Departamento de Seguridad Informática MINSAP

Marzo 2017

Volumen 1, nº 1

Boletín de Seguridad Informática

Contenido:

Puntos de interés especial:

-La seguridad debe ser una solución y no un problema.

-TALOS es una herramienta para defensa activa ante ataques a redes de datos.

-Un experto en seguridad ha recuperado un truco que permite robar las sesiones a otros usuarios.

-El Equipo de Seguridad del Producto de **Red Hat**, la compañía más relevante de las que tienen a Linux como parte central de su negocio, ha publicado este mes su informe correspondiente al año 2016.

8 errores de seguridad en empresas que complican la vida de sus usuarios

Ahora que aprendimos que hay que tener en cuenta a los diferentes perfiles de usuarios, ¡no les compliquemos la vida! En este artículo veremos algunos ejemplos de errores que cometen las empresas al gestionar su seguridad, los cuales generan molestia a los usuarios de una red. ¡No los repitas y evita darles un dolor de cabeza!

#1 Aplican soluciones con configuraciones por defecto para todos, olvidando las necesidades particulares.

Si sus necesidades son diferentes, y por ende debemos tener en cuenta estas diferencias, tampoco podemos aplicar las soluciones o herramientas por default. Correr el antivirus en "piloto automático", no personalizar los filtros de correo o un sistema de detección de intrusos va a resultar en dolores de cabeza.

No existe una **solución mágica** que venga lista para cuidarnos, por lo que es muy importante contar con gente capacitada que pueda sacar el mayor provecho a las herramientas que se van a implementar.

LA SEGURIDAD DEBE SER UNA SOLUCIÓN Y NO UN NUEVO PROBLEMA

Muchas veces, por falta de una buena planificación en el proyecto o por querer apurar las cosas, la configuración de una herramienta queda implementada tal como viene de fábrica. Si bien probablemente de esta forma funcionará, no se está aprovechando todo su potencial.

Además, difícilmente se ajuste a las necesidades de todos los usuarios, por lo que es probable que muchos terminen teniendo problemas.

#2 El otro extremo: aplican una excesiva personalización que complica la administración.

Tampoco hay que irse al otro extremo e implementar soluciones **imposibles de administrar**. Demasiadas configuraciones y excesiva personalización hacen que se terminen teniendo más excepciones que reglas

o, peor aún, demasiados falsos positivos.

Esto es muy común a la hora de implementar sistemas de detección de intrusos (IDS), antivirus y otras herramientas de detección temprana. Si generan muchas excepciones o falsos positivos, algo definitivamente anda mal y a la larga la herramienta **pierde credibilidad**. Si todos los días el log se llena de alertas imposibles de analizar, el día que suceda un incidente, probablemente no se le preste atención o ni siquiera sea advertido. De esta forma, la administración será tan tediosa que resultará poco útil.

#3 Exigen seguridad sin proporcionar las herramientas para alcanzarla.

Por otro lado, cuanto más cerrada es una solución, más difícil es de implementar, mayor es el impacto y mayor la resistencia. Aquí tenemos un ejemplo que es clarísimo: ¡las contraseñas!

Una contraseña segura debe tener letras, números, símbolos y más de 15 caracteres; además, se debe cambiar cada dos meses y no se pueden repetir las últimas 10 claves. Siguiendo estos lineamientos, una contraseña será segura… y probablemente va a terminar pegada en un papelito en el monitor del usuario.

Si bien es necesario utilizar claves seguras, más importante es que las personas **las recuerden**, por lo que, además de implementar una política de contraseñas, también hay que instruir a los usuarios en métodos de creación de combinaciones que sean fáciles de recordar y en el uso de sistemas de gestión de contraseñas.

#4 Crean procesos demasiado engorrosos.

