



Análisis del proceso de Administración de Vulnerabilidades.
Loza Gómez Francisco Alejandro
alejandro<dot>loza<at>gmail<dot>com
Maestría en Administración de Servicios de Tecnología de Información

ABSTRACT

La Administración de Vulnerabilidades es un proceso de gran relevancia en las organizaciones. En este trabajo se exponen algunos de los elementos de riesgo más representativos a los que deben enfrentarse las organizaciones debido a las vulnerabilidades intrínsecas a los ambientes de Tecnología de Información. Además, se propone un análisis de costos que pretende posicionar este proceso como un mecanismo de prevención, ahorro y crecimiento. El trabajo propone un proceso para la atención de vulnerabilidades, además, de algunas prácticas de naturaleza administrativa, operativa y técnica.

INTRODUCCIÓN

La Administración de Vulnerabilidades es un proceso que refleja la madurez de las organizaciones en lo que se refiere a la Tecnología de Información. Prácticamente cualquier organización que utilice las Tecnologías de Información ha tenido que implantar mecanismos de defensa contra las amenazas que enfrentan en sus actividades de negocio. Para este trabajo, se propone la siguiente definición de vulnerabilidad:

Las vulnerabilidades son fallas en diseño, configuración o funcionamiento que pueden ser aprovechadas por entidades maliciosas de manera que se obtengan privilegios de acceso mayores a los dispuestos por los responsables de los servicios de información.

En el 2006 nuevamente, y desde que se tiene registro de las vulnerabilidades ("National Vulnerability Database"), ya fue rebasada la cantidad registros reportados y reconocidos como vulnerabilidades. También es cierto que, especialmente en cuanto a la Tecnología de Información se refiere, muchas organizaciones están fuertemente enfocadas en hacer inversiones que sean efectivas y minimalistas en cuanto al costo. Los profesionales de Tecnología de Información tenemos la responsabilidad de balancear los dos hechos anteriores. Este trabajo pretende ilustrar factores importantes a considerar para tal balance. La Administración de Vulnerabilidades debe ser un proceso de prevención, en comparación de la naturaleza reactiva con la que en muchas ocasiones se procede.

Las vulnerabilidades pueden ser mitigadas mediante diversos mecanismos: instalación de parches, creación de políticas, mecanismos de hardware, mecanismos de software, ajuste de privilegios, ajustes de configuración. La decisión debe estar basada en un análisis de riesgos.

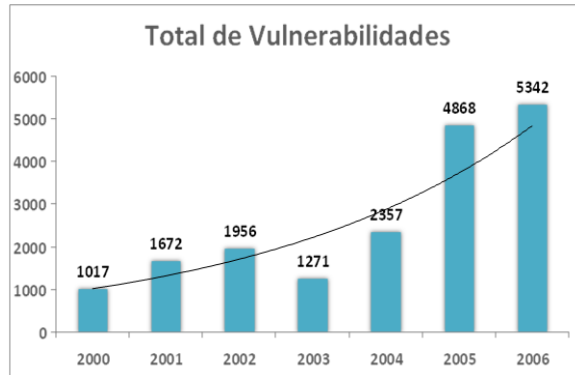


Figura 1. Vulnerabilidades reportadas en ("National Vulnerability Database")¹

UN COSTO QUE NO SE PUEDE SEGUIR DESPRECIANDO

Las vulnerabilidades son elementos intrínsecos en todos los ambientes en los que se involucra la Tecnología de Información. Por tal razón, es necesario que las organizaciones sean conscientes y responsables de los elementos de riesgo y costos que representan. Más aún cuando se combinan las consecuencias de dos situaciones inminentes:

La cantidad de vulnerabilidades, su complejidad y la rapidez con la que surgen códigos explotables de ellas seguirá aumentando. En la Figura 2, se aprecia que en lo transcurrido en 2006 ya se rebasó el número de vulnerabilidades definidas como de alto riesgo. Esta etiqueta se asigna a elementos que combinan factores de explotación remota y relativamente trivial, cuyos efectos sobre la integridad, confiabilidad y disponibilidad de la información y los recursos puede ser inmediata y permanente.

Las nuevas formas de competencia permiten y propician que el papel estratégico de los sistemas de información pueda traducirse en el catalizador para fortalecer estratégicamente a las empresas. Las TI pueden representar un diferenciador importante para los diversos productos o servicios. Los negocios dependerán cada día en mayor medida de la información que se almacena, procesa y transporta en su infraestructura de Tecnología de Información.

