RACCOMANDAZIONI

RACCOMANDAZIONE (UE) 2019/553 DELLA COMMISSIONE

del 3 aprile 2019

sulla cibersicurezza nel settore dell'energia

[notificata con il numero C(2019) 2400]

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 292,

considerando quanto segue:

(1) Il settore europeo dell'energia sta attraversando un momento di grande cambiamento con la transizione verso un'economia decarbonizzata e la necessità di garantire nel contempo la sicurezza dell'approvvigionamento e la competitività. Nel contesto di questa transizione e del correlato decentramento della produzione di energia da fonti rinnovabili, il progresso tecnologico, l'integrazione settoriale e la digitalizzazione stanno trasformando la rete elettrica europea in una «rete intelligente». Tutto ciò comporta però anche nuovi rischi poiché la digitalizzazione espone sempre più il sistema energetico ad attacchi e incidenti informatici che possono compromettere la sicurezza dell'approvvigionamento.

(2) L'adozione di tutte e otto le proposte legislative ([1]) del pacchetto «Energia pulita per tutti gli europei», che comprende come primo passo la governance dell'Unione dell'energia, consente di creare un contesto favorevole alla trasformazione digitale del settore energetico. Esso riconosce altresì l'importanza della cibersicurezza nel settore dell'energia. In particolare, la rifusione del regolamento sul mercato interno dell'energia elettrica ([2]) prevede l'adozione di norme tecniche per l'energia elettrica, come un codice di rete concernente norme settoriali per gli aspetti relativi alla cibersicurezza dei flussi transfrontalieri di energia elettrica, requisiti minimi comuni, la pianificazione, il monitoraggio, la rendicontazione e la gestione delle crisi. Il regolamento sulla preparazione ai rischi nel settore dell'energia elettrica ([3]) segue in larga misura l'approccio scelto nel regolamento sulla sicurezza dell'approvvigionamento di gas ([4]), sottolineando la necessità di valutare adeguatamente tutti i rischi, compresi quelli connessi alla cibersicurezza, e proponendo misure intese a prevenire ed attenuare i rischi individuati.

(3) Al momento dell'adozione della strategia dell'UE per la cibersicurezza ([5]) nel 2013, la Commissione ha individuato come priorità il rafforzamento della resilienza informatica dell'Unione. Uno dei principali risultati della strategia è la direttiva sulla sicurezza delle reti e dei sistemi informativi ([6]) (di seguito «direttiva NIS»), adottata nel luglio 2016. La direttiva NIS, che rappresenta il primo tassello della legislazione orizzontale dell'UE in materia di cibersicurezza, rafforza il livello complessivo di cibersicurezza nell'Unione attraverso lo sviluppo di capacità nazionali in questo ambito, l'intensificazione della cooperazione a livello dell'UE e l'introduzione di obblighi di sicurezza e di segnalazione degli incidenti per le imprese che sono «operatori di servizi essenziali». La segnalazione degli incidenti è obbligatoria nei settori chiave, compreso il settore dell'energia.

([1]) Direttiva (UE) 2018/2001 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, sulla promozione dell'uso dell'energia da fonti rinnovabili (GU L 328 del 21.12.2018, pag. 82); Direttiva (UE) 2018/2002 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che modifica la direttiva 2012/27/UE sull'efficienza energetica (GU L 328 del 21.12.2018, pag. 210); Regolamento (UE) 2018/1999 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, sulla governance dell'Unione dell'energia e dell'azione per il clima che modifica le direttive (CE) n. 663/2009 e (CE) n. 715/2009 del Parlamento europeo e del Consiglio, le direttive 94/22/CE, 98/70/CE, 2009/31/CE, 2009/73/CE, 2010/31/UE, 2012/27/UE e 2013/30/UE del Parlamento europeo e del Consiglio, le direttive del Consiglio 2009/119/CE e (UE) 2015/652 e che abroga il regolamento (UE) n. 525/2013 del Parlamento europeo e del Consiglio (GU L 328 del 21.12.2018, pag. 1); Direttiva (UE) 2018/844 del Parlamento europeo e del Consiglio, del 30 maggio 2018, che modifica la direttiva 2010/31/UE sulla prestazione energetica nell'edilizia e la direttiva 2012/27/UE sull'efficienza energetica (GU L 156 del 19.6.2018, pag. 75). Nella sessione plenaria del marzo 2019 il Parlamento europeo ha confermato gli accordi politici raggiunti con il Consiglio sulle proposte sull'assetto del mercato dell'energia elettrica (regolamento sulla preparazione ai rischi, regolamento relativo all'Agenzia per la cooperazione fra i regolatori nazionali dell'energia (ACER), direttiva sull'energia elettrica e regolamento sull'energia elettrica). L'adozione formale da parte del Consiglio è prevista per aprile; la pubblicazione del testo legislativo nella Gazzetta ufficiale avverrà a breve distanza dall'adozione.

