Nunca sacrifiques
ciberseguridad por velocidad

> La mayoría de las empresas prefieren salir a producción con una nueva aplicación o un sitio dejando al final la ciberseguridad sin considerar el riesgo que esto conlleva.

Cada vez es más común que las organizaciones busquen innovar haciendo uso de la tecnología; transformar cómo se hacían las cosas para buscar mayor comodidad, mayor facilidad o simplemente agregar un servicio que beneficie a los clientes, usuarios o a la misma organización en su conjunto.

Pero en esa presentación, esa junta o reunión donde alguien presenta por primera vez el proyecto que transformará a la organización: pocas veces está presente alguien que pueda ver los riesgos desde el punto de vista tecnológico o de ciberseguridad.

Más de la mitad de las organizaciones ni siquiera tratan de identificar riesgos desde etapas tempranas al plantear una nueva aplicación, un nuevo sitio o una nueva funcionalidad en sus sistemas. Es siempre al finalizar e incluso cuando se lleva a producción que se preguntan: **¿cómo lo aseguramos? Quizá ya es demasiado tarde.**

Las razones de no involucrar a ciberseguridad pueden ser muchas: desconocimiento, pensar que ciberseguridad va a detener el proyecto, que no será el desarrollo tan rápido o inclusive algunos culpan al costo que esto puede involucrar.

Creo que mucho tiene que ver con la velocidad con la que ahora la infraestructura puede desplegarse y configurarse en ambientes de nube. La velocidad nos puede matar. Ya hoy, nos está haciendo limitar las pruebas de ciberseguridad por cumplir con una fecha límite o un objetivo de la alta administración.

¿Deberían entonces estar los proyectos definidos a una fecha o realmente a que se acompañe con una serie de pruebas de ciberseguridad para saber que lo que se está publicando está dentro de un nivel aceptable de ciberseguridad? ¿o ambos? ¿Entiende la alta administración el riesgo que significa que no se tengan esas pruebas? ¿Cómo entonces permitir que ciberseguridad esté desde el primer momento para poder ir a la par?

Hay muchas opciones de cómo responder esto. Si lo vemos por costo: es más económico el identificar riesgos desde las primeras etapas, realizar pruebas de seguridad sobre el código fuente conforme se van realizando los sprints y lograr hacer pruebas al finalizar solo de validación que como se hace hoy en muchas organizaciones. Hoy el problema es que, al finalizar el proyecto, el equipo de ciberseguridad entrará a realizar pruebas y posiblemente encuentre vulnerabilidades que tendrá que regresar al equipo de desarrollo para que rehaga parte del trabajo, haciendo que el desarrollador trabaje horas adicionales. Tan simple como eso.

Otra opción de respuesta es cuando se ve desde la perspectiva de cumplimiento: ¿trataremos datos personales? ¿cómo almacenaremos los datos? ¿los desarrolladores externos se quedarán con el código? ¿cómo se hará la consulta de los datos por parte de la aplicación? ¿usarán datos reales para hacer pruebas? ¿Y si le pasa algo a esos datos? ¿se está ofuscando el código de la aplicación para evitar un ciberataque?, no son preguntas que deberían hacerse al final del proyecto, sino al principio.

La más contundente: Ciberseguridad ya es un tema estratégico dentro de la organización. Una vulneración en esa aplicación o en los datos que maneja, puede dejar con más que un dolor de cabeza para la organización. Planeamos financieramente una organización, pero no planeamos desde el punto de vista de TI y ciberseguridad vinculado al negocio.

Para que esto suceda se requieren muchos esfuerzos, desde el del responsable de ciberseguridad que tiene que dejar de decir que NO a todo, sino buscar el cómo poder realizarlo con el menor riesgo posible; hasta la alta administración con mayor entendimiento de la importancia de contar con la validación de que se está saliendo a producción de una forma segura.

Como algunos saben, también soy piloto privado. Yo no me imagino subiéndome a una avioneta prestada o rentada, iniciar carrera de despegue y en el aire revisar si traigo aceite y combustible. Siempre lo haré en tierra y haré caso a las pruebas que tenga que hacer para decidir si podré volar o no. Lo mismo deberíamos hacer con los sistemas, aplicaciones y tecnología.

Nunca sacrifiques velocidad por ciberseguridad. Ni siquiera en temas personales, es así como caemos en las estafas como phishing y la estafa del CEO: porque nos gana la velocidad, no alcanzamos a pensar. No solo pasa en temas corporativos, también pasa en temas personales.

Aprovecho esta oportunidad para reconocer a todas aquellas organizaciones que no solo están ya creando sus comités de ciberseguridad donde involucran no solo a las áreas operativas sino al negocio; aplauso también a aquellas que están empezando a involucrar a consejeros independientes especializados en temas de ciberseguridad y TI.

Autor: Andrés Velázquez
Fuente de información: www.forbes.com.mx