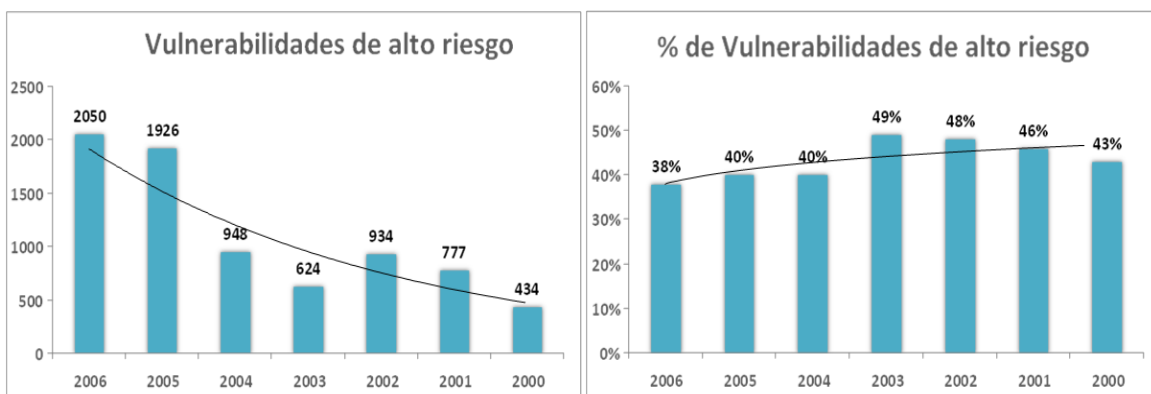


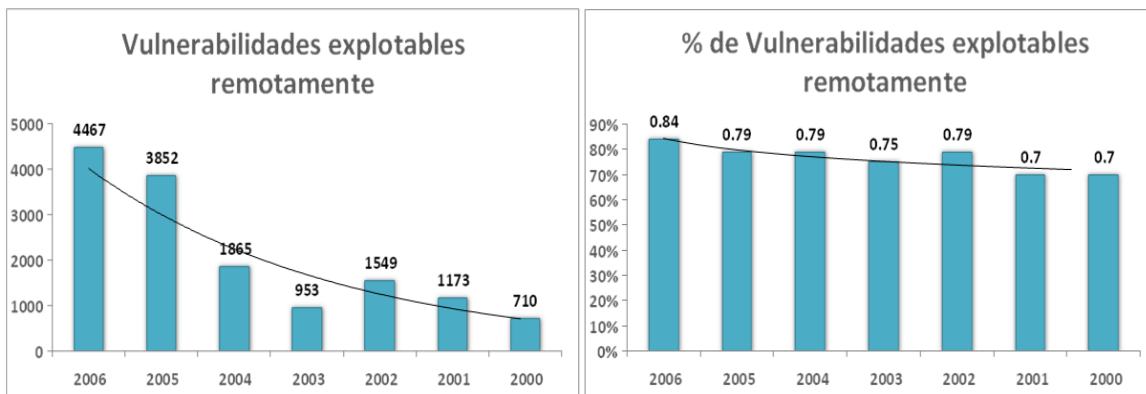
Figura 2. Vulnerabilidades reportadas en ("National Vulnerability Database") y clasificadas como de alto riesgo

¹ Las gráficas de las figuras 1,2 y 3 contemplan el período comprendido del 1 de enero de 2000 al 1 de noviembre de 2006

IDENTIFICAR LOS RIESGOS

Una gran cantidad de factores de riesgo deben ser tomados en cuenta cuando se habla de la Administración de Vulnerabilidades. Muchas organizaciones proporcionan acceso a Internet para sus empleados y colaboradores. No contar con estrategias mínimas de protección, garantiza la proliferación de malware (virus, spyware, adware, etc), cuyas consecuencias van desde la degradación en el desempeño de los equipos hasta la potencial pérdida o fuga de información altamente confidencial. La Figura 3 pone en evidencia un factor preocupante: la cantidad y el porcentaje de vulnerabilidades explotables remotamente ya rebaso este año cualquier precedente.

La atención de los incidentes ocasionados por la explotación de vulnerabilidades es un proceso reactivo (y costoso como adelante veremos). Requiere la asignación de recursos, responsabilidades y funciones extraordinarias para recuperarse de una epidemia masiva. Son de naturaleza extraordinaria debido a que, difícilmente la respuesta a incidentes que pudieron ser evitados forma parte de actividades que adicione valor a los procesos de cualquier tipo de negocio.



Las organizaciones que compiten en ambientes globales multiplican tanto sus oportunidades, como los riesgos que enfrenta. Los parámetros de operación de tales negocios deben cambiar. La continuidad del negocio está condicionada al correcto funcionamiento de todos los elementos necesarios para proporcionar valor a sus servicios.

