CAVILACIONES SEGURAS

La directiva de la Unión Europea NIS2: ¿revolucionará nuestra ciberseguridad?

La ciberseguridad se ha convertido en una prioridad clave para las empresas y los Estados de la Unión Europea (UE) en esta era digital. La Directiva de la UE NIS2 2022/2555, que se adoptó en diciembre de 2022, tiene como objetivo mejorar la ciberseguridad de los Estados miembros y proteger sus infraestructuras ante ciberataques. Tratemos primero de resumir las novedades de NIS2 en sólo seis párrafos.

La Directiva establece medidas para garantizar la seguridad en las redes y en los sistemas de información, tanto para los Estados como para las empresas esenciales e importantes, tanto públicas como privadas, con un tamaño mínimo de 50 empleados o 10 millones de facturación. Sin embargo, hay excepciones: puede afectar también a empresas más pequeñas si son esenciales o importantes. La diferencia entre las empresas esenciales e importantes es que las primeras estarán sujetas a supervisión.

NIS2 define un incidente de seguridad como un evento con efecto adverso en las redes y sistemas de información. La denegación de servicio, al parecer, no intencionada del 19 de julio puede considerarse un incidente de ciberseguridad. Aplicando NIS, ¿cuántos informes de incidentes habría recibido nuestro CERT nacional? ¿Sería CrowdStrike sancionado? ¿Tendría el CEO de dicha compañía responsabilidad penal por una mala gestión de cambios?

La Directiva NIS2 establece la obligación de realizar una evaluación exhaustiva de los riesgos de ciberseguridad y tomar medidas para gestionar los riesgos identificados. Además, se establecen plazos de notificación de incidentes significativos al CERT nacional, que deben realizarse en un plazo de 24 horas, 72 horas y 30 días, así como a los clientes afectados, y se establece la necesidad de un intercambio de información de ciberseguridad a nivel nacional y europeo.

La Directiva NIS2 también establece la obligación de concienciar a los empleados y colaboradores sobre la importancia de la ciberseguridad y la necesidad de proteger los sistemas y datos de la empresa. Sectores como energía, salud, banca, transporte, servicios digitales, administración pública y gestión de agua son considerados esenciales y están sujetos a la directiva.

Los órganos de dirección de las compañías esenciales e importantes tienen la responsabilidad de aprobar las medidas de gestión de riesgos de ciberseguridad y de asistir a formaciones de ciberseguridad. Además, la cadena de suministro también debe ser segura para garantizar la protección de los datos y sistemas de la empresa.

El plazo para la transposición de la Directiva NIS2 a la legislación nacional finaliza el 17 de octubre de 2024. Además, cada Estado miembro debe establecer la lista de entidades esenciales e importantes antes del 17 de abril de 2025. La Directiva NIS2 permite responsabilizar personalmente a los directivos de una compañía por negligencia en caso de incidentes de seguridad, lo que aumenta la importancia de la ciberseguridad en la gestión de las empresas.

En el cumplimiento de la Directiva NIS2, el Centro Criptológico Nacional y el Instituto Nacional de Ciberseguridad (INCIBE) tendrán un papel importante en la supervisión y la asistencia a las empresas en la implementación de las medidas de ciberseguridad necesarias. En resumen, la Directiva NIS2 es una herramienta clave en la protección de las infraestructuras de los estados miembros de la UE y en la gestión de la ciberseguridad en las empresas. Su cumplimiento es esencial para garantizar la protección de los datos y sistemas de las compañías y para evitar el impacto negativo de los ciberataques en la economía y la sociedad europeas.

Estoy escribiendo este artículo la noche del 19 de julio, día que el CEO de CrowdStrike y múltiples compañías europeas, como aerolíneas, bancos y operadores de aeropuertos, recordarán por levantarse con miles de ordenadores ejecutando Microsoft Windows y mostrando la "pantalla azul de la muerte" debido, al parecer, a una actualización defectuosa del software Falcon de CrowdStrike.

La Directiva NIS2 permite responsabilizar personalmente a los directivos de una compañía por negligencia en caso de incidentes de seguridad, lo que aumenta la importancia de la ciberseguridad en la gestión de las empresas.

NIS2 define un incidente de seguridad como un evento con efecto adverso en las redes y sistemas de información. La denegación de servicio, al parecer, no intencionada del 19 de julio puede considerarse un incidente de ciberseguridad. Aplicando NIS, ¿cuántos informes de incidentes habría recibido nuestro CERT nacional? ¿Sería CrowdStrike sancionado? ¿Tendría el CEO de dicha compañía responsabilidad penal por una mala gestión de cambios? Tantas preguntas se me ocurren...

En fin, demos la bienvenida a NIS2 y observemos los detalles de su implementación... hay una oportunidad real de que la ciberseguridad adquiera la relevancia que nuestra sociedad digital exige... siempre que no nos ahoguemos en un mar de detalles legales o administrativos.

Dr. Alberto Partida
Experto en Ciberseguridad
linkedin.com/in/albertopartida