CONSOB
COMMISSIONE NAZIONALE PER LE SOCIETÀ E LA BORSA

COMUNICATO STAMPA

Cybersecurity e società quotate: Sec, Esma e Consob a confronto sulla disciplina di trasparenza

Ciocca: valutare se la resilienza agli attacchi hacker debba entrare nella reportistica periodica

L'Autorità Usa per una comunicazione obbligatoria e non discrezionale

Il punto oggi e domani all'Università Cattolica

Le società quotate in Borsa dovrebbero prepararsi ad includere le informazioni sulla *cybersecurity* nella rendicontazione periodica obbligatoria resa al mercato, perché gli investitori hanno interesse a sapere quanto l'impresa in cui investono i propri soldi sia robusta o vulnerabile rispetto al rischio di attacchi *hacker*.

È questa la posizione espressa da Luna Bloom della Sec (*Securities and Exchange Commission*), l'autorità di regolamentazione e di vigilanza sui mercati finanziari degli Stati Uniti, intervenendo al convegno "Cybersecurity, market disclosure & industry" in corso oggi e domani all'Università Cattolica del Sacro Cuore.

I rischi cyber sono in crescita e hanno subito un'accelerazione a seguito della digitalizzazione dell'economia e della finanza, con forti impatti operativi, legali e reputazionali sulle società quotate, ha osservato Bloom. È cruciale dotarsi di regole stringenti e di competenze nei CdA delle quotate, ha aggiunto Bloom, secondo cui la trasparenza in materia di cybersecurity deve essere obbligatoria e non discrezionale.

"Il rischio cyber ha un potenziale impatto sistemico", ha osservato Paolo Ciocca, Commissario Consob. "La questione non è se dare l'informazione, ma quando darla, come darla e cosa dire al mercato. Questo pone un onere a carico dei CdA".

"Una divulgazione di informazioni sulla cybersecurity, coerente, comparabile e orientata alle decisioni, metterebbe gli investitori – ha commentato Elena Beccalli, preside della Facoltà di Scienze bancarie, finanziarie e assicurative della Cattolica - in una posizione migliore per comprendere rischi e incidenti".

"La pandemia, la guerra in Ucraina e il frequente ricorso a fornitori esternalizzati hanno aumentato la minaccia di rischi sistemici", ha osservato, invece, Alexander Harris dell'Esma, secondo cui è necessaria la collaborazione tra regolatori e gli altri attori del mercato.

Per i mercati finanziari dell'Unione Europea sarebbe un radicale cambiamento di prospettiva. Ad oggi, infatti, gli attacchi *hacker* sono soggetti alla disciplina di trasparenza degli eventi *price sensitive*. Questo significa che devono essere resi noti solo se e quando si verifica l'emergenza. È la stessa società, inoltre, a valutare se l'episodio sia oppure no di interesse per il mercato e in quali tempi eventualmente comunicare.

Se le proposte della Sec fossero recepite anche in ambito Ue, l'informativa sulla *cybersecurity* diventerebbe non più volontaria ma obbligatoria e sarebbe sottoposta ad una disciplina di trasparenza secondo criteri predefiniti e validi per tutti.

Milano, 27 febbraio 2023