Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale dell'ambiente, dei trasporti,
dell'energia e delle comunicazioni DATEC

21 settembre 2023

Rapporto esplicativo concernente l'avamprogetto di revisione di maggio 2024 dell'ordinanza sull'approvvigionamento elettrico (protezione dai ciberattacchi)

1. Situazione iniziale

Le tecnologie dell'informazione e della comunicazione (TIC) supportano lo sviluppo di un approvvigionamento energetico flessibile ed efficiente. In particolare, esse vengono sempre più impiegate per il monitoraggio e il controllo delle reti di approvvigionamento e per la produzione energetica. Se da un lato esse contribuiscono così all'ottimizzazione dei processi, dall'altro aumentano le possibilità di attacco per i criminali informatici e rappresentano quindi nuovi rischi.

La sicurezza dell'approvvigionamento energetico è di importanza strategica. Un esercizio sicuro garantisce la tutela di importanti beni giuridici. Il nostro sistema socio-economico è così fortemente dipendente dall'energia che un'interruzione grave della produzione o della distribuzione avrebbe conseguenze pesanti. La minaccia di un ciberattacco alle reti energetiche è aumentata in modo significativo e oggi è estremamente reale.

La Strategia nazionale per la protezione delle infrastrutture critiche 2018–2022 (Strategia PIC)[1] e la nuova ciberstrategia nazionale (CSN)[2] prevedono misure adeguate per accrescere la capacità di resistenza generale delle infrastrutture critiche. A questo riguardo la CSN sostiene l'attuazione dello Standard minimo sviluppato dall'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) per migliorare la resilienza delle TIC[3] (Standard minimo TIC) e non esclude di renderlo obbligatorio laddove necessario[4]. L'attuazione di questo documento è volontaria e le misure in esso contenute non sono ancora state implementate sistematicamente dall'industria energetica svizzera.

A causa delle crescenti minacce e della criticità della situazione è imperativo poter garantire un elevato livello di cibersicurezza. Sebbene gli sforzi compiuti finora dagli attori del settore siano apprezzabili, non sono ancora sufficienti né abbastanza diffusi, dati il grado di professionalizzazione e l'organizzazione dei gruppi criminali. Il rapporto di base dell'Ufficio federale dell'energia (UFE) sulla cibersicurezza[5], pubblicato nel 2021, mostra che attualmente non esiste un livello di protezione sufficientemente elevato nel settore delle fornitura di energia elettrica e che è quindi necessario un intervento normativo da parte dello Stato. Inoltre gli attuali sviluppi nel campo dell'intelligenza artificiale (ad es. ChatGPT) faciliteranno ulteriormente il lavoro dei cibercriminali. La resilienza della cibersicurezza nel settore elettrico devono essere migliorate per poter affrontare adeguatamente non solo le sfide attuali ma anche quelle future.

2. Punti essenziali del progetto

La revisione dell'ordinanza del 14 marzo 2008 sull'approvvigionamento elettrico (OAEl; RS 734.71) ha lo scopo di rendere lo Standard minimo TIC vincolante per i principali fornitori di energia elettrica. Nell'attuare le misure in esso previste, gli attori tenuti al suo rispetto devono raggiungere un determinato livello di protezione. Per garantire una certa proporzionalità sono previsti vari livelli (profili) di protezione, ciascuno con un differente livello di requisiti.

2.1 Standard minimo TIC

Lo Standard minimo TIC definisce una serie di misure e costituisce uno strumento importante per garantire la protezione dai ciberattacchi. Lo Standard si basa sul Cybersecurity Framework dell'istituto

[1] FF 2018 455
[2] www.ncsc.admin.ch > Strategia SNPC > Ciberstrategia nazionale CSN
[3] Ufficio federale per l'approvvigionamento economico del Paese, «Standard minimo per migliorare la resilienza delle TIC», Berna, 2023
[4] Misura 6, *Resilienza, standardizzazione e regolamentazione*, CSN, pagg. 20-21
[5] Ufficio federale dell'energia, «Cyber-Sicherheit und Cyber Resilienz für die Schweizer Stromversorgung» (Cibersicurezza e ciberresilienza per l'approvvigionamento elettrico svizzero), Berna, giugno 2021; documento disponibile in tedesco

statunitense per gli standard e la tecnologia NIST (National Institute of Standards and Technology)[6]. Esso contiene 108 misure, suddivise in 23 categorie, che possono aiutare a valutare e a migliorare la maturità aziendale nei confronti dell'organizzazione della cibersicurezza.

Le misure di base dello Standard non possono sostanzialmente essere modificate, tuttavia per la loro attuazione occorrono una certa flessibilità, la capacità di adeguarle alle nuove minacce e ai nuovi pericoli per l'azienda, ausili tecnici e competenze adeguate[7]. Non vengono prescritte soluzioni tecniche, che le imprese dovranno invece sviluppare autonomamente. A tal fine possono collaborare nel quadro delle strutture associative esistenti per la definizione di uno standard settoriale specifico.