LOS ELEMENTOS DE COSTO²

Plantear de manera integral los elementos de costo relacionados con el proceso de Administración de Vulnerabilidades es una tarea compleja, debido a que las acciones que generan costos para la organización están dispersas entre diferentes personas, áreas y espacios de tiempo. En un escenario optimista, la organización contará con un grupo especializado (si no exclusivo, bien definido en sus funciones y responsabilidades) que desplegara los ajustes necesarios para la atención de las vulnerabilidades. En la práctica se debe considerar tanto personal interno de la organización como externo. Para llevar a cabo una medida de los costos, una opción conveniente es la de agruparlos de la siguiente forma:

- Costos asociados al equipo encargado de la Administración de las Vulnerabilidades
- Costo de las herramientas utilizadas

2

Las cantidades utilizadas para ilustrar las expresiones y cálculos de costos propuesto, se basan en un 52 semanas al año, con 22 días hábiles al mes con honorarios de \$22,000.

Costos de fallas asociadas al proceso

Los elementos a considerar para cada uno de estos costos identificados se explican con detalle a continuación.

Costos asociados al equipo encargado de la Administración de las Vulnerabilidades

Este costo es relativamente sencillo de identificar y calcular, debido a que involucra los costos asociados al personal que integre el equipo responsable del proceso. Es necesario estimar la cantidad de tiempo que dediquen recursos internos al proceso, además de aquellos recursos de outsourcing que en un momento dado sea necesario utilizar.

Costo de las herramientas utilizadas

En esta partida es necesario tomar en cuenta el software y los elementos técnicos utilizados. Es necesario incluir, por ejemplo, las herramientas de escaneo de vulnerabilidades y de distribución de parches. Igualmente, si el software requiere de actualizaciones y cuotas de mantenimiento, este costo debe ser considerado. La siguiente expresión permite calcular el costo anual estimado de las herramientas utilizadas:

$$\text{Costo Anual Estimado} = \text{Suma total del mantenimiento} + \text{Suma de (precio de compra/años esperados de vida útil)}$$

Así, por ejemplo, para una organización que utilice el software cuya información se presenta en la Tabla 1:

Producto	Precio de compra	Precio de las actualizaciones de versiones	Tiempo de vida	Cuota de mantenimiento actual
Software de Administración de parches	\$300,000	\$150,000	4 años	\$30,000
Escaner de Vulnerabilidades	\$200,000	\$100,000	3 años	\$20,000

Tabla 1. Ejemplo del cálculo del costo anual de las herramientas para la Administración de Vulnerabilidades

Asumiendo que la organización estima llevar a cabo la actualización de su herramienta de detección de vulnerabilidades después de tres años, pero planea cambiar el software de administración de parches después de cuatro años. El costo anual estimado será:

$$\begin{aligned} \text{Costo Anual Estimado} &= (\$30,000 + \$20,000) + (\$300,000/4) + (\$100,000/3) \\ &= \$158,333. \end{aligned}$$

Costos de fallas asociadas al proceso

Este costo representa la medida total del impacto en el negocio ocasionado por fallas propias del proceso de administración de vulnerabilidades. El costo debe incluir tanto pérdidas tangibles (tiempo del personal y datos destruidos) como aquellas intangibles (la reputación de la organización, la falta de credibilidad en el proceso). El costo también debe calcularse en una base anual. El resultado de esta medida es muy importante para evaluar el costo total de la implantación del proceso de Administración de Vulnerabilidades. El costo más común es el originado por parches de seguridad cuyo funcionamiento corrompe el ambiente en el que es instalado. Si el costo asociado a fallas del programa es demasiado alto, la organización puede ahorrar importantes recursos si invierte en mejorar su programa. En otro caso, si este cálculo es bajo, esto puede ser una señal de éxito y la organización puede mantener este nivel o bien optimizar su costo.

Algunos ejemplos:

El parche MS05-051 (<http://www.microsoft.com/technet/security/bulletin/ms05-051.msp>), ocasiono la disrupción en todos los servicios dependientes del componente de transacciones distribuidas.

El parche MS06-042 (<http://www.microsoft.com/technet/security/Bulletin/MS06-042.msp>), el cual estaba marcado como de aplicación crítica (en términos de Microsoft significa que debe ser instalada de inmediato) afectó la funcionalidad de cierto software que utilizaba la versión HTTP 1.1 con compresión. Uno software afectado por este inconveniente fue precisamente el CRM de Microsoft®.

El parche MS06-049 (<http://www.microsoft.com/technet/security/Bulletin/MS06-049.msp>), afectaba archivos individuales que hubieran sido comprimidos mediante la utilería del Sistema Operativo. Los primeros reportes sobre este incidente se presentaron días después de que la vulnerabilidad fue publicada en el boletín mensual de Microsoft. Aunque solamente se presentaba en una versión particular de su familia de Sistemas Operativos, la información afectada por esta falla estaba perdida.

