2015-05-11

CiberNoticias # 30

SCProgress

www.scprogress.com

ÍNDICE

Noticia # 01: **Cyberoam obtiene patente por su nuevo método de seguridad Layer-8**

La compañía adquirió la patente para la seguridad y gestión de la red basada en la identidad del usuario.

Cyberoam, una empresa de Sophos, obtuvo, por parte de la Oficina de Patentes de USA, la patente para la seguridad y gestión de la red basada en la identidad del usuario.

Esta tecnología, que fue creada y desarrollada por el equipo de la compañía en India, ofrece capacidades únicas para conectar la identidad del usuario final con las políticas de seguridad de la red, permitiendo a los gerentes de seguridad de IT una gestión más efectiva de la actividad y el acceso de los usuarios según sus necesidades.

Los firewall tradicionales están diseñados para analizar el tráfico de la red basado en criterios de origen y destino, para permitir o denegar los requerimientos desde Internet o desde la red interna. El innovador sistema y método de Cyberoam puede aplicar reglas y políticas específicas para el usuario, entre el origen y el destino. Esta tecnología de "Layer 8" permite definir políticas específicas por usuario, permitiendo controles de seguridad granulares basadas en la identidad, la hora del día y otros controles pertenecientes a Layer.

Con el nivel adicional de control y visibilidad proporcionada por Cyberoam Layer 8, las organizaciones están mejor capacitados para cumplir con los requisitos de cumplimiento de normas como HIPAA, CIPA, PCI-DSS, GLBA, etc.

Al respecto, Hemal Patel, vicepresidente senior de TI y operaciones de Sophos, y CEO de Cyberoam, añadió: "*la concesión de esta patente valida el liderazgo continuado de Cyberoam en la prestación de la seguridad de red, basada en la identidad, para hacer frente a dos de los retos principales de la seguridad: ayudar a los administradores de red a gestionar el eslabón más débil de la cadena de seguridad con protección definida por usuario, con políticas de acceso a la red; y fortalecer el cumplimiento y la presentación de informes sobre la base de una visibilidad completa de la actividad del usuario en la red*".

Esta tecnología se encuentra en el corazón de la amplia cartera de firewall de próxima generación (NGFW) y la gestión unificada de amenazas (UTM) en todos los dispositivos de seguridad de red de Cyberoam

Fuente: http://www.ebizlatam.com/

Noticia # 02: El 93% de las empresas cree que la seguridad informática es clave para lograr objetivos

País	Crecimiento del Producto Interno Bruto (PIB)	TI retiene la evaluación de riesgos	Realizan análisis de riesgos
Brazil	1.4%	63%	61%
Mexico	3.5%	49%	47%
USA	3.1%	58%	55%
UK	2.7%	66%	59%
Germany	1.2%	67%	37%
France	0.9%	66%	41%

El 93% de las empresas cree que la seguridad informática es clave para lograr objetivos de negocio. Blue Coat Systems, empresa de seguridad empresarial, reveló los resultados de un estudio global que muestra un fuerte vínculo entre el desempeño financiero y la capacidad para hacer frente a crecientes amenazas cibernéticas.

El estudio, ejecutado por la consultora inglesa Vanson Bourne, tomó una muestra de 1.580 encuestados de 11 países diferentes.

Las preocupaciones acerca de la seguridad de TI y el riesgo están frenando el potencial de muchas organizaciones, de acuerdo con el 58% de los encuestados en Brasil, y el 54% en México.

Por otro lado, la toma de riesgos fue aceptada por tener un impacto positivo en el rendimiento del negocio en un 66% de los casos. En América Latina, hubo un fuerte valor positivo a este factor, con un 79% de encuestados en México y 77% en Brasil.

Ignacio Conti, regional manager de Blue Coat, comentó: "Las empresas saben instintivamente que el éxito viene de la toma de riesgos, pero hoy en día la seguridad de TI es el freno de muchas organizaciones".

