Cybercrime Digest

Bi-weekly update and global outlook by the
Cybercrime Programme Office of the Council of Europe (C-PROC)

16-31 May 2018

Source: Council of Europe

Date: May 2018

Towards a Protocol to the Convention on Cybercrime: Invitation to participate in consultations

"Consultations on the ongoing preparation of a 2nd Additional Protocol to the Budapest Convention will be held within the framework of the Octopus Conference on Cybercrime from 11 to 13 July 2018, and specifically on Thursday, 12 July. They are to permit an exchange of views between representatives of the Cybercrime Convention Committee and: Civil society organisations and academia; Data protection experts; Industry (service providers and associations). Interested stakeholders are invited to register for the Octopus Conference by 10 June 2018. Conference space is limited. Interested stakeholders may also send written comments on the questions raised in this guide by 25 June 2018 via e-mail." READ MORE

Source: European Commission

Date: 24 May 2018

Statement by EU Commission ahead of the entry into application of the General Data Protection Regulation

"As of tomorrow, 25 May, new data protection rules will apply across the EU. Andrus Ansip, Vice-President for the Digital Single Market, said: "Europe's new data protection rules will be a reality tomorrow. Europeans' privacy will be better protected and companies benefit from a single set of rules across the EU. Strong data protection rules are the basis for a functioning Digital Single Market and for the online economy to prosper. The new rules ensure that citizens can trust in how their data is used and that the EU can make the best of the opportunities of the data economy. […] Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, added: "Personal data is the gold of the 21st century. And we leave our data basically at every step we take, especially in the digital world. When it comes to personal data today, people are naked in an aquarium. Data protection is a fundamental right in the EU. The new rules will put the Europeans back in control of their data. Now we have a choice and can decide what happens and who has what sort of data. You can ask and companies have to tell you. You can also recover your data if you leave or change service." READ MORE

RELATED ARTICLES

European Commission, Benefits for citizens, Benefits for businesses, What changes after 25 May, 24 May 2018

Source: The Guardian

Date: 25 May 2018

Facebook and Google targeted as first GDPR complaints filed

"Facebook and Google have become the targets of the first official complaints of GDPR noncompliance, filed on the day the privacy law takes effect across the EU. Across four complaints, related to Facebook, Instagram, WhatsApp and Google's Android operating system, European consumer rights organisation Noyb argues that the companies have forced users into agreeing to new terms of service, in breach of the requirement in the law that such consent should be freely given." READ MORE

Source: The Register

Date: 29 May 2018

ICANN Launches GDPR Lawsuit to Clarify the Future of WHOIS

"A fight over private information and the internet's domain name system is heading to a German court, in a proxy battle between European legislators and American intellectual property lawyers. On Friday – the same day that new European GDPR privacy legislation took effect – DNS overseer and US corporation ICANN filed a lawsuit against German domain registrar EPGA in Bonn, asking that it be forced to keep gathering private information on people who buy web addresses. ICANN argued that the registrar is obligated under its contract to keep gathering the information. The registrar's position is that gathering the information breaks GDPR, and so opens it up to legal challenges, tellings off, and potentially ruinous fines." READ MORE

RELATED ARTICLES

ZDNet, ICANN Makes Last Minute WHOIS Changes to Address GDPR Requirements, 23 May 2018

Source: Forbes

Date: 29 May 2018

Seizing Data Overseas from Foreign Internet Companies under the CLOUD Act

"In a significant development for law enforcement's ability to access data stored abroad, Congress recently enacted the Clarifying Lawful Overseas Use of Data Act (the CLOUD Act). The Act enables law enforcement to compel Internet service and email providers to hand over data—whether that data is "located within or outside the United States." Before the Act, which became law in March, the U.S. Supreme Court was poised to decide whether a federal warrant obligated Microsoft to produce data from one of its servers in Ireland. Once the Act specified the extraterritorial reach of U.S. law enforcement, the government obtained a new warrant for the relevant data, and the parties agreed to dismiss the case as moot. In addition to subjecting overseas data to U.S. demands, the Act establishes a procedure for service providers to quash demands for data that involve a non-U.S. citizen or resident, if the demand conflicts with the law of foreign jurisdictions that satisfy certain thresholds for data security and privacy. The Act also creates a mechanism for foreign jurisdictions with adequate data security and privacy laws to seek data stored in the U.S.." READ MORE