CÁLCULO ANTE LA DECISIÓN DE IGNORAR EL RIESGO

El costo potencial de no tomar en cuenta los riesgos asociados al proceso de vulnerabilidades y optar por un enfoque reactivo, puede ser descrito en la ecuación siguiente:

Costo de asumir el riesgo: # Estaciones de Trabajo X Tiempo invertido en el ajuste de los sistemas o la pérdida de productividad X Costo por hora del Recurso Humano

La expresión anterior representa el costo asociado a la respuesta a incidentes causados por la ocurrencia de los riesgos descritos en la Introducción de este trabajo, sin tomar en cuenta otros costos intangibles asociados a la discontinuidad en los servicios. Sin duda, cada organización debe considerar los daños intangibles asociados a la pérdida de productividad.

Un sencillo ejercicio, considerando una organización que se vea afectada por un ataque de virus en 1000 estaciones de trabajo:

Costo de asumir el riesgo: 1000 X 24 horas X \$125

Costo de asumir el riesgo: \$3,000,000

CÁLCULO DE LLEVARLO A CABO EL PROCESO

En primera instancia, se plantea el cálculo de los costos que la organización debería enfrentar en el caso de que se lleve a cabo el proceso de forma manual. Se asume que existe un ajuste aprobado para remediar la vulnerabilidad. Suponiendo, además, que monitorear la existencia de nuevos parches no lleva más allá de 10 minutos cada día y que el remedio de las vulnerabilidades no toma más allá de 10 minutos. De ahí podremos sacar la ecuación:

COSTO DEL MONITOREO

(10 minutos al día * 260 días)/60 minutos = 43.33 horas al año

43.33 horas de monitoreo * \$125 = \$5416.25

COSTO DE LA EJECUCIÓN DE LOS AJUSTES

(Número de equipos a ajustar) * (Número de ajustes) * (Costo del Recurso Humano)

COSTO TOTAL: MONITOREO + EJECUCIÓN DE LOS AJUSTES

Tomando nuevamente el ejemplo de mil máquinas, el costo anual sería:
 $\$5416.25 + 1000 * 80 * (\$125/6)$
 $\$1,672,082.91$

Una segunda opción, es la de adquirir una herramienta para automatizar el despliegue de las soluciones a las vulnerabilidades. Esta solución tendría un costo total compuesto por el costo de la herramienta y el costo del recurso humano asociado a su administración y ejecución. Típicamente, este tipo de soluciones son vendidas de acuerdo al número de equipos a proteger.

COSTO TOTAL: COSTO DE LA HERRAMIENTA + COSTO DEL RECURSO HUMANO

De acuerdo al resto de las opciones, es interesante calcular un costo de licenciamiento que pudiera marcar esta opción como viable

Comparando con el supuesto de ignorar el riesgo:

COSTO VIABLE POR LICENCIA: (COSTO DE IGNORAR EL RIESGO - COSTO DEL RECURSO HUMANO)/NÚMERO DE MÁQUINAS

COSTO VIABLE POR LICENCIA: $(\$3,000,000 - \$22,000*12)/1000$

COSTO VIABLE POR LICENCIA: $\$2736000/1000$

COSTO VIABLE POR LICENCIA: $\$2736$

Comparando con el supuesto de llevar a cabo el proceso manual:

COSTO VIABLE POR LICENCIA: (COSTO DEL PROCESO MANUAL - COSTO DEL RECURSO HUMANO)/NÚMERO DE MÁQUINAS

COSTO VIABLE POR LICENCIA: $(\$1,672,082.91 - \$22,000*12)/1000$

COSTO VIABLE POR LICENCIA: $(\$1408082.91)/1000$

COSTO VIABLE POR LICENCIA: $\$1408.082$

PROCEDIMIENTO DE ADMINISTRACIÓN DE VULNERABILIDADES

Este procedimiento es una propuesta que combina las acciones necesarias para acometer la Administración de Vulnerabilidades.

