2015-04-06

CiberNoticias # 28

SCProgress

www.scprogress.com

ÍNDICE

Noticia # 01: **Buscando evitar ataques de hackers, EEUU actualiza su seguridad informática**

El Departamento de Estado estadounidense ha anunciado que está actualizando la seguridad en su red de ordenadores con información no confidencial, con el objetivo de protegerse de ciberataques. Esta situación ha provocado que varios empleados no hayan podido acceder durante el día a sus correos electrónicos o Internet.

El Departamento de Estado estadounidense ha anunciado que está actualizando la seguridad en su red de ordenadores con información no confidencial, con el objetivo de protegerse de ciberataques. Esta situación ha provocado que varios empleados no hayan podido acceder durante el día a sus correos electrónicos o Internet.

La portavoz del Departamento, Jen Psaki, ha explicado que el objetivo es mejorar la red no confidencial "mediante una suspensión corta y planificada de algunos sistemas relacionados con Internet", además de asegurar que se están vigilando las "actividades preocupantes".

"Ninguno de los sistemas confidenciales del Departamento de Estado se ha visto comprometido, tampoco nuestros sistemas centrales financieros, consulares y de recursos humanos", ha asegurado Psaki en un breve comunicado.

Algunos funcionarios han advertido de que no han podido enviar correos electrónicos a direcciones externas al organismo, aunque las comunicaciones internas seguían fluyendo, y que no podían acceder a Internet desde sus computadores de escritorio.

Esta situación recuerda a la del pasado mes de noviembre, cuando el Departamento de Estado realizó una actualización debido a un ciberataque. Psaki no ha concretado s en esta ocasión también se ha producido un ataque de estas características.

FUENTE: http://www.eleconomista.es/

Noticia # 02: Makros presentó predicciones de seguridad de Cyberoam

Deberá ponerse especial atención en la Internet de las Cosas; geopolítica; protocolos tradicionales y en el sector

La compañía experta en seguridad informática, representada en Chile por Makros, entrega ocho claves a considerar este 2015

Nubes negras sobre Internet de las Cosas (IOT)

Este año IOT ganará visibilidad, tanto por sus avances como por sus vulnerabilidades. Se podrá ver cómo los sistemas SCADA adoptan IOT y su exposición a las amenazas cibernéticas aumentará. Sistemas de control de edificios remotamente conectados y automatizados también se enfrentan a un desafío similar. Alrededor de 2,2 millones de dispositivos SCADA y BACnet ya están expuestos a posibles amenazas cibernéticas ya que son identificables a través de SHODAN - un motor de búsqueda de dispositivos conectados a Internet

Mientras tanto, los requerimientos de seguridad del gobierno, como eCall (reportes de asistencia de emergencia por Internet en vehículos en Europa) y la demanda de conectividad de datos sin interrupción, han abierto las puertas para la infraestructura de autos conectados, lo que está trayendo autofabricantes, empresas de telecomunicaciones y los gigantes de la tecnología como Google, Samsung y Apple a un tablero de diseño común. Mientras tanto, las aplicaciones móviles han comenzado con la infraestructura de "auto conectado", lo que implica que es sólo una cuestión de tiempo antes de que se descubran las vulnerabilidades.

Intervención geopolítica

En 2014, el Departamento de Seguridad Nacional de Estados Unidos reveló un troyano llamado Black Energy, el cual afectó su infraestructura crítica. Exploits del Ejército Electrónico de Siria, como el Malware APT (Advanced Persistance Threath) Regin también ocuparon los titulares.

El paisaje geopolítico está cambiando drásticamente en todo el mundo e Internet no puede permanecer aislada de sus efectos. De hecho, Internet se ha convertido en una herramienta fundamental para las propagandas patrocinadas por el gobierno, espionaje y ataques cibernéticos. Los malwares APT se utilizaron en estas campañas en varias ocasiones, quebrantando los límites legales. Tales malwares se encontraban únicamente esperando ser activados en las redes de oleoductos y gasoductos, redes de transmisión de energía, distribución de agua y sistemas de filtración, turbinas de viento e incluso algunas plantas nucleares en los Estados Unidos. En dichos casos, también las empresas del sector privado se vieron en la línea de fuego de vez en cuando.

