CIBERSEGURIDAD

Security and threat analytics

Cyberoam®

Avira

CRYPTOPHONE™

NEXXT SOLUTIONS

open source™

Índice

CREDITOS:

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

Recopilación y edición:
Consuelo de la Torre
c.delatorre@scprogress.com (+593 979003123)
Marco de la Torre
m.delatorre@scprogress.com (+593 998053611)

Revisado por:
Arturo de la Torre
adltorre@scprogress.com (+593 999025294)

Síguenos en:

www.scprogress.com Facebook Twitter

Seguridad informática: vulnerabilidad, riesgo y amenaza

El acceso a la información se vuelve cada vez más fácil para personas mal intencionadas, el ingresas a los sistemas, sin contar con autorización a través del internet y las redes informáticas causa grandes problemas, tanto si son computadores personales o parte de una red empresarial.

Estas intromisiones ocasionan pérdida de datos, siendo en ocasiones imposible recuperar la totalidad de los mismos, a pesar de haber obtenido respaldos. El robo de información sensible y confidencial, así como, la divulgación de los datos de una determinada empresa acarrea grandes pérdidas económicas, que en ocasiones llegan a ser catastróficas.

Con la constante evolución tanto de los equipos informáticos, como de los conocimientos y métodos para hackearlos, se vuelve imprescindible y fundamental realizar análisis de las vulnerabilidades de las infraestructuras y sistemas, así como, contar con planes de seguridad y continuidad para salvaguardar la integridad y confidencialidad de la información.

En la presente edición, se tratará sobre la importancia de realizar un adecuado análisis de vulnerabilidades informáticas, la elaboración de planes, acciones a considerar entre otros de interés para nuestros lectores. Iniciaremos con la diferencia entre vulnerabilidad, riesgo y amenaza, definiciones que tenemos que tenerlas claras, para que nuestro análisis sea el más adecuado.

Vulnerabilidad.-

En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema, permitiéndole a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

Estas vulnerabilidades son el resultado de Bugs o de fallos en el diseño del sistema. En ocasiones también puede ser el resultado de las propias limitaciones tecnológicas, ya que no existe un sistema 100% seguro. Por lo tanto existen vulnerabilidades teóricas y vulnerabilidades reales.

Las Vulnerabilidades en las aplicaciones pueden corregirse con parches, hotfixs o con cambios de versión. Otras requieren un cambio físico en el Sistema Informático.

Principales vulnerabilidades:

- Symlink races.- O también conocida como carrera de enlace simbólico que es un tipo de vulnerabilidad de seguridad de software que resulta de un programa de creación de archivos de una manera insegura. Un usuario malintencionado puede crear un enlace simbólico a un archivo de otro modo no accesible para él o ella. Esto puede utilizarse para alimentar entradas mal formadas en el destino o para hacer que el objetivo procese información diferente, posiblemente permitiendo al atacante controlar las acciones del objetivo o hacer que el objetivo exponga información al atacante.
- Secuestro de sesiones.
- Desbordes de pila y otros buffers.
- Errores en la validación de entradas como: inyección SQL, bug en el formato de cadenas, etc.
- Ejecución de código remoto.

Bugs.- Un defecto de Software es el resultado de un fallo o deficiencia durante el proceso de creación de programas de ordenador. Este fallo puede presentarse en cualquiera de las etapas del ciclo de vida de un Software; aunque los más evidentes se dan en la etapa de desarrollo y programación.

Amenazas.-

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento de la información se consideran seguras, deben tomarse en cuenta las circunstancias no informáticas que pueden afectar a los datos, las cuales son a menudo inevitables, de modo que la única protección posible es la redundancia y la descentralización.

Las principales causas:

- ***El usuario***: Es la causa mayor del problema de la s
- ***Programas maliciosos***: Son programas destinadc sistema.
- ***Intruso***: Es una persona que consigue acceder a permitido.
- ***Siniestro***: Una mala manipulación o mala mal archivos.

