**NIS2 – Trend Article**

**El camino hacia la seguridad digital: un vistazo a la Directiva NIS2 de la UE**

**Ciberamenazas y respuesta europea**

La creciente digitalización no sólo trae progreso. También plantea un riesgo creciente: los ciberataques. Para hacerle frente, la Unión Europea introdujo en 2016 la Directiva NIS (Network and Information Security). El objetivo era reforzar la ciberseguridad en sectores estratégicos y esenciales, en concreto: energía, transporte, banca, mercados financieros, sanidad, agua e infraestructuras digitales.

Sin embargo, desde entonces se han producido cambios fundamentales en la sociedad, en particular tras la pandemia del COVID. El despliegue masivo de herramientas de videoconferencia (como MS Teams, Zoom o Google Meet) junto con el aumento de la demanda de comercio electrónico y servicios de entrega han intensificado la transición al mundo digital. De hecho, McKinsey calcula que la pandemia aceleró la digitalización entre 3 y 4 años. Esta evolución trajo consigo nuevos retos en materia de ciberseguridad, por lo que la UE tuvo que actualizar su Directiva.

**NIS2: normas más estrictas para un mundo más seguro**

La UE adoptó la nueva Directiva NIS2 en noviembre de 2022. Esta Directiva amplía considerablemente el ámbito de aplicación de la legislación original y endurece las medidas de seguridad. Además de los siete sectores originales, NIS2 abarca ahora nuevas áreas como la fabricación, los servicios postales y de mensajería, la ciencia, la investigación y la educación.

La NIS2 exige a las empresas y organizaciones de todos estos sectores que identifiquen y gestionen los riesgos cibernéticos, protejan los sistemas de información y formen periódicamente al personal. Una de las nuevas normas establece incluso la obligación de notificar los incidentes graves de seguridad en las 24 horas siguientes a su descubrimiento, con un informe detallado en 72 horas y un informe final en 30 días.

La directiva también divide a las organizaciones en dos categorías: entidades «esenciales» y «críticas», y cada categoría tiene obligaciones específicas. Las sanciones por incumplimiento de las normas pueden ser muy severas. Las entidades esenciales se enfrentan a multas de hasta 10 millones de euros o el 2% del volumen de negocios anual mundial, si esta cifra es superior. Las entidades importantes pueden ser multadas con hasta 7 millones de euros o el 1,4% del volumen de negocios.

NIS2 desempeña así un papel clave para garantizar la ciberseguridad en toda la UE. La organización se ha comprometido a introducir nuevas medidas y cumplir normas estrictas para proteger infraestructuras críticas como las redes de energía, agua y sanidad. De este modo se garantiza que los servicios esenciales de los que dependen los ciudadanos sigan funcionando y sean seguros en caso de ciberataque.

**¿Cómo se prepara 2N para NIS2?**

2N debe cumplir la NIS2: somos una entidad obligada (más de 250 empleados y un volumen de negocios anual superior a 10 millones de euros) y entramos en múltiples sectores regulados, como «Fabricación de dispositivos y equipos electrónicos», «Prestación de servicios de comunicaciones electrónicas disponibles al público» y también «Proveedor de servicios de computación en nube».

La empresa lleva mucho tiempo trabajando en el tema de la ciberseguridad y cuenta con la certificación ISO 27001, que mantiene regularmente en las auditorías de vigilancia y recertificación. Este año, 2N también ha obtenido la certificación de seguridad IEC 62443-4-1, que se aplica a sus productos para ascensores.

Pero, ¿qué es lo siguiente? 2N debe cumplir las estrictas normas NIS2 y revisar a fondo y con regularidad las medidas de seguridad existentes. Por ello, estamos llevando a cabo un análisis de deficiencias para determinar qué obligaciones de NIS2 cumplimos ya (a través de la certificación ISO 27001) y qué nos queda por implantar. Dado que la ciberseguridad es una de las principales prioridades de 2N, la empresa espera que el cumplimiento de los requisitos restantes se lleve a cabo sin contratiempos y dentro del plazo legalmente establecido. Puede estar seguro de que, al elegir 2N, no se arriesga a incumplir las directivas de la UE.

**Conocimiento, confianza y transparencia: valores clave**

2N se apoya desde hace tiempo en los amplios conocimientos y experiencia en ciberseguridad de su empresa matriz AXIS. Los expertos de ambas empresas están en contacto diario y comparten las mejores prácticas e ideas para un desarrollo seguro.

Una de las herramientas clave que ha adoptado 2N es el Axis Security Development Model (ASDM), que describe 13 procesos y prácticas de seguridad centrados en la aplicación (y posterior verificación) de medidas de seguridad en cada fase de desarrollo. Este planteamiento minimiza el riesgo de incidentes de seguridad y refuerza la confianza y satisfacción de nuestros clientes.

La confianza y la transparencia entre la empresa y sus clientes son valores clave para 2N. La empresa publica en su sitio web todo el material y la información relacionados con la ciberseguridad, lo que no sólo garantiza la seguridad de sus productos y servicios, sino que también refuerza su confianza en la fiabilidad de los mismos.

**E-Mail – Hardening Guide**

**Asunto:** Refuerce la seguridad de su red con la guía 2N Hardening Guide

**Encabezado:** Descargar

Estimado, [Nombre del destinatario]:

En el vertiginoso panorama actual de la ciberseguridad, **garantizar la seguridad de sus dispositivos basados en IP ha pasado de ser opcional a ser fundamental.** A medida que las amenazas cibernéticas se vuelven más sofisticadas, la necesidad de salvaguardar los sistemas es más urgente que nunca.

Para ayudarle a mantenerse a la vanguardia, le ofrecemos la 2N Hardening Guide, una guía completa que reúne las mejores prácticas para mejorar la seguridad de los dispositivos de red 2N.

Tanto si gestiona dispositivos en un entorno de alta seguridad como hospitales o la administración pública, como si simplemente quiere proteger un edificio residencial o de uso múltiple, estas recomendaciones están diseñadas para minimizar las vulnerabilidades y reforzar la protección.

**Lo que aprenderá**

* **Establecer contraseñas seguras:** establecer credenciales sólidas para evitar accesos no autorizados
* **Actualizaciones periódicas del firmware:** parchear vulnerabilidades conocidas para adelantarse a las amenazas
* **Protocolos de comunicación seguros:** garantizar una comunicación segura entre dispositivos
* **Activación del cifrado:** proteger los datos sensibles durante la transmisión
* **Desactivación de servicios innecesarios:** minimizar las posibles superficies de ataque
* **Limitar el acceso a la red:** reducir la exposición restringiendo el acceso a usuarios de confianza
* **Segmentación de la red:** aislar los dispositivos críticos del tráfico de red más amplio para mejorar la seguridad.

No espere a que se produzca una brecha. Infórmese y proteja su sistema ahora. La guía 2N Hardening Guide es el recurso que necesita para mantener una red robusta y segura.

[Descárguela]

Saludos cordiales,

**Banner - artículo de tendencia**

La visión de 2N sobre la Directiva NIS2

¿Tiene cada vez más preguntas sobre la próxima Directiva NIS2 de la UE y su impacto en las empresas? Descubra qué significa, a quién afecta y cómo 2N, proveedor líder de sistemas de control de accesos, se está preparando para abordarla en este interesante artículo.

>>Seguir leyendo