Si las condiciones se deterioran, lo que parece ser una buena probabilidad en este 2015, habrá un mayor impulso en los ciberataques de los países involucrados, algunos de los cuales podrían ser revelados durante este año.

Protocolos tradicionales en la mira

POODLE, Shellshock y Heartbleed son ejemplos de vulnerabilidades en el código que estuvieron ocultas durante años antes de ser descubiertas y explotadas. Los protocolos tradicionales en los que Internet parece funcionar tan bien están lejos de ser perfectos y los ciberdelincuentes seguirán aprovechando los vacíos legales a su favor. Algunos de estos protocolos son de código abierto, los cuales enfrentan una mayor amenaza.

Por otra parte, a medida que Internet hace la transición de IPv4 a IPv6, los ciberdelincuentes están a la caza de las brechas de seguridad latentes. Además de las vulnerabilidades en los navegadores Web, también pueden esperarse ataques del lado del cliente, explotando vulnerabilidades de las aplicaciones en los frameworks más utilizados como Adobe, Java, etc.; con lo que los retos de seguridad de red se agravan para los administradores de TI en el 2015.

Pérdidas en el sector salud

Teniendo en cuenta que el sector Salud está haciendo rápidos progresos en todo el mundo en adoptar tecnología y digitalización de la atención al paciente, junto con el almacenamiento de información de identificación personal; hay una necesidad crítica de fortalecer la seguridad de la información en este sector, ya que está en un gran riesgo dado el hecho de que estos datos tienen más valor en el mercado negro que los números de tarjetas de crédito, puesto que pueden proporcionar acceso a cuentas bancarias o ayudar en la obtención de recetas de medicamentos controlados.

El sector salud, por tanto, requiere mejoras significativas en su estado de preparación cibernética; un hecho que dejó muy en claro el FBI en 2014, cuando los sistemas de salud comunitaria sufrieron una vulneración en su seguridad, en el cual fueron extraídos 4,5 millones de registros de pacientes en los Estados Unidos. Y se esperan más de dichas infracciones para el 2015.

Malvertising y ataques por email

2014 vio cómo redes de anuncios en sitios Web de renombre -como Yahoo, AOL y Google- se vieron comprometidos para distribuir malvertisements (colocación de anuncios cargados de malware en las páginas Web de renombre / populares) y es probable que sean más de una molestia en 2015. Las redes publicitarias se ven comprometidas continuamente y los atacantes están confiando en el hecho de que el bloqueo de cada anuncio o prueba de cada red de anuncio no es una solución práctica. Malvertisers también están en ventaja como sitios Web de renombre (páginas de noticias y entretenimiento), ya que rara vez son bloqueados por los firewalls de oficina.

Mientras tanto, si los informes son como se cree, el Spam se encuentra en declive. Esto se debe, en parte, al hecho de que los spammers han ideado otras formas más avanzadas para llegar a la bandeja de entrada, mientras que otros han pasado a sofisticados ataques de phishing dirigidos de forma individual a los firewalls corporativos. Sin embargo, la vieja táctica de la elaboración de mails fraudulentos alrededor de los principales eventos mundiales / locales sigue siendo rentable para los spammers. 2015 no va a ser diferente en este sentido, aunque se puede esperar ver algunos trucos nuevos para evadir las soluciones de seguridad de correo electrónico actual.

Demanda de conocimiento de los contextos de seguridad

En la actualidad, las redes generan gran cantidad de datos, los que contienen suficientes indicios para ofrecer patrones de comportamiento humano que se puede utilizar para predecir y prevenir los ataques cibernéticos. Sin embargo, la comprensión y co-relación de datos para obtener información relevante requiere de tiempo y habilidades; además, conlleva el riesgo de supervisión humana. Las empresas necesitan un modelo de seguridad para aprovechar esta información e interpretar el tráfico de la red para identificar patrones y eventos sospechosos. En tal escenario, las herramientas de análisis de Big Data pueden ofrecer gran ayuda en la co-relación de datos, dando un modelo o prototipo de usuario para detectar peligros y tendencias de riesgo en una red.

De hecho, las organizaciones BFSI (Banking, Financial Services and Insurance) ya han comenzado a aprovechar el análisis de seguridad basado en Big Data para la detección anticipada y la prevención de fraudes.

