Cybersecurity Database

Report

Lücke in Microsoft Azure API Management ausgenutzt, der Cyberangriff auf Equinor und die norwegische Energiewirtschaft (2026)

Am 17. November 2026 meldete Equinor einen laufenden Cyberangriff auf einige seiner IT-Systeme; am 20. November brachte die norwegische Sicherheitsbehörde NSM den Angriff auf Equinor und Skagerak Energi mit einer Schwachstelle in Microsoft Azure API Management in Verbindung, die mehrere Sektoren in Norwegen und im Ausland betrifft. Was bekannt ist, wer seine Systeme prüfen muss, welche Regeln und Normen zählen und was jetzt zu tun ist.

Ausgabe	Datenstand: 25. November 2026
Stets aktuelle Fassung	https://www.cybersecuritydatabase.org/de/reports/azure-api-management-equinor-attack/
Lizenz	CC BY 4.0: freie Weiterverwendung mit Quellenangabe

Für wen: Für Journalisten und für alle, die in den betroffenen Sektoren arbeiten: die von amtlichen Quellen bestätigten Fakten, die zugehörigen Gesetze und Normen und die von den Behörden empfohlenen Maßnahmen.

> Am 17. November 2026 meldete Equinor, einer der größten Gaslieferanten Europas, einen laufenden Cyberangriff auf einige IT-Systeme, ohne Auswirkungen auf die Förderung. Am 20. November erklärte die norwegische Sicherheitsbehörde NSM, dass Equinor und Skagerak Energi zu den Opfern einer Schwachstelle in Azure API Management gehören, dem Cloud-Dienst von Microsoft, der Verbindungen zwischen Anwendungen verwaltet: Ein unbekannter Akteur suchte gezielt nach Zugriffstoken, Geheimnissen und im Dienst gespeicherten Werten. Die inzwischen geschlossene Lücke betrifft mehrere Sektoren in Norwegen und auch im Ausland, und die NSM fordert alle Nutzer des Dienstes auf, ihre Geheimnisse als kompromittiert zu betrachten und zu ersetzen. Am selben Tag meldete Equinor, den Angriff gestoppt zu haben.

Was jetzt zu tun ist

Die Maßnahmen von NSM und Microsoft für alle, die Azure API Management nutzen.

1. Alle in Azure API Management gespeicherten Geheimnisse und „Named Values“ als offengelegt betrachten und sämtlich ersetzen: Abonnementschlüssel, Backend-Zugangsdaten, Zertifikate, Verbindungszeichenfolgen, Geheimnisse von Identitätsanbietern.
2. Jede Zugangsdate zuerst beim Aussteller (Backend, Identitätsanbieter) ersetzen und erst danach im Dienst aktualisieren: Eine Änderung nur in API Management widerruft die alte nicht.
3. Die Version der Instanz über die interne Statusseite des Gateways prüfen, wie die NSM erläutert, und Microsoft kontaktieren, wenn sie nicht aktualisiert ist.
4. Erfassen, welche Daten und Systeme hinter jeder Instanz liegen, um zu verstehen, was jemand mit den Geheimnissen erreichen konnte, und in den Protokollen nach Zugriffen aus unbekannten Netzen suchen.
5. Geheimnisse in einen eigenen Tresor (etwa Azure Key Vault) verlagern, statt sie in den Dienst oder seine Richtlinien zu schreiben, und Klartextpasswörter entfernen.
6. Bei Anzeichen einer Kompromittierung das nationale CSIRT oder die zuständige Sektorbehörde (in Norwegen die NSM) informieren und den Vorfall melden, wo das Gesetz es verlangt.