A pesar de la clara correlación entre las empresas que invirtieron fuertemente en TI y el crecimiento de sus ingresos, hay una amplia gama de respuestas cuando se trata de medidas prácticas que ayuden a mitigar los riesgos que conlleva la nueva tecnología.

Sólo el 52% de todas las organizaciones entrevistadas realiza siempre un análisis de riesgos antes de la adopción de nuevas aplicaciones.

Conti finalizó: "La gestión del equilibrio entre el riesgo y el rendimiento financiero es clave para el éxito del negocio. Las soluciones de Blue Coat ayudan a las empresas a desarrollar análisis de riesgos precisos para que puedan tomar las decisiones correctas, sopesar sus riesgos con precisión para ser mucho más exitosos.¨

Fuente: http://www.portinos.com/

Noticia # 03: **Políticas de restricción, clave para garantizar seguridad informática**

Si bien los ataques cibernéticos aprovechan la popularidad de las redes sociales o el uso de dispositivos personales para realizar actividades laborales, la restricción de estas prácticas puede representar un impacto negativo en la productividad de las empresas. En entrevista, el responsable de Ventas de Seguridad de Cisco México, Rafael Chávez, "las empresas no pueden mantener su operación en un esquema de restricciones, tienen que evolucionar para obtener los beneficios que proporcionan las nuevas aplicaciones y servicios, y al mismo tiempo minimizar las posibilidades de un ataque peligroso".

Para dar ese paso, subrayó, la concientizacion de los empleados sobre los riesgos y consecuencias de no seguir las recomendaciones y reglas para evitar vulnerabilidades es una pieza clave. "Si las personas no están sensibilizadas y la atención se centra en las restricciones, tratarán de evadir las reglas porque no han entendido que evitar un procedimiento o violar una política puede provocar problemas no solo de seguridad, sino económicos". Y es que, dijo, es muy común que los problemas relacionados con la seguridad informática sean tratados en los departamentos de tecnología, sistemas o telecomunicaciones como temas ajenos al resto de las personas que trabajan en las organizaciones.

Para Chávez, cuando no existe la información adecuada en materia de seguridad informática es fácil generar pánico, frente a lo cual un buen plan de capacitación, políticas y procedimientos fundamental. "La tecnología sóla no sirve, es necesario que todos los empleados sepan qué hacer en caso de recibir un correo sospechoso, o cuando le aparezca un mensaje solicitando datos, o las vulnerabilidades que se abren al usar dispositivos personales sin la seguridad adecuada". Con el cada vez más común uso de dispositivos personales para actividades laborales, añadió, el reto crece pues los usuarios se enfrentan a prácticas y estrategias del "hackeo" ilegal que buscan infiltrarse en los sistemas informáticos de las empresas, robar su información y obtener beneficios económicos.

La tendencia mundial denominada Bring your Own Device o Trae tu propio dispositivo eleva la productividad de los empleados; sin embargo, sin una infraestructura fuerte y políticas adecuadas puede representar serias amenazas, de acuerdo con el experto. "La clave está en implementar políticas con la seguridad adecuada, soluciones que permitan autenficar al usuario independientemente del dispositivo con el que esté entrando a la red identificando el perfil del usuario dependiendo en donde me conecto y con qué dispositivo".

Datos de Cisco revelan que la actividad ilícita del "hackeo" es un negocio tan redituable que cada año le genera a los delincuentes ingresos por alrededor de 450 mil millones de dólares al año. Frente a lo cual, la única certeza que tienen las empresas es que en algún momento de su existencia serán atacadas; sin embargo, la diferencia será el nivel del impacto generado dependiendo de la fortaleza de su infraestructura de seguridad y de sus políticas en la materia

Fuente: http://www.20minutos.com.mx/

Noticia # 04: Cinco vacíos en seguridad informática

Estas son cinco señales básicas que ponen de manifiesto si un usuario puede ser víctima de un ataque informático. Es muy frecuente que los ciber delincuentes aprovechen los errores de los usuarios para realizar sus actividades delictivas, por ello los expertos en seguridad informática de Eset detallan cuáles son esos errores.