2.2 Livello di protezione (profilo di protezione)

Il livello di protezione definisce i requisiti relativi al grado di attuazione delle misure stabilite nello Standard minimo TIC (valori/tier level indicati al capitolo 3 dello Standard minimo TIC). Al livello di protezione A corrispondono i requisiti più elevati, mentre i livelli di protezione B e C prevedono ciascuno requisiti leggermente inferiori rispetto al livello precedente. Per gli operatori di mercato più piccoli il livello di protezione C prevede indicazioni al riguardo solo per un numero limitato di misure. Le misure per le quali non viene fissato alcun valore non devono essere attuate obbligatoriamente e rimangono pertanto raccomandazioni non vincolanti. I singoli livelli di protezione sono indicati nel nuovo allegato 1*a*. I valori in esso fissati per ogni livello di protezione sono stati definiti in base alla criticità delle imprese e tenendo conto delle risorse necessarie per l'implementazione. Essi sono stati stabiliti da un gruppo di lavoro dell'Associazione delle aziende elettriche svizzere (AES) in collaborazione con esperti dell'UFE.

L'attribuzione di un determinato livello di protezione (A, B o C) alle imprese si basa su criteri predefiniti: un'impresa che risponde ai criteri di un determinato livello di protezione verrà attribuita a tale livello. Ad esempio, il livello di protezione A viene attribuito ai gestori di rete che trasportano almeno 450 GWh di elettricità all'anno (n. 1.1 all. 1*a*). Per la definizione dei suddetti criteri si è tenuto conto delle analisi e della prassi di altri servizi specializzati: ad esempio, il criterio dei 450 GWh/anno per l'attribuzione dei gestori di rete al livello di protezione A corrisponde a un valore stabilito dall'Ufficio federale della protezione della popolazione (UFPP) per le infrastrutture critiche di importanza nazionale; allo stesso modo il criterio dei 112 GWh/anno per l'attribuzione dei gestori di rete e dei fornitori di servizi al livello di protezione B corrisponde essenzialmente al valore annualizzato che secondo l'AES caratterizza una crisi[8].

Per l'attribuzione dei produttori e dei gestori di impianti di stoccaggio ai livelli di protezione A e B è stata scelta rispettivamente una potenza di 800 MW e di 100 MW. Quest'ultimo valore corrisponde a quello definito nell'ordinanza sull'energia[9] per le centrali di stoccaggio con pompaggio di interesse nazionale.

Nel caso di una potenza inferiore a 100 MW i produttori, gli operatori di impianti di stoccaggio e i rispettivi fornitori di servizi di entrambi gli attori non sono soggetti all'obbligo di rispettare lo Standard minimo TIC. Per loro non è previsto un livello di protezione C. Fintanto che non viene raggiunta la soglia di 100 MW, per loro lo Standard rimane solo una raccomandazione. Ciò dipende, da un lato, dal fatto che la loro influenza sulla sicurezza dell'approvvigionamento è minore rispetto a quella dei gestori di rete che accedono direttamente alla rete tramite un'apposita tecnologia di comando e, dall'altro, anche dal fatto che non possono includere i costi della cibersicurezza nelle tariffe, a differenza dei gestori di rete.

---

6 www.nist.gov/cyberframework

7 Ogni impresa può stabilire autonomamente attraverso un'analisi dei rischi se le misure minime obbligatorie sono sufficienti o se sono necessarie misure aggiuntive. La Guida alla protezione delle infrastrutture critiche (Guida PIC), pubblicata dall'Ufficio federale della protezione della popolazione (UFPP), può aiutare le imprese in questo compito. La guida può essere scaricata all'indirizzo www.infraprotection.ch > Protezione delle infrastrutture critiche > Guida PIC.

8 Associazione delle aziende elettriche svizzere (AES), «ICT Continuity», 2011

9 Art. 8 cpv. 4 dell'ordinanza del 1° novembre 2017 sull'energia (OEn; RS 730.01)

I fornitori esterni di servizi cui un'impresa affida la gestione dei propri sistemi TIC e che hanno accesso permanente ai sistemi di comando della stessa (sistemi di controllo operativi) devono rispettare le medesime regole valide per l'impresa committente.

3. Conseguenze finanziarie, a livello di personale e di altro tipo per Confederazione, Cantoni e Comuni

L'attuazione delle modifiche previste non comporterà costi finanziari o a livello di personale significativi per Confederazione, Cantoni e Comuni . Il progetto di revisione mira ad aumentare il livello di cibersicurezza nel settore energetico, offrendo una migliore protezione dalle ciberminacce a medio e lungo termine, di cui beneficeranno in ultima analisi la Confederazione, i Cantoni e i Comuni. Eventuali interruzioni dell'approvvigionamento dovuti a ciberattacchi comporterebbero conseguenze economiche di vasta portata.