Source: Le Matin

Date: 24 May 2018

Internet: Pour une adresse en Suisse des réseaux sociaux

"Facebook et les autres opérateurs de réseaux sociaux devraient disposer d'une représentation ou d'un domicile de notification en Suisse pour faciliter si besoin les procédures judiciaires. Le Conseil fédéral est prêt à légiférer en ce sens. Les inquiétudes des parlementaires se réfèrent notamment à une décision du Tribunal fédéral datant de 2016. Le Ministère public vaudois avait alors fait chou blanc dans sa tentative de contraindre Facebook Suisse à lui livrer des données dans le cadre d'un procès pour calomnie, diffamation et injure déposée par un journaliste belge. La requête devait être faite en Irlande. Dans une motion, la commission des affaires juridiques du Conseil des Etats souhaite éviter aux autorités pénales helvétiques de recourir à l'entraide pénale internationale en cas de procédure judiciaire. Le texte demande parallèlement à trouver une solution au niveau international." READ MORE

Source: Once Noticias

Date: 23 May 2018

Costa Rica estudia sus fortalezas y debilidad en ciberseguridad con el Consejo Europeo

"En el Colegio de Abogados acoge el encuentro "Evaluación de la Ciberseguridad en Costa Rica", en donde representantes del Consejo de Europa, expertos internacionales en ciberdelincuencia y funcionarios de instituciones como el Ministerio Público, el OIJ, la Corte Suprema de Justicia y la Procuraduría General de la República, formularán un diagnóstico de las fortalezas y debilidades del país en la materia. Esta actividad que dio inicio este lunes y finalizará el jueves, forma parte de los compromisos adquiridos por el país con la ratificación, en setiembre del 2017, del Convenio de Budapest. La Oficina de Asesoría Técnica y Relaciones Internacionales del Ministerio Público (Oatri) fue designada por Decreto Ejecutivo como la autoridad central para la implementación del Convenio en Costa Rica, por lo que tiene a su cargo un rol de coordinación interinstitucional." READ MORE

Source: ENISA, EDA, EC3, CERT-EU

Date: 23 May 2018

Four European Union cybersecurity organisations enhance cooperation

"The European Union Agency for Network and Information Security (ENISA), the European Defence Agency (EDA), the European Cybercrime Centre (EC3) and the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU) today signed a Memorandum of Understanding (MoU) to establish a cooperation framework between their organisations. […] The MoU aims at leveraging synergies between the four organisations, promoting cooperation on cyber security and cyber defence and is a testament to the trusted partnership that exists between these EU agencies. More specifically, it focuses on five areas of cooperation, namely Exchange of information; Education & Training; Cyber exercises; Technical cooperation; and Strategic and administrative matters. It also allows for cooperation in other areas identified as mutually important by the four organisations." READ MORE

Source: Europol

Date: 23 May 2018

EUR 8 million, 700 bank accounts and money mules: the little-known tricks of social engineering fraudsters

"Operation Valcea-Cruces began in early 2017 when law enforcement authorities exchanged information on different fraud cases. The busted crime ring, operating in different cells across Europe, was led from Romania where 5 individuals were arrested alongside 14 in Spain, resulting in 33 arrests in total […]. The criminal group was dismantled by the Spanish National Police, Mossos d'Esquadra and the Romanian Police with active support and coordination from Europol and Eurojust. The group operated in two ways: (i) Posing as suppliers for public sector organisations and claiming organisations had payments outstanding. Once contact had been established, the organisations were told to transfer money to a new bank account – opened by a money mule; (ii) Committing online fraud against private bodies either by phishing or copying pictures from websites and republishing them, pretending to be official rental websites. […] Social engineering-based fraud remains one of the most significant transnational crime threats in Europe. […] It is considered to be the second biggest source of criminal proceeds after drug trafficking." READ MORE

