. Estas varían de acuerdo al fabricante tanto en cantidad como en eficiencia de detección y es importante poner atención en el tipo de perfil que cubra mejor las necesidades de evaluación de vulnerabilidades.
2. La ejecución de una herramienta de esta índole lleva siempre asociado un tiempo de afinación para lograr los objetivos planteados. Considero primordial no perder de vista este punto y para ilustrar el porqué de mi consideración, les comento que al realizar pruebas de laboratorio para probar funcionalidades de herramientas de escaneo de vulnerabilidades, en 70% de los casos se elevan exponencialmente los falsos positivos cuando se usan políticas genéricas de escaneo, además de que el riesgo de impactar la operación siempre es más alto puesto que hay pruebas que conllevan el riego de generar una situación de denegación de servicio. Para definir una política de escaneo primero se tienen que contemplar dos aspectos esenciales:
    a. Conocimiento de la herramienta: si el personal que ejecutará la tarea no tiene dominio sobre la solución, será muy complicado que se logre crear una política adecuada que dé valor al escaneo. Los diversos fabricantes ofrecen cursos y certificaciones de sus soluciones por lo que es acertado invertir en el entrenamiento del personal correspondiente.
    b. Conocimiento de la infraestructura a evaluar: si no se cuenta con el conocimiento del tipo de infraestructura o aplicaciones a evaluar, tampoco será posible la correcta determinación de las políticas de escaneo. La información necesaria para adquirir este conocimiento se encuentra regularmente en memorias técnicas de los sistemas o se puede obtener por medio de entrevistas con los administradores y desarrolladores de estos.



3. Se debe comprender el contexto en el cual se realiza el ejercicio; no es lo mismo ejecutar una herramienta en red interna estando en el mismo segmento de red de los sistemas objetivo, que escaneo desde Internet o detrás de infraestructura de seguridad. Cada uno de estos escenarios brinda una visión diferente que no necesariamente es descartable, al contrario, serán complementarias dentro de un servicio integral. Para ejemplificar el punto supongamos que se realiza un AV con acceso total a los sistemas y esto proporciona una determinada cantidad de hallazgos x; ahora, al ejecutar el mismo análisis desde un nodo de red de usuarios normales nos enfrentamos a diversos controles como *firewalls* e IPS, y esto descubre una cantidad de hallazgos y (los cuales típicamente deberían ser menores). Contando con estas dos visiones es posible priorizar de una manera más eficaz los hallazgos detectados.
4. Todo hallazgo se clasifica de acuerdo a su impacto y muchas de las herramientas disponibles comercialmente usan *Common Vulnerability Scoring System* versión 2 (CVSS v2) como escala de graduación. Este sistema contempla tres métricas para valorar el impacto de una vulnerabilidad; la más común se llama *Base Score* y considera factores como el vector de ataque, complejidad, nivel de acceso e impacto sobre confidencialidad, integridad y disponibilidad. De acuerdo con un cálculo matemático el *Base Score* arroja un valor que finalmente determina si la vulnerabilidad debe catalogarse de impacto alto, medio o bajo. No obstante que este valor permite clasificar los hallazgos, siempre es recomendable conocer el contexto del hallazgo, por ejemplo, si al ejecutar un escaneo se detecta una vulnerabilidad con *Base Score* 9.2 Critical, pero nos percatamos de que el código que aprovecha dicha vulnerabilidad (*exploit*) es privado y, además, cuando se realiza un escaneo desde Internet se evidencia que el IPS bloquea dicha actividad, entonces, aunque CVSS señala que es de impacto crítico, no forzosamente es de prioridad alta de atención para la organización.
5. La mayoría de las herramientas modernas tienen diversos enfoques al realizar un escaneo. A continuación listo los más comunes:
    a. Escaneo de puerto y servicios: permite la identificación de puertos TCP/UDP y detecta los servicios o demonios que están en ejecución.
    b. Escaneo de vulnerabilidades: de acuerdo a los servicios detectados, las herramientas cuentan con un *set* de pruebas que validan las vulnerabilidades conocidas para ese servicio y determinan también la falta de actualizaciones de seguridad.
    c. Escaneo de vulnerabilidades con privilegios: mediante un usuario con privilegios de administración o la instalación de un agente, la herramienta puede conectarse al sistema y realizar una auditoría de configuración de manera interna. Un escaneo de este tipo lleva a cabo una revisión con más profundidad, incluso de contenidos dentro de los sistemas.
    d. Escaneo de cumplimiento: como parte de las políticas de escaneo se pueden configurar para efectuar validaciones de cumplimiento respecto de regulaciones como PCI, SoX, HIPAA o incluso normatividad de la organización.
    e. Inventario de *software*: permite realizar un inventario del *software* instalado en el sistema. En muchas ocasiones esto ayuda a validar si existen componentes como antivirus instalados en los equipos y su nivel de actualización.