Chronologie

Datum	Was geschah	Quellen
17. November 2026	Equinor meldet einen laufenden Cyberangriff auf einige IT-Systeme. Es gibt keine Hinweise auf Datendiebstahl, Betrieb und Förderung sind nicht betroffen; das Unternehmen steht mit den nationalen Sicherheitsbehörden in Kontakt und hat Anzeige bei der Polizei erstattet. In den folgenden Tagen ergänzt es, dass es sich nicht um einen Virenangriff handelt, sich der Angriff nicht ausbreiten kann und nicht gezielt gegen Equinor gerichtet zu sein scheint.	[2]
20. November 2026	Die NSM veröffentlicht Maßnahmen gegen die Schwachstelle in Azure API Management: Ein unbekannter Akteur suchte aktiv nach Zugriffstoken, Geheimnissen und „Named Values“ im Dienst; die Lücke gilt inzwischen als geschlossen, doch Nutzer des Dienstes müssen ihre Geheimnisse als offengelegt betrachten und alle austauschen. Equinor und Skagerak Energi gehören zu den betroffenen Unternehmen; die Schwachstelle wurde zuerst von der norwegischen Energiewirtschaft entdeckt und betrifft mehrere Sektoren in Norwegen und im Ausland. Bisher hat die NSM keine Hinweise auf Folgen für die Lieferungen norwegischer Unternehmen.	[1]
20. November 2026	Equinor meldet, dass der Angriff gestoppt wurde: Die Förderung läuft normal, und es gibt keine Hinweise auf gestohlene oder veränderte Daten oder auf Folgen für Mitarbeitende, Partner oder Lieferanten.	[2]
21. November 2026	Microsoft veröffentlicht eine Anleitung, um die in Azure-API-Management-Instanzen hinterlegten Geheimnisse und Zugangsdaten zu finden und zu ersetzen (Abonnementschlüssel, Backend-Zugangsdaten, Geheimnisse von Identitätsanbietern, Verbindungszeichenfolgen), mit der Reihenfolge, die Dienstunterbrechungen vermeidet. Die Anleitung erwähnt weder die Schwachstelle noch die Angriffe in Norwegen.	[3]

Betroffene Länder

Land	Gemeldete Fälle
Norwegen	Betroffen sind Equinor, bei dem einige interne Dienste bis zur Eindämmung am 20. November gestört waren, und Skagerak Energi, ein von Statkraft kontrollierter Stromerzeuger, bei dem es laut Presse keine Auswirkungen auf Betrieb und Erzeugung gab. Laut NSM nutzen weitere norwegische Unternehmen aus mehreren Sektoren den verwundbaren Dienst, das Ausmaß der Ausnutzung ist noch unklar; das nationale Cyberrisiko bleibt hoch. Laut Presse erkannte Microsoft das Problem am 18. November, schloss es am Folgetag und gibt an, dass es die „Classic“-Stufen des Dienstes betrifft, vor allem Kunden, die Geheimnisse dort statt in Azure Key Vault speicherten (The Record, 23. November). [1] [2] [4]

Warum eine Cloud-Lücke zum Angriff auf die Energiewirtschaft wird

Azure API Management steht vor den APIs eines Unternehmens und speichert die Zugangsdaten für die dahinterliegenden Systeme: Schlüssel, Token, Dienstpasswörter. Wer sie lesen kann, muss nichts weiter aufbrechen: Er meldet

sich mit gültigen Zugangsdaten an. Deshalb verlangt die NSM nicht nur ein Update, sondern den Austausch aller Geheimnisse und eine Klärung, welche Daten und Systeme hinter jeder Instanz lagen.

Der Fall zeigt das Konzentrationsrisiko der Cloud: Eine einzige Lücke in einem weltweit genutzten Dienst trifft auf einen Schlag Unternehmen verschiedener Sektoren und Länder, auch kritische Infrastrukturen. Die Verantwortung bleibt geteilt: Der Anbieter schließt die Lücke, doch der Kunde muss Geheimnisse am richtigen Ort aufbewahren, regelmäßig austauschen und Zugriffe überwachen.

Was die Regeln sagen

Die Rechtsakte der Datenbank, die die Sicherheit von Energieversorgern und Cloud-Diensten betreffen.

