Istruzione 1/2024

Vigilanza sulla cibersicurezza della ElCom

8 febbraio 2024 / Update 1° aprile 2025[1]

1 Situazione iniziale

Secondo il nuovo articolo 8*a* della legge federale del 23 marzo 2007 sull'approvvigionamento elettrico (LAEl; RS 734.7) e l'articolo 5*a* del progetto di revisione dell'ordinanza del 14 marzo 2008 sull'approvvigionamento elettrico (OAEl; RS 734.71), che entreranno in vigore nel luglio 2024, i gestori di rete, i produttori, i gestori di impianti di stoccaggio e i fornitori di servizi (di seguito «imprese») devono adottare misure per proteggere adeguatamente i loro impianti contro le ciberminacce. Per il funzionamento sicuro e stabile delle reti elettriche svizzere ciò significa che l'«information technology» (tecnologie dell'informazione; IT)[2] e, in particolare, l'«operational technology» (tecnologia operativa; OT)[3] devono essere protette contro le ciberminacce.

Secondo l'articolo 22 capoverso 1 LAEl, la ElCom vigila sul rispetto della legge federale sull'approvvigionamento elettrico e, di conseguenza, anche sullo stato di attuazione delle misure di protezione contro le ciberminacce. In questo contesto la ElCom accorda la priorità al funzionamento sicuro e stabile delle reti elettriche svizzere. Il NIST Cybersecurity Framework fornisce il quadro di riferimento per il compito di vigilanza della ElCom, utilizzato, tra l'altro, anche per lo standard minimo TIC dell'Ufficio federale per l'approvvigionamento economico del Paese (UFAE), i documenti di settore dell'Associazione delle aziende elettriche svizzere (AES) e per la definizione delle future disposizioni legali.

Per consentire alla ElCom di svolgere il proprio compito di vigilanza, le imprese sono tenute a fornire alla ElCom le informazioni necessarie all'attuazione della legge e a mettere a disposizione i documenti necessari conformemente all'articolo 25 capoverso 1 LAEl.

---

1 Nuova cifra 4 «Obbligo di informazione in caso di ciberincidenti secondo la LSIn»

2 Il concetto di «information technology» (IT) comprende tutte le tecnologie per l'elaborazione dei dati che non hanno a che fare direttamente con la messa a disposizione di energia elettrica (p. es. gestione dei dati dei clienti, gestione dei dati del personale, applicazioni per ufficio).

3 Il concetto di «operational technology» comprende le tecnologie necessarie per la messa a disposizione o la fornitura di energia elettrica (p. es. SCADA, PIA, accesso remoto a impianti situati in sottostazioni, sistemi di telecomando centralizzati, gestione dei dati energetici [MDE], smart meter, sistemi di controllo e di regolazione intelligenti).

Commissione federale dell'energia elettrica ElCom
Christoffelgasse 5, 3003 Berna
Tel. +41 58 462 58 33, Fax +41 58 462 02 22
info@elcom.admin.ch
www.elcom.admin.ch

In vista dell'imminente entrata in vigore delle versioni rivedute della LAEl e della OAEl nel luglio 2024, che contengono nuove disposizioni in materia di protezione contro le ciberminacce, la ElCom ha rielaborato il suo piano di vigilanza. La presente istruzione ha lo scopo di specificare i punti chiave dell'attuazione normativa di tale vigilanza. La ElCom si riserva il diritto di modificare le presenti istruzioni qualora al momento della sua stesura i principi in vigore dovessero cambiare in modo significativo.

Con la prevista entrata in vigore della revisione dell'OAEl nel luglio 2024, i gestori di rete, i produttori, i gestori di impianti di stoccaggio e i fornitori di servizi dovranno rispettare standard minimi di cibersicurezza. Nella nuova OAEl gli standard minimi sono definiti in virtù delle cinque categorie NIST «Identify, Protect, Detect, Respond e Recover», considerate le basi per aumentare la resilienza dell'approvvigionamento elettrico svizzero nei confronti delle ciberminacce.

Gli standard minimi variano a seconda delle dimensioni e del tipo di impresa e, a seconda della sua esposizione al rischio, possono non essere sufficienti per garantire un esercizio sicuro e stabile. Spetta comunque sempre alle imprese garantire un'adeguata protezione contro le ciberminacce per i propri impianti e sistemi. Gli standard minimi sono vincolanti a partire dall'entrata in vigore della nuova OAEl senza periodo di transizione. Rientra tuttavia nei compiti di vigilanza della ElCom disciplinare i termini e le procedure per verificare l'adempimento degli standard minimi.