Al conocer estos aspectos, se cuenta con una visión más clara de lo que se puede esperar de un estudio de análisis de vulnerabilidades y de esta manera ser más específicos en la solicitud de requerimientos hacia proveedores de este tipo de servicio, ya sean internos o externos, además de que permite estar en posición de exigir mejores resultados.

Desde la trinchera

Marcos Polanco
CISSP, CISM y CISA
mpolanco@scitum.com.mx

Súperusuarios: el talón de Aquiles de la seguridad

Cuenta la mitología griega que cuando Aquiles nació se predijo que moriría en una batalla, por lo que su madre lo baño en un río que le daría el poder de ser invencible, pero como lo sostuvo del talón al sumergirlo, esa parte de su cuerpo no fue tocada por el agua. Aquiles peleó y sobrevivió muchas batallas grandiosas, pero un día una flecha envenenada dio justo en el talón, causándole la muerte.

Cuando pienso en los usuarios privilegiados -mejor conocidos como súperusuarios- siempre viene a mi mente esta historia y no puedo evitar pensar que la falta de gestión de los súperusuarios es el talón de Aquiles de la seguridad.

Derivado de lo anterior, me surgen algunas preguntas: ¿Es que ahora ya no confiamos en los administradores?, ¿hasta dónde se debe confiar en los usuarios privilegiados?, ¿están ocurriendo cambios alrededor de este tema?

En los últimos años nos hemos enfocado con gran dedicación a proteger las diversas capas de infraestructura (perimetral, red interna, bases de datos, aplicaciones, etcétera) pero no hemos hecho lo mismo con la capa más interna donde precisamente están los administradores de los sistemas. Si analizamos fríamente, siempre hemos reconocido que las amenazas más importantes y de mayor impacto están en los usuarios internos, sin embargo la prioridad se ha enfocado más a protegerse de los externos porque estos representan un mayor volumen y sus ataques tienen mucha más visibilidad.

Pero, ¿qué riesgos realmente implican los usuarios privilegiados? Antes de responder esta pregunta, recordemos que un usuario privilegiado es aquel que tiene más permisos que cualquier otro usuario, y que si bien los requieren para hacer su trabajo, suelen darle acceso a partes críticas, sensibles o incluso a todo el sistema. Es como tener la combinación de la caja fuerte donde se guardan las joyas de la corona.

De manera general podemos identificar amenazas tales como abuso de privilegios, errores y malas configuraciones (como usar las contraseñas por omisión para las cuentas de administración), las cuales pueden derivar en robo de información, inserción de código malicioso (intencional o no), indisponibilidad de los sistemas, etcétera.

Como resultado de esta problemática, ha surgido un concepto denominado “Gestión de Usuarios Privilegiados”, que durante el último año ha generado más y más interés debido a cambios en el entorno de los usuarios y de los fabricantes.

Por el lado de los usuarios, en casi todas las organizaciones ahora existe mayor conciencia sobre el tema de seguridad y también hay más conocimiento sobre el riesgo que representan los usuarios privilegiados; en la mayoría se evidencia una gran preocupación por prevenir fugas de información, además de que hay diversas regulaciones que deben cumplir o estándares que se deciden seguir y que solicitan de manera explícita una adecuada gestión de usuarios privilegiados (por ejemplo la Ley Federal de Protección de Datos Personales en Posesión de Particulares, regulaciones de la CNBV, PCI, SOX, ISO27001, etcétera) .

