Cybercrime Digest

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

1-15 September 2018

Source: Council of Europe

Underground Economy Conference opened by the Deputy Secretary General of the Council of Europe

Date: 6 Sep 2018

"On 5 September 2018, Deputy Secretary General Gabriella Battaini-Dragoni opened the Underground Economy Conference 2018, which takes place in the Council of Europe premises in Strasbourg, France. This prominent international information security (closed) event, co-organised by Team Cymru and the Council of Europe, is bringing together around 400 representatives from the law enforcement agencies, cyber security community, private industry and academia from across the globe. The Deputy Secretary General put the Council of Europe's work on cybercrime in context, noting that it is at the crossroads of human rights, democracy and the rule of law – the Organisation's three pillars. She also highlighted that cooperation between state authorities and the private sector is of particular relevance in this field." READ MORE

Source: The Independent

UK mass surveillance programme violates human rights, European court rules

Date: 12 Sep 2018

"The UK government's mass surveillance programme violated human rights and had "no real safeguards", the European Court of Human Rights (EHCR) has said in a landmark ruling. The Strasbourg court said British intelligence agencies' interception regime violated the right to a private and family life, since there was "insufficient oversight" over which communications were chosen for examination. Not enough protection was given to journalistic sources by the government's mass information collection programme, violating the right to freedom of expression, it also said. But the court ruled that sharing the information with foreign governments did not violate either the right to a private and family life, or to free speech. The case, brought by a group of charities including human rights groups Big Brother Watch and Amnesty International, centred on complaints about powers given to security services under the Regulation of Investigatory Powers Act 2000 (Ripa)." READ MORE

RELATED ARTICLES

European Court of Human Rights, Some aspects of UK surveillance regimes violate Convention – Press Release, 13 Sep 2018

Source: EU Neighbours

Workshop on the Budapest Convention on Cybercrime in Algeria

Date: 11 Sep 2018

"The Council of Europe in cooperation with the Ministry of Justice and Ministry of Foreign Affairs of Algeria held a workshop on Budapest Convention on Cybercrime on 2 September 2018 in Algiers. This workshop was an opportunity to present the Budapest Convention to Algerian authorities and the benefits for Algeria to join this international treaty. The workshop aimed to open discussions on concerns that a State might have before joining the Convention and also addressed some of the requirements of this treaty." READ MORE

Source: Washington Post

Date: 4 Sep 2018

Working with Russia on cybercrime is like hiring a burglar to protect the family jewels

"Imagine a bully who's pounding your head against a wall. When you complain that it hurts and threaten to punch back, he offers to sign an international agreement against bullying. Meanwhile, he keeps pounding your head. That's a shorthand summary of the peculiar situation that has developed in the United Nations' discussions about regulating cyberspace. The Russians are aggressively hacking U.S. and European political parties and infrastructure, according to U.S. intelligence reports. At the same time, they are pushing for international regulation of cyberspace — on their own terms. Russian plans to offer new U.N. cyber-regulation pacts were floated last month by Anatoly Smirnov, a top computer scientist at the Moscow State Institute of International Relations, in an interview with Nezavisimaya Gazeta. He said Russia would soon introduce a cyber "code of conduct" and a pathway to a new cybercrime convention to replace one signed in Budapest in 2001." READ MORE

RELATED ARTICLES

Council of the European Union, EU Lines to take on cybercrime developments in the framework of the UN, 14 Sep 2018

Source: Microsoft

Date: 11 Sep 2018

A call for principle-based international agreements to govern law enforcement access to data

"Governments around the world have started to modernize the processes by which law enforcement accesses digital evidence across borders. In the United States, passage of the CLOUD Act created the foundation for a new generation of international agreements that allows governments to engage with each other to create lasting rules to protect privacy and facilitate legitimate law enforcement access to evidence. In Europe last week, the European Commission presented its proposed e-Evidence legislation to the European Parliament. Many other governments are similarly seeking to update their laws to protect privacy, promote digital security and address the challenge of an increasingly borderless world. As a global company entrusted by millions of users, we believe it is important for Microsoft to make clear how governments should address these issues. For that reason, we are sharing six principles that have driven, and will continue to drive, our advocacy as governments reform their laws and negotiate international agreements." READ MORE

RELATED ARTICLES

Microsoft, Six principles for international agreements governing law enforcement access to data, 11 Sep 2018

Source: Reuters

Date: 13 Sep 2018

Cyber attacks cost German industry almost $50 billion

"Two thirds of Germany's manufacturers have been hit by cyber-crime attacks, costing industry in Europe's largest economy some 43 billion euros ($50 billion), according to a survey published by Germany's IT sector association on Thursday. […]German security officials have long been sounding the alarm about the risk of well-resourced foreign spy agencies using cyber attacks to steal the advanced manufacturing techniques that have made Germany one of the world's leading exporters." READ MORE