Otro ejemplo son los **procesos largos y burocráticos**, sobre todo para conseguir aprobaciones. Si conseguir la autorización para la apertura de un puerto o para una determinada conexión resulta tedioso y burocrático, termina siendo más fácil para el usuario enviar la información desde su cuenta o equipo personal y se pierde totalmente el control. La mayoría optará por llevarla en sus equipos personales, utilizar servicios de proxys para **evadir los controles** o cualquier otra artimaña antes de pasar por un proceso engorroso.

#5 No son específicos al hablar de seguridad.

Hoy en día, la mayoría de la gente **acepta sin leer** las condiciones y permisos que otorga, se conecta a redes Wi-Fi con solo apretar un botón y guarda las contraseñas en todos los dispositivos de manera que estén siempre sincronizadas. ¿Por qué? Porque esto es fácil y, sobre todo, **cómodo**.

Si bien los que nos dedicamos a la seguridad de la información intentamos cambiar estos hábitos en los usuarios, no podemos obligarlos a que se involucren en temas que no les atraen o les resultan complicados.

A la hora de comunicar, es importante **ir al grano** y ser específico. A los usuarios no les interesa leer una política de seguridad de 20 hojas ni todas las ventajas que tiene el último firewall que se instaló.

La seguridad debe ser una solución y no un nuevo problema. Charlas cortas, concretas, guías con buenas prácticas que sean fáciles de leer y tengan la información necesaria serán mucho más atractivas y comunicarán mejor el mensaje.

#6 No clasifican la información y pierden el foco de lo que se está protegiendo.

Antes de aplicar cualquier medida de seguridad, es importante entender el negocio y la **información crítica** que se debe proteger. Esto significa desde clasificarla hasta conocer el alcance de una medida de seguridad.

En el caso de una empresa de medicina, no es lo mismo cuidar el historial médico de un paciente que la lista de cumpleaños de los empleados. Muchas empresas gastan recursos, tiempo y esfuerzo en proteger información irrelevante, mientas dejan afuera otra más valiosa por no haberla tenido en cuenta.

Es importante realizar **auditorías** que revisen qué información se está resguardando, ya que muchas veces se gastan gigas de cintas y espacio de almacenamiento (que se traduce en un costo de infraestructura) en respaldar archivos personales que no son representativos para el negocio, o se dejan afuera bases enteras de información por no tener conocimiento de las mismas.

Si no se releva qué información es crítica para la organización… ¿cómo saber qué se debe proteger?

La **clasificación** es el primer paso para entender qué datos son críticos y cómo deben protegerse. Un error común respecto a la clasificación de la información es no determinar el dueño de los datos. Muchas veces en las empresas se piensa que el departamento de seguridad o de sistemas es el responsable de la seguridad de los datos, cuando el verdadero responsable es el dueño de esa información. Por ejemplo, el gerente de RR. HH. es responsable de la información personal de los empleados, sus análisis de desempeño, legajos etc. De la misma manera, el gerente de administración es responsable de la información contable, el comercial de los contratos con clientes, etc.

El **dueño de la información** es quien debe clasificarla e indicar qué necesita proteger; el área de seguridad debe proveerle las herramientas para proteger esa información según los requerimientos.

#7 No ven a la seguridad como un proceso.

Otro problema recurrente es creer que la seguridad es un producto y no un proceso. Sin embargo, hoy en día no se puede pensar en la seguridad como algo estático, como un problema que se soluciona configurando un firewall o un antivirus y dejándolo ahí para que haga su trabajo.

En una época tan dinámica, donde todos los días aparecen nuevas amenazas, es importante entender a la seguridad como un **proceso de mejora continua**. Para esto hay que realizar análisis de riesgos y auditorías periódicas, evaluar continuamente los resultados y establecer objetivos claros y medibles.

#8 Implementan estándares sin conocer realmente sus alcances.

Por último, implementar normas o estándares solo para que figuren en los papeles es la peor inversión.