Tipos de amenazas:

Al conectar una red a un entorno externo, se le está dando la oportunidad al intruso de entrar a ella, logrando robar la información o alterar el funcionamiento de la red. Sin embargo no conectar la red a un entorno externo no garantiza la seguridad de la red.

Existen dos tipos de amenazas:

Amenazas internas.- Generalmente estas amenazas pueden ser más peligrosas que las externas por las siguientes razones:

- Los usuarios conocen la red y saben su funcionamiento.
- Tienen nivel de acceso a la red por las necesidades de trabajo.
- Los Firewalls son mecanismos no efectivos en las amenazas internas.

Amenazas externas.- Son aquellas amenazas que se originan afuera de la red. Al no tener información específica de la red, un atacante debe realizar ciertos pasos para poder conocer que es lo que hay en ella y buscar la manera de acceder para atacarla. La ventaja de este tipo de amenaza, es que el administrador de la red puede prevenir una buena parte de los ataques externos.

La amenaza informática del futuro:

Antes el objetivo de los ataques fue cambiar las plataformas tecnológicas ahora las tendencias cibercriminales indican que la nueva modalidad es manipular los significados de la información digital. El área semántica, era reservada para los humanos, pero se convirtió en el núcleo de los ataques debido a la evolución de la Web 2.0 y de las redes sociales, lo que llevo al nacimiento de la generación 3.0.

Se afirma que esta generación de Web 3.0 otorga contenidos y significados de tal manera que pueden ser comprendidos por los computadores, los cuales por medio de técnicas de inteligencia artificial son capaces de mejorar la obtención de nuevo conocimiento, y hasta el momento es reservado para humanos.

Se trata de dotar el significado de las páginas Web y de ahí el nombre de Web semántica o Sociedad de Conocimiento, como la evolución de la ya pasada Sociedad de la Información.

Es decir, las amenazas informáticas que vienen en el futuro ya no son los troyanos en los sistemas o el software espía, sino que como los ataques se han profesionalizado y manipulan el significado del contenido virtual.

La Web 3.0 se basa en conceptos como compartir, elaborar y significar, está representando un gran desafío para los hackers que ya no utilizan las plataformas convencionales de ataque, sino que optan por modificar los significados de contenido digital, provocando así la confusión lógica del usuario y permitiendo de este modo la intrusión en los sistemas. La amenaza ya no necesita la clave de un ingenuo usuario, sino que modifica el balance de la cuenta, asustando al internauta y luego proceder con el robo de su capital.

Para prevenir ser la victima de estos nuevos ataques, se recomienda:

- Evitar realizar operaciones comerciales o bancarias, en un café internet.
- Mantener los Antivirus activados y actualizados.
- Verificar los archivos adjuntos de mensajes sospechosos y evitar su descarga.

Riesgo.-

Deriva del latín “marenchu”, es la vulnerabilidad de bienes jurídicos protegidos ante un posible daño para las personas o cosas, particularmente para el medio ambiente.

Es decir, cuanto mayor es la vulnerabilidad mayor es el riesgo, pero cuanto más factible es el daño o perjuicio mayor es el peligro. Por lo que el Riesgo se refiere solo a la teórica posibilidad de daño bajo algunas circunstancias, mientras que el peligro se refiere solo a la teórica probabilidad de daños bajo algunas circunstancias.

Ejemplos de algunos tipos de riesgo son:

- Riesgo geológico: Terremotos o sismos, erupciones volcánicas, corrimiento de tierra.
- Riesgo financiero: Riesgo de crédito, riesgo de liquidez, riesgo de mercado.

Riesgo vs amenaza.-

Los métodos de probabilidad bayesiana permiten asignar cierto grado de creencia al riesgo, en función del grado de verosimilitud y de la magnitud de la causa. Además, del peligro una causa de riesgo previo es la amenaza.

