Boletin de Seguridad UNAM-CERT-2011-014 Recomendaciones de seguridad para prevenir intrusiones electrónicas

US-CERT provee esta alerta técnica de seguridad en respuesta a intrusiones recientes y bien pubilicitadas sobre redes de computadoras de diferentes gobiernos, así como en el sector privado. Los administradores de red y administradores técnicos deben no solo seguir los sistemas de información para controles de seguridad delineados en NIST 800-53, sino también considerar las siguientes medidas. Estas incluyen tanto mitigaciones tácticas como estratégicas y pretenden mejorar los programas de seguridad existentes.

- **Fecha de Liberación:** 22-Jul-2011
- **Ultima Revisión:** 22-Jul-2011
- **Fuente:** US-CERT
- **Riesgo** Alto
- **Problema de Vulnerabilidad** Local y remoto
- **Tipo de Vulnerabilidad** Múltiples vulnerabilidades

1. Recomendaciones

- Implementar un Sistema de Detección de Intrusiones de Host (HIDS) que ayude a bloquear e identificar ataques comunes
- Utilizar un proxy de aplicación delante de servidores web para filtrar peticiones maliciosas
- Asegurar que "allow URL_fopen" esté deshabilitado en el servidor web para ayudar a limitar las vulnerabilidades en PHP, específicamente sobre ataques de inclusión remota de archivos.
- Limitar el uso de código SQL dinámico utilizando declaraciones preparadas, queries con parámetros, o procedimientos almacenados siempre que sea posible.
- Seguir las mejores prácticas de programación segura y validación de entradas; utilice las guías de código seguro disponibles en https://www.owasp.org/index.php/Top_10_2010 y en https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/coding/305-BSI.html
- Revisar la documentación del US-CERT pertinente a ataques de negación de servicio distribuidos: http://www.us-cert.gov/cas/tips/ST04-015.html y http://www.us-cert.gov/reading_room/DNS-recursion033006.pdf
- Considere añadir las siguientes medidas para su plan de protección de cuentas y contraseñas:

1. Utilizar autenticación de dos factores para cceder cuentas con privilegios de administrador/root.
2. Utilizar una longitud de contraseña mínima de 15 caracteres para cuentas de administrador.
3. Requerir el uso de contraseñas con caracteres alfanuméricos y símbolos.
4. Habilitar historial de contraseñas para prevenir la reutilización de contraseñas anteriores.
5. Prevenir el uso de información personal como contraseña, tales como números telefónicos y fechas de nacimiento.
6. Requerir cambios de contraseña cada 60 a 90 días.
7. Implementar NTLMv2 como el método mínimo de autenticación y deshabilitar el uso de contraseñas administradas por LAN.
8. Utilizar una longitud de contraseña mínima de 8 caracteres para usuarios con privilegios normales.
9. Deshabilitar registro (cache) de credenciales de equipo local, si no se requiere, a través de la utilización de Objetos de Política de Grupo (GPO). Para más información sobre este tema

consulte los artículos de Microsoft Suppor 306992 y 555631.

10. Implementar una política de almacenamiento seguro de contraseñas que utilice encriptación de contraseñas.

- Si una cuenta de administrador resulta comprometida, cambie la contraseña inmediatamente para prevenir la explotación continua. Los cambios a las contraseñas de administrador solo deben realizarse desde equipos que se han verificado como limpios y libres de malware.
- Implementar políticas y guías para restringir el uso de equipo personal en el procesamiento o acceso a la información o sistemas oficiales (e.g. trabajar desde casa o utilizar un dispositivo personal en la oficina).
- Desarrollar políticas para limitar cuidadosamente el uso de todos los dispositivos de almacenamiento removible, excepto cuando exista un caso de negocio válido y documentado para su uso. Estos casos de negocio deberán ser aprobados por la organización con lineamientos para su uso.
- Implementar políticas y guías para limitar el uso de servicios de redes sociales desde el trabajo, como correo electrónico personal, mensajería instantánea, Facebook, Twitter, etc., excepto cuando exista un caso de negocio válido y documentado para su uso.
- Adherirse a las mejores prácticas de seguridad en red. Ver http://www.cert.org/governance/ para mayor información.
- Implementar entrenamiento recurrente para educar a los usuarios sobre los peligros que involucra abrir correo electrónico no solicitado, y hacer click en links o archivos adjuntos de fuentes desconocidas. Referirse al NIST SP 800-50 para guías adicionales.
- Requerir a los usuarios completar el curso de entrenamiento "política de uso aceptable" de su organización (que debe incluir sitios de ingeniería social y usos diferentes a los laborales) de manera recurrente.
- Asegurar que todos los sistemas tienen actualizaciones recientes de fuentes confiables. Recordar escanear o validar con sumas de seguridad para eliminar la posibilidad de virus o modificaciones como parte del proceso de actualización.

La Subdirección de Seguridad de la Información/UNAM-CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- José Roberto Sánchez Soledad (rsanchez at seguridad dot unam dot mx)

UNAM-CERT
Equipo de Respuesta a Incidentes UNAM
Subdirección de Seguridad de la Información

incidentes at seguridad.unam.mx
phishing at seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 47