Comprender la DORA: una guía para la Ley de Resiliencia Operativa Digital

Barracuda

La Ley de Resiliencia Operativa Digital (DORA, por sus siglas en inglés) es una normativa de la Unión Europea (UE) que entra en vigor el 17 de enero de 2025 y que tiene como objetivo reforzar la resiliencia en materia de ciberseguridad de las instituciones financieras.

La legislación marca un cambio significativo en la forma en que la gente y los reguladores perciben la ciberseguridad y la transparencia corporativa. Reconoce la necesidad que tienen las empresas de tomarse la defensa en serio. También considera que comunicar abiertamente las filtraciones crea un panorama más seguro para todo el mundo.

La DORA es un reconocimiento de la creciente dependencia del sector de los servicios financieros de la infraestructura digital y de la importancia de proteger dicha infraestructura. Representa las prácticas recomendadas, lo que obliga a las empresas a establecer prácticas resilientes e informar de las filtraciones y los fallos.

La legislación refleja la conciencia de que un ataque exitoso a la infraestructura financiera digital podría afectar negativamente a toda la sociedad. Los efectos podrían perdurar en el tiempo y la recuperación sería larga y costosa. Los ciberdelincuentes y actores que cuentan con el beneplácito de estados tienen acceso a herramientas de ataque cada vez más sofisticadas y automatizadas. La seguridad digital ha dejado de ser un complemento opcional para convertirse en una obligación empresarial.

En este libro electrónico se ofrece una descripción general de la DORA, las fuentes para obtener más información y las prácticas recomendadas para el cumplimiento normativo. Además, identifica los recursos de Barracuda que le pueden ayudar a prepararse para una implementación.

Barracuda

¿A quién afecta la DORA?

La DORA aplica a la mayoría de las instituciones financieras, entre las que se incluyen:

- Bancos, aseguradoras, sociedades de inversión y entidades de crédito
- Proveedores de pagos y FinTechs
- Gestoras de activos y plataformas de trading

En esencia, la DORA aplica a cualquier entidad involucrada en el sector financiero que utilice servicios de tecnología y comunicación, así como a sus proveedores de servicios externos de TIC esenciales. Abarca no solo a las empresas de la UE, sino también a cualquier empresa del mundo con operaciones o clientes en la región. Mientras que las empresas británicas sin clientes en la UE no tienen que cumplir con la DORA, se espera que el gobierno del Reino Unido cree su propio marco normativo que, probablemente, se ajustará mucho a las regulaciones europeas. Pero, además del cumplimiento normativo, asegurarse de que su organización está en línea con las recomendaciones de DORA significa que está siguiendo las prácticas recomendadas modernas.

Barracuda

¿Cuáles son los cinco componentes clave de las regulaciones de la DORA?

El objetivo general de la DORA es reforzar la resiliencia operativa de las instituciones financieras frente a los ciberataques y armonizar las normas en toda la UE. La normativa tiene cinco componentes clave

Gestión de riesgos: las instituciones financieras deben contar con procedimientos sólidos de gestión de riesgos de TI. Aquí se incluyen los procedimientos para identificar, evaluar y mitigar los riesgos potenciales relacionados con sus sistemas de TI, sistemas en la nube y redes de la cadena de suministro.

Pruebas de resiliencia: la DORA reconoce que ninguna medida de seguridad es fiable a menos que se ponga a prueba. Las instituciones financieras deben contar con un plan de respuesta ante incidentes adecuado y con personal que entienda cómo funciona. Estas instituciones deben probar con regularidad la solidez de su infraestructura digital frente a las interrupciones operativas, por ejemplo, mediante pruebas de penetración, pruebas de stress y evaluaciones de vulnerabilidad.

Informes de incidentes: realice evaluaciones de riesgos exhaustivas e implemente políticas sólidas relacionadas con la seguridad del sistema de información. Esto garantizará un enfoque proactivo para identificar y mitigar cualquier amenaza potencial. Defina procesos para la respuesta ante incidentes, realice simulaciones y capacite a su personal para que esté preparado.

