5 claves

para agilizar procesos de desarrollo sin dejar de lado **la seguridad**

mexis®

Managed secure IT | no matter what

5 claves
para agilizar procesos de desarrollo sin dejar de lado **la seguridad**

Hoy en día sabemos que hay que ir a la velocidad que demande cada negocio, pero sin olvidar la precisión en términos de seguridad. Esto sólo se consigue con una combinación de automatización efectiva e inteligencia humana, que resulta fundamental para detectar todas las vulnerabilidades en los sistemas evaluados y reducir el número de falsos positivos y negativos. "Así pues, siempre es recomendable que el factor humano esté presente dentro de cada ciclo de vida de desarrollo de un software".

A continuación les compartimos 5 claves sobre cómo agilizar los procesos de desarrollo sin dejar de lado la seguridad, mediante pruebas integrales a los repositorios y ambientes pares de los sistemas:

01.

Ataque determinístico: Se trata de una fase donde de forma automática se buscan solamente las vulnerabilidades sobre las cuales no existe duda alguna de que efectivamente son vulnerabilidades.

02.

'Triage' al código: En este punto se trabaja para acrecentar la velocidad del factor humano mediante una herramienta basada en Machine Learning que permite a hackers éticos priorizar su búsqueda dentro del código y determinar las partes donde hay mayores probabilidades de que existan vulnerabilidades..

03.

Equipo de ataque: En esta etapa ingresa el equipo de hackers expertos que tienen el conocimiento para atacar el software de manera dinámica y estática. Ellos toman lo reportado por la herramienta de Machine Learning y recorren todo el código con base en la priorización (triage). Es aquí donde logran combinarse la tecnología y el talento humano.

04.

Equipo de fugas: Ya en este punto se realiza un ataque transversal por parte de un equipo independiente al que encontró las vulnerabilidades en los pasos anteriores. Con esto se pretende validar que no haya falsos negativos y reducir al máximo esa falsa sensación de seguridad que tienen las empresas.

05.

Equipo de Re-ataque: Finalmente, se llevan a cabo re-ataques sobre la tecnología, para verificar el cierre de las vulnerabilidades encontradas; y es que el objetivo no es sólo hallar las vulnerabilidades, sino que además logren ser cerradas. Todo esto antes de que el ciclo llegue a producción, para que así el software verdaderamente sea seguro.

La automatización es una de las maneras de acelerar los procesos de construcción de software, pero en términos de seguridad, las herramientas de búsqueda automática de vulnerabilidades tienen dos grandes retos: (1) los **falsos positivos**, que son aquellos reportes que cuando se revisan no corresponden a verdaderas vulnerabilidades (alrededor del 50% de las detectadas por las herramientas no son reales), y (2) los **falsos negativos**, que son básicamente las que se fugan o se omiten en los procesos de detección (representan para las herramientas cerca del **80%** de las vulnerabilidades). Estas últimas son las más complejas y las que realmente pueden afectar al negocio, ya que no se conocen y, por ende, no se puede actuar para mitigar el riesgo que suponen.

Fuente de información:
https://cio.com.mx/