Cybersecurity Database

REPORT

Falla di Microsoft Azure API Management sfruttata, l’attacco informatico a Equinor e all’energia norvegese (2026)

Il 17 novembre 2026 Equinor ha annunciato un attacco informatico in corso contro alcuni suoi sistemi IT; il 20 novembre l’autorità norvegese per la sicurezza (NSM) ha collegato l’attacco a Equinor e a Skagerak Energi a una vulnerabilità di Microsoft Azure API Management, che colpisce più settori in Norvegia e fuori. Cosa sappiamo, chi deve controllare i propri sistemi, quali norme e standard contano e cosa fare subito.

Edizione	Dati al 25 novembre 2026
Versione sempre aggiornata	https://www.cybersecuritydatabase.org/it/reports/azure-api-management-equinor-attack/
Licenza	CC BY 4.0: libero riuso citando la fonte

A chi serve: Per i giornalisti e per chi lavora nei settori colpiti: i fatti confermati dalle fonti ufficiali, le norme e gli standard collegati e le misure raccomandate dalle autorità.

> Il 17 novembre 2026 Equinor, uno dei maggiori fornitori di gas d'Europa, ha comunicato di aver individuato un attacco informatico in corso contro alcuni sistemi IT, senza effetti sulla produzione. Il 20 novembre l'autorità norvegese per la sicurezza (NSM) ha spiegato che Equinor e Skagerak Energi sono fra le vittime di una vulnerabilità di Azure API Management, il servizio cloud di Microsoft che gestisce le connessioni fra applicazioni: un attore sconosciuto ha cercato in modo mirato token di accesso, segreti e valori salvati nel servizio. La falla, ora chiusa, tocca più settori in Norvegia e anche fuori dal paese, e l'NSM chiede a chiunque usi il servizio di considerare compromessi i propri segreti e di sostituirli. Lo stesso giorno Equinor ha annunciato di aver fermato l'attacco.

Cosa fare subito

Le misure indicate dall'NSM e da Microsoft per chi usa Azure API Management.

1. Considerare esposti tutti i segreti e i «named values» salvati in Azure API Management e sostituirli tutti: chiavi di sottoscrizione, credenziali verso i backend, certificati, stringhe di connessione, segreti dei fornitori di identità.
2. Sostituire prima la credenziale presso chi la emette (backend, fornitore di identità) e solo dopo aggiornarla nel servizio: cambiarla solo in API Management non revoca quella vecchia.
3. Controllare la versione dell'istanza dalla pagina di stato interna del gateway come indica l'NSM e, se non risulta aggiornata, contattare Microsoft.
4. Mappare quali dati e sistemi stanno dietro ogni istanza, per capire cosa poteva raggiungere chi ha letto i segreti, e cercare nei registri accessi da reti mai viste.
5. Spostare i segreti in un archivio dedicato (come Azure Key Vault) invece di scriverli nel servizio o nelle policy, e togliere le password scritte in chiaro.
6. In caso di segni di compromissione avvisare il CSIRT nazionale o l'autorità di settore (in Norvegia l'NSM) e notificare l'incidente quando la legge lo prevede.

Cronologia

Data	Cosa è successo	Fonti
17 novembre 2026	Equinor comunica di aver individuato un attacco informatico in corso contro alcuni sistemi IT. Non ci sono segni di furto di dati e produzione e attività non sono toccate; l'azienda è in contatto con le autorità di sicurezza nazionali e ha denunciato il fatto alla polizia. Nei giorni seguenti precisa che non si tratta di un virus, che l'attacco non può propagarsi e che non sembra mirato specificamente a Equinor.	[2]
20 novembre 2026	L'NSM pubblica le misure contro la vulnerabilità di Azure API Management: un attore sconosciuto ha cercato attivamente token di accesso, segreti e «named values» nel servizio; la falla ora risulta chiusa, ma chi usa il servizio deve considerare i propri segreti esposti e sostituirli tutti. Equinor e Skagerak Energi sono fra le aziende colpite; la vulnerabilità è stata scoperta per prima dal settore energetico norvegese e colpisce più settori in Norvegia e fuori. L'NSM non ha finora indizi di effetti sulle forniture delle aziende norvegesi.	[1]

Data	Cosa è successo	Fonti
20 novembre 2026	Equinor annuncia che l'attacco è stato fermato: la produzione procede normalmente e non ci sono segni di furto o modifica dei dati né conseguenze per dipendenti, partner o fornitori.	[2]
21 novembre 2026	Microsoft pubblica una guida per trovare e sostituire i segreti e le credenziali configurati nelle istanze di Azure API Management (chiavi di sottoscrizione, credenziali verso i backend, segreti dei fornitori di identità, stringhe di connessione), con l'ordine da seguire per non interrompere i servizi. La guida non cita la vulnerabilità né gli attacchi in Norvegia.	[3]