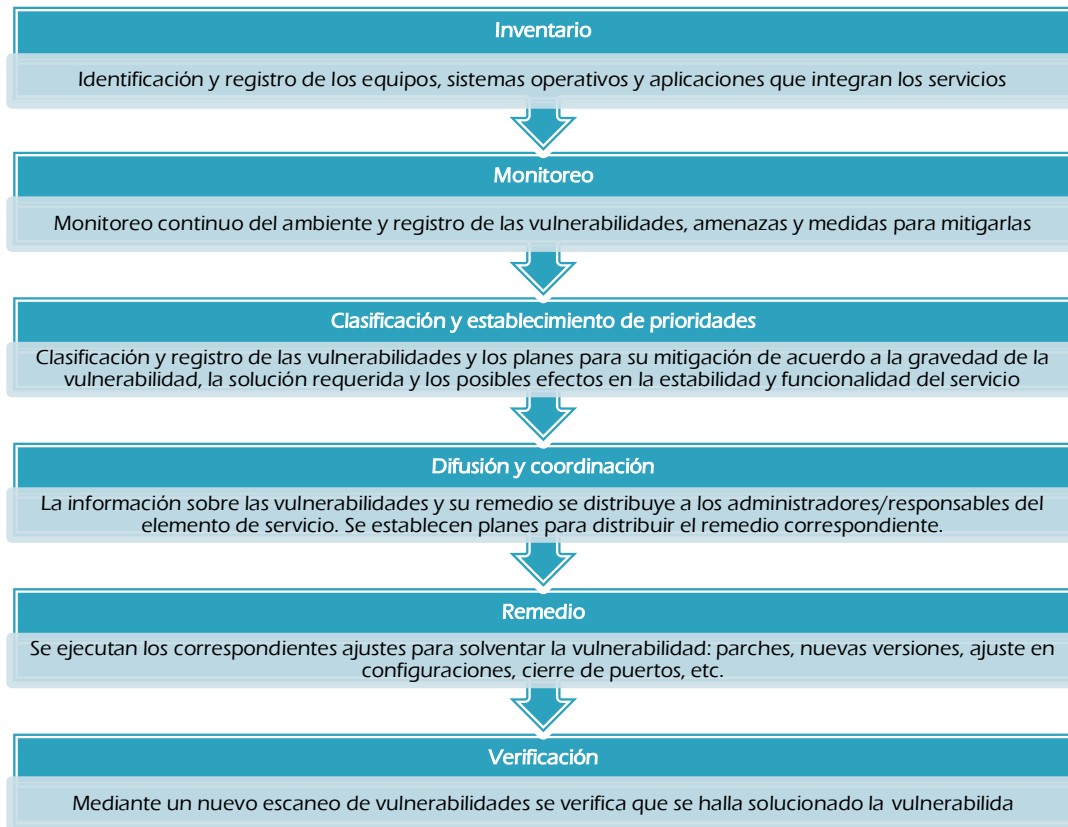


Figura 4. Procedimiento propuesto para la Administración de Vulnerabilidades

Las organizaciones deben contar con un equipo que sea explícitamente responsable de coordinar y/o llevar a cabo las diversas tareas asociadas con la Administración de Vulnerabilidades. Las funciones específicas de este grupo será la de monitorear las bases de datos de vulnerabilidades, la estabilidad del ambiente, la correcta aplicación de las soluciones y, en general, las especificadas en la Figura 4.

CONCLUSIONES

Crear un grupo que coordine el proceso de Administración de Vulnerabilidades

La integración de este grupo puede resultar útil en un aspecto adicional al de la coordinación del propio proceso. Si se decide, por ejemplo, llevar a cabo algunas funciones con recursos de soporte técnico y atención a usuarios, sus habilidades técnicas irán creciendo hasta atender vulnerabilidades que requieran ajustes de configuraciones, cierre de puertos y servicios, ajuste en listas de control de acceso, etc.

Implementar mecanismos para el control de inventarios de recursos

Muchas vulnerabilidades escapan a su identificación y registro debido a que residen en recursos que no se encuentran propiamente administrados. La identificación de los recursos debe estar

acompañada de un proceso claro para establecer prioridades. El valor que una organización le da a sus recursos de tecnología debe ser establecido tomando en cuenta los factores siguientes: el trabajo requerido para desarrollarlo, los costos de mantenimiento, el daño que causaría a la organización si fuera destruido o perdido, los beneficios que los competidores tendrían con la afectación del servicio, etc. Para establecer una relación costo/beneficio efectiva, es indispensable que la organización establezca de manera precisa el valor de la información y los recursos que pretende proteger.

Estandarizar las configuraciones de los equipos

La Administración de Vulnerabilidades es uno más de los procesos fuertemente beneficiados por la estandarización de configuraciones. Al ser publicadas nuevas vulnerabilidades y los correspondientes remedios propuestos, la estandarización incrementa notablemente la confiabilidad de los procedimientos de prueba y administración de cambios en todo el ambiente de la organización. Si el ambiente cuenta con un proceso de despliegue y actualización de configuraciones estándar en sus equipos, también se reduce de forma importante el tiempo de recuperación a las diferentes contingencias.

Wake On Lan

Para estaciones de trabajo de usuarios, la solución de vulnerabilidades puede tener lugar en horarios que no interfieran con su actividad productiva. Aunque existe la posibilidad de coordinar ventanas de tiempo (y es una opción importante), es conveniente hacer uso de las capacidades de WOL (wake on lan), que permiten la aplicación de parches, el ajuste de configuraciones y cualquier otra medida dispuesta por el equipo de Administración de Vulnerabilidades de una manera imperceptible para los usuarios. Sin embargo, el equipo debe manejar los riesgos que el propio uso de esta tecnología introduce.

