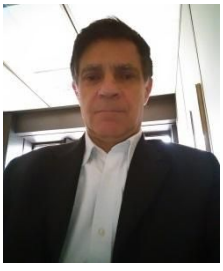
10/2019 Cybersecurity nella transizione energetica e digitale

OPINIONI

Giovanna Dondossola Giovanna.Dondossola@rse-web.it

Leading Scientist Dipartimento Tecnologie di Trasmissione e Distribuzione di RSE

" Gli obiettivi del piano nazionale integrato per l'energia e il clima, in risposta ai target europei del Clean Energy Package, sono perseguibili solo attraverso infrastrutture digitali per i servizi energetici che garantiscono alle reti, ai sistemi, ai componenti e ai servizi ICT, nonché ai dati associati, livelli alti di disponibilità, integrità, confidenzialità e tracciabilità delle operazioni. Le misure di cybersecurity utilizzate per soddisfare tali requisiti di sicurezza devono rispettare le esigenze operative in tutte le condizioni di esercizio del processo fisico. Il successo del nostro futuro energetico dipenderà anche dalla capacità di tutti i soggetti coinvolti nella catena del valore (istituzioni, autorità di regolazione, operatori, enti di standardizzazione, università e centri di ricerca, fornitori di prodotti e di servizi) di procedere efficacemente nell'integrazione dei requisiti e delle misure per la gestione del rischio cyber negli assetti legislativi, nella regolamentazione e nei rispettivi processi organizzativi".



Franco Guida fguida@fub.it

Responsabile Area Cyber Security Fondazione Ugo Bordoni

“Per ciò che concerne la cyber security nel contesto dei sistemi energetici, una importante novità è intervenuta a livello normativo prima con l’approvazione del decreto-legge 21 settembre 2019, n. 105 e poi della legge 18 novembre 2019, n. 133 che lo ha convertito con modifiche. La nuova norma prevede infatti l’istituzione del cosiddetto perimetro di sicurezza nazionale cibernetica nel quale saranno inseriti, su proposta del Comitato Interministeriale per la Sicurezza della Repubblica (CISR), i soggetti che forniscono un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e che per la fornitura di tale servizio si avvalgono di reti, sistemi informativi e servizi informatici dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. E’ importante il riferimento alla sicurezza nazionale in quanto ciò dovrebbe preludere all’individuazione di un insieme più ristretto di soggetti rispetto a quelli già individuati ai fini della Direttiva UE 2016/1148 del 6 luglio 2016 (meglio nota con il nome Direttiva NIS). I soggetti che saranno inseriti nel perimetro saranno tenuti al rispetto di una serie di misure e obblighi indicati nella legge. Tra questi si possono citare: la comunicazione con cadenza almeno annuale della lista delle predette reti, sistemi informativi e servizi informatici; la notifica di incidenti aventi impatto sulle predette reti, sistemi informativi e servizi informatici; la realizzazione e il rispetto delle misure di gestione della sicurezza che saranno definite in un apposito DPCM; il rispetto di particolari procedure nell’affidamento di forniture di beni, sistemi e servizi ICT, destinati a essere impiegati sulle predette reti, sistemi informativi e servizi informatici, e appartenenti a categorie individuate, sulla base di criteri di natura tecnica, con apposito DPCM. Riguardo alle forniture di beni, sistemi e servizi ICT, un ruolo importante sarà svolto dal Centro di Valutazione e Certificazione Nazionale (CVCN) istituito presso il Ministero dello Sviluppo Economico. Tale Centro potrà infatti effettuare verifiche preliminari sui predetti beni, sistemi e servizi ICT oggetto della fornitura ed imporre condizioni e test di hardware e software”.

Fonte: www.dossierse.it