Source: Irish Government

Date: 16 May 2018

Irish Minister for Justice and Equality on national cybercrime legislation

"One requirement, an important one, in dealing with cybercrime is having in place strong legislation with effective, proportionate and dissuasive penalties. Ireland has recently introduced legislation to deal with attacks on information systems and their data. The Criminal Justice (Offences Relating to Information Systems) Act 2017, which came into operation last June, is the first piece of dedicated cybercrime legislation in this jurisdiction. […] The new legislation seeks to protect information systems and infrastructures, and their important data, from cyberattacks from both within and outside the State. The Act makes it an offence to engage in cybercrime activity and provides strong penalties for those found guilty of offences relating to information systems, including up to 10 years' imprisonment if the crime is sufficiently serious. The Act also implements key legal provisions in the Council of Europe Convention on Cybercrime, often known as the Budapest Convention. I am pleased to say that the vast majority of the provisions in the Convention are now covered on the Irish Statute Book. There is more work to be done, and some further legislation is in train to enable formal ratification of the Treaty, to which Ireland is already a signatory." READ MORE

Source: UK Government

Date: 23 May 2018

Cyber and International Law in the 21st Century, UK Attorney General

"It is the UK's view that when states and individuals engage in hostile cyber operations, they are governed by law just like activities in any other domain. […] Perhaps the most useful starting point is the UN Charter and three specific rules are particularly relevant. First, there is the rule prohibiting interventions in the domestic affairs of states both under Article 2(7) of the Charter and in customary international law. […] The next relevant provision of the UN Charter is in Article 2(4) which prohibits the threat or use of force against the territorial independence or political integrity of any state. Any activity above this threshold would only be lawful under the usual exceptions – when taken in response to an armed attack in self-defence or as a Chapter VII action authorised by the Security Council. […] Thirdly, the UK considers it is clear that cyber operations that result in, or present an imminent threat of, death and destruction on an equivalent scale to an armed attack will give rise to an inherent right to take action in self- defence, as recognised in Article 51 of the UN Charter." READ MORE

Source: Coindesk

Date: 29 May 2018

German Authorities Sold $14 Million in Seized Cryptos Over Price Fears

"Concerns over high price volatility have prompted prosecutors in Germany to make an emergency sale of seized cryptocurrencies worth over €12 million. Bavarian prosecutors ordered the sale on Feb. 20. At the time, bitcoin's price had rebounded to nearly $10,000 after hitting a yearly low of $5,947 on Feb. 6. Taking nearly two months to complete, the sale reportedly disposed of 1,312 bitcoins, 1,399 bitcoin cash, 1,312 bitcoin gold and 220 ether via over 1,600 transactions on a German trading platform. The cryptocurrencies were all seized during two ongoing investigations being conducted by Bavarian cybercrime agencies. Although the prosecutor has not yet brought charges in the two cases, German legislation allows for emergency sales if assets seized in ongoing investigations face an immediate threat of loss of value." READ MORE

Source: CGTN Africa

Date: 30 May 2018

Kenya court suspends portions of new cybercrime law

"A High Court judge in Kenya suspended sections of a controversial new law which had been contested by bloggers and rights groups who argued it would limit freedom of expression and freedom of the press. The Computer Misuse and Cybercrimes Act was signed into law earlier this month by President Uhuru Kenyatta and was due to come into effect on Wednesday, but the court ruled that large sections should be suspended until the case is heard in July. Justice John Mativo issued the directive Tuesday in a case in which Bloggers Association of Kenya sued the Attorney-General, the Speaker of the National Assembly, the Inspector-General of Police and the Director of Public Prosecution over the Computer Misuse and Cyber Crimes Act 2018." READ MORE

Source: The Jordan Times

Date: 22 May 2018

Jordan Government ready with cybercrime bill 'to curb hate speech'