Gestión de riesgos de terceros: la DORA también reconoce el peligro de los ataques a la cadena de suministro. Exige a las instituciones financieras que supervisen a los proveedores de servicios de terceros, especialmente a los proveedores de servicios como las empresas de computación en la nube. Las instituciones deben suscribir acuerdos por escrito con sus proveedores que aborden los temas indicados en el artículo 30 de la DORA, como disponer de una descripción por escrito de todos los servicios prestados y, si procede, de compromisos de nivel de servicio.

Intercambio de información: la normativa tiene por objeto armonizar las obligaciones de notificación dentro de la UE y reforzar la postura en materia de seguridad de todo el sector al fomentar una mejor cooperación e intercambio de información entre las empresas. Esto supone que se debe informar rápidamente de los incidentes que se produzcan. Anteriormente, esto ocurría de forma ad hoc y poco transparente.

Cumplimiento normativo y aplicación

Con lo expuesto antes, puede dar la sensación de que la DORA no representa un cambio radical de las practicas recomendadas ya establecidas. Y sería una suposición razonable. Sin embargo, la diferencia con la DORA radica en que la normativa exigirá a las instituciones demostrar que están cumpliendo con sus obligaciones. No existe un único certificado o prueba de cumplimiento normativo, pero la DORA añadirá una carga en cuanto al control y la documentación a muchas empresas. La aplicación de la ley irá a cargo de los tres reguladores financieros de la UE: las Autoridades Europeas de Supervisión.

Sanciones

Los reguladores tienen potestad para imponer sanciones a las organizaciones que incumplan la normativa. Los Estados miembros también tienen la facultad de imponer sanciones penales.

¿Cuáles son los primeros pasos para cumplir con la DORA?

Lo primero es determinar si la DORA afectará directamente a su empresa. Como se ha mencionado con anterioridad, aunque no afecte directamente, las instituciones financieras deberían tener en cuenta la serie de prácticas recomendadas de ciberseguridad razonables que aparecen en la DORA. Si sus planes de crecimiento implican la expansión a la UE o desarrollar actividades con instituciones financieras que operan en la UE, es aconsejable trabajar ahora para lograr el cumplimiento normativo. Si se le exige cumplir plenamente con la normativa, y tiene de plazo hasta enero, tendrá que actuar con rapidez y, cuando sea necesario, buscar ayuda externa. Si presta servicios a empresas de la UE que operan en el sector de los servicios financieros, debería colaborar estrechamente con ellas para alinear sus estrategias.

El siguiente paso es realizar un análisis gap para evaluar la madurez de su postura en ciberseguridad y en qué medida sus sistemas reflejan los exigidos por la normativa. Una vez completado, puede comenzar a cubrir los gaps y a poner en marcha los requisitos del personal, los procesos y la tecnología requerida.

Barracuda

Más información

La Autoridad Europea de Seguros y Pensiones de Jubilación ofrece una buena guía de la DORA orientada a las empresas. Si desea obtener más información, aquí tiene la legislación vigente (PDF de 75 páginas).

Barracuda Networks puede ayudar a su organización a cumplir con los cinco componentes principales de la DORA. Nuestro conjunto completo de herramientas de ciberseguridad puede reforzar su postura de seguridad en todas las áreas, desde el correo electrónico hasta las aplicaciones web y la seguridad de la red.

Contamos con una gran cantidad de recursos en línea para ayudarle a hacer frente a la DORA, que incluye XDR para mejorar su detección y respuesta a la gestión de amenazas y cómo conseguir que la junta respalde las estrategias de ciberseguridad.

También podemos ayudarle a perfeccionar su respuesta ante incidentes. Por último, la información de seguridad de Barracuda le puede proporcionar la inteligencia activa que precisa para potenciar su análisis de riesgos.

Barracuda

Sobre Barracuda

En Barracuda nos esforzamos por hacer del mundo un lugar más seguro. Creemos que todas las empresas merecen acceso a soluciones de seguridad de nivel empresarial cloud-first y que sean fáciles de comprar, implementar y usar. Protegemos el correo electrónico, las redes, los datos y las aplicaciones con soluciones innovadoras que crecen y se adaptan a la trayectoria de nuestros clientes. Más de 200 000 organizaciones de todo el mundo confían en Barracuda para que las proteja, de formas que ni siquiera saben que están en riesgo, con el fin de que puedan centrarse en llevar su negocio al siguiente nivel. Para obtener más información, visite barracuda.com.