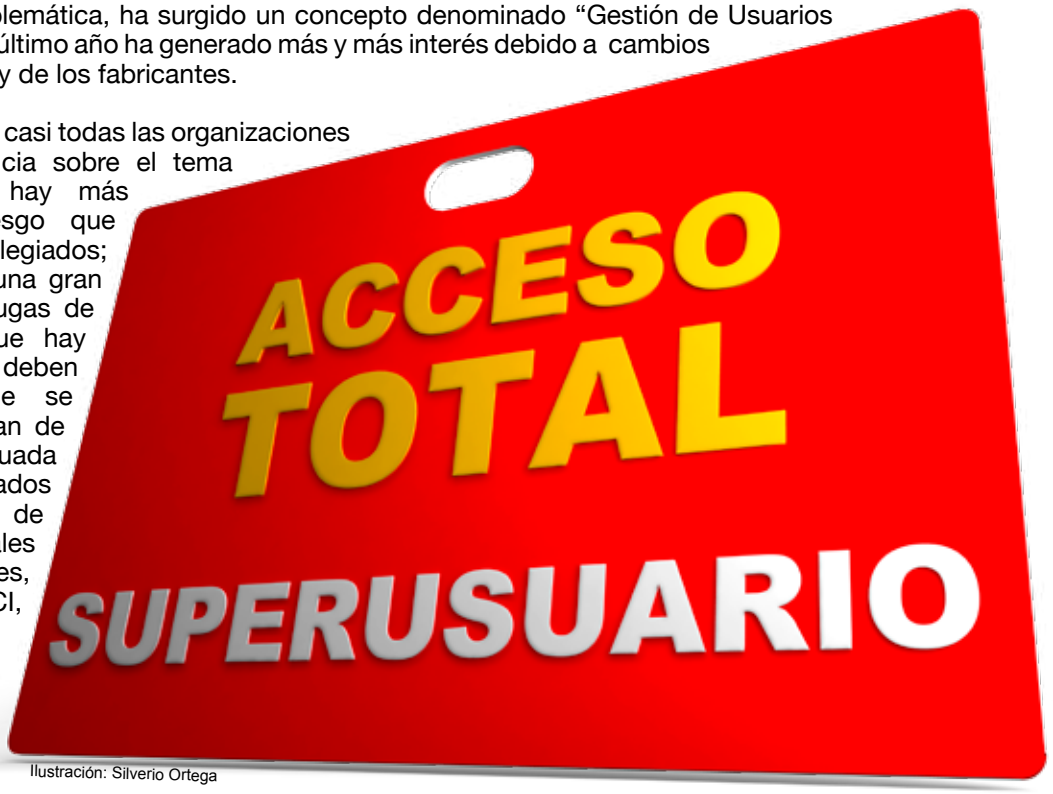


Ilustración: Silverio Ortega

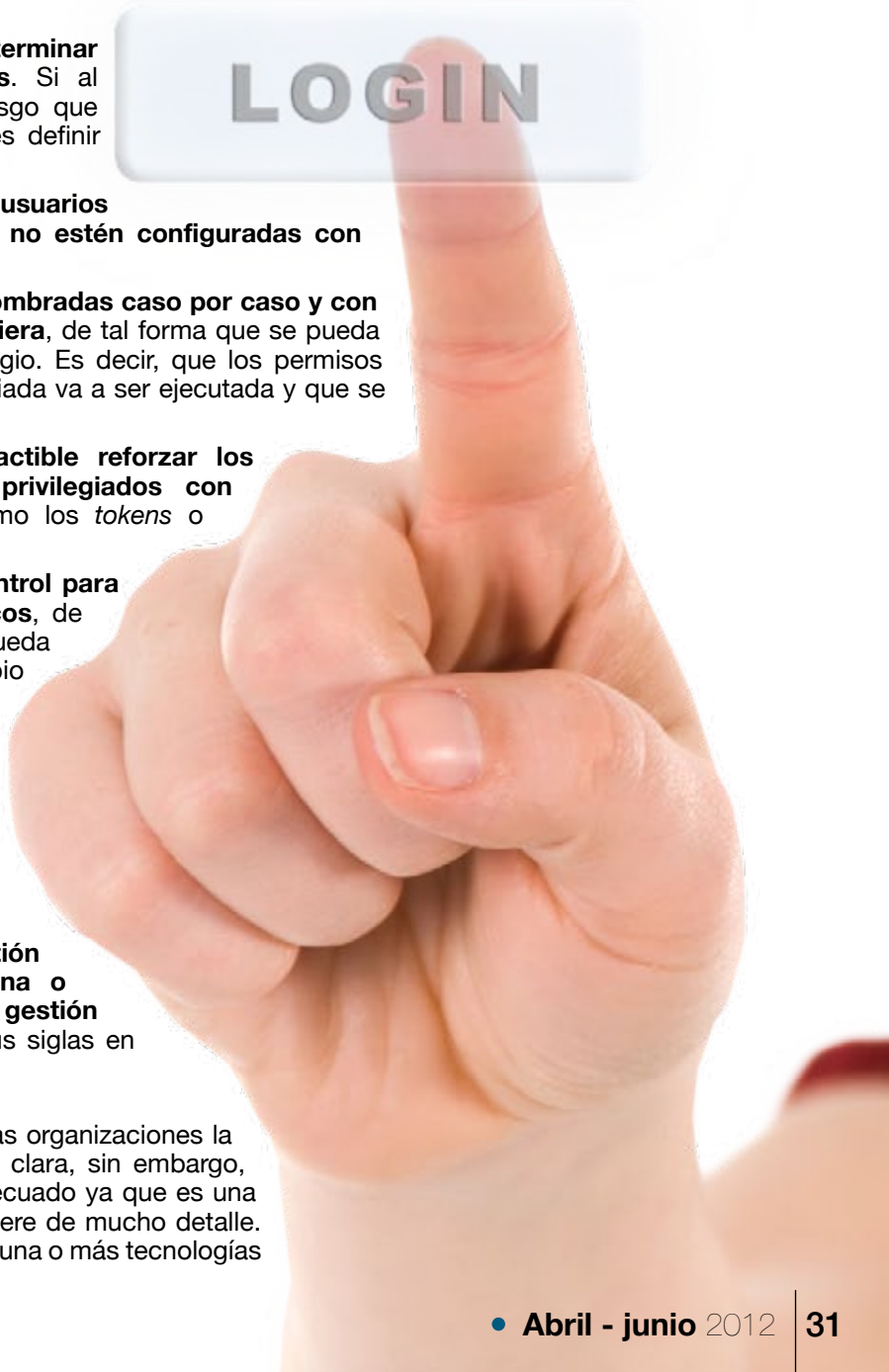
En lo que se refiere al entorno de los fabricantes, ya se encuentran en el mercado productos para la gestión de usuarios privilegiados que son suficientemente maduros para implementarse en un ambiente de producción.

