IBM Security

IBM

Gestione eficazmente los riesgos para la seguridad de las aplicaciones en la nube

Un sencillo sistema de comprobación automatizado puede optimizar y reforzar su seguridad

Artículo monográfico sobre seguridad de IBM

¿Por qué es vital la seguridad de las aplicaciones?

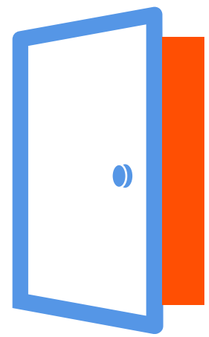
Es probable que se haya esforzado en fomentar la seguridad de los datos pero ¿es posible que las aplicaciones que ejecuta sean el equivalente a una puerta abierta por la que cualquiera puede acceder a su empresa? La seguridad de los datos en su organización depende de mucho más que simplemente bloquear archivos y registros individuales. Usted necesita reforzar también la seguridad a nivel de las *aplicaciones,* ya que estas pueden controlar el acceso a sus datos e incluso a la infraestructura del Internet de las cosas (IoT) de su organización.

Muchas de las vulneraciones de la seguridad más destacadas se han producido no por malas prácticas de seguridad de los datos sino por la vulnerabilidad de las aplicaciones. La implementación de seguridad en las aplicaciones contribuye a evitar que software malintencionado o vulnerable permita a los ciberdelincuentes apropiarse de datos que consideraba seguros.

Aún así, la seguridad de las aplicaciones sigue siendo un área de la ciberseguridad que muchas veces se descuida[1] y las vulneraciones continúan. ¿Por qué? En parte, porque bloquear aplicaciones es más complicado que cifrar archivos o proteger redes con firewalls. También han aumentado el número y la diversidad de las aplicaciones con la llegada de los app stores y aplicaciones especializadas que acceden a infraestructuras en la nube. Mientras, la adopción generalizada de políticas BYOD (traiga su propio dispositivo) ha provocado un aumento en el número de aplicaciones no autorizadas y la rápida proliferación de fuentes de datos de IoT conectadas a aplicaciones.

La seguridad de las aplicaciones es vital para:

- Prevenir daños a la reputación;
- Mantener la confianza de los clientes;
- Evitar costes de corrección;
- Detectar y responder a los riesgos antes de que lleguen a provocar daños.



En un estudio, el

77 %

de los desarrolladores entrevistados dijeron que las aplicaciones son vulnerables porque la presión por publicar rápidamente nuevas versiones impide realizar las comprobaciones adecuadas.[2]

▸ Vea una demostración de lo que IBM Application Security on Cloud puede hacer por usted.

1 "How to Make Application Security a Strategically Managed Discipline" (Cómo convertir la seguridad de las aplicaciones en una disciplina gestionada estratégicamente), *Ponemon Institute*, marzo de 2016.

2 "The State of Mobile Application Insecurity" (El estado de la inseguridad de las aplicaciones móviles), *Ponemon Institute*, febrero de 2015

¿Por qué las organizaciones no consiguen seguridad plena en sus aplicaciones?

La seguridad de las aplicaciones se ve complicada por factores relacionados con los desarrolladores, el personal de TI y los usuarios finales. La combinación de estos factores puede hacer que las organizaciones sean susceptibles a vulnerabilidades.

Prisas por publicar una nueva versión
Las constantes 'prisas por publicar una nueva versión' hacen que con frecuencia los desarrolladores no dispongan de recursos para realizar pruebas. Sin embargo, la seguridad de las aplicaciones no es solo responsabilidad de los desarrolladores. A la vez, los usuarios quieren conocer las eficiencias del nuevo software, lo que se traduce en prisas por instalar rápidamente las aplicaciones.

Aplicaciones complejas
El software varía enormemente en ámbito, requisitos de datos, idioma y plataforma. Una aplicación afectada con acceso directo a datos de la empresa puede constituir un riesgo tan elevado como perder un portátil con los mismos datos en su disco duro, o incluso peor en el caso de no advertirse la vulnerabilidad. Una aplicación maliciosa o insegura puede dejar a la vista sus datos, tanto si se ha visto afectada por una vulnerabilidad de seguridad como si no hubiera tenido seguridad desde el primer momento.

