Universidad de Alcalá

Servicio de Explotación
SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 22

AMENAZAS PARA LA SEGURIDAD EN LA WEB

1 de abril de 2008

Información extraída de la revista "Sun Inner Circle". Tiene conceptos bastante alineados con los contenidos expuestos en el VI Foro de la Seguridad de RedIRIS.

En el último año, más del 50% de las vulnerabilidades de las tecnologías de la información y comunicaciones corresponden a la escala Web. La seguridad debería ser esencial en todo despliegue a escala Web, aunque a veces se pasa por alto debido a la urgencia por ofrecer nuevas aplicaciones y servicios. El equilibrio entre facilidad de uso, rendimiento y seguridad es fundamental para el éxito en la escala Web.

Amenaza 1: Acelerar las actualizaciones de servicios y de código sin considerar las implicaciones para la seguridad

Los programas se suelen probar para funcionar en situaciones ideales en lugar de adversas. Los ataques familiares, como desbordamientos de buffer, inyecciones SQL y scripts entre sitios, se basan en la premisa de que, con frecuencia, el software no se escribe para tratar adecuadamente las excepciones.

Empezar por bloques modulares y patrones bien probados es esencial para el éxito de la escala Web. Una vez ensamblados, los servicios Web se deben instalar en un lugar accesible, lo que suele conllevar permitir el acceso a través de defensas tradicionales, como firewalls de red. Los *firewalls de nivel de aplicación* pueden ser eficaces para implementar arquitecturas de defensa de profundidad.

Nada puede sustituir el desarrollo de software defensivo.

Amenaza 2: Incapacidad de proteger y auditar el número creciente de interacciones de los clientes

Cuando una organización determina que sus aplicaciones Web pueden crecer, la *gestión de identidades* es el siguiente paso para que la seguridad pueda adaptarse al crecimiento a escala Web.

Disponer de herramientas que permitan a los usuarios asignar derechos de acceso a los usuarios es esencial para que la seguridad. Esto significa que es posible asignar reglas y políticas basadas en funciones a clases concretas de usuarios.

Amenaza 3: Vincular sin criterio nuevos servicios a escala Web a otros entornos

La información que antes era inaccesible externamente ahora puede obtenerse desde cualquier lugar y con distintos dispositivos. Es un gran avance, pero vincular lo viejo, lo nuevo y lo que no guarda relación multiplica el número de riesgos potenciales para la seguridad.

También aumenta los problemas de confianza cuando los sistemas y dispositivos interconectados pertenecen a distintas entidades. Ésta es la razón por la que la capacidad de *federación de identidades* debe formar parte de todo buen arsenal de seguridad a escala Web.

Amenaza 4: No comprender la naturaleza de lectura-escritura de las tecnologías de la escala Web

La capacidad de lectura-escritura de la Web 2.0 permite integrar protocolos tales como Ajax entre distintos entornos. Esta capacidad también puede exponer a los clientes y servidores a ataques que pueden traspasar fácilmente los firewalls tradicionales.

La tendencia hacia el contenido Web auto-actualizable tiene sus pros y sus contras. Al permitir el acceso, la ejecución y la agregación de contenidos desde el cliente, se abre una nueva puerta en la que los atacantes pueden engañar a los usuarios y dirigirles a programas malintencionados que pueden infiltrarse en las redes corporativas.

Por ejemplo, Ajax permite emitir de forma asincrónica llamadas JavaScript desde un navegador. Sin embargo, la descarga de JavaScript desde sitios que no sean de confianza puede permitir a los atacantes ejecutar llamadas Ajax malintencionadas en los navegadores. Los ataques de scripts entre sitios pueden apropiarse de cuentas de usuario, lanzar intentos de *phishing* y ejecutar programas malintencionados en los sistemas de los usuarios.

Amenaza 5: Pasar por alto los fundamentos de los servicios Web

A pesar de que los despliegues a escala Web pueden parecer entornos totalmente nuevos, muchas de las consideraciones en materia de seguridad deberían resultar familiares. Los fundamentos de los servicios Web requieren la seguridad de la prueba del tiempo, la autenticación, autorización, confidencialidad, integridad y la auditoría de sistemas, redes, almacenamiento y servicios. Sin estos factores, la seguridad, sencillamente, no puede funcionar.

Los entornos a escala Web no pueden llegar muy lejos si no se basan en un fundamento seguro. La elección de hardware y sistema operativo es esencial para que los servicios Web puedan crecer con seguridad. Pero la seguridad es mucho más que una combinación de productos y tecnologías.

Las buenas prácticas, la formación, la educación, los procesos y la política son elementos importantes para desplegar aplicaciones a escala Web.