Toda norma tiene un alcance (también conocido como *scope*), y determinar ese alcance es tan importante como la norma en sí. Debe **focalizarse** en negocio, en los procesos que realmente son el corazón de la compañía y para los cuales resulta **útil** una certificación. Implementar una norma u obtener una certificación no es algo sencillo ni económico; por lo tanto, si se invierte tiempo y dinero en alcanzarla, que sea para que realmente contribuya a cuidar la información y sea un valor agregado al negocio.

Entonces… ¿qué hacemos?

Con algunas buenas prácticas y prestando atención a estos puntos se cubrirá bastante terreno:

1.Entender el negocio: cómo funciona la empresa, cuáles son las áreas críticas y sus objetivos. Implementar medidas de seguridad que realmente sean un valor agregado y no una traba.

2.Clasificar la información: una vez que fue entendido el negocio, se debe clasificar la información. Entender cuál es crítica y por qué (si es por confidencialidad, integridad o disponibilidad).
Para esta tarea se debe involucrar a los dueños de esos datos, para que sean quienes realicen la clasificación y sean responsables de proteger esa información.
3.Hacer correctamente un análisis de riesgos que ayude a identificar todos aquellos puntos débiles que comprometan la disponibilidad, integridad o confidencialidad de la información y enfocar allí las medidas para mitigar los riesgos. Además, esto debe ser un proceso de mejora continua, por lo que se debe contar con un plan de acción que también incluya revisiones y auditorías periódicas.

4.Tener en cuenta a los usuarios. Después de todo, son ellos quienes terminarán utilizando los sistemas y medidas que se implementen, y serán los primeros en verse afectados si algo sale mal.
5.Contar con personal capacitado y dispuesto a investigar las diferentes herramientas y configuraciones que se van a implementar.
Con todo el esfuerzo que requirió lograr que las empresas inviertan en seguridad, ahora es nuestra responsabilidad utilizar esa inversión de manera efectiva y cuidar los activos importantes.

Herramienta para defensa activa ante ataques a redes de datos.

TALOS es una herramienta para defensa activa ante ataques a redes de datos. Fue creado para llenar un vacío evidente en las metodologías defensivas, una frase que lo definiría es: “Nunca se puede ganar un combate de espadas intentando nada más que paralizar los ataques del adversario”. Esta el la base de la metodología de la defensa activa, que ofrece la respuesta a este enigma. Hay un montón de cosas que se pueden hacer para detener a un atacante, que van mucho más allá de un simple “endurecimiento” de la seguridad. Talos fue creado con el objetivo de proporcionar un centro control, a través del cual los encargados de la seguridad de red puedan operar. Y de forma sencilla y poderosa, implementar herramientas de defensa activa en sus redes.

TALOS se puede lanzar mediante la ejecución de la consola principal mediante el archivo programado en Python: “talos.py”. Una vez en la consola, es posible escribir el comando “help” para ver una lista de comandos disponibles. Y también para mostrar información sobre comandos específicos y módulos. La herramienta ha sido creada intentado que fuera lo más inteligente posible dotándolo de opciones como:

1.Historial de línea de comandos que puedes, que se puede navegar a través de ella con las teclas cursoras.
2.Autocompletar inteligente.
3.En caso de que accidentalmente se escriba mal un comando la herramienta ejecuta igual el comando real.

Funciona de una manera muy similar a muchos frameworks conocidos. Fue escrito inspirado en dos frameworks: Metasploit y Recon-ng. Tiene una interfaz entre módulos y la consola a efectos de ejecución. Cada módulo incluirá en él una clase de comandos. Estos comandos son necesarios para analizar las variables enviadas desde la consola, en términos que son comprensibles para el módulo. Estos comandos ejecutan el módulo de la manera especificada por el comando específico. Aunque muchos módulos contienen comandos especificos, el comando más común para ver es el comando “run” . Se puede obtener un listado del comando para el módulo actualmente cargado ejecutando “list commands”. Si el módulo admite el comando “run” también permite “run -j”.

Esta opción de ejecución le dice al módulo que bifurque un proceso individual y que se ejecute en segundo plano. Esta característica puede ser increíblemente útil si necesita ejecutar más de un módulo a la vez. Para ejecutar su módulo, simplemente ejecute el comando específico del módulo deseado, tal como se imprime en la salida de "list commands".