Las amenazas es un contexto de seguridad de la información, incluyen actos dirigidos, deliberados y sucesos no dirigidos, aleatorios e impredecibles. Amenaza es la causa de Riesgo que crea aptitud dañina sobre personas o bienes. En el ámbito económico las amenazas que existen son la perdida de dinero.

FUENTES: http://seguridadanggie.blogspot.com/2011/11/vulnerabilidad.html
https://en.wikipedia.org/wiki/Symlink_race&prev=search

Cooperativa de Ahorro y Crédito "General Rumiñahui"

Promoviendo el desarrollo y bienestar de sus socios militares y civiles desde 1993.

- Créditos sin garante hasta 3.000 dólares.
- Otorgamos créditos para consumo, emprendedores y microempresarios.
- Las tasas de interés más bajas del mercado.
- Inversiones a plazo fijo.
- Pagos de créditos y ahorros, a través de ventanillas o con autorización de débitos bancarios del Banco Pichincha, General Rumiñahui e ISSFA.
- Asistencia ambulatoria
- Consultas médicas de primer nivel ilimitadas en cualquiera de las patologías derivadas de: medicina general, ginecología y pediatría.
- Cobertura en asistencia dental.
- Examen clínico y diagnóstico.
- Higiene dental, alivio del dolor.
- Rayos X periapical, profilaxis (Limpieza dental profunda).
- Restauraciones en resina simple.
- Extracciones simples.

Calle Manuel Cabeza de Vaca N53-240 y Av. Los Pinos a 30 mts. Del Cuartel Rumiñahui.
Teléfonos: 2411-731 / 2406-117 / 0984977204
www.cooprumi.fin.ec

¿Qué es un Análisis de Vulnerabilidades Informáticas?

Hoy en día todas las organizaciones y personas utilizan dispositivos inteligentes, computadoras, redes inalámbricas, etc. Están expuestas a diferentes amenazas cibernéticas derivadas de la utilización de páginas web, apps, documentos, correos electrónicos, servicios de chat, redes sociales, etc.

La mayoría de estas amenazas están siendo creadas para extraer información personal o corporativa y con esto realizar ataques dañinos que vulneran nuestra capacidad para realizar transacciones, acceso a documentos, sistemas internos, etc.

Mientras que por un lado hoy tenemos a la disposición cientos de servicios de interconexión entre personas y organizaciones, por el otro estamos teniendo mucha mayor exposición de nuestra información personal y corporativa hacia personas no autorizadas que utilizan diferentes métodos para atacar y estos están siendo cada vez más complejos, más difíciles de prevenir y sobre todo más dañinos. Esto ha llevado a las organizaciones a poner mucho más énfasis en la ciberseguridad y los aspectos preventivos y correctivos ante un ataque.

Dentro de una correcta planeación de protección preventiva y correctiva se debe de considerar el análisis de vulnerabilidades como una actividad clave para asegurar que estamos al día ante la creciente ola de amenazas que día a día va creciendo de manera exponencial.

¿Qué es un análisis de vulnerabilidades informáticas?

Por definición una vulnerabilidad informática se puede considerar como una debilidad de cualquier tipo que afecta o compromete la seguridad de un componente informático.

Las vulnerabilidades informáticas las podemos agrupar en función de:

- Diseño de la seguridad perimetral.
- Debilidad en el diseño de protocolos utilizados en las redes.
- Políticas de seguridad deficientes e inexistentes.
- Implementación.
- Errores de programación.
- Existencia de “puertas traseras” en los sistemas informáticos.
- Descuido de los fabricantes.
- Uso.
- Configuración inadecuada de los sistemas informáticos.
- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
- Disponibilidad de herramientas que facilitan los ataques.
- Limitación gubernamental de tecnologías de seguridad.

- Vulnerabilidad del día cero.

