BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE No. 0029-2012-GTI000

SOFTWARE PARA EVALUACIÓN DE LA SEGURIDAD DE LA RED Y GESTIÓN DE ACTUALIZACIONES

1. **NOMBRE DEL ÁREA:**

   Dpto. de Redes, Telecomunicaciones y Bases de Datos

2. **RESPONSABLE DE LA EVALUACIÓN:**

   Alexander Gamboa Inga

3. **CARGO:**

   Especialista en Seguridad Informática en Redes

4. **FECHA:**

   25 de octubre de 2012.

5. **JUSTIFICACIÓN:**

   Uno de los principales medios a través de los cuales se materializan los incidentes de seguridad informática, es la explotación por parte de los atacantes, de las vulnerabilidades existentes en el software empleado.

   La aplicación proactiva de actualizaciones de seguridad o parches es esencial para mantener la disponibilidad operacional y la integridad de los sistemas de TI de las organizaciones, pues reduce la probabilidad de explotación de vulnerabilidades. Sin embargo los ataques más importantes en los últimos años se han dirigido a las vulnerabilidades conocidas cuyos parches ya existían. Aunque muchas organizaciones sean competentes en el mantenimiento de sus servidores críticos, por lo general el mismo nivel de atención no se les da a los equipos de escritorio de los usuarios y las computadoras portátiles, a pesar de que estadísticamente es aquí donde se producen la mayoría de las vulnerabilidades.

   La gestión de actualizaciones es un proceso que debe hacerse de manera rutinaria y deben ser lo más amplio posible para que sea más eficaz. En una red de cientos de sistemas, todo lo que necesita es que un equipo llegue a ser comprometido para que múltiples equipos sean comprometidos también. Esto no quiere decir que todos los sistemas deben ser tratados por igual, cada empresa debe asignar prioridades a sus activos y proteger a los más críticos en primer lugar. Lo que es importante es asegurarse de que la aplicación de parches se realice en todos los equipos y no sólo en los más críticos. El proceso de aplicación de actualizaciones no sólo requerirá el esfuerzo de los administradores del sistema, sino que también requiere el apoyo de la organización en lo que respecta a la coordinación de las ventanas de mantenimiento.

   La gestión de actualizaciones juega un rol importante en la postura de seguridad de la empresa, pero no debe ser entendida como la solución para todas las

INFORMETECNICO00029-2012-GTI000

Alexander Gamboa Inga
Reg. 2092

MIGUEL TEJADA MALASPINA
Sub-Gerente de Servicios de Tecnologías de Información

vulnerabilidades de seguridad. Contar con múltiples controles de seguridad, de los cuales la gestión de actualizaciones es parte, es el medio más eficaz de protegerse contra las amenazas potenciales.

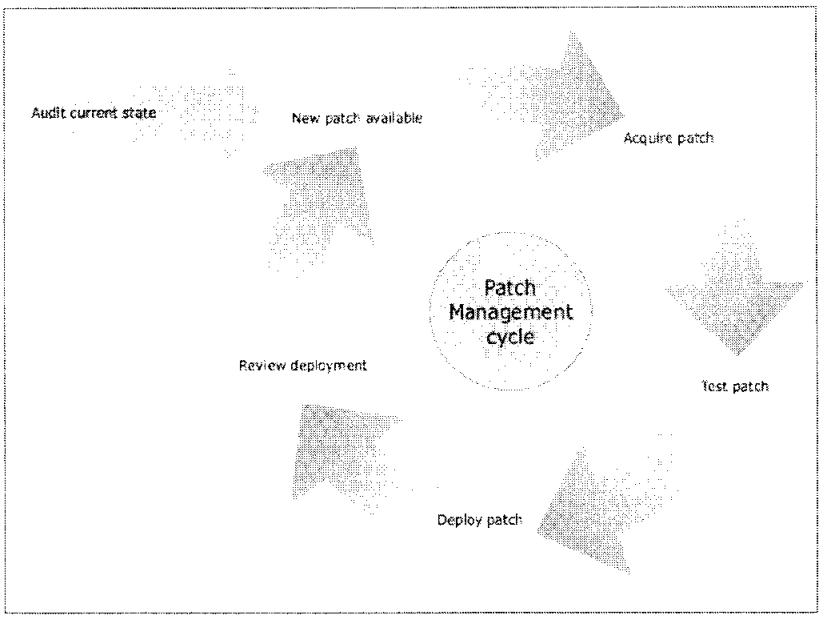

Figura N° 1: Patch Management Cycle
Fuente: *Patch Management (SANS Institute InfoSec Reading Room)*

La gestión de vulnerabilidades es algo más que aplicar parches. Para construir un sistema verdaderamente robusto se necesita incorporar la gestión de inventarios, gestión de configuración y gestión de cambios en el ciclo de vida de aplicación de actualizaciones. Además, para un control más eficaz se necesita ejecutar evaluaciones de seguridad periódicas.