Gesetz über digitale Sicherheit (Norwegen)

Das norwegische Gesetz über digitale Sicherheit, das die erste NIS-Richtlinie umsetzt: Es gilt für Betreiber wesentlicher Dienste im Energiesektor und für Cloud-Anbieter, mit Pflichten zu Sicherheitsmaßnahmen und zur Meldung erheblicher Vorfälle.

Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie)

In der EU gehören Energie und Cloud-Computing-Dienste zu den Sektoren mit hoher Kritikalität der NIS 2: Die Risikomanagementmaßnahmen umfassen die Sicherheit der Lieferkette, die Beziehungen zu Dienstleistern und die Zugriffskontrolle (Art. 21), erhebliche Vorfälle sind binnen 24 Stunden zu melden (Art. 23).

Die maßgeblichen Normen

Die Normen der Datenbank, die für eine sichere Cloud-Nutzung und den Schutz von Zugangsdaten am nützlichsten sind.

ISO/IEC 27017 e 27018 – Informationssicherheitsmaßnahmen und Schutz personenbezogener Daten für Cloud-Dienste

Sicherheitsmaßnahmen für Cloud-Dienste mit der Aufgabenteilung zwischen Anbieter und Kunde: wer was schützt, wer aktualisiert und wer überwacht.

CSA CCM v4.1 – Cloud-Kontrollmatrix (CCM) und Bewertungsfragebogen (CAIQ) v4.1

Die Matrix der Cloud Security Alliance: Ihre Bereiche zu Schlüssel-und Geheimnisverwaltung, Identität und Zugriff sowie geteilter Verantwortung sind die, die dieser Fall berührt.

CIS Controls v8.1 – Kritische Sicherheitskontrollen des CIS

Control 3 (Datenschutz einschließlich Geheimnissen), die Controls 5 und 6 (Konten-und Zugriffsverwaltung) und Control 15 (Verwaltung von Dienstleistern) setzen die Forderungen der NSM praktisch um.

Zur Vertiefung: der Report „Der weltweite Ausfall von Outlook, Teams und Microsoft 365 am 12. und 13. November und das Risiko für die Produktion (2026)“.

Quellen der Analyse

1. **Amtliche Quellen:** Nasjonal sikkerhetsmyndighet (NSM), NSM deler tiltak mot sårbarhet i Azure API Management ↗, 20. November 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. November 2026.https://www.equinor.com/news/20261711-equinor-detected-cyber-attack
3. Microsoft, Rotating credentials in Azure API Management ↗, 21. November 2026.https://techcommunity.microsoft.com/blog/integrationsonazureblog/rotating-credentials-in-azure-api-management/4575478
4. **Presse:** The Record (Recorded Future News), Norway says hackers exploited Microsoft security flaw to attack energy firms Equinor, Skagerak Energi ↗, 23. November 2026.https://therecord.media/norway-microsoft-cyberattack-equinor

Für eine praktische Antwort

- Wem und wie schnell ein Vorfall zu melden ist, Land für Land
- Die nationalen Behörden und CSIRTs jedes Landes
- Die Seite Ihres Sektors: EU-Gesetze, spezifische Rechtsakte und Normen

Quellen und Daten

„Was bekannt ist“ auf Grundlage amtlicher Mitteilungen der norwegischen Sicherheitsbehörde NSM und von Equinor, der öffentlichen Hinweise von Microsoft und, wo angegeben, von Medienberichten. Stand zum angegebenen Datum: Der Angreifer ist nicht identifiziert, das Ausmaß der Ausnutzung ist noch unklar. Maßgeblich sind die zitierten Quellen.

- Interaktive Seite: Normen und Frameworks https://www.cybersecuritydatabase.org/de/standards/
- Offene Daten (JSON): documents.json https://www.cybersecuritydatabase.org/api/v1/documents.json

Zitiervorschlag

Cybersecurity Database, „Lücke in Microsoft Azure API Management ausgenutzt, der Cyberangriff auf Equinor und die norwegische Energiewirtschaft (2026)“, Datenstand 25. November 2026, https://www.cybersecuritydatabase.org/de/reports/azure-api-management-equinor-attack/. Lizenz CC BY 4.0.