4. Conseguenze su economia, ambiente e società

Un ciberattacco può avere conseguenze economiche, ambientali e sociali molto gravi. Ad esempio, i costi causati da un attacco ransomware (riscatto, perdita di dati, tempo di ripristino dell'esercizio, ecc.) possono superare gli investimenti necessari per la protezione dell'infrastruttura aziendale. Le spese che si possono evitare grazie a un adeguato livello di protezione informatica e quindi i benefici della presente proposta di revisione sono pertanto elevati.

Poiché la normativa vigente richiede già l'adozione di misure adeguate per garantire un esercizio sicuro della rete (art. 8 della legge del 23 marzo 2007 sull'approvvigionamento elettrico [LAEl; RS 734.7] e art. 5 OAEl), non dovrebbero intervenire costi aggiuntivi rilevanti. Le imprese più attente ai rischi, che hanno già attuato misure di sicurezza, dovranno sostenere costi aggiuntivi minimi o addirittura nulli. Devono aspettarsi pesanti contraccolpi solo le imprese che finora, contrariamente alle prescrizioni in vigore, sono rimaste inattive a questo riguardo.

In generale si stima che i costi che un'impresa deve sostenere per la cibersicurezza si aggirino attorno al 6-14 % delle spese IT o allo 0,3-0,5 % circa del fatturato annuo. Tuttavia questi costi devono essere comparati con quelli di un'eventuale ciberattacco, come ad esempio di un'estorsione operata da un hacker dopo un attacco ransomware, che secondo le stime costa a una PMI in media 1,4 milioni di franchi[10] e alle grandi imprese molto di più.

5. Rapporto con il diritto europeo

L'Unione europea è impegnata a migliorare la cibersicurezza in tutto il suo territorio e ad aumentare la resilienza delle sue infrastrutture critiche. Si considerino in particolare a questo riguardo la cosiddetta direttiva NIS[11] e la successiva NIS 2[12]. In queste norme l'UE stabilisce in particolare che gli Stati membri prevedano apposite misure per la protezione delle imprese energetiche importanti[13]. L'UE ha già inasprito i requisiti generali di sicurezza e punta a renderli ancora più severi. A tal fine l'UE sta attualmente sviluppando i cosiddetti Network Codes on Cybersecurity, che conterranno regole riguardanti vari aspetti della cibersicurezza nel settore elettrico.

[10] Sophos, «The State of Ransomware 2021», consultabile all'indirizzo news.sophos.com/en-us/2021/04/27/the-state-of-ransomware-2021/

[11] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, GU L 194 del 19.7.2016, pag. 1

[12] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che modifica il regolamento (UE) n. 910/2014 e la direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2), GU L 333 del 27.12.2022, pag. 80

[13] Cfr. in particolare l'art. 21 par. 1 e l'all. I della direttiva NIS 2

La presente regolamentazione migliora la cibersicurezza nel settore elettrico, prevedendo a tal fine l'elaborazione di misure di protezione adeguate. Essa è pertanto in linea con gli sforzi dell'UE di migliorare ulteriormente la cibersicurezza nel settore elettrico.

6. Commento alle singole disposizioni

Articolo 1 capoverso 2

Conformemente all'articolo 1 capoverso 2 OAEl la rete di trasporto delle ferrovie svizzere (rete della corrente di trazione), gestita con una frequenza di 16,7 Hz e un livello di tensione di 132 kV, sottostà alla LAEl nella misura in cui questa intende creare le condizioni per garantire un approvvigionamento di energia elettrica sicuro. L'articolo 8*a* LAEl[14] ha lo scopo di assicurare l'approvvigionamento elettrico e si applicherebbe pertanto anche al settore della corrente di trazione. Per le applicazioni telematiche in tale settore esistono invece già requisiti di diritto speciale relativi alla cibersicurezza, sul cui rispetto vigila l'Ufficio federale dei trasporti (UFT). [15] Per evitare la doppia attribuzione delle stesse competenze (UFT e Commissione federale dell'energia elettrica [ElCom]), questo ambito viene escluso pertanto dal campo di applicazione dell'articolo 8*a* LAEl e delle corrispondenti disposizioni di esecuzione, contenute nell'articolo 5*a* OAEl.