Establecer métricas para las vulnerabilidades

La única forma de conocer el progreso de la organización en el tratamiento de sus riesgos y amenazas es la de contar con las métricas dispuestas y adecuadas. Algunos índices que pueden ser de utilidad son los siguientes;

- Ponderar el número de vulnerabilidades publicadas contra el número correspondiente a las vulnerabilidades aplicadas
- Tiempo de despliegue de un mitigador a lo largo de la organización
- Número de incidentes ocasionados por agentes que aprovecharon vulnerabilidades de solución conocida
- Número de vulnerabilidades efectivamente mitigadas
- Tiempo de indisposición de servicios ocasionado por la mitigación de vulnerabilidades
- Tiempo de los Recursos Humanos directamente invertido en el proceso de Administración de Vulnerabilidades
- Número de vulnerabilidades identificadas por host
- Número de vulnerabilidades mitigadas por host

Centralizar el proceso de Administración de Parches

De acuerdo a lo expuesto en el trabajo, llevar a cabo el despliegue de parches de forma manual es demasiado costoso, o bien, muy riesgoso para la continuidad del negocio. La centralización de la administración de parches representa ahorros muy importantes en cuestiones que parecen triviales, como el consumo de ancho de banda. Un solo repositorio descarga los parches liberados por los proveedores.

Las herramientas dispuestas para la gestión de parches contribuyen de forma muy importante para la productividad del grupo de Administración de Vulnerabilidades. Entre otras, funciones importantes la centralización del proceso tiene las siguientes ventajas

Uno de los costos más importantes es el de llevar a cabo los ajustes necesarios cuando se distribuyen parches cuyo funcionamiento no convive de manera adecuada con el ambiente de TI de la organización. Estas herramientas permiten llevar a cabo ajustes masivos o desinstalación de parches que causen interrupción al entrar en contacto con el ambiente de servicios de la organización

Verificar la integridad del software descargado de Internet para prevenir corrupciones casuales o intencionales

Combinar herramientas de software comercial con Open Source

Ninguna herramienta puede representar una solución que integre todas alternativas, funcionalidades y necesidades que los distintos tipos de organizaciones exigen para sus procesos de Administración de Vulnerabilidades. Además, algunas herramientas de distribución gratuita (Open Source) son muy útiles y tienen la suficiente madurez para incorporarse para su utilización en ambientes corporativos. Los resultados y la funcionalidad de herramientas comerciales y gratuitas pueden compararse, contrastarse y complementarse para buscar la mejora continua de este proceso.

Seguridad en profundidad

La mejor manera de proteger un ambiente de las amenazas es contando con una estrategia de seguridad en profundidad. Aún cuando exista una buena práctica de despliegue de parches y atención de vulnerabilidades, es conveniente contar prácticas de asignación de permisos basados en el principio del menor privilegio, y de acuerdo a los recursos de la organización, establecer mecanismos de protección frontera que puedan ser configurados para repeler una buena cantidad y naturaleza de amenazas en conjunción con herramientas de detección de intrusos en cada host. Finalmente, y de ninguna manera menos importante, proteger los bienes de las organizaciones exige la combinación de diversas prácticas, tanto culturales, como de disciplina y entrenamiento de los usuarios.

Handle with care

Así describe Mitnick un ataque en *The Art of Intrusion* (Mitnick, 2006): "*Fort he White House hack, Zyklon says he initially ran a program called a CGI (common gateway interface) scanner, wich scans the target system for CGI vulnerabilities. He discovered the Web site was susceptible to attack using the PHF exp bit.* ". La misma actividad precede una gran cantidad de ataques descritos en este libro, una vez que los perpetradores consiguen acceso a un equipo. Cuando una organización decide implementar un procedimiento de Administración de Vulnerabilidades, la información que las herramientas de escaneo producen, deben ser tratadas como extremadamente confidenciales. Sí un reporte de vulnerabilidades se encuentra en manos equivocadas, el siguiente paso para su explotación puede ser incluso trivial.

OCTAVE®

OCTAVE® es la abreviatura de *Operationally Critical Threat Asset, and Vulnerability Evaluation*, que significa evaluación de amenazas críticas para la operación, inventarios y vulnerabilidades. Se trata de un enfoque propuesto desde Carnegie Mellon University que está llamado a convertirse en un estándar para la Administración de Vulnerabilidades.

OCTAVE® se enfoca en una evaluación sistemática, dependiente del contexto operativo de las organizaciones y que esta concebida para aplicarse utilizando recursos con registros internos. Este enfoque está contenido en un conjunto de criterios que define los elementos esenciales para llevar a cabo una evaluación de riesgos de seguridad de la información. OCTAVE® es un proceso que se propone en tres fases, resumido en la figura siguiente.

