Published on *Digital Agenda for Europe* (https://ec.europa.eu/digital-agenda)

Proposed Directive on Network and Information Security – frequently asked questions

Published on 07/02/2013
Information systems can be affected by security incidents, such as human mistakes, natural events, technical failures or malicious attacks. These incidents are becoming bigger, more frequent, and more complex. 57% of people who responded to a Commission consultation said they had experienced Network Information Security (NIS) incidents over the previous year. A lack of NIS can compromise vital services: it can stop businesses functioning, generate substantial financial losses for the EU economy and negatively affect societal welfare. Digital information systems, in particular the internet, work across borders. A disruption in one EU country can have a knock-on effect in other Member States or the EU as a whole - for example, cross-border movement of goods, services and people could be hampered.
Share this
Date:
07/02/2013
Venue:
Speaker:
Read full text [1]
Contact:

Newsroom Item Type:

- Press releases [2]

Our Targets:

- Pillar III: Trust & Security [3]
- Action 28: Reinforced Network and Information Security Policy [4]
- Action 29: Combat cyber-attacks against information systems [5]
- Action 30: Establish a European cybercrime platform [6]
- Action 31: Analyse the usefulness of creating a European cybercrime centre [7]
- Action 32: Strengthen the fight against cybercrime and cyber-attacks at international level [8]
- Action 33: Support EU-wide cyber-security preparedness [9]
- Action 38: Member States to establish pan-European Computer Emergency Response Teams [10]
- Action 39: Member States to carry out cyber-attack simulations [11]
- Action 41: Member States to set up national alert platforms [12]

Source URL: https://ec.europa.eu/digital-agenda/en/news/proposed-directive-network-and-information-security-%E2%80%93-frequently-asked-questions

Links
[1] http://europa.eu/rapid/press-release_MEMO-13-71_en.htm
[2] https://ec.europa.eu/digital-agenda/en/newsroom/all/press-releases
[3] https://ec.europa.eu/digital-agenda/en/our-goals/pillar-iii-trust-security
[4] https://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-28-reinforced-network-and-information-security-policy
[5] https://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-29-combat-cyber-attacks-against-information-systems
[6] https://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-30-establish-european-cybercrime-platform
[7] https://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-31-analyse-usefulness-creating-european-cybercrime-centre
[8] https://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-32-strengthen-fight-against-cybercrime-and-cyber-attacks
[9] https://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-33-support-eu-wide-cyber-security-preparedness
[10] https://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-38-member-states-establish-pan-european-computer-emergency-response
[11] https://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-39-member-states-carry-out-cyber-attack-simulations
[12] https://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-41-member-states-set-national-alert-platforms