Ante todos estos factores, el análisis de vulnerabilidades es un servicio por medio del cual se comprueban a través de herramientas de software y servicios de consultoría la debilidad o fortaleza ante el conjunto de amenazas conocidas al día de la evaluación tanto para elementos externos (Servicios SAAS, Servicios de Cloud Computing, Servicios BYOD, Usuarios no autorizados, sniffers, robots, etc.) como para elementos internos (Usuarios, sistemas implementados, estaciones de trabajo, dispositivos móviles, sistemas operativos, etc.)

Un correcto análisis de vulnerabilidades no solo detecta las áreas de mejora, sino que también propone la correcta arquitectura necesaria para proteger la infraestructura de una organización y los diferentes cambios de políticas de seguridad que se requiere implementar para asegurar una continuidad de operación, la asistencia que se debe proveer cuando se ve comprometida la seguridad informática y la recuperación ante desastres ante amenazas e intrusiones.

Los pasos necesarios para un análisis de vulnerabilidades se pueden resumir a continuación:

- Diagnóstico de Seguridad:
  1. Escaneo de vulnerabilidades externas.
  2. Escaneo de vulnerabilidades internas.
- Revisión de Políticas de Seguridad
- Revisión de procesos, pólizas de soporte y configuraciones que comprometan la seguridad informática.
- Reforzamiento de la topología de red.
- Generación de documento de recomendaciones de buenas prácticas de seguridad informática, arquitectura ideal para la organización,
- Planeación ante eventos que comprometan la seguridad.
- Revisión de políticas de respaldos, sistemas de redundancia, planes de recuperación de desastres.
- Generación de documento recomendaciones ante eventos de seguridad.

¿Qué hacer después de implementar las recomendaciones de un análisis de vulnerabilidades?

Es importante que los esfuerzos realizados posteriormente a la implementación de un análisis de vulnerabilidades, se realicen procesos de auditoría por lo menos dos veces al año para asegurar que todas las recomendaciones estén en funcionamiento y los procedimientos y políticas se encuentren acordes a la situación actual de la organización.

FUENTE: http://blog.cerounosoftware.com.mx/que-es-un-analisis-de-vulnerabilidades-inform%C3%A1ticas

Rincón de los expertos

RIESGO INFORMÁTICO.- es la posibilidad de que una amenaza explote o se aproveche de las vulnerabilidades que mantiene un activo de información provocando un determinado impacto en la institución. Generalmente y de acuerdo a la definición al riesgo se lo mide por la relación impacto por probabilidad, una amplia documentacion de lo que es, se lo puede encontrar en la norma ISO/IEC 27005:2011. Los profesionales interesados en esta norma podrán encontrar un detalle completo de la misma en la URL:

http://www.iso.org/iso/catalogue_detail?csnumber=56742

"Si piensas que la tecnología puede solucionar tus problemas de seguridad, está claro que ni entiendes los problemas ni entiendes la tecnología"

— Bruce Schneier —

Empresas o personas interesadas en promocionarse en nuestra revista, por favor contactarse con c.delatorre@scprogress.com

Noticias

Fallo grave en PHPMailer compromete millones de web en todo el mundo

Se ha descubierto una vulnerabilidad crítica en PHPMailer, una de las bibliotecas Open Source de PHP más utilizadas para enviar emails y que es utilizada por millones de usuarios en todo el mundo.

PHP es la tecnología a nivel de servidor más popular de la web, habiéndose convertido en el puntal principal de muchos CMS populares como WordPress, Drupal, 1CRM, SugarCRM, Yii y Joomla. Por otro lado, todos esos gestores de contenidos incluyen PHPMailer para enviar correos electrónicos utilizando varios métodos, entre los que se encuentra el SMTP.

La vulnerabilidad ha sido descubierta por el investigador en seguridad polaco Dawid Golunski, de Legal Hackers, y se le ha asignado el código CVE-2016-10033. Según cuenta el investigador, un atacante podría ejecutar código arbitrario de forma remota en el contexto del servidor web y comprometer componentes de la aplicación web objetivo como los formularios de contacto y retroalimentación, formularios de registro, restablecimientos de contraseñas y otros mecanismos que terminen emitiendo correos electrónicos.

