Opinión

SecDevOps: La madurez de DevOps

«El software se está comiendo el mundo». Esta frase tan provocadora fue el tema central de un artículo de Marc Andreessen en el Wall Street Journal, allá por 2011. Su contenido sigue siendo válido, pues la mayoría de las empresas más poderosas del mundo son empresas relacionadas de algún modo con el software. Además, muchas empresas tradicionales están reorientando sus negocios de forma que se parecen cada vez más a una empresa de software (la banca, sin ir más lejos). Esto que ha venido a llamarse la transformación digital está motivado por muchas causas, pero uno de los factores fundamentales es que muchos de los procesos que tradicionalmente implicaban elementos físicos, ahora pueden hacerse de forma virtual por una fracción del coste.

Uno de los obstáculos para esta transformación es que en el mundo real los procesos de operaciones utilizan piezas estandarizadas y probadas (ya sea una tuerca, un motor o el timón de cola de un avión). En el mundo software, en cambio, esas piezas son intangibles y su puesta en producción siempre ha estado muy vinculada a los propios desarrolladores.

Esta separación entre desarrolladores y operadores es la que aspira resolver la filosofía DevOps: acortar la distancia que separa esos dos ámbitos mediante una serie de herramientas y prácticas que facilitan al desarrollador desplegar sus productos y al operador ejecutarlos y mantenerlos de la forma menos disruptiva posible. El objetivo siempre es acortar tiempos e incorporar nuevas funcionalidades de forma ágil; *Agile* es precisamente otra de las metodologías que orbitan alrededor de DevOps.

De la misma manera que con el desarrollo y las operaciones, la seguridad siempre ha trabajado en su propia parcela separada de las anteriores. Conseguir conectar un nuevo sistema a la red, pasando por el cortafuegos corporativo, supone en muchas empresas un problema más burocrático que técnico. No es viable mantener esa forma de trabajar si queremos un flujo continuo de entregas como el que propugna DevOps, pero el aspecto que más se descuida con este enfoque es la ciberseguridad. El lema clásico de los desarrolladores de Facebook «muévete rápido y rompe cosas» es una invitación a añadir nuevas funcionalidades con la tranquilidad de que los fallos se corregirán pronto. Sin embargo la ciberdelincuencia también es muy rápida y puede aprovechar esos resquicios si apenas los detecta.

Se hace preciso adoptar la misma filosofía DevOps al mundo de la seguridad y tender hacia la SecDevOps, en la que el objetivo no es una cadena de producción con principio, final y fronteras estrictas entre equipos, sino un proceso iterativo en el que cada equipo complementa las funciones del otro. La inclusión de la ciberseguridad, que transforma DevOps en SecDevOps, puede usarse entonces como una medida de la madurez de estos procesos. Para asegurar que en nuestro esquema DevOps no estamos dejando de lado la gestión de riesgos y de vulnerabilidades debemos integrar en el ciclo DevOps las mejores prácticas de seguridad desde la fase de diseño (*Secure by Design*), incorporar a las operaciones herramientas que automaticen las operaciones de seguridad al máximo, y asumir, en definitiva, que la seguridad es un proceso y que puede (y debe) gestionarse su ciclo de vida de una forma integrada con el desarrollo y las operaciones.

José Pedro Mayo
Jefe de Sección de Consultoría, Arquitectura y Diseño de Sistemas de Secure e-Solutions de GMV

«Se hace preciso adoptar la misma filosofía DevOps al mundo de la seguridad y tender hacia la SecDevOps, en la que el objetivo no es una cadena de producción con principio, final y fronteras estrictas entre equipos, sino un proceso iterativo en el que cada equipo complementa las funciones del otro»