Articolo 5a

Capoverso 1: l'articolo contiene un rimando diretto allo Standard minimo TIC. La succitata versione dello Standard (2023) è dichiarata vincolante, pertanto le raccomandazioni in esso contenute devono essere rispettate dagli attori a cui lo Standard si rivolge, a seconda del livello di protezione definito all'allegato 1*a* (cfr. più avanti nel testo). I produttori e i gestori di impianti di stoccaggio (lett. b) nonché i loro rispettivi fornitori di servizi (lett. c n. 2) sono soggetti a questo obbligo solo se l'accesso alla potenza stabilita è possibile attraverso un unico sistema. In vista di un eventuale ciberattacco, per il calcolo della potenza totale è determinante l'influenza dell'attore sul sistema di comando (sistema di controllo industriale/operativo). Ai fini di questa disposizione, se più sistemi di controllo sono collegati tra loro in modo tale che la compromissione di uno di essi può compromettere anche gli altri, tali sistemi devono essere considerati come un unico sistema. Non sarebbe soggetto a tale obbligo, ad esempio, un produttore che gestisce vari impianti con meno di 100 MW di potenza ciascuno attraverso differenti sistemi di comando non collegati tra loro. In virtù dell'articolo 8*a* capoverso 2 LAEl, i gestori delle centrali nucleari (titolari della licenza di esercizio per una centrale nucleare) sono esonerati dal campo di applicazione di questa nuova disposizione perché per essi esistono già prescrizioni equivalenti, sul cui rispetto vigila l'Ispettorato federale della sicurezza nucleare (IFSN)[16]. L'accesso di un fornitore di servizi (lett. c) è da ritenersi permanente se gli è stato concesso nell'ambito di un rapporto obbligatorio di durata, senza cioè che il committente debba concedergli ogni volta i diritti di accesso necessari.

Capoverso 2: la disposizione chiarisce che le norme (riferimenti) citate nello Standard minimo TIC non sono vincolanti.

Capoverso 3: Data la sua competenza sussidiaria generale (art. 22 cpv. 1 LAEl), la ElCom vigila sul rispetto dell'articolo 8*a* LAEl e dell'articolo 5*a* OAEl.

Allegato 1a I livelli di protezione (profili di protezione) definiscono i requisiti in merito al grado di attuazione delle misure indicate nello Standard minimo TIC. I requisiti più elevati sono quelli del livello di protezione A, che viene attribuito alle imprese più importanti per l'approvvigionamento elettrico. Requisiti meno stringenti sono quelli dei livelli di protezione B e C, rispettivamente per gli attori medi e più

[14] Non ancora in vigore; cfr. il messaggio del 2 dicembre 2022 concernente la modifica della legge sulla sicurezza delle informazioni (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), 22.073, FF 2023 84

[15] DE-Oferr relative all'art. 42, DE 42.2; Disposizioni d'esecuzione dell'ordinanza sulle ferrovie (DE-Oferr; RS 742.141.11); attualmente in fase di revisione

[16] Art. 5 e 6 dell'ordinanza del DATEC sulle ipotesi di pericolo e le misure di sicurezza per impianti nucleari e materiali nucleari (RS 732.112.1)

piccoli. I requisiti sono definiti in base alla procedura di verifica specificata nel capitolo 3 dello Standard minimo TIC mediante cosiddetti valori (tier level). Questi ultimi vanno da un'implementazione «parziale» (valore 1) a un'implementazione «dinamica» (valore 4). Per elettricità trasportata dai gestori di rete (n. 1.1 e 1.2) si intende tutta l'elettricità condotta attraverso la loro rete (distribuzione ai consumatori finali o trasporto verso altre reti). Per determinare il livello di protezione per i fornitori di servizi viene considerata la somma dell'elettricità trasportata (gestori di rete) o della potenza installata (produttori e gestori di impianti di stoccaggio) di tutti i loro committenti. Se, ad esempio, un fornitore di servizi ha accesso attraverso un unico sistema (cfr. più sopra le osservazioni relative all'art. 5*a* cpv. 1) ai sistemi di comando di dieci gestori di rete con un'elettricità trasportata di 13 GWh/anno ciascuno, il totale dell'elettricità trasportata è pari a 130 GWh/anno; di conseguenza il fornitore di servizi in questione deve osservare i valori del livello di protezione B, mentre per ogni singolo operatore di rete varrebbe il livello di protezione C. Il livello di protezione C, previsto per gli operatori di mercato più piccoli, contiene requisiti vincolanti solo per circa 40 delle 108 misure totali dello Standard minimo TIC. Secondo il principio della proporzionalità devono quindi essere adottate solo le misure classificate come prioritarie. Se un attore soddisfa i criteri di più livelli di protezione, prevale il livello di protezione più elevato. Per la verifica dei valori fissati nell'allegato 1*a* l'UFAE mette a disposizione sul proprio sito web un apposito modulo[17].

[17] ICT-Minimum-Standard Assessment Tool, disponibile all'indirizzo www.ufae.admin.ch > Temi > TIC > Standard minimo per le TIC