European Cybercrime Centre

Advisory Groups

Public-private partnership in the fight against cybercrime

Strategic and operational goals

EUROPOL BASIC PROTECTION LEVEL
RELEASABLE TO ALL EC3 STAKEHOLDERS

EUROPOL | EC3 European Cybercrime Centre

Public-private partnership in the fight against cybercrime

An increasingly connected world also offers more ways for criminals to abuse technology and to reach a broader number of victims. For the fight against cybercrime to continue to be successful it is crucial that the public and the private sector keep on working together. To this end, EC3 has established a network of more than 80 trusted private companies divided into three Advisory Groups covering three major industries. This powerful network enables us to work shoulder to shoulder to keep the European Union a safe and online-friendly environment.

Three sector-specific groups

- Internet Security
- Financial Services
- Communication Providers

A network of industry experts

- Platform to foster trust and cooperation between law enforcement (LE) and industry
- Strategic exchange of key threats, global trends and industry-specific challenges
- Coordination on joint prevention and awareness campaigns
- Capacity building through the provision of cutting-edge training opportunities
- Intelligence-sharing in a trusted community
- Operational cooperation on cases affecting a specific industry

Intelligence-sharing

- Industry-specific threats: ATM malware, DDoS attacks, ransomware, etc.
- Sharing of latest cybercrime-related technological developments
- Ad hoc information exchange in case of major cross-border cyber-attack

Operational cooperation

- Suggestion of specific cases
- Coordination on cross-border operations with national law enforcement agencies facilitated by Europol
- Joint operational actions on high-profile cybercrime cases such as Operation Taiex (takedown of Carbanak group leader responsible for over €1bn in damages to financial institutions) and Operation Power Off (takedown of world's largest DDoS marketplace)
- Expert input into Europol operational priorities

Strategic analysis

Providing input to the annual Internet Organised Crime Threat Assessment (IOCTA) and other strategic products such as the Quarterly Quantitative Report, ad hoc Advisory Group strategic papers, white papers, etc.

Capacity building

Delivering training sessions on technical issues for LE; creating training materials for the EUCTF mentoring programme on specific internet governance policy and technical issues:

- Investigation of domain names
- Techniques for online attribution of carrier grade NAT IP addresses (CGN)

Stakeholder engagement

Delivering presentations and participating in EC3 events and initiatives:

- Advisory Group meetings
- Europol-ENISA IoT Security Conference
- Europol-INTERPOL Cybercrime Conference

Prevention and awareness

Promoting and developing awareness and prevention activities to help EU citizens, business and governments protect themselves online:

- No More Ransom
- eCommerce Action, European Money Mule Action, Global Action Against Online Fraudsters in the Airline Sector, Cyber Scams campaign
- #SayNo campaign against online child sexual coercion and extortion

Internet governance

Representing the European LE community in the global discussion on internet governance to contribute to the security, safety and stability of the internet and to reduce the criminal abuse of its infrastructure:

- Engaging with the ICANN community to mitigate the abuse of the domain name system and to ensure that the LE community has timely access to WHOIS registration data. EC3 is a member of the ICANN Public Safety Working Group (PSWG)
- Working with the RIPE community to improve the accuracy of the RIPE database of IP addresses
- Organising training sessions to improve the general knowledge of the LE community of internet governance tools for criminal investigations

For more information: EC3@europol.europa.eu