Per i gestori di rete i costi dell'attuazione delle misure di cibersicurezza rappresentano costi di rete computabili, a condizione che soddisfino i requisiti di computabilità di cui all'articolo 15 capoverso 1 LAEl. Con la comunicazione del 28 settembre 2022 sulla computabilità dei costi della cibersicurezza, la ElCom ha chiarito i dubbi circa questo aspetto.

2 Vigilanza

Per quanto riguarda la vigilanza, la ElCom persegue un approccio basato sul rischio per garantire un funzionamento sicuro e stabile delle reti elettriche svizzere. L'obiettivo della vigilanza è rafforzare la resilienza nei confronti delle ciberminacce. Le varie imprese vengono pertanto monitorate in misura diversa, a seconda della loro rilevanza e della situazione di rischio per il funzionamento sicuro e stabile delle reti elettriche svizzere. Gli strumenti di vigilanza devono consentire alla ElCom di valutare se le misure adottate corrispondono alle considerazioni sui rischi dell'impresa e se sono state rispettate le disposizioni legali. Ciò significa che, in virtù della sua attività di regolazione, la ElCom può formulare raccomandazioni e/o ordinare misure. Per l'attuazione delle misure, la ElCom può avvalersi dei consueti rimedi giuridici. Attualmente la ElCom prevede di impiegare e combinare in modo complementare tre strumenti di vigilanza.

2.1 Sondaggi

Dopo l'entrata in vigore della revisione dell'OAEl le imprese dovranno soddisfare determinati standard minimi. In una prima fase, la ElCom verificherà il rispetto degli standard minimi attraverso un'autovalutazione nel quadro di un assessment tool dell'UFAE. Le autovalutazioni presentate dovranno essere avallate dalla direzione dell'impresa. Il sondaggio, condotto ogni anno presso tutte le imprese interessate secondo la revisione dell'OAEl, consente alla ElCom di stilare una panoramica sull'adempimento delle disposizioni legali nonché di ottenere e analizzare informazioni sullo stato di attuazione delle misure di cibersicurezza.

2.2 Colloqui di sensibilizzazione

I colloqui di sensibilizzazione si svolgono in primo luogo con le imprese particolarmente rilevanti per il funzionamento sicuro e stabile delle reti elettriche svizzere. Essi sono previsti anche in caso di risposte sospette nei sondaggi oppure nel quadro di controlli a campione. L'obiettivo è ottenere informazioni concrete sull'attuazione delle misure di cibersicurezza, integrando così i risultati del sondaggio dal punto di vista qualitativo. I colloqui di sensibilizzazione si svolgono regolarmente in loco presso le imprese più rilevanti. I relativi risultati costituiscono la base per la valutazione della cibersicurezza dell'impresa e per

la formulazione di eventuali raccomandazioni di misure, la cui attuazione può essere verificata nell'ambito dei successivi colloqui di sensibilizzazione.

2.3 Audit

Il terzo strumento di vigilanza della ElCom è l'audit individuale, che consente di fornire informazioni più approfondite su determinati aspetti tecnici a seguito di anomalie emerse nel quadro del sondaggio o del colloquio di sensibilizzazione. È possibile effettuare audit anche sulla base di segnalazioni esterne o di controlli a campione. A seconda dell'obiettivo e dello scopo, gli audit vengono svolti dalla ElCom o da un auditor esterno.

3 Transizione verso gli standard minimi secondo l'OAEI

La revisione dell'OAEI non prevede un periodo di transizione per raggiungere gli standard minimi richiesti. Per fare in modo che le autovalutazioni fornite nel quadro del sondaggio presso le imprese riflettano il più fedelmente possibile la situazione attuale, la ElCom accorda un periodo di transizione di al massimo 24 mesi dopo l'entrata in vigore della revisione dell'OAEI per dimostrare l'adempimento degli standard minimi richiesti.