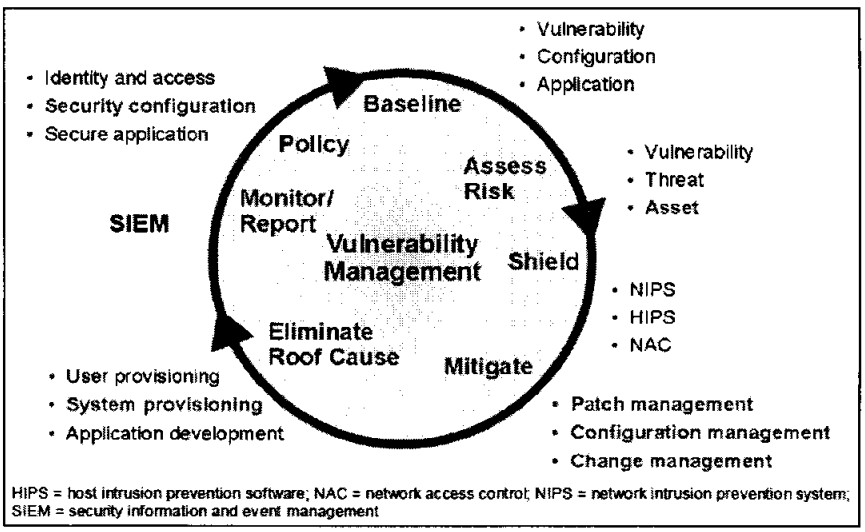

Figura N° 2: Vulnerability Management Life Cycle
Fuente: *Understanding Vulnerability Management Life Cycle Functions (Gartner)*

Alexander Gamboa Inga
Reg. 2092

La Norma Técnica Peruana NTP-ISO/IEC 17799 2007 establece que "*una vez identificadas las vulnerabilidades técnicas potenciales, la organización debe identificar los riesgos asociados y las acciones a ser tomadas en cuenta. Estas acciones pueden implicar el parchado de los sistemas vulnerables y/o la aplicación de otros controles*".

En el mercado existen soluciones que abordan estos requerimientos proporcionando las siguientes funcionalidades:

- ✓ Son capaces de gestionar actualizaciones para software no Microsoft, tales como Adobe Flash Player y SUN Java Runtime, de uso común en las estaciones.
- ✓ Proporcionan un agente de gestión independiente.
- ✓ Pueden operar en modo push, realizando actualizaciones directas desde la consola hacia las estaciones.
- ✓ Permiten la funcionalidad de evaluación de seguridad (análisis de vulnerabilidad y auditorías de seguridad de la red).
- ✓ Permiten realizar reportes de las evaluaciones realizadas y del estado de distribución de actualizaciones.

En lo que respecta al BCRP, desde fines del año 2009 se ha venido utilizando el software Microsoft WSUS, de uso gratuito, para la gestión de actualizaciones. Dicho software presenta las siguientes limitaciones:

- ✓ Sólo es posible gestionar actualizaciones de productos Microsoft.
- ✓ El software cliente (agente WSUS) depende de otros servicios de Windows para su adecuado funcionamiento y en caso de falla su reporte de error es genérico.
- ✓ Opera sólo en el modo pull por lo que, aunque es posible programar que una estación solicite la descarga de una actualización, no es posible forzar la aplicación de actualizaciones directamente desde la consola.
- ✓ No incluye la funcionalidad de evaluaciones de seguridad.
- ✓ Las opciones de reporte son limitadas.

6. ALTERNATIVAS:

En el mercado local se han encontrado productos de los siguientes fabricantes: GFI, BeyondTrust y ManageEngine.

7. ANÁLISIS COMPARATIVO TÉCNICO:

Característica	GFI	BeyondTrust	ManageEngine
Permitir la gestión de actualizaciones de productos Microsoft.	Si	Si	Si
Permitir la gestión de actualizaciones de productos no Microsoft, tales como Adobe Acrobat Reader, Adobe Flash Player y SUN Java Rutime.	Si	Si	No
Ejecutar escaneos de vulnerabilidad para determinar las actualizaciones pendientes de instalación.	Si	Si	Si
Administración centralizada	Si	Si	Si

Alexander Gamboa Inga
Reg. 2092

8. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

Beneficios:

- Gestión de actualizaciones para productos Microsoft.
- Gestión de actualizaciones para productos no Microsoft, tales como Adobe Acrobat Reader, Adobe Flash Player y SUN Java Runtime.
- Evaluación de la seguridad de la red mediante la ejecución de escaneos de vulnerabilidad, que permitan determinar actualizaciones faltantes entre otros problemas de seguridad de los equipos.

Costos:

- Software
  Software para evaluación de la seguridad de la red y gestión de actualizaciones, incluyendo el mantenimiento de software (actualizaciones) y el soporte técnico por el periodo de un (01) año.

  Se obtuvieron cotizaciones referenciales por montos de S/. 35 282,00, S/. 36 585,90 y S/. 47 276,20 incluido IGV.

- Hardware necesario para su funcionamiento
  El software solicitado se ejecutará en equipos virtuales que serán proporcionados por el BCRP.

- Plazo de implementación del servicio, con las condiciones exigidas por el BCRP
  El plazo de entrega no será mayor de 15 días calendario, contabilizados a partir de la suscripción de la orden de compra o contrato.
  El plazo de implementación no será mayor de 60 días calendario, contabilizados a partir de la fecha de entrega.

9. CONCLUSIONES:

Por lo expuesto anteriormente, se considera conveniente la adquisición de un software para evaluación de la seguridad de la red y gestión de actualizaciones.

10. FIRMAS:

Leandro Alvarez Figueroa
Jefe, Dpto. de Redes, Telecomunicaciones y Bases de Datos

Alexander Gamboa Inga
Reg. 2092