Por suerte los desarrolladores de PHPMailer han parcheado la vulnerabilidad nada más ser descubierta en la versión 5.2.18. Todas las versiones anteriores contienen la vulnerabilidad, por lo que se recomienda encarecidamente llevar a cabo el proceso de actualización de esta biblioteca de PHP.

FUENTE: http://muyseguridad.net/2016/12/26/fallo-phpmailer-expone-millones-web/

RecuperaBit – Herramienta forense para la Reconstrucción del Sistema de Archivos

RecuperaBit es un software de seguridad informática que intenta reconstruir las estructuras del sistema de archivos y recuperar archivos. Actualmente sólo soporta NTFS.

RecuperaBit intenta reconstruir la estructura de directorios independientemente de:

- Tabla de particiones ausente
- Límites de particiones desconocidos
- Metadatos parcialmente sobrescritos
- Formato rápido

```
usage: main.py [-h] [-s SAVEFILE] [-w] [-o OUTPUTDIR] path

Reconstruct the directory structure of possibly damaged filesystems.

positional arguments:
  path                  path to the disk image

optional arguments:
  -h, --help            show this help message and exit
  -s SAVEFILE, --savefile SAVEFILE
                        path of the scan save file
  -w, --overwrite       force overwrite of the save file
  -o OUTPUTDIR, --outputdir OUTPUTDIR
                        directory for restored contents and output files
```

El argumento principal es el path para una imagen bitstream de un disco o partición. RecuperaBit determina automáticamente los sectores desde los que se inician las particiones explica Salvador Ruiz, experto de seguridad informática de iicybersecurity IICS.

- RecuperaBit no modifica la imagen del disco, sin embargo, lee algunas partes de ella varias veces a través de la ejecución. También debería funcionar en dispositivos reales, como / dev / sda, pero esto no es recomendable por los expertos de seguridad informática.
- Opcionalmente, se puede especificar un archivo guardado con -s. La primera vez, después del proceso de escaneado, los resultados se guardan en el archivo. Después de la primera ejecución, el archivo se lee para analizar únicamente sectores interesantes y acelerar la fase de carga.
- La sobrescritura del archivo guardado se puede forzar con -w.
- RecuperaBit incluye una pequeña línea de comandos que permite los consultores de seguridad informática recuperar archivos y exportar el contenido de una partición en formato CSV. Éstos se exportan en el directorio especificado por -o (o recuperabit_output).

Pypy.- RecuperaBit se puede ejecutar con la implementación estándar de cPython, sin embargo la velocidad puede incrementarse al usarla con el intérprete Pypy y el compilador JIT según expertos de seguridad informática: pypy main.py /path/to/disk.img

Recuperación del contenido del archivo.- Los archivos se pueden restaurar uno a la vez o recursivamente, comenzando desde un directorio. Una vez finalizado el proceso de análisis, puedes comprobar la lista de particiones que se pueden recuperarse mediante el siguiente comando en el indicador:

Recoverable.- Si desea recuperar archivos a partir de un directorio específico, puedes imprimir el tree en pantalla con el comando tree o puede exportar una lista de archivos CSV.

Acuerdo a expertos de seguridad informática, si prefieres extraer todos los archivos de los nodos Root y Lost Files, debes conocer el identificador del directorio raíz, dependiendo del tipo de sistema de archivos.

