Seguridad y compliance: los principales frenos para la innovación empresarial

Tres de cada cinco directivos españoles preferirían enfrentarse a un desastre natural que a un problema de seguridad en la cadena de suministro de software, según un informe de CloudBees.

Fuente: COMPUTING.ES

• Las herramientas que se usan son una mezcla. Tres de cada cinco (59%) directores dicen que tienen todas, o casi todas, las herramientas externas que necesitan para gestionar la seguridad y el compliance, frente al 29% que declara usar una mezcla de herramientas internas y externas. Solo el 11% utiliza principalmente herramientas internas.

• La automatización es útil, pero no está al alcance de todos. Solo un 22% de los directivos afirma que su cadena de suministro de software está completamente automatizada y el 37% dice que está cerca de conseguirlo. Del mismo modo, un 22% de ellos asegura que sus procesos de compliance están totalmente automatizados y el 35% afirma estar cerca de conseguirlo.

• Los equipos directivos confían en sus equipos. Nueve de cada 10 altos ejecutivos aseguran que su equipo de gestión de riesgos tiene las herramientas, el conocimiento y la experiencia para construir y/o mantener una cadena de suministro de software segura.

• Cuando es posible elegir entre velocidad y seguridad, gana la seguridad. Más de tres cuartas partes de los directivos (76%) aseguran que para ellos es más importante garantizar la seguridad y el cumplimiento de la normativa que contar con velocidad y cumplimiento (24%). En el caso de las empresas españolas, sus directivos apuestan por la seguridad y el compliance de forma más mayoritaria, con un 84% apostando por la seguridad frente al 16% que valoran más la velocidad.

• Existen diferencias entre países en relación con la confianza que los directivos tienen respecto a la seguridad y el compliance. La encuesta revela que los ejecutivos estadounidenses son los que más piensan en la seguridad y el cumplimiento de la normativa, mientras que los de España y Reino Unido son los que más tiempo dedican a aplicar las políticas de

compliance. Los directores alemanes demuestran el nivel más bajo de confianza entre todos los encuestados, con un 23% afirmando que su cadena de suministro de software no es segura.

Otras conclusiones destacadas

En esta línea, el 86% de los altos directivos asegura centrarse más ahora en el cumplimiento normativo que hace dos años, y el 82% expresa una mayor preocupación por los ataques. Por otra parte, en el caso de España, el 81% de los directivos están ahora mismo más preocupados por los ataques a su cadena de suministro de lo que lo estaban dos años atrás, con casi la mitad mucho más preocupada y más de un tercio algo más preocupada.

En España, los directivos que aseguran que su cadena de suministro de software es segura ascienden al 90% de los entrevistados, pero solo 1 de cada 5 (20%) afirma que su cadena de suministro es muy segura. En cuanto al cumplimiento normativo y frente al 33% global, solo el 16% de los ejecutivos españoles considera que su cadena de suministro cumple de forma íntegra con las normativas, aunque más de la mitad de los españoles encuestados (52%) afirma que es casi completamente conforme con las normativas.

Según el reporte, también se observa un descenso en la confianza que los ejecutivos tienen en la seguridad de cadena de suministro y el compliance, así como una mayor atención a este punto. En 2022, el 88% de los directivos afirma que su cadena de suministro de software es segura o muy segura, frente al 95% que lo hacía en 2021. Además, el 33% asegura que su cadena de suministro de software cumple de forma íntegra con las normativas, lo que supone un 19% menos que el año anterior.

A nivel más general, casi todos los directivos españoles encuestados (97%) dicen estar preocupados por los ataques a la cadena de suministro de software, y dos tercios (67%) dicen estar muy preocupados. A pesar de ello, 3 de cada 5 directivos en España aseguran que preferirían enfrentarse a un desastre natural que a un problema de seguridad en su cadena de suministro de software.

Preocupados por los ataques a la cadena del suministro de software

En el caso de España, el enfoque shift left genera opiniones divididas. Un 47% de los directivos españoles considera que este enfoque es importante para ellos como empresa, mientras que otro 47% asegura que supone una carga para sus equipos de desarrolladores. A pesar de ello, el 80% declara estar implementando una estrategia de seguridad shift left y compliance en su empresa.

Los directivos encuestados por CloudBees afirman estar abrumadoramente a favor de un enfoque shift left, estrategia que consiste en trasladar las pruebas y la evaluación del software a las primeras fases del ciclo de vida del desarrollo de software, depositando en los desarrolladores la carga que supone el aspecto del cumplimiento normativo. De hecho, el 83% de los ejecutivos asegura que este enfoque es importante para ellos como empresa, y el 77% afirman estar implementando un enfoque de seguridad shift left y compliance. Esto es a pesar de que el 58% de los directivos informan de que desplazar la seguridad a la izquierda supone una carga para sus desarrolladores.

La carga para los desarrolladores del Shift Left

Tres cuartas partes de los altos ejecutivos a nivel global afirman que los problemas de compliance (76%) y de seguridad (75%) limitan la capacidad de innovación de su empresa. Esto se debe, en parte, al excesivo tiempo que conllevan las auditorías de compliance, los riesgos y los defectos. De hecho, los altos ejecutivos de empresas españolas afirman que sus equipos invierten de media casi dos meses (49 días al año) en auditorias de compliance.

El informe CloudBees 2022 Global C-suite Security revela que los retos de seguridad y compliance son un importante obstáculo para las estrategias de innovación de la mayoría de las empresas. La mayor parte de los 600 altos ejecutivos encuestados pertenecientes a empresas con al menos 250 empleados en Estados Unidos, Australia, Francia, Alemania, España y Reino Unido entre el 27 de junio y el 11 de julio de 2022, están de acuerdo en que una estrategia de seguridad shift-left supone una carga para los equipos de desarrollo de software.

FUENTE: COMPUTING.ES