Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Aprile 2023

Rapporto esplicativo concernente la revisione del novembre 2023 dell'ordinanza sulla sicurezza degli impianti di trasporto in condotta

Indice

1. Situazione iniziale

Le tecnologie dell'informazione e della comunicazione (TIC) sostengono lo sviluppo di un approvvigionamento energetico flessibile ed efficiente. A tal fine, sono sempre più utilizzate per sorvegliare e gestire le reti di approvvigionamento. Se da un lato è vero che ne risulta un'ottimizzazione del sistema, dall'altro aumenta l'esposizione agli attacchi ad opera di cibercriminali e nascono nuove fonti di rischio.

La sicurezza dell'approvvigionamento energetico è di importanza strategica. L'esercizio sicuro dei sistemi che lo forniscono garantisce la protezione di beni giuridici rilevanti. La dipendenza del nostro sistema socioeconomico dalle fonti energetiche è tale che un'avaria di ampia portata produrrebbe effetti devastanti. Al giorno d'oggi la minaccia di un ciberattacco alle reti energetiche è alquanto realistica.

La Strategia nazionale per la protezione delle infrastrutture critiche 2018–2022 (PIC)[1] e la Strategia nazionale per la protezione della Svizzera contro i ciber-rischi (SNPC) 2018–2022[2] stabiliscono misure per aumentare la resilienza complessiva delle infrastrutture critiche. A tal fine, la SNPC[3] prevede l'elaborazione e l'introduzione di standard minimi facoltativi per la sicurezza delle TIC, che hanno trovato attuazione con il cosiddetto standard minimo TIC[4]. Si tratta di una serie di misure che rappresentano un importante ausilio per garantire la protezione contro gli attacchi informatici. Su questa base il settore ha elaborato delle raccomandazioni[5] che per la prima volta gettano le indispensabili basi della cibersicurezza nel sistema di approvvigionamento del gas. Tuttavia, questi standard di settore hanno natura essenzialmente facoltativa e non sono ancora applicati con sistematicità. Il crescente stato di minaccia[6] rende perciò improcrastinabile un'affermazione a medio termine del carattere obbligatorio di tali raccomandazioni per quelle imprese in cui un'avaria produrrebbe le conseguenze più gravi. Le raccomandazioni non potranno essere dichiarate vincolanti se i loro contenuti non saranno sufficientemente precisi e chiari. A tal fine è necessaria una revisione mirata e celere delle basi esistenti, come pure una chiara attribuzione delle responsabilità.

2. Punti essenziali del progetto

Già oggi l'articolo 39 capoverso 3 dell'ordinanza del 4 giugno 2021 sulla sicurezza degli impianti di trasporto in condotta (OSITC; RS *746.12*) prevede che gli esercenti proteggano i loro impianti dalle interferenze esterne – e quindi anche dalle ciberminacce. Il nuovo articolo 39*a* introduce l'obbligo di protezione dalle ciberminacce come norma specifica, e stabilisce una procedura per l'elaborazione delle misure necessarie a tal fine. A causa dell'interconnessione tecnica dei sistemi TIC e dei relativi rischi, la prescrizione si rivolge a tutti gli esercenti, vale a dire anche a quelli che operano infrastrutture con una pressione pari o inferiore a 5 bar (art. 1 cpv. 2).

Il Consiglio federale chiarisce così la responsabilità relativa alla protezione dalle ciberminacce. In vista di un rimando a standard di settore che in futuro siano direttamente vincolanti, è necessario che questi siano redatti o rielaborati in modo mirato e con la partecipazione dell'Ufficio federale dell'energia (UFE). La presente regolamentazione affida questo compito agli esercenti. Le direttive da elaborare

[1] FF **2018** 455
[2] https://www.ncsc.admin.ch/dam/ncsc/it/dokumente/strategie/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_IT.pdf.download.pdf/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_IT.pdf
[3] Misura 8, Standardizzazione/ regolamentazione, SNPC 2018–2022, pag. 11
[4] Ufficio federale per l'approvvigionamento economico del Paese (UFAE); «Standard minimo per migliorare la resilienza alle TIC», Berna, 2018 (attualmente in fase di revisione)
[5] Raccomandazione G1008, «Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) in der Gasversorgung», edizione di dicembre 2020
[6] SNPC 2018–2022, pag. 2

dovrebbero basarsi sullo standard minimo TIC dell'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) e sulle direttive del settore esistenti. Dovrebbero precisare i requisiti operativi e tecnici, tenendo conto delle seguenti condizioni quadro in base alle conoscenze attuali:

1. definizione di vari profili di protezione, ognuno dei quali includa misure tecniche e organizzative a un diverso livello di protezione (p. es. profilo di protezione A per requisiti elevati, B per requisiti medi e C per requisiti bassi);
2. criteri per l'assegnazione di un profilo di protezione a ogni esercente. Spesso questi criteri, che permettono di raggruppare gli esercenti in base alla loro criticità, vengono definiti «profili aziendali»;
3. definizione dei singoli requisiti tratti dagli standard esistenti. Da un'analisi condotta con il settore è emersa la necessità di precisare alcuni dei requisiti previsti dallo standard minimo TIC o dalla direttiva del settore.