Bueno y, ¿qué es y para qué sirve la gestión de usuarios privilegiados? Tiene como objetivo permitir que los súperusuarios realicen sus labores cotidianas pero bajo un ambiente controlado, es decir, apegado a las políticas establecidas, monitoreado y auditado. Consiste en:

- **Controles normativos** que incluyen políticas y procedimientos que establezcan claramente quién, qué, cuándo y dónde se pueden usar comandos o permisos de súperusuario, tratando de apegarse a buenas prácticas de seguridad como la segregación de funciones o de privilegio mínimo (*least privilege*), así como el uso de políticas de contraseñas robustas.
- **Controles tecnológicos y operativos** que permitan traducir esas políticas en mecanismos para definir qué comandos y bajo qué condiciones se ejecutan, para monitorear todas las actividades realizadas y para auditar en cualquier momento las acciones tomadas por cualquier administrador.

Estos controles pueden aplicarse a todos los niveles, es decir, a nivel sistema operativo, bases de datos, aplicaciones, equipos de redes e, inclusive, a los propios sistemas de seguridad.

A continuación presento algunas consideraciones a tomar en cuenta para la correcta implementación de una estrategia de gestión de usuarios privilegiados:



- **Iniciar con un análisis de riesgos y determinar realmente en qué situación estamos**. Si al hacerlo se considera que existe un riesgo que debe ser atendido, entonces lo mejor es definir una estrategia de mitigación integral.
- **Analizar las cuentas de los usuarios privilegiados para asegurarse de que no estén configuradas con valores por omisión o de fábrica**.
- **Asignar los privilegios a las cuentas nombradas caso por caso y con la granularidad especifica que se requiera**, de tal forma que se pueda garantizar el principio del mínimo privilegio. Es decir, que los permisos se otorguen cuando la operación privilegiada va a ser ejecutada y que se remuevan cuando ya no se requieran.
- **En caso de sistemas críticos es factible reforzar los sistemas de gestión de usuarios privilegiados con sistemas de autenticación fuerte** como los *tokens* o sistemas OTP (*one time password*).
- **Considerar la posibilidad de doble control para sistemas sensibles y comandos críticos**, de tal forma que una sola persona no pueda ejecutar la transacción completa (principio de segregación de funciones).
- **Asegurarse de que cada operación privilegiada ejecutada se registre en una bitácora** que posteriormente pueda ser auditada e, inclusive, ser enviada a un sistema de correlación para un monitoreo de seguridad proactivo.
- **Analizar cómo la estrategia de gestión de usuarios privilegiados se relaciona o integra con la estrategia general de gestión de identidades y accesos** (IAM, por sus siglas en inglés) de la organización.

Como conclusión, diremos que para la mayoría de las organizaciones la gestión de usuarios privilegiados es una necesidad clara, sin embargo, pensar en procesos manuales no es un enfoque adecuado ya que es una actividad sumamente compleja, sensible y que requiere de mucho detalle. Lo mejor es utilizar un enfoque integral soportado por una o más tecnologías específicas.