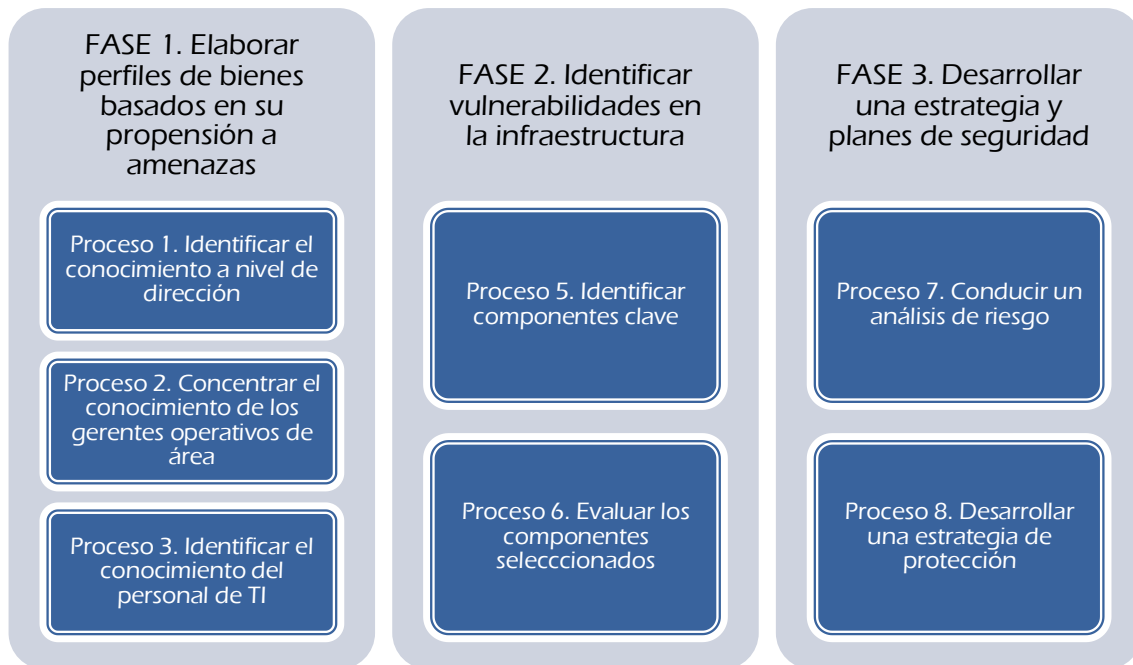


Figura 5. OCTAVE®

Aunque la documentación indica que esta guía esta concebida para organizaciones de tamaño considerable (incluso se precisa que está en desarrollo una versión para pequeños departamentos de TI), se trata de una herramienta que integra un procedimiento completo que puede ser adaptado al tamaño y necesidades de diversas organizaciones.

El material esta disponible de manera gratuita e incluye plantillas y hojas de trabajo que facilitarían el proceso para una organización que decida comprometerse a integrar un proceso de Administración de Vulnerabilidades.

Bibliografía

- Jeff Jones *Security Blog : 2006 January through September Vulnerability Trends*. (s.f.). Recuperado el Noviembre 3, 2006 de <http://blogs.technet.com/security/archive/2006/10/17/2006-january-through-september-vulnerability-trends.aspx>.
- Alberts, C. J., & Dorofee, A. J. (Diciembre, 2001). *OCTAVE® Publications*. Recuperado el Septiembre 9, 2006 de <http://www.cert.org/octave/pubs.html>: <http://www.cert.org/archive/pdf/01tr016.pdf>.
- DHS National Cyber Security Division/US-CERT. (s.f.). *National Vulnerability Database*. Recuperado el Noviembre 1, 2006 de <http://nvd.nist.gov/>: <http://nvd.nist.gov/statistics.cfm>.
- Foster, J. C. (2005). *Buffer Overflow Attacks*. Rockland, MA: Syngress.
- Fyodor. (s.f.). *SecLists.Org Security Mailing List Archive*. Recuperado el Junio, 2006 de <http://seclists.org/>.
- Harris, S. (2005). *CISSP All-in-One Exam Guide, Third Edition*. Emeryville, California: McGraw-Hill/Osborne.
- Mell, P., Bergeron, T., & Henning, D. (2005, Noviembre). *NIST Computer Security Special Publications*. Recuperado el Septiembre 9, 2006 de <http://csrc.nist.gov/publications/nistpubs/index.html>: <http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>.
- Mitnick, K. D. (2006). *The Art of Intrusion*. Indianapolis, IN: Wiley Publishing Inc.
- Wipro Technologies. (Abril, 2005). *The Total Cost of Security Patch Management*. Retrieved Septiembre 9, 2006 from <http://download.microsoft.com>: http://download.microsoft.com/download/1/7/b/17b54d06-1550-4011-9253-9484f769fe9f/TCO_SPM_Wipro.pdf.

APÉNDICE A. RECURSOS PARA LA ADMINISTRACIÓN DE VULNERABILIDADES

Listas de distribución

Las listas de distribución son de gran utilidad para el grupo de Administración de Vulnerabilidades. Es muy común que las vulnerabilidades recién descubiertas, los problemas introducidos por parches de reciente liberación y las mejores prácticas del tema suelen tener como primicia este tipo de listas.