Nell'elaborazione dei punti menzionati il settore deve lavorare a stretto contatto con l'UFE quale autorità di vigilanza o autorità di alta vigilanza per gli impianti di trasporto in condotta. L'UFE assicura il coordinamento con i servizi competenti dell'Amministrazione federale centrale (UFAE, Ufficio federale della protezione della popolazione [UFPP], Centro nazionale per la cibersicurezza [NCSC]) e con l'Ispettorato federale degli oleo- e gasdotti (IFO).

3. Ripercussioni finanziarie, sull'effettivo del personale e di altro genere per Confederazione, Cantoni e Comuni

Per attuare le modifiche perseguite, la Confederazione, i Cantoni e i Comuni non devono sostenere costi finanziari o di personale di rilievo. Il presente adeguamento comporta solo un moderato ampliamento del mansionario dell'UFE, che può essere coperto con le risorse umane e finanziarie disponibili.

L'avamprogetto mira ad aumentare il livello di cibersicurezza degli impianti di trasporto in condotta, così da migliorare a medio e lungo termine la protezione contro le ciberminacce a tutto vantaggio, in ultima analisi, di Confederazione, Cantoni e Comuni. Eventuali disservizi dovuti ad attacchi informatici porterebbero con sé costi ingenti.

4. Ripercussioni sull'economia, l'ambiente e la società

I contraccolpi economici, ambientali e sociali di un ciberattacco possono essere molto gravi per la Svizzera e la società. Le conseguenze di un ciberattacco, infatti, possono rivelarsi estremamente serie, come dimostra il caso «Colonial Pipeline»[7] negli Stati Uniti d'America. Ad esempio, il dispendio provocato da un attacco ransomware (riscatto, perdita di dati, tempo necessario per ripristinare l'esercizio ecc.) può essere maggiore dei costi richiesti dalla protezione dell'infrastruttura di un'impresa. I costi evitati grazie all'adozione di un adeguato livello di protezione informatica e quindi i vantaggi della revisione auspicata sono, perciò, elevati.

L'attuazione di appositi provvedimenti sul piano informatico comporta per le imprese determinati costi in termini di personale e risorse finanziarie. Tuttavia, dato che già la normativa vigente prevede l'obbligo di adottare precauzioni, non dovrebbero risultare cospicui oneri aggiuntivi. Solo le imprese che finora, contrariamente alle prescrizioni, sono rimaste inattive al riguardo possono aspettarsi ripercussioni sostanziali. Le imprese attente ai rischi che, di fronte alle minacce attuali, hanno già adottato misure di sicurezza conformemente alla direttiva del settore, dovranno sostenere costi aggiuntivi minimi o nulli.

[7] https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

5. Rapporto con il diritto europeo

L'UE si adopera per migliorare la cibersicurezza in tutto il suo territorio e aumentare la resilienza delle sue infrastrutture critiche. In questo contesto si deve tenere conto in particolare della cosiddetta direttiva NIS[8] e del testo che le fa seguito, la direttiva NIS 2[9]. In queste norme l'UE prevede in particolare che gli Stati membri debbano porre in essere apposite misure per la protezione di importanti imprese energetiche[10]. I requisiti generali di sicurezza sono aumentati con la direttiva NIS 2.

La presente regolamentazione migliora la cibersicurezza nel settore delle energie trasportate in condotta e prevede a tal fine l'elaborazione di misure di protezione adeguate. Essa è pertanto in linea con le summenzionate prescrizioni dell'UE. Il lavoro finora svolto sugli standard di settore si rifà agli standard internazionali.

6. Commento ai singoli articoli

Art. 39a Protezione dalle ciberminacce

Capoverso 1: le misure che gli esercenti sono tenuti ad adottare devono prevenire o eventualmente risolvere nel minor tempo possibile le disfunzioni dei relativi impianti. Si tratta di interventi tanto sul piano organizzativo (p. es. processi di inventariazione, regolamentazione delle competenze, sensibilizzazione), quanto su quello tecnico (p. es. backup, utilizzo di soluzioni tecnologiche di protezione).

Il *capoverso 2* incarica gli esercenti di elaborare direttive contenenti misure di protezione contro le ciberminacce. Gli esercenti possono organizzarsi a questo fine nell'ambito delle strutture associative esistenti (SSIGA, ASIG). Il lavoro svolto finora, basato sullo standard minimo TIC dell'UFAE, andrà portato avanti e precisato in questo contesto. La consultazione prevista in questo capoverso garantisce il coinvolgimento di tutti gli attori interessati. Oltre agli organi esplicitamente menzionati nella disposizione verranno consultati in particolare l'NCSC, l'UFAE e i consumatori. Lo svolgimento della consultazione spetta agli esercenti.

Capoverso 3: la disposizione secondo la quale le direttive devono essere pubblicate su un sito Internet liberamente accessibile garantirà che l'accesso a tali documenti non venga complicato con login o simili. Dopo che gli esercenti avranno ultimato e pubblicato le direttive, il Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni (DATEC) verificherà la loro idoneità ad acquisire carattere vincolante per mezzo di un rimando diretto a livello di ordinanza (cfr. art. 3 cpv. 2 e 3 OSITC). Gli esercenti hanno quindi un incentivo a elaborare una soluzione il più possibile a regola d'arte (autoregolamentazione controllata).

[8] 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. 1–30
[9] 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; non ancora in vigore)
[10] Cfr. in particolare l'art. 21 par. 1 e l'all. I della direttiva NIS 2.