ENTREVISTA CON UN EXPERTO

NIS2 y el nuevo modelo de responsabilidad en la gobernanza de accesos

Guido Kraft
Field CISO en WALLIX

Más de 20 años de experiencia en ciberseguridad, gobierno corporativo, ISO 27001, TISAX y programas de seguridad operativa en infraestructuras críticas y entornos regulados.

Q ¿Cómo cambia la NIS2 la relación entre el CISO, la dirección y el consejo de administración?

Con la NIS2, la ciberseguridad deja de ser solo un asunto de IT y pasa a convertirse en un riesgo de negocio. La alta dirección y el consejo de administración son directamente responsables de las medidas de ciberseguridad y de la resiliencia de la organización.

Eso cambia el papel del CISO, que pasa a ser el puente entre las operaciones técnicas y la toma de decisiones ejecutivas. El consejo también tiene que asumir una supervisión activa, entender los riesgos cibernéticos y hacer las preguntas adecuadas.

Q ¿Por qué la gobernanza de accesos está ganando tanta importancia con la NIS2?

Prácticamente todo en IT y OT depende del acceso. El riesgo aparece cuando los usuarios tienen más privilegios de los que necesitan o cuando los permisos no están alineados con sus responsabilidades reales.

La gobernanza de accesos define quién puede acceder a qué, en qué condiciones y con qué nivel de responsabilidad. Por eso las organizaciones deberían tratarla como una capa estratégica que refuerza la seguridad y el cumplimiento normativo.

ENTREVISTA CON UN EXPERTO

wallix

¿Qué barreras impiden a las organizaciones del sector público implantar una gobernanza de accesos más sólida?

Las principales barreras suelen ser los sistemas heredados, los entornos fragmentados y los presupuestos limitados.

Muchas aplicaciones antiguas no soportan modelos modernos de acceso, lo que obliga a seguir usando cuentas compartidas o privilegios excesivos.

Aun así, es posible reforzar el control con gestión de accesos privilegiados, autenticación avanzada y accesos auditables.

¿Por qué siguen siendo tan habituales las cuentas administrativas compartidas?

Las cuentas compartidas siguen siendo habituales por los sistemas heredados y la comodidad operativa. Muchas aplicaciones antiguas no soportan modelos modernos de acceso basado en roles.
Siempre que sea posible, conviene avanzar hacia cuentas individuales. Y cuando no lo sea, aplicar controles de acceso privilegiado para ganar trazabilidad y control.

¿En qué podría centrarse la próxima gran regulación europea de ciberseguridad?

Probablemente, el próximo gran foco será la gobernanza de la IA.A medida que la inteligencia artificial se integre más en las operaciones de negocio, las organizaciones necesitarán políticas más claras sobre el uso de datos, la responsabilidad, la gestión del riesgo y el cumplimiento normativo.

¿Cómo deberían equilibrar las organizaciones la prevención y la investigación posterior a un incidente bajo NIS2?

La prevención y la investigación son igual de importantes.

Las organizaciones necesitan controles que reduzcan el riesgo, pero también visibilidad y trazabilidad una vez ocurre un incidente.

Los equipos de seguridad deben poder entender quién accedió a qué sistemas, cuándo se produjo el acceso y qué acciones se realizaron.

¿Cómo debería ser una buena gestión del acceso de terceros bajo NIS2?

El acceso de terceros debe gestionarse con el mismo nivel de exigencia que el acceso privilegiado interno.

Una buena práctica implica que el acceso esté controlado, limitado en el tiempo, monitorizado y completamente trazable. Las organizaciones deberían evitar accesos externos sin supervisión, privilegios permanentes para proveedores y cuentas remotas genéricas.

¿Las organizaciones deberían abordar NIS2 desde el cumplimiento o la resiliencia?

La mejor forma de abordar NIS2 es verla como una oportunidad para mejorar la resiliencia operativa y no solo como un requisito de compliance.

Si una organización mejora la visibilidad, la gobernanza de accesos y la disciplina operativa, el cumplimiento normativo acaba siendo una consecuencia natural de tener mejores controles.