([2]) COM(2016) 861 final.

([3]) COM(2016) 862 final.

([4]) Regolamento (UE) 2017/1938 del Parlamento europeo e del Consiglio, del 25 ottobre 2017, concernente misure volte a garantire la sicurezza dell'approvvigionamento di gas e che abroga il regolamento (UE) n. 994/2010 (GU L 280 del 28.10.2017, pag. 1).

([5]) JOIN(2013) 1.

([6]) 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).

(4) Nell'attuare le misure di preparazione in materia di cibersicurezza, i portatori di interessi, compresi gli operatori di servizi essenziali nel settore dell'energia individuati nella direttiva NIS, dovrebbero tener conto degli orientamenti orizzontali emanati dal gruppo di cooperazione NIS istituito dall'articolo 11 della medesima direttiva. Il gruppo di cooperazione, composto da rappresentanti degli Stati membri, dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA) e della Commissione, ha adottato documenti di orientamento riguardanti le misure di sicurezza e la segnalazione degli incidenti. Nel giugno 2018 il gruppo ha creato un workstream dedicato in materia di energia.

(5) La comunicazione congiunta sulla cibersicurezza del 2017 ([7]) riconosce l'importanza di considerazioni e prescrizioni settoriali specifiche a livello dell'UE, anche nel settore dell'energia. Negli ultimi anni la cibersicurezza e le possibili implicazioni politiche sono state oggetto di un ampio processo di discussione nell'Unione. Di conseguenza, oggi vi è crescente consapevolezza circa il fatto che ciascun comparto economico si trova a fronteggiare problemi specifici di cibersicurezza e, pertanto, ha bisogno di sviluppare il proprio approccio settoriale nel più ampio contesto delle strategie generali di cibersicurezza.

(6) La condivisione delle informazioni e la fiducia sono elementi essenziali della cibersicurezza. La Commissione si è proposta di aumentare la condivisione delle informazioni tra i portatori di interessi organizzando appositi eventi (per esempio, la tavola rotonda ad alto livello sulla cibersicurezza nel settore dell'energia organizzata a Roma nel marzo 2017 e la conferenza ad alto livello sulla cibersicurezza nel settore dell'energia tenutasi a Bruxelles nell'ottobre 2018). La Commissione intende inoltre rafforzare la cooperazione tra i portatori di interessi e gli organismi specializzati, come il centro europeo di condivisione e di analisi delle informazioni per l'energia.

(7) Il regolamento relativo all'ENISA (l'Agenzia dell'UE per la cibersicurezza) e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione («regolamento sulla cibersicurezza») ([8]) rafforzerà il mandato dell'Agenzia dell'Unione europea per la cibersicurezza in modo da sostenere meglio gli Stati membri nella lotta contro le minacce e gli attacchi informatici. Esso crea inoltre un quadro europeo della cibersicurezza per la certificazione di prodotti, processi e servizi che sarà valido in tutta l'Unione e che riveste particolare interesse per il settore dell'energia.

(8) La Commissione ha presentato una raccomandazione ([9]) sui rischi relativi alla cibersicurezza nella quinta generazione (5G) delle tecnologie di rete fornendo orientamenti su adeguate misure nazionali di analisi e gestione dei rischi, sullo sviluppo di un'analisi dei rischi coordinata a livello europeo e sulla definizione di un processo per sviluppare strumenti comuni costituiti dalle migliori misure di gestione dei rischi. Una volta introdotte, le reti 5G costituiranno la struttura portante di una vasta gamma di servizi essenziali per il funzionamento del mercato interno e la gestione di funzioni essenziali per la società e l'economia come l'energia.