La seguridad de las aplicaciones no es una prioridad
Las vulnerabilidades en la capa de aplicaciones suelen considerarse de baja prioridad, y las organizaciones no suelen clasificar las aplicaciones por la importancia de su protección. Además, tanto las aplicaciones como la responsabilidad de su seguridad suelen estar dispersas por toda la organización, con escasa visibilidad de cuáles se utilizan y cuáles son las más vulnerables.

Falta de estándares
Los usuarios no pueden dedicar tiempo a comprobar la seguridad, ni saben cómo hacer una comprobación eficaz. Existen pocos estándares universales sobre seguridad de las aplicaciones, por lo que puede resultar complicado evaluar las orientaciones o hacer uso de los recursos locales.

Un reciente estudio de Ponemon Institute descubrió que el

47 %

de los entrevistados afirmaron un aumento signiticativo del riesgo en las aplicaciones móviles de su organización.[1]

- Obtenga más información acerca de la gestión de la seguridad de las aplicaciones basada en los riesgos.

1 "How to Make Application Security a Strategically Managed Discipline" (Cómo convertir la seguridad de las aplicaciones en una disciplina gestionada estratégicamente) (El estado de la inseguridad de las aplicaciones móviles), *Ponemon Institute*, marzo de 2016.

¿En qué consiste la seguridad eficaz de las aplicaciones?

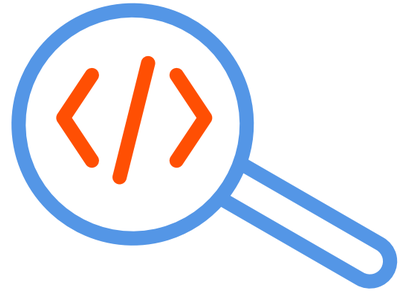
Las prácticas más eficaces para la seguridad de las aplicaciones confirman que es necesario considerar la seguridad como un proceso, no como una serie de puntos que ir marcando en una lista. La comprobación de la seguridad de las aplicaciones (AST) ha de ser exhaustiva y continuada.

Para los desarrolladores, el proceso de AST debe integrarse en el ciclo de vida de desarrollo del software, con análisis continuado del código fuente. Para las organizaciones de los usuarios finales, el proceso continúa con la comprobación de todo el nuevo software implementado, así como con la aplicación de nuevas pruebas a las aplicaciones ya en uso en la organización.

Un sistema exhaustivo de seguridad de las aplicaciones deberá incluir:

- **Descubrimiento y catalogación de** las aplicaciones que se utilizan actualmente;
- **Ensayos estáticos:** examinar el código fuente de las aplicaciones en busca de vulnerabilidades es la forma más directa de descubrir el código que esconde una vulnerabilidad concreta para la seguridad;
- **Comprobación dinámica:** evaluar lo que hace el software que se despliega (por ejemplo, ¿es vulnerable a potenciales ataquesde inyección SQL y secuencias de comandos entre sitios?);
- **AST móvil**, debido a la proliferación de nuevas aplicaciones móviles en el mercado;
- **Implementación** del nuevo software solo después de superar las pruebas.

Las aplicaciones deberán volver a evaluarse con regularidad utilizando fuentes como la lista prioridades del Open Web Application Security Project (OWASP):[1] las nuevas amenazas pueden poner en riesgo aplicaciones que antes eran seguras.



En septiembre de 2016 había

2 millones de *aplicaciones para Apple iOS disponibles para descargar,[2] y más de*

2,4 millones de *aplicaciones para Google Android.[3]*

▸ Obtenga más información sobre los riesgos que hacen que la seguridad de las aplicaciones sea una cuestión vital.

1 Paul Ionescu, "The 10 Most Common Application Attacks in Action" (Cómo actúan los 10 ataques más habituales a las aplicaciones), *IBM Security Intelligence*, 8 de abril de 2015.

2 "Number of apps available in leading app stores as of June 2016" (Número de apps disponibles en los principales app stores a partir de julio de 2016), *Statista*, junio de 2016.

3 "Number of Android Applications" (Número de aplicaciones para Android), *AppBrain*, acceso realizado el 13 de octubre de 2016.