Demos claridad y orden a la oferta en el mercado

José Juan Cejudo Torres
jjcejudo@scitum.com.mx

En la edición pasada de Magazcitum se abordaron dos temas que son parte del amplio espectro de servicios de seguridad en la nube (SecaaS): protección Web y protección de correo electrónico, y fue lo que me motivó a escribir sobre la oferta de servicios de este tipo, que, de acuerdo a Gartner crecerán a más del triple para 2013[1], para tener un visión general, saber dónde estamos parados y no perdernos en el mar de posibles servicios que con el genérico X-aaS puedan surgir en los próximos meses.

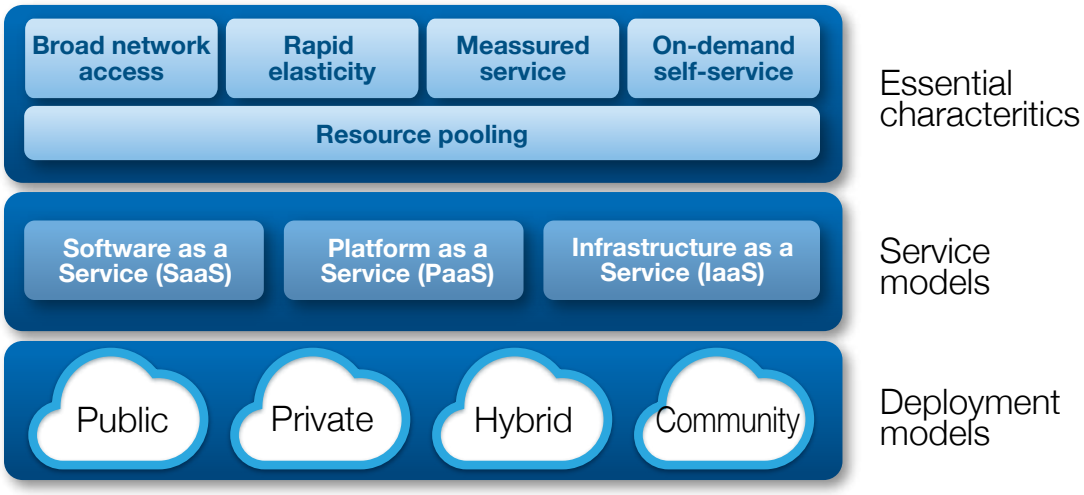
Un poco de historia: en noviembre de 2008 en el foro *ISSA CISO* (*Information Systems Security Association-Chief Information Security Officer*) de Las Vegas nació el concepto del *Cloud Security Alliance* (CSA) como una llamada a la acción para asegurar el cómputo en la nube. Una serie de encuentros en el cercano diciembre de 2008 formalizó la creación de la CSA como una organización sin fines de lucro formada para promover el uso de las mejores prácticas y proveer garantías de seguridad en la nube. Sus principales objetivos son:

- Promover niveles comunes de entendimiento entre los consumidores y proveedores de cómputo en la nube relacionados con los requerimientos de seguridad y certificados de garantía.
- Promover desarrollos independientes dentro de las mejores prácticas para la seguridad del cómputo en la nube.
- Poner en marcha campañas de concientización y programas educacionales sobre el uso apropiado del cómputo en la nube y soluciones de seguridad en el mismo entorno.
- Crear consenso y directrices para garantizar la seguridad en la nube[2].

Como ya se asentó en otros artículos, a partir de las definiciones del NIST (*National Institute of Standards and Technology*) y la CSA, se generó el modelo visual del cómputo en la nube, que comprende tres modelos de servicio: *software* como servicio (*software as a service*, SaaS), plataforma como servicio (*platform as a service*, PaaS) e infraestructura como servicio (*infrastructure as a service*, IaaS).

Visual Model of NIST Working Definition of Cloud Computing

http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html



Este modelo es el que la CSA emplea en las definiciones de servicios de la nube y en el Dominio 1 (marco de la arquitectura de cómputo en la nube) de su Guía para la Seguridad en Áreas Críticas de Atención en *Cloud Computing*[3].

¿Por qué el desarrollo de estas definiciones y categorías?

Los clientes que evalúan y observan la proliferación de servicios en la nube encuentran gran motivación por las oportunidades que en disminución de costos pueden representar dichos servicios, además del aliciente para pasar de ser administradores de infraestructura a dedicarse a lo que saben hacer: explotar sus fortalezas y habilidades. Sin embargo, por otro lado está la preocupación por la pérdida de control directo sobre los sistemas de seguridad.

