Cybersecurity Database

INFORME

Fallo de Microsoft Azure API Management explotado en el ciberataque a Equinor y a la energía noruega (2026)

El 17 de noviembre de 2026 Equinor anunció un ciberataque en curso contra algunos de sus sistemas informáticos; el 20 de noviembre la autoridad noruega de seguridad (NSM) vinculó el ataque a Equinor y a Skagerak Energi con una vulnerabilidad de Microsoft Azure API Management que afecta a varios sectores en Noruega y fuera. Qué se sabe, quién debe revisar sus sistemas, qué normas y estándares cuentan y qué hacer ya.

Edición	Datos a 25 de noviembre de 2026
Versión siempre actualizada	https://www.cybersecuritydatabase.org/es/reports/azure-api-management-equinor-attack/
Licencia	CC BY 4.0: libre reutilización citando la fuente

A quién sirve: Para periodistas y para quien trabaja en los sectores afectados: los hechos confirmados por las fuentes oficiales, las normas y estándares relacionados y las medidas recomendadas por las autoridades.

> El 17 de noviembre de 2026 Equinor, uno de los mayores proveedores de gas de Europa, comunicó que había detectado un ciberataque en curso contra algunos sistemas informáticos, sin efectos en la producción. El 20 de noviembre la autoridad noruega de seguridad (NSM) explicó que Equinor y Skagerak Energi están entre las víctimas de una vulnerabilidad de Azure API Management, el servicio en la nube de Microsoft que gestiona las conexiones entre aplicaciones: un actor desconocido buscó de forma dirigida tokens de acceso, secretos y valores guardados en el servicio. El fallo, ya cerrado, afecta a varios sectores en Noruega y también fuera del país, y la NSM pide a quien use el servicio que considere comprometidos sus secretos y los sustituya. Ese mismo día Equinor anunció que había detenido el ataque.

Qué hacer ya

Las medidas indicadas por la NSM y por Microsoft para quien usa Azure API Management.

1. Considerar expuestos todos los secretos y «named values» guardados en Azure API Management y sustituirlos todos: claves de suscripción, credenciales hacia los backends, certificados, cadenas de conexión, secretos de los proveedores de identidad.
2. Sustituir primero cada credencial ante quien la emite (backend, proveedor de identidad) y solo después actualizarla en el servicio: cambiarla solo en API Management no revoca la antigua.
3. Comprobar la versión de la instancia desde la página de estado interna de la pasarela como indica la NSM y, si no está actualizada, contactar con Microsoft.
4. Identificar qué datos y sistemas hay detrás de cada instancia, para entender qué podía alcanzar quien leyó los secretos, y buscar en los registros accesos desde redes nunca vistas.
5. Llevar los secretos a un almacén dedicado (como Azure Key Vault) en lugar de escribirlos en el servicio o en sus políticas, y eliminar las contraseñas en claro.
6. Si hay indicios de compromiso, avisar al CSIRT nacional o a la autoridad del sector (en Noruega la NSM) y notificar el incidente cuando la ley lo exija.

Cronología

Fecha	Qué ocurrió	Fuentes
17 de noviembre de 2026	Equinor comunica que ha detectado un ciberataque en curso contra algunos sistemas informáticos. No hay indicios de robo de datos y las operaciones y la producción no se ven afectadas; la empresa está en contacto con las autoridades nacionales de seguridad y ha denunciado los hechos a la policía. En los días siguientes precisa que no se trata de un virus, que el ataque no puede propagarse y que no parece dirigido específicamente contra Equinor.	[2]

Fecha	Qué ocurrió	Fuentes
20 de noviembre de 2026	La NSM publica medidas contra la vulnerabilidad de Azure API Management: un actor desconocido buscó activamente tokens de acceso, secretos y «named values» en el servicio; el fallo ya está cerrado, pero quien use el servicio debe considerar expuestos sus secretos y sustituirlos todos. Equinor y Skagerak Energi están entre las empresas afectadas; la vulnerabilidad la descubrió primero el sector energético noruego y afecta a varios sectores en Noruega y fuera. Por ahora la NSM no tiene indicios de efectos en los suministros de las empresas noruegas.	[1]
20 de noviembre de 2026	Equinor anuncia que el ataque se ha detenido: la producción sigue con normalidad y no hay indicios de robo o alteración de datos ni de consecuencias para empleados, socios o proveedores.	[2]
21 de noviembre de 2026	Microsoft publica una guía para encontrar y sustituir los secretos y credenciales configurados en las instancias de Azure API Management (claves de suscripción, credenciales hacia los backends, secretos de los proveedores de identidad, cadenas de conexión), con el orden que hay que seguir para no interrumpir los servicios. La guía no menciona la vulnerabilidad ni los ataques en Noruega.	[3]

Países afectados

País	Casos notificados
Noruega	Resultaron afectadas Equinor, con algunos servicios internos alterados hasta la contención del 20 de noviembre, y Skagerak Energi, productora de electricidad controlada por Statkraft, que según la prensa no tuvo efectos en sus operaciones ni en la producción. Según la NSM, otras empresas noruegas de varios sectores usan el servicio vulnerable y el alcance de la explotación sigue sin estar claro; el nivel nacional de riesgo cibernético sigue siendo alto. Según la prensa, Microsoft detectó el problema el 18 de noviembre, lo cerró al día siguiente e indica que afecta a los niveles «Classic» del servicio, sobre todo a quien guardaba allí los secretos en lugar de en Azure Key Vault (The Record, 23 de noviembre). [1] [2] [4]