Uso de nuestras eficaces prácticas recomendadas de seguridad para aplicaciones

A la hora de examinar los riesgos de las aplicaciones, las organizaciones sufren restricciones que abarcan desde presupuestos limitados hasta las pesadas cargas de trabajo del personal de seguridad y de TI. Sin embargo, estas restricciones no pueden suponer un obstáculo en la mejora de la protección. Por el contrario, su organización debería hacer uso de prácticas recomendadas como las que se indican a continuación.

- **Supervisión:** una comprobación planificada y automatizada proporciona resultados más exhaustivos y fiables que las pruebas a medida.
- **Continuidad:** las aplicaciones tienen que crearse y testearse pensando en la seguridad y volver a examinarse para mantenerlas al día en cuanto a vulnerabilidades.
- **Priorización:** clasificar los problemas relacionados con la seguridad de las aplicaciones según su gravedad e impacto potencial en el negocio permite abordar los problemas en el orden más lógico desde el punto de vista empresarial.
- **Flexibilidad:** evitar requisitos de implementación restrictivos es fundamental para evaluar la totalidad de las aplicaciones desplegadas en su organización.
- **Adaptabilidad:** las amenazas cambian con el tiempo y un enfoque flexible implica menos cambios para mantener el control de la seguridad de las aplicaciones.
- **Oportunidad:** para evitar tener que interferir en los procesos de desarrollo (o volver a iniciarlos), es preciso comprobar las aplicaciones en todas las fases del ciclo de desarrollo.

Una solución integrada de seguridad de las aplicaciones como IBM® Application Security on Cloud puede ayudarle a minimizar lagunas en la seguridad e identificar potenciales vulnerabilidades. La integración con otros productos y prácticas de seguridad convierte la mitigación de riesgos para las aplicaciones en parte de un completo programa de seguridad, en lugar de un añadido de última hora.

58 %

de las organizaciones afirma que la preocupación por la seguridad inhibe la implementación total de una estrategia de seguridad móvil.[1]

▸ Vea cómo IBM Application Security on Cloud identifica y corrige las vulnerabilidades.

1 "2016 Mobile Security & Business Transformation Study" (Estudio sobre la transformación del negocio y la seguridad móvil 2016), *Information Security Media Group*, patrocinado por IBM Corp., 2016.

AST completo basado en la nube

Refuerce la gestión de riesgos para la seguridad de las aplicaciones mediante una solución integrada en lugar de recurrir a una disparidad de herramientas. IBM Application Security on Cloud es una solución completa, económica, fácil de utilizar y de implementar basada en la nube para aplicaciones web y móviles, que abarca todas las fases de testeo de la seguridad de las aplicaciones. Nuestro producto basado en la nube se beneficia de los años de experiencia de IBM en comprobación de seguridad on premise y funciona con otras herramientas de seguridad para posibilitar una protección de ciberdefensa exhaustiva.

IBM Application Security on Cloud es una solución completa mediante suscripción que le permite comprobar sus aplicaciones y mejorar la seguridad mediante datos de utilidad inmediata. Con IBM Application Security on Cloud podrá evaluar rápidamente el índice de riesgo de las aplicaciones para centrar sus esfuerzos de corrección en las vulnerabilidades más importantes.

- Regístrese para utilizar una versión de prueba de IBM Application Security on Cloud, o descargue la versión local de IBM Security AppScan.

Vista del panel de IBM Application Security on Cloud.

Puede realizar una comprobación estática de la seguridad del código de las aplicaciones en gran diversidad de lenguajes de programación, realizar análisis dinámico para aplicaciones web antes y después de la fase de producción y comprobar las aplicaciones para Android e iOS antes de desplegarlas. IBM Application Security on Cloud identifica y genera informes sobre problemas de seguridad, los clasifica según el nivel de exposición y gravedad y recomienda actuaciones para su corrección. Todos los resultados pueden integrarse en distintos sistemas de DevOps y entornos de desarrollo integrado (IDE).

También está disponible una completa cartera de servicios de consultoría que permiten a su equipo de seguridad aprovechar plenamente todas las prestaciones de IBM Security.