Algunos fabricantes ya están intentando satisfacer esta demanda ofreciendo servicios de seguridad en la plataforma, lo que se manifiesta en una gran variedad de formas que poco a poco han venido a generar más confusión que claridad en el mercado. Es aquí donde cobra importancia la *CSA* proveyendo orden sobre los campos de acción de la SecaaS (*security as a service*) y sus modos de entrega.

De acuerdo a un artículo anterior de Magazcitum, la SecaaS es “la implementación de controles de seguridad que son entregados y gestionados a través de infraestructura tecnológica, operativa y física perteneciente al proveedor” y dado que los clientes están ahora evaluando más críticamente la oferta, necesitan comprender la naturaleza única de servicios basados en la nube, por ello a continuación presento una revisión de las áreas de SecaaS definidas por la CSA:

- **Administración de identidades y acceso** (identity and access management, IAM)**.**
- **Prevención de pérdida de datos** (data loss prevention, DLP)**.**
- **Seguridad Web** (Web security).
- **Seguridad de correo electrónico** (email security)**.**
- **Auditoría de seguridad** (security assessments).
- **Administración de intrusos** (intrusion management).
- **Administración de eventos y seguridad de la información** (*security information and event management*, SIEM).
- **Cifrado** (encryption).
- **Continuidad del negocio y recuperación de desastres** (*business continuity and disaster recovery*).
- **Seguridad de la red** (*network security*).

Ilustración: Silverio Ortega

Muchas de ellas son ya conocidas como servicios internos, pero ¿Cómo pueden ser ofertadas en la nube? Describiré brevemente cada categoría y me concentraré en los puntos más relevantes de cada una.

Administración de identidades y acceso (identity and access management, IAM)[4,5]

Este servicio debe proveer todos los controles que aseguren la identidad y la administración de accesos. Incluye la gente, los procesos y los sistemas que típicamente son empleados para ingresar a los recursos de las empresas, de manera que la identidad es verificada y los permisos son otorgados en el nivel adecuado.

Los proveedores actuales de este servicio ofrecen soporte a integraciones con sistemas de directorio activo, *kerberos*, *Radius* y otros. Los registros de la actividad derivada de este servicio -como son autenticaciones exitosas o fallidas, por ejemplo- son parte esencial de la garantía que un proveedor puede brindar a su cliente ya sea como parte de los niveles de servicio acordados o con fines de cobro en la modalidad pago por consumo, tan típica en los modelos en la nube.

Prevención de pérdida de datos (data loss prevention, DLP)

Esta modalidad se encarga de verificar la seguridad, monitorear y proteger la información (o datos) en cualquiera de sus estados (en reposo o en movimiento), si son usados en equipos dentro de las instalaciones de la empresa o en la nube. Esta protección de datos se basa en reglas definidas de movimiento de la información, tales como capacidad de copiar o no información en unidades de almacenamiento externas, permiso para mover información de un equipo a otro, realizar el cifrado de la información, entre otras muchas.

Seguridad Web (Web security).

Explicada con amplitud en la edición pasada de Magazcitum, la protección en la navegación Web protegida con este esquema agrega una capa de seguridad, previniendo el ingreso o navegación a sitios con contenido malicioso, paginas con *phishing* o *malware*, y controlando sistemas de mensajería y chat en sus diversas modalidades, etcétera.

La entrega se hace por software o por *hardware* en las instalaciones del proveedor o vía la nube a través de la implementación de *proxy* o redirección de tráfico. La administración de ancho de banda y el control de tráfico son otras de las actividades de gran relevancia en las empresas y de las cuales el servicio de Web *security* se hace cargo.

Seguridad de correo electrónico (email security)

La protección en este nivel controla el tráfico entrante y saliente de correo, previniendo anexos maliciosos, cadenas de correos, ingreso a páginas de *phishing* por cadenas publicitarias y proporciona algunas opciones para asegurar la continuidad del servicio de correo electrónico.

La solución puede permitir además el cifrado basado en políticas, uso de firma digital para identificación y no repudiación, además de complementarse con esquemas de seguridad como DLP.

Auditoría de seguridad (security assessments)

Este servicio brinda, desde soluciones provistas en la nube, evaluaciones a los servicios en la nube o a los sistemas de los clientes, obviamente con estricto apego a estándares. Como es sabido, los análisis de seguridad se conforman -de entre muchas otras actividades- con pruebas de penetración y análisis de vulnerabilidades. Los análisis tradicionales están avalados por estándares como NIST*, ISO* o *CIS* y las herramientas empleadas están relativamente maduras.