(9) La presente raccomandazione dovrebbe fornire orientamenti non esaustivi agli Stati membri e ai portatori di interessi, in particolare ai gestori di rete e ai fornitori di tecnologia, al fine di conseguire un livello più elevato di cibersicurezza in considerazione delle esigenze specifiche di un contesto in tempo reale individuate per tale settore, degli effetti a cascata e della coesistenza di tecnologie preesistenti e tecnologie all'avanguardia. I presenti orientamenti intendono aiutare i portatori di interessi a tener conto delle esigenze specifiche del settore dell'energia nell'attuazione delle norme tecniche in materia di cibersicurezza riconosciute a livello internazionale ([10]).

(10) La Commissione intende riesaminare periodicamente la presente raccomandazione, in consultazione con gli Stati membri e i portatori di interessi, sulla base dei progressi compiuti in tutta l'Unione. La Commissione continuerà ad adoperarsi per rafforzare la cibersicurezza nel settore dell'energia, in particolare attraverso il gruppo di cooperazione NIS, che assicura la cooperazione strategica e lo scambio di informazioni tra gli Stati membri in materia di cibersicurezza,

HA ADOTTATO LA PRESENTE RACCOMANDAZIONE:

OGGETTO

(1) La presente raccomandazione illustra le principali questioni relative alla cibersicurezza nel settore dell'energia, in particolare le esigenze di un contesto in tempo reale, gli effetti a cascata e la combinazione di tecnologie preesistenti e all'avanguardia, e individua le principali azioni per l'attuazione delle pertinenti misure di preparazione.

([7]) JOIN(2017) 450.

([8]) Il regolamento sulla cibersicurezza è stato adottato dal Parlamento europeo nel marzo 2019. L'adozione formale da parte del Consiglio è prevista per aprile; la pubblicazione del testo legislativo nella Gazzetta ufficiale avverrà a breve distanza dall'adozione.

([9]) Decisione d'esecuzione della Commissione C(2019) 2335.

([10]) Gli organismi internazionali di normazione hanno pubblicato varie norme tecniche in materia di cibersicurezza (ISO/IEC 27000: Information Technologies) e gestione del rischio (ISO/IEC31000: Implementation of risk management). Nell'ambito della serie ISO/IEC 27000 nell'ottobre 2017 è stata emanata una norma tecnica specifica per il settore dell'energia (ISO/IEC 27019: Information security controls for the energy utility industry).

(2) Nell'applicare la presente raccomandazione gli Stati membri dovrebbero incoraggiare i portatori di interessi a sviluppare le conoscenze e le competenze in materia di cibersicurezza nel settore dell'energia. Se del caso, gli Stati membri dovrebbero inoltre includere tali considerazioni nel loro quadro nazionale della cibersicurezza, in particolare attraverso strategie, leggi, regolamenti e altre disposizioni amministrative.

ESIGENZE DELLE COMPONENTI DELL'INFRASTRUTTURA ENERGETICA IN UN CONTESTO IN TEMPO REALE

(3) Gli Stati membri dovrebbero provvedere affinché i portatori di interessi, specialmente i gestori delle reti energetiche e i fornitori di tecnologie, e in particolare gli operatori che forniscono i servizi essenziali individuati nella direttiva NIS, attuino le pertinenti misure di preparazione in materia di cibersicurezza relative alle esigenze in tempo reale del settore energetico. Alcuni elementi del sistema energetico devono operare in «tempo reale», ossia eseguendo i comandi entro pochi millisecondi, il che rende difficile, se non addirittura impossibile, introdurre misure di cibersicurezza a causa della mancanza di tempo.