SecurityFocus.com. Las listas de distribución que se encuentran en securityfocus.com, manejadas por Symantec, contienen excelentes recursos sobre amenazas, vulnerabilidades y exploits.

Bugtraq@securityfocus.com

Focus-MS@securityfocus.com

Pen-Test@securityfocus.com

patchmanagement@patchmanagement.org. Esta lista es una herramienta muy valiosa para la investigación de asuntos relacionados con la distribución de parches para diferentes proveedores de parches.

Vulnwatch. Esta lista de distribución proporciona detalles técnicos y vulnerabilidades recientemente descubiertas. La suscripción puede realizarse en www.vulnwatch.org.

Sindicación de contenidos en (Fyodor).

- <http://seclists.org/rss/bugtraq.rss>
Un de las lista de distribución de seguridad más populares. Es común que las vulnerabilidades sean publicadas primeramente en esta lista.
- <http://seclists.org/rss/dailydave.rss>
Lista de discusión con un alto enfoque técnico. Su alcance abarca la investigación de vulnerabilidades, el desarrollo de exploits y la divulgación de eventos de seguridad. Fue iniciada por el fundador de la compañía ImmunitySec Dave Aitel.
- <http://seclists.org/rss/fulldisclosure.rss>
Foro de discusión que funciona sin moderador. En ocasiones, las vulnerabilidades se vislumbran horas antes de que se publiquen en la lista Bugtraq. Un problema con esta lista es que cerca del 80% de su contenido no trasciende en vulnerabilidades reales, por lo que se requiere un poco de tiempo para revisarla y encontrar algo interesante.
- <http://seclists.org/rss/pen-test.rss>
En esta lista de discuten, presentan y desarrollan técnicas y estrategia que pudieran resultar de gran utilidad para aquellos con interés en seguridad y auditorías de red.

Software para la Administración de Parches (Mell, Bergeron y Henning, 2005)

Software	Proveedor	URL
Altiris Patch Management Solution	Altiris	http://www.altiris.com/products/patchmanagement/
ANSA	Autonomic Software, Inc.	http://www.autonomic-software.com/patch.html
BigFix Patch Manager	BigFix, Inc.	http://www.bigfix.com/ (El trabajo original contenía un link erróneo: http://www.bigfix.com/products/products_patch.html)
BindView Patch Management	BindView Corporation	http://www.bindview.com/Solutions/VulnMgmt/ManagePatches.cfm
C5 Enterprise Vulnerability Management Suite	Secure Elements	http://www.secure-elements.com/products/
Ecora Patch Manager	Ecora Software	http://www.ecora.com/ecora/products/patchmanager.asp

eTrust Vulnerability Manager	Computer Associates International, Inc.	http://www3.ca.com/Solutions/Product.asp?ID=4707
GFI LANguard Network Security Scanner	GFI Software Ltd.	http://www.gfi.com/lannetscan/
Hercules	Citadel Security Software	http://www.citadel.com/hercules.asp
HFNetChkPro	Shavlik Technologies, LLC	http://www.shavlik.com/
HP OpenView Patch Manager using Radia	Hewlett-Packard Development Company	http://www.managementsoftware.hp.com/products/radia_patm/index.html
Kaseya Patch Management	Kaseya, Inc.	http://www.kaseya.com/prod1/pl/patch_management.phtml
LANDesk Patch Manager	LANDesk Software	http://www.landesk.com/Products/Patch/Index.aspx
LiveState Patch Manager	Symantec Corporation	http://www.symantec.com/enterprise/products/overview.jsp?pcid=1025&pvid=925_1 (El documento original tiene este link: http://sea.symantec.com/content/product.cfm?productid=30)
ManageSoft Security Patch Management	ManageSoft Corporation Ltd.	http://www.managesoft.com/product/patchmanagement/index.xml
Marimba Patch Management	BMC Software, Inc.	http://www.bmc.com/products/proddocview/0,2832,19052_19429_18225689_106792,00.html (El documento original tiene este link: http://www.marimba.com/products/solutions/patch-mgmt.html)
NetIQ Vulnerability Manager	NetIQ Corporation	http://www.netiq.com/products/vsm/default.asp
Opsware Server Automation System	Opsware, Inc.	http://www.opsware.com/products/serverautomation/patchmgmt/
PatchLink Update	PatchLink Corporation	http://www.patchlink.com/products_services/patchlink_update.html
PolicyMaker Software Update	DesktopStandard Corporation	http://www.desktopstandard.com/PolicyMakerSoftwareUpdate.aspx
Prism Patch Manager	New Boundary Technologies	http://www.newboundary.com/products/prismpatch/prismpatch_info.htm
SecureCentral PatchQuest	AdventNet, Inc.	http://www.securecentral.com/products/patchquest/
Security Update Manager	ConfigureSoft	http://www.configuresoft.com/SUMMain.aspx