FUENTE: http://noticiasseguridad.com/importantes/recuperabit-herramienta-forense-para-la-reconstruccion-del-sistema-de-archivos/

Humor

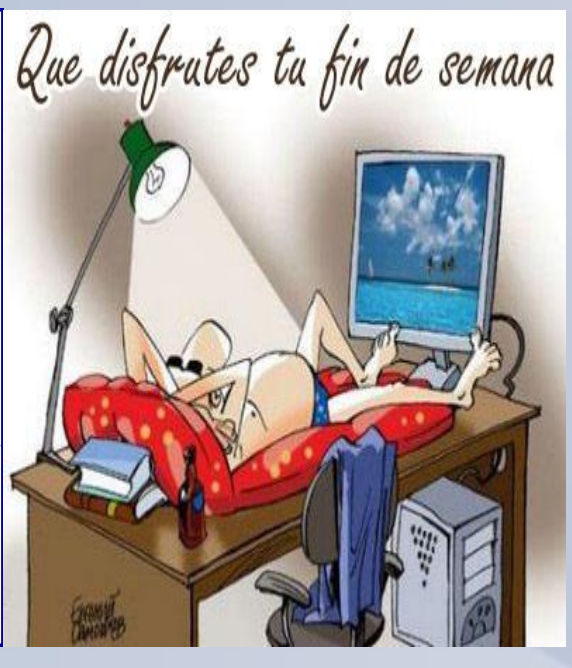

Él tiene WiFi


GLASBERGEN
Querido Andy, ¿Cómo has estado? Tu mamá y yo estamos bien. Te extrañamos mucho. Por favor, apaga la computadora y baja para comer algo.
Con amor, Papá


No lo niegues, me engañas con el raton del ordenador. El niño tiene bolita en la barriga.


¿ El móvil?. ¿Se coloca a la izquierda o a la derecha?


- ¿Sigues enfadada?
- Me prometiste que le dirías feliz nochevieja a mi madre.
- ...se lo he dicho...
- Mentiroso !, le dijiste... "Feliz noche, vieja"
www.consejosdelimpieza.com


Que disfrutes tu fin de semana

Las tendencias en ciberseguridad que marcarán 2017

Incremento de ataques a dispositivos móviles, las vulnerabilidades del «Internet de las Cosas» o las infraestructuras críticas están en el punto de mira de los ciberdelincuentes y seguridad informática es uno de los mayores quebraderos de cabeza para los desarrolladores y, cada vez más, para los usuarios que sienten la preocupación de dejar la puerta abierta a sus datos personales para fines comerciales ilícitos.

En esta era en la que la sociedad se adentra, que han bautizado como «Internet de las Cosas», se ha demostrado que no hay ningún aparato electrónico conectado a internet que sea 100% seguro. Los ciberdelincuentes lo saben y adaptan sus técnicas a los nuevos escenarios. Pero, ¿hacia dónde vamos? ¿Qué nos deparará el futuro en estas lides? El uso de dispositivos móviles, ataques a infraestructuras críticas o la hiperconectividad son algunas de las predicciones clave sobre ciberseguridad que se mantendrán para 2017, según los pronósticos de la firma de seguridad informática Check Point.

Ataques a dispositivos móviles

Los dispositivos móviles se han colocado en el punto de mira de los ciberdelincuentes. Desde hace algún tiempo se ha roto el mito que este tipo de aparatos están libres de virus informáticos y no son objeto de ataques. Nada más lejos de la realidad. En los últimos años el uso de «Smartphone» ha aumentado un 394% y el de tabletas un 1.700%. A la luz de estos datos, no es de extrañar que los ataques a terminales móviles sigan creciendo. De acuerdo con un informe reciente elaborado por la compañía, uno de cada cinco empleados será en 2017 el responsable de alguna brecha de seguridad que afecte a datos corporativos. Lo harán, involuntariamente, a través de malware móvil o de redes WiFi maliciosas.

«Mientras continúe esta tendencia - rezan los expertos Check Point- las brechas generadas desde Smartphone y tablets serán un problema de seguridad empresarial cada vez más importante. Los recientes ataques a móviles de periodistas por parte de países ponen de manifiesto que este tipo de ofensiva está a la orden del día. Es probable que bandas criminales organizadas comiencen a lanzar amenazas parecidas. La seguridad móvil continúa siendo un desafío para las empresas, ya que tiene que luchar para no romper el equilibrio entre la productividad, la privacidad y la protección», vaticinan.