Paesi colpiti

Paese	Casi segnalati
Norvegia	Colpite Equinor, che ha avuto alcuni servizi interni disturbati fino al contenimento del 20 novembre, e Skagerak Energi, produttore di elettricità controllato da Statkraft, che secondo la stampa non ha avuto effetti sulle attività né sulla produzione. Secondo l'NSM altre aziende norvegesi di più settori usano il servizio vulnerabile e la portata dello sfruttamento è ancora incerta; il livello nazionale di rischio cyber resta alto. Secondo la stampa Microsoft ha individuato il problema il 18 novembre, lo ha chiuso il giorno dopo e indica che riguarda i livelli «Classic» del servizio, in particolare chi vi conservava i segreti invece che in Azure Key Vault (The Record, 23 novembre). [1] [2] [4]

Perché una falla nel cloud diventa un attacco all'energia

Azure API Management sta davanti alle API di un'azienda e conserva le credenziali per raggiungere i sistemi che stanno dietro: chiavi, token, password di servizio. Chi riesce a leggerle non ha bisogno di forzare altro: entra con credenziali valide. Per questo l'NSM chiede non solo di aggiornare, ma di sostituire tutti i segreti e di capire quali dati e sistemi stavano dietro ogni istanza.

Il caso mostra il rischio di concentrazione del cloud: una sola falla in un servizio usato in tutto il mondo raggiunge in un colpo aziende di settori e paesi diversi, comprese infrastrutture critiche. La responsabilità resta condivisa: il fornitore chiude la falla, ma tocca al cliente custodire i segreti nel posto giusto, ruotarli e controllare gli accessi.

Cosa dicono le norme

Gli atti del database che riguardano la sicurezza degli operatori dell'energia e dei servizi cloud.

Legge sulla sicurezza digitale (Norvegia)

La legge norvegese sulla sicurezza digitale, che recepisce la prima direttiva NIS: si applica agli operatori di servizi essenziali dell'energia e ai fornitori di servizi cloud, con obblighi di misure di sicurezza e di notifica degli incidenti significativi.

Direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (Direttiva NIS 2)

Nell'UE energia e servizi cloud sono settori ad alta criticità della NIS 2: le misure di gestione del rischio comprendono la sicurezza della catena di fornitura, i rapporti con i fornitori di servizi e il controllo degli accessi (art. 21), e gli incidenti significativi vanno notificati entro 24 ore (art. 23).

Gli standard di riferimento

Gli standard del database più utili per usare il cloud in sicurezza e custodire le credenziali.

ISO/IEC 27017 e 27018 – Controlli di sicurezza e protezione dei dati personali per i servizi cloud

Controlli di sicurezza per i servizi cloud, con la divisione dei compiti fra fornitore e cliente: chi custodisce cosa, chi aggiorna e chi controlla.

CSA CCM v4.1 – Matrice dei controlli per il cloud (CCM) e questionario di valutazione (CAIQ) v4.1

La matrice della Cloud Security Alliance: i domini sulla gestione delle chiavi e dei segreti, sull'identità e sugli accessi e sulla responsabilità condivisa sono quelli toccati da questo caso.

CIS Controls v8.1 – Controlli di sicurezza critici del CIS

Il controllo 3 (protezione dei dati, compresi i segreti), il 5 e il 6 (gestione degli account e degli accessi) e il 15 (gestione dei fornitori di servizi) traducono in pratica le richieste dell'NSM.

Per approfondire: il report «Il blocco globale di Outlook, Teams e Microsoft 365 del 12-13 novembre e il rischio per la produzione (2026)».

Fonti dell'analisi

1. **Fonti ufficiali:** Nasjonal sikkerhetsmyndighet (NSM), NSM deler tiltak mot sårbarhet i Azure API Management ↗, 20 novembre 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 novembre 2026.https://www.equinor.com/news/20261711-equinor-detected-cyber-attack
3. Microsoft, Rotating credentials in Azure API Management ↗, 21 novembre 2026.https://techcommunity.microsoft.com/blog/integrationsonazureblog/rotating-credentials-in-azure-api-management/4575478

4. **Stampa:** The Record (Recorded Future News), Norway says hackers exploited Microsoft security flaw to attack energy firms Equinor, Skagerak Energi ↗, 23 novembre 2026.https://therecord.media/norway-microsoft-cyberattack-equinor

Per una risposta pratica

- A chi e entro quando notificare un incidente, paese per paese
- Le autorità nazionali e i CSIRT di ogni paese
- La pagina del tuo settore: leggi UE, atti specifici e standard

Fonti e dati

Ricostruzione «cosa sappiamo» basata sui comunicati ufficiali dell'autorità norvegese per la sicurezza (NSM) e di Equinor e sulle indicazioni pubbliche di Microsoft e, dove indicato, su testate giornalistiche. Vale per i fatti noti alla data indicata: l'autore non è stato identificato e la portata dello sfruttamento è ancora incerta. Fanno fede le fonti citate.

- Pagina interattiva: Standard e framework https://www.cybersecuritydatabase.org/it/standards/
- Dati aperti (JSON): documents.json https://www.cybersecuritydatabase.org/api/v1/documents.json

Come citare

Cybersecurity Database, «Falla di Microsoft Azure API Management sfruttata, l'attacco informatico a Equinor e all'energia norvegese (2026)», dati al 25 novembre 2026, https://www.cybersecuritydatabase.org/it/reports/azure-api-management-equinor-attack/. Licenza CC BY 4.0.