"The Cabinet on Monday endorsed the 2018 cybercrime law, which aims at limiting cybercrimes to curb hate speech, privacy violation and other crimes, especially those committed on social media platforms. The bill stipulates an imprisonment penalty of no less than a year and no more than three years and a fine between JD5,000 and JD10,000 for people who publish or share whatever can be described as hate speech through the Internet, websites or information systems. Those who establish or run websites or publish information online with the intention of promoting the use of weapons, ammunition or explosives that are not allowed by the law can face prison terms of no less than six months, according to the draft. The bill defines hate speech as each statement or act that can fuel religious, sectarian, ethnic or regional sedition; calling for violence and justifying it; or spreading rumours against people with the aim of causing them physical harm or damage to their assets or reputation." READ MORE

Source: Caribbean 360

Date: 17 May 2018

Spike in cyber-attacks on Caribbean Organizations

"With cyber attacks on the rise across the Caribbean, Chief Executive Officer of the Caribbean Israel Centre for Cyber Defense (CICCD), Andre Thomas, has recommended that authorities in Barbados and the region make provision for enhanced legislation and law enforcement capacity, to counter the issue. "They've been major hacks recently in the last six weeks. There was a major hack in St. Maarten, another one in Guyana….We're aware of hacks taking place all over the region. And they're mostly underreported," he revealed yesterday. […] While expressing concern about the reluctance to report such incidents, the CICCD official maintained that insufficient training and legislative provisions were among some of the hindrances." READ MORE

Source: Jamaica Observer

Date: 18 May 2018

Guyana to reconsider Cyber Crime Bill

"Attorney General Basil William told reporters that while he endorsed the sentiments of some of his colleagues regarding the legislation, he will bring the matter before the Cabinet for further discussion. […] The Bill, which is currently before the National Assembly, makes it an offence for people to use a computer to excite disaffection to the Government, even as the Government maintains that it does not affect the freedom of expression. The Government has also come under criticism for the inclusion of a sedition clause in the Bill." READ MORE

Latest reports

- European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law - 2018 edition, 25 May 2018
- UNODC, Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 3 to 5 April 2018, submitted to the 27th Session of the UN Commission on Crime Prevention and Criminal Justice in Vienna 14-18 May 2018, 13 April 2018
- MIT Technology Review, Inside the business model for botnets, 14 May 2018
- ENISA, Efail Vulnerability Targeting PGP Email Clients, 18 May 2018
- Facebook, Facebook Publishes Enforcement Numbers for the First Time, 15 May 2018
- Estonian e-Governance Academy, National Cyber Security Index, May 2018

Upcoming events

- 4 June 2018, Tbilisi, Georgia – Steering Committee, PGG 2018: Cybercrime@EAP
- 4 – 6 June 2018, Amman, Jordan – Assessment visit, CyberSouth
- 4-15 June, Naples, Italy – Participation of one Ghanaian officer in a Cybercrime Training organized by the Italian Police, GLACY+
- 5 – 6 June 2018, Tbilisi, Georgia – Participation in EuroDIG 2018 – focus on criminal justice action in cyberspace, iPROCEEDS, PGG 2018: Cybercrime@EAP
- 11 June 2018, Yerevan, Armenia – Participation in Council of Europe Armenia Action Plan steering committee, PGG 2018: Cybercrime@EAP
- 11 – 12 June 2018, Cyprus – Participation in the 3rd International Conference "Cyber Crime Trends and Threats: Europe and International Dimensions", iPROCEEDS
- 11-15 June, Santo Domingo, Dominican Republic – ECTEG Course: Live-Data Forensics for law enforcement officers, GLACY+
- 12 – 15 June, 2018, Belgrade, Serbia – Pilot training session on introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors, iPROCEEDS
- 12-15 June, Nuku'alofa, Tonga – Second Annual PILON Cybercrime Workshop, GLACY+

The Cybercrime Digest appears bi-weekly. News are selected by relevance to the current areas of interest to C-PROC and do not represent official positions of the Council of Europe. You receive this digest as you have taken part in Council of Europe activities on cybercrime. It is not intended for general publication.

For any additional information, contributions, subscriptions or removal from this distribution list, please contact: cybercrime@coe.int

www.coe.int/cybercrime