EU: new manual on cybersecurity for safeguarding EU elections

The EU Member States, with the support of the Commission and the EU Agency for Cybersecurity (ENISA), have published a new Compendium on how to safeguard the integrity of the elections against cybersecurity threats. “Since the last EU elections in 2019, the elections threat landscape has evolved significantly” with the rapid growth of hacktivists-for-hire (hackers) and the increased “sophistication of threat actors”. At the same time, the electoral processes “have seen technological advances”. Therefore, the key elements of this edition of the Compendium include: an update on the elections threat landscape, new and revised case studies, the best practices in cybersecurity, and an analysis of potential threats arising from emerging technologies that could impact elections, particularly foreign interference and cyber manipulation, social media disinformation, artificial intelligence, and “deep fakes”. The new edition of the Compendium includes recommendations to Member States, actions to be taken, and useful suggestions for dealing with potential cyber incidents during electoral processes.

Gianni Borsa