Este servicio analiza puntos muy sensibles de cómo se entregan los servicios en la nube y permiten demostrar cómo se asegura el aislamiento de los datos y servicios en ambientes de multi-arrendamiento.

Administración de intrusos (intrusion management)

Con base en el reconocimiento de patrones, este servicio detecta y reacciona a eventos inusuales en la red. En caso de que un patrón sospechoso sea captado, se puede realizar la reconfiguración de componentes para detener o prevenir intrusiones. También se puede incluir el análisis de comportamientos con plataformas de protección contra ataques de DoS o DDoS.

Las tecnologías disponibles ya están muy maduras, sin embargo el crecimiento de entornos virtualizados o entornos de arrendamiento masivos imponen nuevos retos respecto a nuevos objetivos de intrusión y a las arquitecturas de implementación. Este servicio lo puede brindar el proveedor de servicios, un tercero ruteando tráfico por la infraestructura de SecaaS, o en un esquema "híbrido", administrado por un tercero y basado en dispositivos virtuales corriendo en el contexto de la nube.

Administración de eventos y seguridad de la información (security information and event management, SIEM)

Los sistemas *SIEM* son herramientas que recolectan información acerca de la operación de los equipos y sistemas en el entorno de red de una empresa; esto puede incluir desde equipos de interconectividad hasta aplicaciones propietarias o soluciones *ERP*. Una vez recolectados los datos, se almacenan como eventos, y son analizados y correlacionados entre ellos para proveer reportes en tiempo real o alertas sobre eventos de seguridad que eventualmente requieran intervención para iniciar un proceso de manejo de incidentes.

Resulta relevante mantener íntegra la información que estos sistemas recolectan, a fin de que sea empleada como evidencia en investigaciones o auditorías de cumplimiento. La retención por largos periodos, tal como es requerido por la mayoría de las regulaciones, implica uno de los retos importantes a solventar.

Cifrado (encryption)

Este es básico para mantener la CIA (confidencialidad, integridad y disponibilidad) de los datos almacenados en la nube y apoya a otros servicios como validación de datos, autenticación de mensajes, integridad de datos y mensajes, firma de código, validación de identidad y detección de falsificaciones, entre otros.

En el mercado hay una gran cantidad de ofertas y en algunos casos el cifrado como servicio (*EaaS*) es ofrecido desde los propios fabricantes.

Ilustración: Silverio Ortega

Continuidad del negocio y recuperación de desastres (business continuity and disaster recovery)

Todos los esfuerzos orientados a asegurar la operatividad del negocio ante cualquier circunstancia causal de interrupción conforman el servicio de continuidad del negocio y recuperación de desastres.

Un plan BC/DR centrado en servicios en la nube aprovecharía naturalmente la flexibilidad de crecimiento o demanda de servicios en un caso de contingencia, reduciendo el costo de implementación. Los escenario típicos incluyen replicación de aplicaciones o datos en la nube, recuperación de información o respaldo de bases de datos, información de bitácoras y cumplimiento, respaldos seguros, conectividad a servicios de terceros, replicación de datos, sitios de operación alternos, infraestructura o centros de datos distribuidos geográficamente.

Los servicios de alojamiento administrado no son nuevos, han ido evolucionando y han encontrado, válgase la expresión, "acomodo" en el escenario del cómputo en la nube.

Seguridad en la red (network security)

La seguridad en la red se enfoca principalmente en la infraestructura que protege los servicios de una empresa, dando accesos y controlándolos. En un entorno dentro de la nube estos servicios pueden ser proporcionados a través de equipos tanto físicos como virtuales disponibles en las instalaciones del proveedor.

La completa visibilidad con el *Hipervisor* sería fundamental para dominar todo el tráfico del segmento virtual a fin de proveerle seguridad con tareas como la administración de los *gateways* de seguridad (*firewalls*), protección y mitigación contra *DoS* o *DDoS*, monitoreo de tráfico, controles de autenticación y acceso, aseguramiento de servicios como *DNSSec*, *DNS, NTP, RAS, DHCP* y la propia integración con el *Hipervisor*.

Hay muchos retos para este servicio ofrecido en la nube, como la exacta delimitación de las fronteras entre un cliente y otro, mayormente en entornos virtuales, y la visibilidad limitada del tráfico entre entornos virtuales, por ejemplo cuando se encuentran ambientes productivos y no productivos.

Conclusión

Al buscar una solución de *SecaaS* es obligado preguntar tanto a los proveedores como a los clientes los pros, contras y alguno que otro dato más del ámbito de administración de riesgos o de negocio que seguramente ambos deberían responder, de preferencia de manera conjunta.