Casos de uso de IBM Application Security on Cloud en el mundo real

Las organizaciones que despliegan soluciones de seguridad de las aplicaciones de IBM comprenden el valor de la integración y de la automatización dentro de su estrategia de seguridad general, tanto para crear como para desplegar aplicaciones.

Protección del código durante todo el ciclo desarrollo de software

- Concur Technologies de Bellevue (Washington) está especializada en gestión de gastos corporativos, por lo que maneja a diario información financiera confidencial. Proteger esta información resulta absolutamente prioritario, pero no es tarea fácil. Como organización con una gran presencia móvil, incluidas sus propias aplicaciones móviles, Concur desplegó AppScan con la misma tecnología de comprobación de vulnerabilidades que impulsa IBM Application Security on Cloud. Con AppScan, Concur puede examinar la seguridad de sus aplicaciones en busca de riesgos para la seguridad durante la fase de desarrollo y analizar fácilmente el código en producción.

Gestión del riesgo en una empresa en rápido crecimiento

- Migros, un gigante de la distribución minorista en Turquía que está experimentando un vertiginosocrecimiento en su país y en el extranjero, tiene que proteger una infraestructura a gran escala, con aplicaciones que transmiten datos de inventario y pagos mediante una red que abarca casi 1500 establecimientosy más de 100 000 dispositivos conectados a Internet. Para organizar su crecimiento, la empresa se veía ante importantes desafíos a la hora de trasladar sus operaciones a la nube con la implementación de una política de BYOD. La utilización de soluciones de seguridad de aplicaciones de IBM ha permitido a Migros escalar el negocio y al mismo tiempo minimizar el riesgo.

IBM ofrece una
completa cartera
de herramientas AST que utilizan algunas de las principales empresas en sectores tan diversos como la fabricación[1] y los servicios financieros[2] para contribuir a proteger sus aplicaciones, dispositivos y datos.

▸ Regístrese para disfrutar de un plan de prueba gratuito de IBM Application Security on Cloud.

1 "Importante fabricante global de automóviles: protección del ecosistema de coches conectados" (Estudio sobre la transformación del negocio y la seguridad móvil 2016), *IBM Corp.*, julio de 2016.

2 "Seguro progresivo: protección proactiva de los datos mediante la creación de controles apropiados" (Estudio sobre la transformación del negocio y la seguridad móvil 2016), *IBM Corp.*, mayo de 2016.

Más información

Para obtener más información acerca de las soluciones IBM Security, póngase en contacto con su representante de IBM o IBM Business Partner (BP), o bien visite: **ibm.com**/applicationsecurity

Acerca de las soluciones IBM Security
IBM Security ofrece una de las carteras más avanzadas e integradas de productos y servicios de seguridad para empresas. La cartera, respaldada por el desarrollo y la investigación de prestigio internacional de IBM X-Force, proporciona inteligencia en seguridad para ayudar a las organizaciones a proteger de forma global a sus empleados, infraestructuras, datos y aplicaciones, ofreciendo soluciones para la gestión de accesos e identidades, seguridad de bases de datos, desarrollo de aplicaciones, gestión de riesgos, gestión de puntos finales y seguridad de las redes, entre otras opciones. Estas soluciones permiten a las organizaciones gestionar los riesgos de forma eficaz e implementar una seguridad integrada para entornos móviles, cloud, redes sociales y otras arquitecturas empresariales. IBM opera una de las organizaciones de investigación, desarrollo y entrega de seguridad más extensas del mundo; monitoriza al día 15 000 millones de incidentes relacionados con la seguridad en más de 130 países y posee más de 3000 patentes de seguridad.

También puede utilizar IBM Security Services según las necesidades de su organización a medida que construye y ejecuta programas de seguridad de las aplicaciones. Esto le proporciona acceso a expertos en seguridad de las aplicaciones en el momento que lo necesite y durante el tiempo que precise. Tanto si necesita una reunión rápida para que su equipo pueda comenzar a trabajar, servicios de consultoría exhaustiva, hackers éticos que analicen manualmente sus aplicaciones o cualquier otra cuestión, IBM cubre todas sus necesidades.

Sta. Hortensia 26-28
28002 Madrid
España

El sitio web de IBM está disponible en **ibm.com**/es

WGW03254-ESES-02