Source: The Portugal News

Date: 6 Sep 2018

Portugal has third greatest number of cybercrime victims in EU

"According to the report, compiled by the Economy Ministry's Bureau for Strategy and Studies, "Portugal is the country where citizens least share their personal data" (43%) and contacts (15.2%), over the internet. Figures which are far below the corresponding EU averages of 71.4% and 61.1%, respectively. But, the report found, when it comes to sharing photographs and location data in areas such as health and income, 33.5% of online users do so, which is higher than the 22.4% EU benchmark. "In terms of daily internet users, Portugal has one of the worst results", the study further concluded, with just 51% of people using mobile internet on phones or other devices, and therefore, given the low number of users, "the value of financial losses is also low" regarding crimes committed over the internet. However, the number of victims of cybercrimes in Portugal is still the third highest in the EU, after Romania and Holland" READ MORE

Source: Daily Observer

Date: 4 Sep 2018

ECOWAS Parliament Wants Member States Make Laws to Fight Cyber-crime

"The 15 member states of the Economic Community of West African States (ECOWAS) have been encouraged to develop a National Cybersecurity Strategy as well as make laws to fight cyber-crimes in all ECOWAS member states, to facilitate the creation of a safer cyber environment in West Africa. Members of the Joint Committee on Communications and Information Technology/ Education, Science and Technology/ Labour, Employment, Sport and Culture of the ECOWAS Parliament unanimously voted to adopt it in their report, which will be subsequently submitted to the full Plenary of ECOWAS Parliament of the Fourth Legislature. […] According to Joint Committee's reports, about 70% of cybercrimes in Africa has to do with social network, and there is a need for an aggressive sensitization campaign or law for the safe use of social media. "The cybersecurity in the region is hampered by lack of appropriate legislation and national cybersecurity strategies. There is a desperate need for capacity building and the establishing of CERT/CIRT. Towards this end the Community has developed and adopted some Acts to promote a safer cyber environment within ECOWAS. And these include Directive on Fighting against Cybercrime; Supplementary Act on Electronic Transactions; and Supplementary Act on Personal Data Protection." READ MORE

Source: Council of Europe

Date: 10 Sep 2018

Data Protection in Nigeria

"Carried out under the GLACY+ Project notably aimed at providing advice on legislation in line with the Budapest Convention and rule of law and human rights, including data protection standards, the Residential Drafting Retreat on Data Protection Legislation in Nigeria is being held in Calabar, Cross-River State, on 10 – 14 September 2018. The Data Protection Unit assisted by two data protection experts has the privilege, with the support of the Cybercrime Division, to take part in this workshop which will deliver the first ever, robust and modern draft privacy legislation for Nigeria. The draft is to be shortly sent to the National Assembly in order to initiate the legislative procedure. This initiative will hopefully assist Nigeria further in acceding to Council of Europe's conventions on cybercrime and data protection and serve as possible inspiration for other countries in the region." READ MORE

Source: Europol

Date: 14 Sep 2018

Germany and Sweden take action against cyber fraud gang

"With the support of Europol and Frontex, two suspects were arrested on 12 September in a series of coordinated raids across Germany and Sweden in an investigation targeting a Syrian organised crime group suspected of cyber fraud. House searches were carried out in Aachen, Dortmund and Essen (Germany), and in Nörrköping, Malmö and Helsingborg (Sweden), where police recovered some EUR 54 000 and USD 55 000. The arrestees are believed to be the key organisers of a cyber fraud gang. The German Federal Police initiated Operation GOLDRING in October 2017. The intelligence-led operation uncovered the organised crime group, composed of Syrian nationals, which was involved in fraudulently purchasing airline and train tickets. According to information from Germany, more than 493 fraudulent bookings were identified. In most cases the tickets were one way tickets from Beirut to European Member States. The tech-savvy smugglers avoided detection by making the bookings using compromised corporate credit cards and credentials, purchased online from other criminals offering them for sale." READ MORE

Source: Rappler

Date: 5 Sep 2018

Saudi Arabia declares online satire a punishable offense

"Saudi Arabia will punish online satire that "disrupts public order" with up to 5 years in prison, the public prosecutor said Tuesday, September 4, as the kingdom cracks down on dissent. "Producing and distributing content that ridicules, mocks, provokes and disrupts public order, religious values and public morals through social media ... will be considered a cybercrime punishable by a maximum of 5 years in prison and a fine of 3 million riyals ($800,000)," the public prosecution tweeted late Monday." READ MORE

Source: Reuters

Date: 14 Sep 2018

Southeast Asian cyber security center opens in Thailand

"A cyber security center opened in Thailand on Friday to train personnel from countries in the Association of Southeast Asian Nations (ASEAN) to help combat cyber threats in the attack-prone region. The idea of the ASEAN-Japan Cyber Security Capacity Building Centre came from a meeting between ASEAN and Japan's ministers in Cambodia last year. About 700 cybersecurity personnel from Southeast Asia are expected to graduate from the Japan-designed programs, which include cyber defense, digital forensics and malware analysis. […] Thailand is currently drafting cyber security and data protection bills, which it expects to become law by the end of the year." READ MORE