Algunos módulos de TALOS están escritos para poder enviar notificaciones de nuevo a la consola de comandos. Esto puede ser increíblemente útil para detectar y frustrar un ataque a su red. Uno de los módulos capaces de enviar notificaciones de nuevo a la consola de comandos es el módulo utilizado en el modulo Honeypot.

Se pueden aprender los comandos TALOS para en el momento del ataque ser rápido y preciso. O pueden usarse alias que le permiten interartuar con el intérprete de diferentes maneras. Por ejemplo, el comando TALOS para cargar un nuevo módulo es "module". Pero es posible utilizar en lugar de este un alias en lugar de este comando. Por ejemplo, podría cargar un módulo con los comandos "load" o "use" o incluso (para enfatizar el sistema de archivos como la naturaleza de los módulos) "cd". El comando para mostrar qué variables pueden ser modificadas para un módulo es "list variables". Pero puede usar otros alias como "show options", "show variables", "list options" o incluso "ls".

También puede añadir sus propios alias. Como por ejemplo: creando una lista propia de atajos de un solo carácter para hacer la técnica de defensa aún más rápida. Simple editando el archivo de "aliases" ubicado en el directorio "conf".
El modulo mas importante es Phantom, un agente hecho para ser desplegado en una infraestructura de red, que llama TALOS y acepta comandos de TALOS. En resumen, Phantom es a TALOS como Meterpreter es a Metasploit. Mientras Metasploit es una herramienta ofensiva, TALOS es una herramienta diseñada para ayudar proteger los activos de red. Pero no siempre puede esperar que un el encargado de defender la de red tenga instalado TALOS en cada una de las máquinas de toda su red. Ahí es donde entra Phantom, puede desplegar módulos en cualquier maquina a la que tenga acceso.

Windows: Recuperan un viejo truco para robar sesiones de otros usuarios.

Aunque es antigua, un experto en seguridad ha recuperado un truco que permite robar las sesiones a otros usuarios. Funciona en todas las versiones de Windows y no necesita utilizar privilegios de administrador del equipo. Lo realmente importante, es que permite el robo de las sesiones de otros usuarios sin conocer la contraseña de acceso a la cuenta.

Que todavía no se haya corregido confunde a los expertos en seguridad. Muchos la han reportado a Microsoft, pero desde la compañía tampoco han salido al paso ni han confirmado si se trata de una función disponible en las diferentes versiones. El investigador Alexander Korznikov ha sido el encargado de reportar el ataque conocido como "escalada de privilegios y robo de sesión". Para llevar a cabo este ataque no se necesita de acceso directo de forma necesaria, pero sí es una vía que permitiría la realización del mismo. La complementaria sería la utilización de la herramienta Escritorio Remoto de Microsoft.

Este ataque resulta muy útil, ya que permitiría el robo de archivos existentes en otras cuentas del equipo o bien la escalada de privilegios a través de otra cuenta, permitiendo la instalación de software de forma no autorizada.

El único requisito que debe existir es que en la cuenta a la que se quiere acceder se haya iniciado sesión con anterioridad. Es decir, que esté activa pero bloqueada.

Cómo robar una sesión en Windows

Lo más preocupante es que es un ataque bastante sencillo de ejecutar. Una vez se ha comprendido el proceso, en menos de un minuto se puede aplicar. Todo esto, sin necesidad de tener unos conocimientos extensos en Windows ni administración de sistemas.

Existen tres formas de llevar a cabo el ataque:

1.A través de la creación de servicios.
2.Utilizando CMD.
3.Utilizando CMD y el gestor de tareas.

En principio, tanto el segundo como el tercero son los métodos más sencillos de utilizar. En ambos casos, el proceso total no supera los dos minutos.