(4) In particolare, i gestori delle reti energetiche dovrebbero:

a) applicare, ove opportuno, le più recenti norme tecniche di sicurezza per le nuove installazioni e prendere in considerazione misure di sicurezza fisica complementari qualora la base installata dei vecchi impianti non possa essere sufficientemente protetta dai meccanismi di cibersicurezza;

b) attuare le norme tecniche internazionali in materia di cibersicurezza e norme tecniche specifiche adeguate per la comunicazione sicura in tempo reale non appena i prodotti in questione diventano disponibili sul mercato;

c) considerare le contingenze in tempo reale nella concezione generale della sicurezza degli asset, in particolare nella classificazione degli asset;

d) considerare le reti private per i sistemi di teleprotezione al fine di garantire il livello di qualità del servizio richiesto per le contingenze in tempo reale; quando utilizzano reti di comunicazione pubbliche i gestori dovrebbero valutare la possibilità di assicurare un'assegnazione della larghezza di banda, requisiti di latenza e misure di sicurezza della comunicazione specifici;

e) suddividere il sistema complessivo in zone logiche e, all'interno di ciascuna zona, definire i limiti di tempo e i vincoli di processo al fine di consentire l'applicazione di adeguate misure di cibersicurezza o di prendere in considerazione altri metodi di protezione.

(5) Se possibile, i gestori delle reti energetiche dovrebbero inoltre:

a) scegliere un protocollo di comunicazione sicuro, tenendo conto delle esigenze di un contesto in tempo reale, ad esempio per la comunicazione tra un impianto e i relativi sistemi di gestione (sistema di gestione dell'energia/sistema di gestione della distribuzione);

b) introdurre un adeguato meccanismo di autenticazione per la comunicazione tra macchine (M2M) al fine di affrontare le esigenze di un contesto in tempo reale.

EFFETTI A CASCATA

(6) Gli Stati membri dovrebbero provvedere affinché i portatori di interessi, specialmente i gestori delle reti energetiche e i fornitori di tecnologie, e in particolare gli operatori che forniscono i servizi essenziali individuati nella direttiva NIS, attuino le pertinenti misure di preparazione in materia di cibersicurezza relative agli effetti a cascata nel settore energetico. Le reti elettriche e i gasdotti sono strettamente interconnessi in tutta Europa e un attacco informatico che causa indisponibilità o interruzioni in una parte del sistema energetico potrebbe innescare effetti a cascata di vasta portata in altre sue parti.

(7) Nell'applicare la presente raccomandazione gli Stati membri dovrebbero valutare le interdipendenze e le criticità dei sistemi di produzione di energia e di consumo flessibile, delle sottostazioni e delle linee di trasmissione e distribuzione e tener conto dei portatori di interessi coinvolti (anche nelle situazioni transfrontaliere) in caso di attacchi o incidenti informatici andati a segno. Gli Stati membri dovrebbero inoltre provvedere affinché i gestori delle reti energetiche dispongano di un quadro per la comunicazione con tutti i principali portatori di interessi per poter condividere i primi segnali di allarme e cooperare nella gestione delle crisi. Dovrebbero essere predisposti canali di comunicazione strutturati e formati concordati per la condivisione delle informazioni sensibili con tutti i portatori di interessi, i gruppi di intervento per la sicurezza informatica in caso di incidente e le autorità competenti.

(8) In particolare, i gestori delle reti energetiche dovrebbero:

a) provvedere affinché i nuovi dispositivi, compresi i dispositivi IoT (Internet delle cose), abbiano e mantengano un livello di cibersicurezza adeguato alla criticità del sito;

b) tenere debitamente conto degli effetti ciberfisici al momento della definizione e della revisione periodica dei piani di continuità operativa;

c) stabilire criteri di progettazione e un'architettura atti a garantire la resilienza delle reti, obiettivo questo che potrebbe essere conseguito:

— mettendo in atto per ciascun sito misure di difesa particolareggiate, adattate alle criticità del sito;

— individuando i nodi critici, sia in termini di capacità di produzione di energia che di impatto sui clienti. Le funzioni essenziali di una rete dovrebbero essere progettate in modo da attenuare i rischi che possono provocare effetti a cascata considerando la ridondanza, la resilienza alle oscillazioni di fase e la protezione contro il distacco del carico a cascata;

— collaborando con altri operatori pertinenti e con i fornitori di tecnologia per prevenire gli effetti a cascata mediante il ricorso a misure e servizi adeguati;

— progettando e realizzando reti di comunicazione e di controllo al fine di arginare gli effetti di eventuali guasti fisici e logici in parti limitate delle reti e di garantire misure di attenuazione rapide adeguate.