Per le categorie in cui gli standard minimi non sono stati raggiunti, occorre presentare un piano di attuazione delle misure con obiettivi concreti vincolanti, avallato dalla direzione dell'impresa. Se la ElCom reputa che le misure proposte in tale piano non vengano attuate in modo sufficientemente tempestivo, contatta le imprese interessate. Se vi sono ragioni giustificabili che hanno impedito il raggiugimento degli standard minimi durante il periodo di transizione, in via eccezionale la ElCom può accordare una deroga.

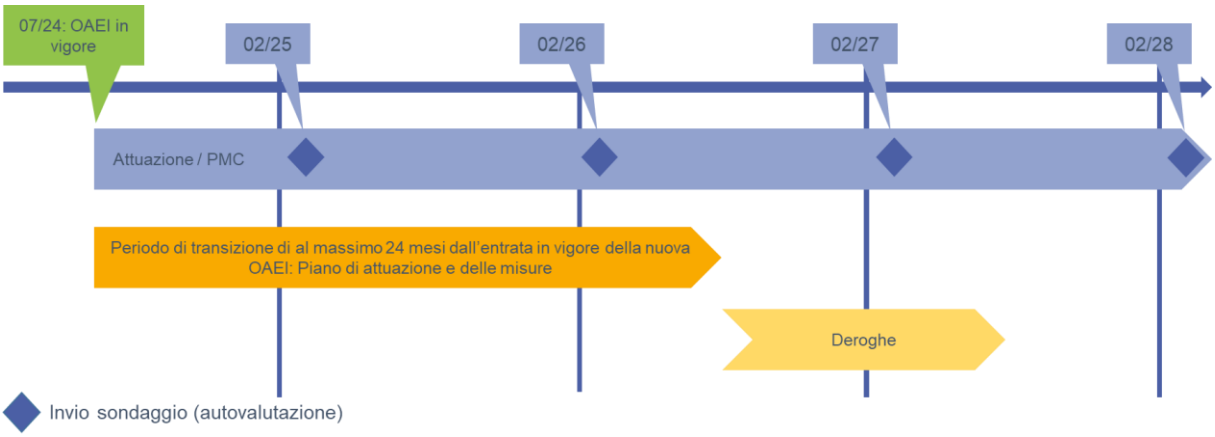

Figura: Raffigurazione schematica dell'attuazione degli standard minimi di cibersicurezza

4 Obbligo di informazione in caso di ciberincidenti secondo la LSIn

Con l'entrata in vigore, il 1° aprile 2025, della revisione della legge sulla sicurezza delle informazioni (LSIn; RS 128) vale l'obbligo di segnalare all'Ufficio federale della cibersicurezza (UFCS) eventuali ciberincidenti che interessino infrastrutture critiche (art. 74*a* segg. LSIn). L'UFCS ha creato un apposito modulo per la segnalazione. Tra i vari soggetti a cui si applica tale obbligo rientrano anche le imprese attive nel settore dell'approvvigionamento energetico secondo l'articolo 6 capoverso 1 della legge federale del 30 settembre 2016 sull'energia nonché le imprese attive nel commercio, nella misurazione e nella gestione dell'energia (art. 74*b* cpv. 1 lett. d LSIn).

Ai sensi dell'articolo 8 capoverso 3 LAEI i gestori di rete devono informare la ElCom in merito ad avvenimenti straordinari. La segnalazione all'UFCS di un ciberincidente di cui all'articolo 74*d* LSIn costituisce un avvenimento straordinario. Ciò significa che a partire dal 1° aprile 2025 i gestori di rete dovranno

comunicare anche alla ElCom le stesse informazioni di cui all'articolo 74*e* capoverso 2 LSIn che devono trasmettere all'UFCS in merito ad eventuali ciberincidenti. Sono esonerati da tale obbligo i gestori di rete che ai sensi dell'articolo 5*a* capoverso 1 e dell'allegato 1*a* OAEl non sono tenuti a rispettare né il livello di protezione A né il livello di protezione B (art. 12 cpv. 1 lett. b dell'ordinanza del 1° aprile 2025 sulla cibersicurezza [OCS; RS 128.51]).

In tal caso il gestore di rete adempie al proprio obbligo di informazione nei confronti della ElCom attraverso la segnalazione all'UFCS. A questo riguardo, conformemente all'articolo 73*d* capoverso 1 LSIn, deve dare il proprio consenso all'inoltro alla ElCom delle informazioni del caso nel modulo di segnalazione dell'UFCS, che contiene un apposito campo.