Consecuencias a nivel de seguridad

Ahora que la seguridad y privacidad son dos temas importantes, este "fallo" aviva un poco más la polémica. Tal y como hemos indicado, desde Microsoft no han hecho ninguna puntualización y el robo de sesiones aún se puede realizar.

Para ver cuál es el calado de este "fallo", nos imaginamos que nos encontramos en una empresa en la que en un equipo existe un usuario de administrador y otro con sus documentos correspondientes. El usuario "normal" inicia sesión realiza gestiones y bloquea su equipo. Entonces el usuario administrador inicia sesión y utiliza uno de los métodos anteriores. En menos de dos minutos tendrá acceso a los documentos del otro usuarios. Si hablamos de una empresa, muchos de ellos pueden ser confidenciales.El inicio de todo esto radica en el año 2011, cuando se descubrió un comportamiento similar en las versiones de Windows. Sorprende que desde entonces Microsoft no haya tomado medidas. La única justificación es

problema de seguridad para los usuarios.

Red Hat publica su informe de riesgo de seguridad del producto 2016.

El Equipo de Seguridad del Producto de **Red Hat**, la compañía más relevante de las que tienen a Linux como parte central de su negocio, ha publicado este mes su informe correspondiente al año 2016, en el cual se ofrece **información sobre las amenazas y vulnerabilidades halladas en todos sus productos**.

Entre todos los descubrimientos plasmados en el informe, se pueden destacar los siguientes tres puntos:

1.Solo mirando los problemas que afectaron a **Red Hat Enterprise Linux**, se encontraron 38 avisos críticos que abordaron 50 vulnerabilidades críticas. Todas ellas fueron corregidas el mismo o un día después de hacerse públicas.
2.Durante el mismo periodo de tiempo, a través de todo el catálogo de Red Hat, el 76% de los problemas críticos tuvieron actualizaciones para corregirlos el mismo día o siguiente después de hacerse públicos, con un 98% que fueron corregidos como mucho una semana después de hacerse públicos.
3.El Equipo de Seguridad del Producto de Red Hat ayuda a los clientes a determinar el impacto actual de una vulnerabilidad. La mayoría de los problemas hallados en 2016 no afectaban a ninguna marca concreta.

Contando todos los productos de Red Hat, se **corrigieron en total unas 1.300 vulnerabilidades a través de la publicación de 600 avisos de seguridad** en 2016. Las vulnerabilidades más críticas fueron halladas en el navegador o sus componentes, por lo que las instalaciones de Red Hat Enterprise Linux a nivel de servidor quedaron afectadas por vulnerabilidades menos severas.

Según la compañía, una forma de reducir los riesgos es apostando por sus productos modulares, los cuales aseguran la instalación la variante correcta y la revisión del conjunto de paquetes, eliminando lo que no es necesario.

La compañía resalta en su informe el duro trabajo que supone la supervisión y corrección a nivel de seguridad de sus productos, debido a que estos están compuestos por miles de paquetes individuales.

Por otro lado, también se recalca que *"el manejo de vulnerabilidades a través de miles de componentes de terceros es una tarea significante"*, lo que da a entender que Red Hat tiene que lidiar con problemas procedentes de distintos frentes.

El Equipo de Seguridad del Producto de Red Hat tiene un gran reconocimiento por parte de la comunidad Linux, habiendo **investigado más de 2.600 potenciales vulnerabilidades** que podrían afectar a los productos de la compañía, corrigiendo un total de 1.346 vulnerabilidades.

Esto supone un aumento del 30% con respecto 2015, cuando el equipo investigó unas 2.000 potenciales vulnerabilidades.

En 2016, el 29% de las vulnerabilidades (394) fueron corregidas antes de hacerse públicas, suponiendo una disminución con respecto al 32% de 2015. La compañía espera que este dato varíe año tras año.

Por otro lado, el tiempo de embargo (estado en el que una vulnerabilidad puede no hacerse pública) medio de las vulnerabilidades fue de 7 días, reduciendo de forma notable los 13 días de 2015.