Por qué un fallo en la nube se convierte en un ataque a la energía

Azure API Management se sitúa delante de las API de una empresa y guarda las credenciales para llegar a los sistemas que hay detrás: claves, tokens, contraseñas de servicio. Quien consigue leerlas no necesita forzar nada más: entra con credenciales válidas. Por eso la NSM pide no solo actualizar, sino sustituir todos los secretos y averiguar qué datos y sistemas había detrás de cada instancia.

El caso muestra el riesgo de concentración de la nube: un solo fallo en un servicio usado en todo el mundo alcanza de golpe a empresas de sectores y países distintos, incluidas infraestructuras críticas. La responsabilidad sigue siendo compartida: el proveedor cierra el fallo, pero corresponde al cliente guardar los secretos en el lugar adecuado, rotarlos y vigilar los accesos.

Qué dicen las normas

Los actos de la base de datos que afectan a la seguridad de los operadores de energía y de los servicios en la nube.

Ley de seguridad digital (Noruega)

La ley noruega de seguridad digital, que transpone la primera Directiva NIS: se aplica a los operadores de servicios esenciales de la energía y a los proveedores de servicios en la nube, con obligaciones de medidas de seguridad y de notificación de incidentes significativos.

Directiva (UE) 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva SRI 2)

En la UE, la energía y los servicios de computación en nube son sectores de alta criticidad de NIS 2: las medidas de gestión del riesgo incluyen la seguridad de la cadena de suministro, la relación con los proveedores de servicios y el control de acceso (art. 21), y los incidentes significativos deben notificarse en 24 horas (art. 23).

Los estándares de referencia

Los estándares de la base de datos más útiles para usar la nube con seguridad y proteger las credenciales.

ISO/IEC 27017 e 27018 – Controles de seguridad y protección de datos personales para los servicios en la nube

Controles de seguridad para los servicios en la nube, con el reparto de tareas entre proveedor y cliente: quién protege qué, quién actualiza y quién vigila.

CSA CCM v4.1 – Matriz de controles para la nube (CCM) y cuestionario de evaluación (CAIQ) v4.1

La matriz de la Cloud Security Alliance: sus dominios sobre gestión de claves y secretos, identidad y accesos y responsabilidad compartida son los que toca este caso.

CIS Controls v8.1 – Controles de seguridad críticos del CIS

El control 3 (protección de datos, incluidos los secretos), los controles 5 y 6 (gestión de cuentas y accesos) y el 15 (gestión de proveedores de servicios) llevan a la práctica lo que pide la NSM.

Para saber más: el informe «La caída mundial de Outlook, Teams y Microsoft 365 del 12 y 13 de noviembre y el riesgo para la producción (2026)».

Fuentes del análisis

1. **Fuentes oficiales:** Nasjonal sikkerhetsmyndighet (NSM), NSM deler tiltak mot sårbarhet i Azure API Management ↗, 20 de noviembre de 2026.https://nsm.no/aktuelt/nsm-deler-tiltak-mot-sarbarhet-i-azure-api-management
2. Equinor, Cyber-attack stopped (Equinor has detected a cyber-attack) ↗, 17 de noviembre de 2026.https://www.equinor.com/news/20261711-equinor-detected-cyber-attack
3. Microsoft, Rotating credentials in Azure API Management ↗, 21 de noviembre de 2026.https://techcommunity.microsoft.com/blog/integrationsonazureblog/rotating-credentials-in-azure-api-management/4575478
4. **Prensa:** The Record (Recorded Future News), Norway says hackers exploited Microsoft security flaw to attack energy firms Equinor, Skagerak Energi ↗, 23 de noviembre de 2026.https://therecord.media/norway-microsoft-cyberattack-equinor

Para una respuesta práctica

- A quién y en qué plazo notificar un incidente, país por país
- Las autoridades nacionales y los CSIRT de cada país
- La página de su sector: leyes de la UE, actos específicos y normas

Fuentes y datos

Resumen «qué se sabe» basado en los comunicados oficiales de la autoridad noruega de seguridad (NSM) y de Equinor, en las indicaciones públicas de Microsoft y, donde se indica, en medios de comunicación. Vale para los hechos conocidos en la fecha indicada: no se ha identificado al autor y el alcance de la explotación sigue sin estar claro. Prevalecen las fuentes citadas.

- Página interactiva: Normas y marcos https://www.cybersecuritydatabase.org/es/standards/
- Datos abiertos (JSON): documents.json https://www.cybersecuritydatabase.org/api/v1/documents.json

Cómo citar

Cybersecurity Database, «Fallo de Microsoft Azure API Management explotado en el ciberataque a Equinor y a la energía noruega (2026)», datos a 25 de noviembre de 2026, https://www.cybersecuritydatabase.org/es/reports/azure-api-management-equinor-attack/. Licencia CC BY 4.0.