1. Confiar en cualquier enlace que aparece en redes sociales. A pesar de que en 2014, según el reporte DBIR de Verizon, cayó significativamente la tentación de acceder a un contenido publicado en Twitter o Facebook, todavía algunos siguen ingresando, especialmente luego de algún desastre natural o acontecimiento de interés general.

Al hacer clic en ellos, redirigen a los usuarios a sitios maliciosos o a sitios legítimos que han sido comprometidos, con el objetivo de robar credenciales (mediante una página de login bancario por ejemplo) o un ataque drive-by-download para inyectar malware en la computadora. Por este motivo, antes de hacer click, hay que analizar si la fuente es confiable, y considerar herramientas para verificar redirecciones.

2. Reutilizar contraseñas. Hay quienes siguen anotándolas en papeles o en otros lugares de sus computadoras y las reutilizan en distintos servicios online. Si un atacante logra comprometer una cuenta utilizando correos de phishing (suplantación) y ataques de fuerza bruta, puede acceder a las demás usando las mismas credenciales.

Por ello, las contraseñas deben ser complejas y únicas para distintas plataformas. También es aconsejable la utilización de herramientas para gestionarlas y así administrarlas con una sola clave maestra. Además, no se deben descuidar las del router, cámara web o dispositivos conectados a la Internet de las Cosas (IoT). Muchas vienen con contraseñas por defecto que, de no ser cambiadas, pueden ser vulneradas.

3. No actualizar el software. Los usuarios pueden verse expuestos al robo de datos, fraudes financieros y demás problemas de seguridad que, en ocasiones, podrían evitarse si se actualizara el software y se aplicaran los parches correspondientes en tiempo y forma. Estos están diseñados para corregir vulnerabilidades, y en muchos casos son programados en forma regular.

El año pasado, Heartbleed, la falla en el cifrado SSL, implicó que el tráfico web de millones de usuarios quedara expuesto, los atacantes lograron el acceso sin restricciones a contraseñas, detalles de tarjetas de crédito y más, por ello, es recomendable la aplicación del parche.

4. Descargar desde tiendas de terceros no oficiales. Los usuarios de iOS a menudo realizan un jailbreak a sus dispositivos con el fin de evadir los controles impuestos por Apple y así instalar apps de repositorios no oficiales. Lo mismo sucede en Android el sistema operativo móvil de Google, en donde los usuarios instalan aplicaciones de repositorios no oficiales que suelen contener algún código malicioso.

Esto conlleva ciertos riesgos en términos de seguridad, porque permite que las apps se comporten en modos impredecibles, y además estas tiendas no oficiales ofrecen aplicaciones maliciosas u otras legítimas que han sido modificadas por cibercriminales. Para evitar toparse con alguna de ellas, es recomendable descargar desde tiendas oficiales.

5. Enviar información sensible a través de W-Fi abierto. Si se navega por Internet desde una casa, probablemente el router esté protegido por una contraseña fuerte y por un firewall. Pero distinto es si se usa una red Wi-Fi abierta en un espacio público, especialmente hoteles y cafés, donde la conexión es frecuentemente libre e insegura.

Esto permite que los atacantes se sitúen en medio del dispositivo y el servidor del usuario, en un ataque Man-In-The-Middle (MITM), con el objetivo de robar datos sensibles o ejecutar malware. Algunos incluso han logrado comprometer el punto de acceso causando que aparezca una ventana emergente durante el proceso de conexión, ofreciendo una actualización de un software popular -y con solo hacer clic, se instala un código malicioso. En tanto, otros han usado herramientas online para pretender que son el punto de acceso en sí mismo.

Fuente: http://www.dinero.com/

CREDITOS:

Revista de seguridad informática, recopilación de los mejores artículos de la prensa internacional.

Recopilación y edición:
Ing. Marco de la Torre
m.delatorre@scprogress.com

Supervisado por:
Ing. Arturo de la Torre
adltorre@scprogress.com