El cliente tendría que preguntar como mínimo: ¿Cuáles de esos servicios necesito en mi empresa? ¿De los que aún desconozco o no tengo implementados, cuáles son necesarios en mi ambiente de trabajo? ¿Cuáles estoy dispuesto a dejar en manos del proveedor y cuáles no? ¿Qué garantías ofrece la entrega del servicio por el proveedor A o por el proveedor B? ¿Cuál es el nivel de servicio que me ofrecen y cómo es medido? ¿Cómo se deben modificar mis modelos operativos para incluir estos servicios dentro de mi dinámica de negocio bajo esta nueva entrega? Y otras muy importantes: ¿Quién tendrá la capacidad de ofrecer una seguridad holística en la nube? ¿Implicará múltiples contratos de arrendamiento con diferentes proveedores para cubrir todas mis necesidades? ¿Cuál es el nivel de comunicación entre sistemas de diferentes proveedores de acuerdo a cada uno de los servicios ofertados-adquiridos?

Sin duda la respuesta a estas preguntas es una labor muy seria y consultiva al interior y exterior de las organizaciones. Considero que todas las bondades de estos servicios, descritas por un sinfín de artículos y ofertas comerciales, solo serán posibles si existe claridad y si las respuestas que den los proveedores satisfacen al menos estas preguntas.

A usted, como lector ¿Cuáles otras preguntas le parece importante incluir? ¿Se ha enfrentado a dar respuesta a algunas de ellas? Una vez que hemos presentado un panorama de la seguridad como servicio, ¿puede definir con mayor claridad las necesidades de su empresa y la instrumentación de los servicios en la nube a implementar para asegurar su mayor beneficio?

Ilustración: Silverio Ortega

[1]Gartner. (2010, September 2). Securing and Managing Private and Public Cloud Computing (G00206019). Pescatore, J.
[2]https://cloudsecurityalliance.org/
[3]https://cloudsecurityalliance.org/research/
[4]https://cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf
[5]CSA Silicon Valley cloud authorization policy automation presentation: http://www.objectsecurity.com/en-resources-video-20110208-webinar-79898734.htm

¿Sabías que

Scitum MR

es el único
Centro de Entrenamiento
autorizado en México?

(ISC)² ®
EDUCATION AFFILIATE
Authorized Provider

Por lo que ahora puedes:

1.- Tomar el Seminario Oficial de CISSP de (ISC)² del **6 al 10 de agosto del 2012**, **en Scitum** a un precio de $1,500.00 Dlls. mas IVA.
2.- Presentar el examen de certificación con costo de $599.00 Dlls. a través de uno de los centros autorizados.

La sede del seminario es:
Torre Telmex, Oficinas de Scitum, Cd. de México.
Av. Insurgentes Sur No. 3500, colonia Peña Pobre, C.P. 14060,
delegación Tlalpan.

Más informes, comuníquense al 9150.7496, lunes a viernes de 9:00 a 18:00 hrs. o bien al correo electrónico: **capacitacion-isc2@scitum.com.mx**

La fecha límite de inscripciones es el 27 de julio de 2012.

Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Check Point 3D seguridad, combina políticas, personas y aplicaciones de protección inmejorables.

POLÍTICAS

POLÍTICAS que apoyan las necesidades del usuario y la transformación de la seguridad dentro del proceso del negocio.

PERSONAS

Seguridad que educa y compromete a las PERSONAS en la definición de políticas, concientización y la solución de incidentes.

CUMPLIMIENTO

Visibilidad y control en todos los niveles de seguridad - red, aplicaciones y datos-.

www.checkpoint.com

¿PUEDES VER EN TODAS PARTES A LA VEZ?

TU PUEDES.

No se puede detener las amenazas si no las puede detectar. Esto es por lo que HP Enterprise Security ofrece soluciones probadas que ofrecen amplia visibilidad en riesgos de seguridad. No hay mejor manera de detectar de forma proactiva problemas de seguridad y manejar conscientemente la situación a través de sus aplicaciones, operación e infraestructura. La Inteligencia de seguridad de HP y la plataforma de gestión de riesgos ofrece correlación integrada, protección de aplicaciones y defensas de la red que pueden dar seguridad moderna en entornos TI con amenazas sofisticadas.

Para más información visite: www.hpenterprisesecurity.com.

Protección avanzada contra amenazas avanzadas.

ArcSight + FORTIFY + TippingPoint = hp

HP ENTERPRISE SECURITY
Advanced Protection Against Advanced Threats