03-FEB-2023
da pag. 16 / foglio 1 / 2

Il Sole 24 ORE
Quotidiano - Dir. Resp.: Fabio Tamburini
Tiratura: 71008 Diffusione: 132572 Lettori: 715000 (0001998)



# Perché è necessario includere gli esperti di cybersecurity nei cda

## Corporate governance/2

Stefano Mele

Archiviata la fase dello *spoil system*, tra marzo e giugno arriverà per il governo di Giorgia Meloni il momento del rinnovo dei consigli di amministrazione di alcune tra le principali società controllate e partecipate dallo Stato, i cui organi amministrativi sono arrivati a scadenza il 31 dicembre 2022.

Secondo l'ultimo rapporto del servizio di controllo parlamentare della Camera, dovranno essere rinnovati i consigli di amministrazione di circa 70 società. I nomi spaziano da Eni, Ferrovie dello Stato, Leonardo, Rai, Poste Italiane e da buona parte della loro galassia di aziende partecipate, fino a società come Enel, CDP Venture Capital Sgr, Infratel, Enav, Difesa Servizi, Italia Trasporto Aereo (ITA), Consip e Istituto Poligrafico e Zecca dello Stato (IPZS).

In considerazione delle attività e del ruolo svolto da tali società, risulta chiaro come il fascicolo sul rinnovo dei componenti dei consigli di amministrazione – oggi sulle scrivanie di alcuni tra i Ministri di maggior peso di questo governo, come Crosetto, Giorgetti e Urso – sarà strategico per la sicurezza nazionale e per la futura crescita economica del nostro Paese.

In tale contesto, ciò che appare fin da subito auspicabile – se non imprescindibile – è che venga colta l'opportunità di riservare finalmente un posto al tavolo dei consigli di amministrazione di queste società anche agli esperti di *cybersecurity*. Professionisti, quindi, capaci di comprendere lo scenario attuale e futuro delle minacce cibernetiche, le loro ricadute sul business e sull'operatività dei servizi delle aziende, nonché le loro conseguenze in termini di *compliance* normativa, processi interni e reputazione.

Tale esigenza è testimoniata dal fatto che quello appena trascorso è stato l'anno peggiore di sempre per numero e, soprattutto, per qualità di attacchi informatici subiti dai soggetti pubblici e privati a livello internazionale, Italia inclusa.

Lo si apprende in maniera molto chiara dalle parole del Direttore dell'Agenzia per la Cybersicurezza Nazionale (ACN), Roberto Baldoni. Lo si tocca quasi con mano nello scenario fotografato dai recentissimi dati diffusi dalla Polizia Postale e delle Comunicazioni, guidata da Ivano Gabrielli, in cui viene mostrato un 2022 caratterizzato da un incremento di ben il 138% degli attacchi cibernetici alle infrastrutture critiche nazionali, ai sistemi finanziari e alle aziende operanti in settori strategici, come ad esempio, quelle delle telecomunicazioni e della difesa. Si è passati, infatti, da circa 5.400 attacchi informatici nel 2021 a quasi 13.000 nel 2022.

Una situazione di tale gravità non riguarda ovviamente solo l'Italia. Simili statistiche – in alcuni casi anche peggiori – si possono riscontrare nei dati ufficiali di ogni Stato.

Proprio per questo, ad esempio, il governo degli Stati Uniti, attraverso l'azione della Securities and Exchange Commission (SEC), un organo simile alla Consob italiana, presto obbligherà i consigli di amministrazione delle società quotate a dare il giusto peso al tema della *cybersecurity*. Nello specifico, in base alle regole che dovrebbero essere finalizzate già il prossimo aprile, si richiederà a tali società di condividere con la SEC le informazioni sugli incidenti informatici considerati – singolarmente o nel loro complesso – come "rilevanti" e di comunicare a tale autorità le competenze dei membri del cda in materia di *cybersecurity*, nonché le loro azioni più significative a sostegno della governance della sicurezza. Queste richieste dovrebbero far sì che i consigli di amministrazione delle società quotate vedano finalmente la

Il Sole 24 ORE
Quotidiano - Dir. Resp.: Fabio Tamburini
Tiratura: 71008 Diffusione: 132572 Lettori: 715000 (0001998)



*cybersecurity* come un asset capace di creare valore e non come una questione puramente tecnico-informatica.

Non è un caso che alcune tra le più importanti aziende quotate italiane abbiano riscontrato, già dallo scorso anno, un'elevata attenzione da parte delle principali società americane di *rating* verso le competenze in materia di *cybersecurity* dei membri dei loro consigli di amministrazione, così come delle attività svolte durante l'anno per governare il cosiddetto *"rischio cyber"*.

Occorre comprendere che la *cybersecurity* è oggi più che mai un tema legato alla crescita e alla stabilità economica, ai piani strategici, alla governance e alla gestione dei rischi, allo sviluppo del business, alla continuità operativa, così come ai posti di lavoro e alla reputazione delle società. Per alcune tipologie di società è anche un tema di partecipazione alla sicurezza nazionale. L'imminente ricambio dei board è il momento migliore per agire.

*Socio di Gianni & Origoni*