Source: Modern Ghana

Date: 7 Sep 2018

Cybercrime rises in Ghana, but Industry recovers GH¢160m in 2017

"An estimated 80% of the value of all cyber fraud cases was recovered in 2017, the Bank of Ghana has stated. However, instances of cyber fraud continue to rise as the figure went up by about 42% between 2016 and 2017. The central bank is therefore embarking on new strategies to reduce the crime to the barest minimum. […] The comments also come at a time where Ghana has been listed as one of the top ten most attacked countries in Africa." READ MORE

Source: Leadership

Date: 6 Sep 2018

Shaping Nigeria's Digital Future through Positive Legislation

"The Digital Rights and Freedom Bill, which was developed through deliberate, multi-stakeholder consultations, and has been passed by both houses of Nigeria's Congress, provides a comprehensive legislative framework that describes and clarifies relevant obligations and responsibilities for human rights online. Making it law will boost Nigeria's burgeoning Internet economy, improve governance, and further Nigeria's position as a regional and global leader in information, communications, and technology issues. The Digital Rights and Freedom Bill addresses a range of critical digital policy issues, such as data in the cloud; surveillance and a lawful interception; data privacy; and freedom of expression online. The bill also provides for the protection of citizens from errant behaviours such as hate speech and misinformation, as defined by a competent court of law." READ MORE

Source: Estrategia

Date: 13 Sep 2018

Ciberseguridad, un nuevo desafío para Chile

"Durante los últimos años nuestro país ha recibido de ataques a las redes públicas, interfiriendo, en muchas oportunidades, la eficiencia de los servicios del Estado. […] En el ámbito privado la situación ha sido más grave, destacándose como ejemplos más visibles del último tiempo, la sustracción, a través de las redes, de una cuantiosa suma de dinero al Banco de Chile y la filtración de miles de tarjetas de bancos y tiendas de retail. […] Autoridades gubernamentales durante los últimos años han concretado varias iniciativas, entre las que podemos mencionar: la elaboración de una Política Nacional de Ciberseguridad, una Política Nacional de Ciberdefensa, un Comité Interministerial de Ciberseguridad, una hoja de ruta con medidas a cumplir antes del término del presente año, y la adhesión al Convenio de Budapest, considerado el instrumento internacional más serio de cooperación entre Estados para investigar y perseguir estos delitos que no tienen fronteras." READ MORE

Latest reports

- European Commission, Proposal for a regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres – Impact Assessment, 12 Sep 2018
- Australian Government, ACORN Evaluation Report, published on 4 Sep 2018
- Harvard Business Review, How a Cyber Attack Could Cause the Next Financial Crisis, 14 Sep 2018

Upcoming events

- 17 – 18 September, Bucharest, Romania – Study visit in cybercrime specialized units and CERT.RO, CyberSouth
- 18 – 20 September, Singapore – Participation in the Global Forum on Cyber Expertise (GFCE) Annual Meeting 2018, GLACY+, CyberSouth
- 18 – 20 September, Singapore – INTERPOL-Europol Cybercrime Conference, iPROCEEDS, GLACY+, Cybercrime@EAP 2018, CyberSouth
- 20 – 21 September, Belgrade, Serbia – Regional Ministerial Conference on High-Tech Crime and Information Security "Connect securely!", iPROCEEDS
- 23 – 27 September, Alger, Algeria – Basic Judicial Training, CyberSouth

- 24 September, Apia, Samoa – Participation in the Pacific Judicial Conference, GLACY+
- 24 – 26 September, Washington DC, US – Advisory mission on cybercrime legislation for Chile, in collaboration with the OAS, Cybercrime@Octopus
- 24 – 26 September, Bucharest, Romania – Second preparatory meeting to finalise the Cybercrime Exercise Scenario, iPROCEEDS
- 24 – 26 September, Kyiv, Ukraine – Workshop on practical aspects of CSIRT/LEA cooperation, combined with advisory visit to CERT.GOV.UA and SSU technical division, Cybercrime@EAP 2018
- 26-28 September, Fiji – Participation in the bi-annual Policy Network Meeting in the Pacific, organized by the Australian Federal Police, Cybercrime@Octopus
- 26-28 September, Accra, Ghana – Participation in the Forum on Internet Freedom in Africa (FIFAfrica) organized by CIPESA, GLACY+
- 26-28 September, Abuja, Nigeria – 3rd National Conference on Cybercrime and Electronic Evidence, GLACY+
- 27 September – 2 October, Nairobi, Kenya – Workshop on data protection legislation, Cybercrime@Octopus
- 27 – 28 September 2018, Kyiv, Ukraine – National Cybercrime Cooperation Forum with participation of law enforcement and Internet industry at the IGF-UA and Youth-IGF, Cybercrime@EAP 2018