Empleando los avances en el análisis de grandes volúmenes de datos, soluciones de seguridad sensibles al contexto, como User Threat Quotient de Cyberoam (UTQ) pueden ayudar a los administradores de TI en tareas afines a encontrar una aguja en un pajar – identificando usuarios que representan riesgo de seguridad en una red. En 2015, este tipo de soluciones seguramente serán empleadas por las organizaciones que buscan inteligencia de seguridad activa.

IOS en el radar de los cibercriminales y continúan los ataques para Android

Empleando los avances en el análisis de grandes volúmenes de datos, soluciones de seguridad sensibles al contexto, como User Threat Quotient de Cyberoam (UTQ) pueden ayudar a los administradores de TI en tareas afines a encontrar una aguja en un pajar – identificando usuarios que representan riesgo de seguridad en una red. En 2015, este tipo de soluciones seguramente serán empleadas por las organizaciones que buscan inteligencia de seguridad activa.

Resolviendo el rompecabezas password

La búsqueda de reemplazar una password como procedimiento de autenticación ganará impulso. Se ha informado que un número cada vez mayor de la generación millennials en Estados Unidos prefieren la propuesta de autenticación por huella digital de Apple. Sin embargo, el incremento de las técnicas de autenticación biométrica como el análisis de la huella digital es un gran reto.

Por otra parte, la autenticación biométrica no es una solución tan eficaz como se pensaba. Teniendo en cuenta los recientes incidentes de vulneración de datos y robo de credenciales en mente, la Alianza FIDO lanzó su esperado reporte de especificaciones para autenticación sin contraseña y multifactorial 1.0. Por lo que, un mayor impulso para alejarse de las contraseñas, hará que los piratas informáticos hagan mucho más que cambiar sus asientos.

FUENTE: http://www.dirigentesdigital.com

Noticia # 03: ¿Cuáles son los desafíos que enfrenta la seguridad informática de los bancos?

Sólo en fraudes bancarios, clonación y robo de credenciales, se estima que por cada $10.000 que se muevan en una cuenta, 20 se pierden por fraudes

Para nadie es un secreto que así como existen personas tratando de proteger a las entidades financieras y a sus clientes, también hay individuos que pueden convertirse en delincuentes tratando de ingresar a los sistemas y a los correos empresariales y personales para obtener un beneficio propio o de terceros.

Muchas empresas han tenido incidentes por fallas en sus modelos de seguridad, impactando sus objetivos estratégicos y, consecuentemente afectando su prestigio y su valor, por lo que sus directivos buscan continuamente estrategias efectivas para proteger la información.

El sector financiero basa su modelo de negocio en la confianza**,** que está directamente relacionada con la seguridad. Los clientes, basándose en la confianza, entregan su patrimonio para que sea protegido y les genere ingresos.

Hace algunos años, la seguridad era física, protegiendo el papel moneda y los documentos.

En la actualidad, el patrimonio se desmaterializa y se convierte en un registro, un dato, en los sistemas de información del sector, lo que hace que la ciberseguridad se vuelva muy importante.

La confianza se basa en modelos adecuados que velan por la generación de valor para todos los interesados y la revisión por parte de entes independientes, controladores o entidades gubernamentales del gobierno que avalen esa confianza.

La seguridad se basa (y descansa) en modelos y arquitecturas de seguridad. El sector financiero enfrenta tres desafíos claros en los temas de ciberseguridad:

Cumplimiento: la implementación de controles que estén alineados con las definiciones normativas y regulatorias.
Gestión de riesgos: orientado a hacer uso adecuado de los recursos a los temas más críticos que pueden impactar la seguridad de la información.
Eficiencia: cómo generar más valor en la operación del modelo de seguridad, con menos recursos.

Los modelos y las arquitecturas de seguridad evolucionan con la tecnología y con las nuevas amenazas.

El sector financiero ha invertido grandes sumas de dinero en estrategias que ayudan a enfrentar los nuevos desafíos, pero se olvidan de que los modelos de seguridad y las arquitecturas deben comunicarse y sumar para gestionar los riesgos de forma efectiva.