De hecho, datos recopilados por un laboratorio de ciberseguridad muestran que la mitad de los dispositivos móviles en todo el mundo «están en riesgo por no tener una protección adecuada» contra posibles ataques y «malware». Algunos - muy pocos, dicen los expertos- usuarios sí intentan proteger sus dispositivos móviles. Sin embargo, se limitan en gran medida al uso de contraseñas - el 81% tiene clave de acceso en sus ordenadores y el 82% han protegido sus Smartphone con esta medida de seguridad.

El «Internet de las Cosas» en el punto de mira

Que a nadie le queda duda: no hay nada 100% seguro. Siempre se queda algún hueco sin rellenar o algún agujero que alguien -los ciberdelincuentes- puede llegar a explotar. Los expertos lo tienen claro: actualizar y

parchear dispositivos inteligentes puede suponer un riesgo, especialmente si sus desarrolladores no han tenido en cuenta la seguridad como ha sucedido recientemente en el mayor ciberataque de la última década. «El año que viene las compañías deben estar preparadas para luchar contra ciberataques dirigidos a todo tipo de elementos conectados, como por ejemplo las impresoras», aseguran.

Pero también en aparatos industriales

Se espera que en 2017 se produzcan nuevas ofensivas contra el «Internet de las Cosas» de perfil industrial. La convergencia entre las tecnologías de la información y la operativa las hace más vulnerables. «Las empresas tendrán que extender los controles de seguridad de ambos sistemas. Además, deberán implementar soluciones de prevención de amenazas para ambos ecosistemas», prevén.

Y es que de acuerdo con la investigación realizada por Fortinet, otra importante firma de seguridad informática, el 50% de los responsables de tecnología españoles consideran que la mejor respuesta al incremento de brechas de seguridad es invertir en nuevas tecnologías de ciberseguridad que ofrezcan protección en todo el ciclo de vida de la amenaza.

Mejorar las infraestructuras críticas

Como ha quedado demostrado en los últimos años, los ciberdelincuentes han fijado sus intereses en demostrar las vulnerabilidades de las llamadas «infraestructuras críticas» -consideradas como estratégicas- y que, en caso de ser atacadas, puede poner en riesgo la seguridad nacional o la economía. «Casi todas se construyeron antes de que el malware fuera un peligro real, por lo que en su diseño no están integrados los principios básicos de seguridad», añaden las mismas fuentes. A comienzos de 2016, de hecho, se desveló el primer apagón causado por ciberdelincuentes. Según los expertos, «los responsables de seguridad deben prepararse para posibles ataques a sus redes y sistemas, provenientes de tres actores potenciales: países, terrorismo y criminales organizados».

Vulnerabilidades de la «nube»

Otra de las previsiones que apuntan los expertos está relacionado con los servicios y plataformas que gestionan los datos a través de la llamada «nube». Y todo eso va a más. Las compañías siguen almacenando datos bajo estos sistemas y utilizan infraestructuras de red híbridas que crean «puertas traseras» tradicionales «con los que los hackers tienen acceso a otros sistemas de la empresa», consideran desde Check Point. El problema es que cualquier ataque que interrumpa el servicio o tumbe a uno de los principales proveedores cloud afectará a todos sus clientes. «Estas ofensivas suelen realizarse para impactar a una empresa en especial, pero al afectar a muchas otras, es muy difícil averiguar el motivo», dicen.

Aumento de los «secuestros online»

También han crecido los ataques de «ransomware» -secuestro virtual- que afectan a centros de datos basados en la nube. «Cuantas más empresas se pasen al cloud, más ataques de este tipo se dirigirán a sus infraestructuras emergentes. Lo harán tanto a través de archivos encriptados que se propaguen de cloud a cloud como con hackers que utilicen la nube como un multiplicador de volumen», consideran.

FUENTE: http://www.abc.es/tecnologia/redes/abci-tendencias-ciberseguridad-marcara-2017-201611021337_noticia.html