TECNOLOGIE PREESISTENTI E TECNOLOGIE ALL'AVANGUARDIA

(9) Gli Stati membri dovrebbero provvedere affinché i portatori di interessi, specialmente i gestori delle reti energetiche e i fornitori di tecnologie, e in particolare gli operatori che forniscono i servizi essenziali individuati nella direttiva NIS, attuino le pertinenti misure di preparazione in materia di cibersicurezza relative alla coesistenza nel settore dell'energia di tecnologie preesistenti e tecnologie all'avanguardia. Di fatto, nell'attuale sistema energetico coesistono due diversi tipi di tecnologie: tecnologie più vecchie con una durata di vita di 30-60 anni, progettate prima che si tenesse conto delle questioni connesse alla cibersicurezza, e apparecchiature moderne che riflettono lo stato dell'arte della digitalizzazione e dei dispositivi intelligenti.

(10) Nell'applicare la presente raccomandazione gli Stati membri dovrebbero incoraggiare i gestori delle reti energetiche e i fornitori di tecnologia a rispettare, ove possibile, le pertinenti norme tecniche in materia di cibersicurezza riconosciute a livello internazionale. Allo stesso tempo, nel connettere i dispositivi alla rete, i portatori di interessi e i clienti dovrebbero adottare un approccio orientato alla cibersicurezza.

(11) In particolare, i fornitori di tecnologia, non appena vengono a conoscenza di un problema di sicurezza nelle tecnologie preesistenti o nuove, dovrebbero fornire gratuitamente soluzioni collaudate.

(12) In particolare, i gestori delle reti energetiche dovrebbero:

a) analizzare i rischi inerenti alla connessione della tecnologia preesistente e di quella basata sull'Internet delle cose e conoscere le interfacce interne ed esterne e le loro vulnerabilità;

b) adottare misure adeguate contro gli attacchi dolosi provenienti da un numero elevato di applicazioni o dispositivi di largo consumo controllati da malintenzionati;

c) stabilire una capacità automatizzata di monitoraggio e analisi per gli eventi relativi alla sicurezza negli ambienti preesistenti o IoT, come i tentativi di accesso falliti, allarmi sulle porte per l'apertura delle cabine o altri eventi;

d) effettuare periodicamente un'analisi dei rischi specifici per la cibersicurezza su tutti gli impianti preesistenti, soprattutto quando si connettono tecnologie vecchie e nuove; e) poiché gli impianti preesistenti spesso rappresentano una parte molto consistente degli asset, l'analisi dei rischi può essere condotta per classe di asset;

e) aggiornare se del caso alla versione più recente il software e l'hardware dei sistemi preesistenti e dei sistemi IoT; qualora una correzione (patch) o un aggiornamento sia opportuno ma impossibile, ad esempio per i prodotti non supportati, i gestori delle reti energetiche dovrebbero prendere in considerazione misure complementari come la separazione dei sistemi o l'aggiunta di barriere di sicurezza esterne;

f) formulare i bandi delle gare di appalto tenendo conto delle questioni connesse alla cibersicurezza, ossia richiedere informazioni sulle caratteristiche di sicurezza, esigere il rispetto delle norme tecniche esistenti in materia di cibersicurezza, provvedere a che siano proposte ininterrottamente misure di segnalazione, correzione (patch) e attenuazione qualora emergano vulnerabilità; chiarire inoltre le responsabilità del fornitore in caso di attacchi o incidenti informatici;

g) collaborare con i fornitori di tecnologia per sostituire i sistemi preesistenti ogni volta in cui ciò potrebbe apportare benefici in termini di sicurezza, tenendo tuttavia conto delle funzionalità essenziali del sistema.

MONITORAGGIO

(13) Entro 12 mesi dall'adozione della presente raccomandazione, e successivamente ogni due anni, gli Stati membri dovrebbero comunicare alla Commissione informazioni dettagliate sullo stato di attuazione della presente raccomandazione attraverso il gruppo di cooperazione NIS.

RIESAME

(14) Sulla base delle informazioni trasmesse dagli Stati membri, la Commissione riesaminerà l'attuazione della presente raccomandazione e valuterà l'eventuale necessità di ulteriori misure, se del caso in consultazione con gli Stati membri e con i portatori di interessi.

DESTINATARI

(15) Gli Stati membri sono destinatari della presente raccomandazione.

Fatto a Bruxelles, il 3 aprile 2019

Per la Commissione
Miguel ARIAS CAÑETE
Membro della Commissione