Aunque las decisiones en términos de seguridad se han vuelto estratégicas, el modelo de seguridad no tiene una madurez en las organizaciones ya que los tomadores de decisiones no cuentan con las habilidades para comprender los temas de ciberseguridad y los responsables no tienen las habilidades para explicarles y poner en términos de negocio los desafíos sobre el tema.

El sector financiero es muy atractivo para los ciberdelincuentes porque ellos pueden obtener valor por sus actividades delictivas.

La cadena del cibercrimen inicia con el robo de información (datos de autenticación, información personal, información confidencial de las organizaciones) a través de amenazas como el phishing, hacking, malware.

Posteriormente, alguien puede comprar dicha información, lo que puede representar un pago para el hacker. La información puede ser utilizada para llevar a cabo ataques más sofisticados como movimientos fraudulentos a cuentas mulas, espionaje industrial, amenazas avanzadas persistentes (APT, por su sigla en inglés).

En términos de impacto económico, las pérdidas por crimen cibernético a nivel mundial son de más de 300 mil millones de dólares.

Sólo en fraudes bancarios, clonación y robo de credenciales, se estima que por cada 10 mil pesos que se muevan en una cuenta, 20 pesos se pierden por fraudes.

Los cibercriminales están logrando fácilmente sus objetivos a partir de abusar de la confianza y naturaleza del ser humano.

Un señuelo que utiliza algo de interés para la víctima del fraude puede ser la puerta para que abra un documento, acceda a un sitio y descargue un malware que le provee el acceso al atacante.

Los eventos publicados en medios últimamente como los que involucraron a BBVA, JP Morgan, El robo del siglo o Sony, ponen en duda la efectividad de los modelos de gobierno y arquitecturas de seguridad.

La complejidad de las arquitecturas encubre la debilidad de los modelos de seguridad.

El sector debe orientar sus esfuerzos a comprender que la ciberseguridad es un tema de riesgo empresarial y proveer de herramientas a los miembros del directorio para que entiendan las implicaciones legales de los riesgos cibernéticos y que tengan acceso a experticia en ciberseguridad.

Por último, debemos lograr medir el daño de los eventos de ciberseguridad lo que nos dará el conocimiento para que nuestras decisiones de seguridad futuras sean más efectivas.

FUENTE: http://www.iprofesional.com

Noticia # 04: **Seguridad informática: Los expertos piden sanciones más rigurosas por violación de datos**

Websense realizó una encuesta internacional a 102 profesionales de seguridad informática. El 98% de los encuestados cree que la ley debe abordar mejor las violaciones de datos serias, con castigos como multas (65%), divulgación obligatoria (68%), indemnizaciones a consumidores afectados (55%) e incluso arresto y penas de prisión (16%)

El 45% de los encuestados siente que las empresas no están tomando medidas contra la pérdida y el robo de datos, porque la seguridad informática no es una prioridad alta. Por otra parte, el 70% dice que el CEO debería tener la última responsabilidad en una brecha de información.

El 93% de los encuestados cree que la llegada de "Internet de las Cosas" hará que las empresas sean aún más vulnerables al robo de datos, mientras que el 35% afirma que la tecnología que utilizan las compañias no es la adecuada para combatir el robo de datos.

Al parecer, las noticias acerca de la pérdida de datos han ayudado de forma inadvertida a concientizar a las empresas sobre el problema. Los profesionales de seguridad consideran que la publicidad ha ayudado a otras compañías a crear un escenario para obtener presupuesto, enfoque y recursos. Solo el 15% cree que los titulares han obstaculizado este escenario, al hacer que las empresas se sientan impotentes para protegerse de estos ataques.

Neil Thacker, information security officer, de Websense explica: "Cuanto más hablamos de los problemas, de compartir las técnicas usadas para violar las seguridad de las organizaciones, y robar o dañar los datos, mejor. Ante la cantidad de datos que aumentará con "Internet de las Cosas" y el dilema de tener cada vez más habilidades de seguridad, las organizaciones tienen un duro desafío por delante."

"Implementar controles para prevenir el robo de datos, un enfoque en la seguridad de información, junto con la construcción de una cultura de responsabilidad y seguridad en toda la empresa a través de la colaboración, son cosas esenciales para mantener los datos protegidos", añadió Thacker.

Todos los encuestados asistieron al e-Crime Congress en Londres el 10 de marzo de 2015.

FUENTE: http://www.portinos.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