Cybercrime Digest

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

16-31 July 2018

Source: Council of Europe

Date: 19 Jul 2018

Octopus Conference 2018 – Key messages

"Some 360 cybercrime experts from 95 countries, including representatives of 8 international and 75 private sector, civil society organisations and academia met at the Council of Europe in Strasbourg, France, from 11 to 13 July 2018 for the Octopus 2018 Conference on cooperation against cybercrime. Key messages resulting from Octopus 2018 are:

- The participation of ministers and other senior representative from States of Africa, Asia/Pacific and Latin America underlined the global interest in the Budapest Convention on Cybercrime and related capacity building programmes. […]
- During the past two years, cybercrime has reached even more threatening proportions affecting the security of individuals and core values of societies. […]
- Interference with elections through attacks against computers and data used in elections and election campaigns combined with disinformation operations, as experienced in particular since 2016, violate rules to ensure free, fair and clean elections and represent attacks against, and undermine trust in, democracy. […]
- As the European Court of Human Rights has found, governments have the obligation to protect society and individuals against crime, including through criminal law. […]
- The Additional Protocol to the Budapest Convention is expected to offer meaningful ways to render mutual legal assistance more efficient while also enabling direct cooperation with providers across jurisdictions and extending searches to access evidence in the cloud with the necessary rule of law safeguards. […]
- Domain name registration data is often the starting point for criminal investigations but is also used by other organisations with a legitimate interest, including privacy, consumers protection or cybersecurity organisations. […] An international legal basis for requests to WHOIS data may need to be considered.
- Specific legislation, consistent with human rights and rule of law requirements, is the basis for criminal justice action on cybercrime and electronic evidence. Many governments around the world have undertaken legal reforms in recent years, often using the Budapest Convention on Cybercrime as a guideline. […]
- Capacity building is considered one of the most effective means to address the challenges of cybercrime and electronic evidence. Based on broad international consensus, governments, international organisations, civil society and private sector initiatives in recent years have made resources available and supported programmes in all regions of the world to strengthen legislation, provide training to criminal justice officials, promote public-private cooperation and make international cooperation more efficient.
- Cyberviolence comprises a broad range of conduct that most directly affects the dignity and rights of individuals. […] While prevention is essential and should be given priority, criminal justice is part of the response.
- The rapid progress of artificial intelligence and machine learning raises critical questions on the future of humanity but also specific questions regarding benefits and risks related to cybercrime and criminal justice. […]" READ MORE

Source: Council of Europe

Date: 30 Jul 2018

Paraguay ratifies the Convention on Cybercrime and the Additional Protocol on Xenophobia and Racism

Today, Paraguay has deposited the instruments of accession to the Budapest Convention on Cybercrime and its Additional Protocol on Xenophobia and Racism. With Paraguay's accession, the Convention on Cybercrime has now 61 states parties. A further 10 States have signed it or been invited to accede. READ MORE

Source: Business Ghana

Date: 21 Jul 2018

Ghana conducts judicial training on cybercrime for English speaking countries of the ECOWAS region

"The three-day programme is being attended by 30 judges, magistrates, and prosecutors from five Anglophone countries, namely Ghana, Gambia, Liberia, Nigeria and Sierra Leone and the participants would be taken through the current technology trends and challenges with investigations and prosecutions on cyber crimes. […] The Minister of Communications, Ursula Owusu-Ekufful in a speech read on her behalf by her deputy, Vincent Sowah Odotei, lauded COE and EU for sponsoring a second training for judges, magistrates and prosecutors from the Anglophone countries of ECOWAS. She said Ghana was in the process to ratify the Budapest and Malabo conventions, indicating that her ministry had submitted a memo to Parliament for the Malabo Convention to be passed into law." READ MORE

Source: Opinion y Salud

Date: 22 Jul 2018

Al aprobar Ley contra la ciberdelincuencia, Colombia se compromete a luchar contra la pornografía infantil

"El presidente de la república Juan Manuel Santos, sancionó la ley 1928 de 2018, por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia, aprobado en el año 2001 en Budapest. Los estados firmantes del Convenio, reconocen la necesidad de una cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los legítimos intereses en la utilización y el desarrollo de las tecnologías de la información. […] Para los efectos del Convenio se entenderá por pornografía infantil, todo material pornográfico que contenga la representación visual de: a un menor comportándose de una forma sexualmente explícita o imágenes que representen a un menor comportándose de una forma sexualmente explícita. El Convenio sobre la Ciberdelincuencia resulta necesario para prevenir a los ciudadanos contra la confidencialidad, la integridad y la disponibilidad de los sistemas redes y datos así como el abuso de dichos sistemas y la tipificación de delitos, facilitando su detección, investigación y tanto a nivel nacional como internacional." READ MORE

Source: Gestion

Date: 31 Jul 2018

Ciberataques al sector energético en Perú cuestan US$ 17.20 millones al año

"Uno de los sectores más afectados por el cibercrimen en Perú es el energético, donde estudios revelan un incremento sustancial en los ataques durante los últimos años, con un costo aproximado de US$ 17.20 millones al año. La industria que se dedica a la generación, transporte y distribución de energía está registrando un elevado índice de incidentes y se ubica en segundo lugar en cuanto a ciberataques después del sector financiero." READ MORE

Source: The Hill

Date: 31 Jul 2018

Facebook reveals evidence to Congress of new disinformation campaign ahead of midterm elections

"Facebook has revealed a new coordinated disinformation campaign ahead of November's elections that used dozens of fake accounts and pages on its platform. The company said it has removed 32 pages and accounts across Facebook and Instagram involved in "inauthentic behavior" after discovering them last week. It has briefed lawmakers on its discoveries and has been working with the FBI on the matter since discovering the accounts last week. "We're still in the very early stages of our investigation and don't have all the facts — including who may be behind this," Facebook said in a post." READ MORE

Source: Europol

Date: 20 Jul 2018

Online scammers captured after causing EUR 18 million of damage in more than 35 000 cases

"After six years of preparation and coordination, the international Operation Warenagent has seen the arrest of 15 individuals, thought to be members of a network responsible for online fraud causing EUR 18 million worth of damage. The operation was conducted by the German Prosecutor's Office of Dresden, the Saxon State Office of Criminal Investigation, the Lithuanian Police and the Lithuanian Prosecutor's Office, with help from Europol and Eurojust at the international level. […] Since 2012 more than 35 000 cases of online fraud have been detected. In all cases, high-quality goods were ordered from various mail order companies with fraudulently obtained credit card data through a network of merchandise agents. The recipients of these goods, known as package mules, were mostly recruited in Germany. After receiving the illegally obtained goods, the package mules were asked to send the packages to new addresses, primarily in Eastern Europe. These schemes are often disguised as legitimate job opportunities and the mules may receive a commission for their service. They were used as intermediaries and played a crucial role in online payment fraud as criminal networks gain access to the stolen goods or funds without revealing their identity." READ MORE

Source: Reuters

Date: 19 Jul 2018

Vietnam says controversial cybersecurity law aims to protect online rights

"Vietnam's new cybersecurity law is designed to protect online rights and create a "safe and healthy cyberspace," the foreign ministry said on Thursday, although critics have warned it gives the Communist-ruled state more power to crack down on dissent. Seventeen U.S. lawmakers wrote to the chief executives of Facebook and Google on Wednesday, urging them to resist changes wrought by the new law that require foreign tech firms to store locally personal data on users in Vietnam and open offices there. "As in any other country, the activities of foreign businesses and investors should comply with the laws of the host country," foreign ministry spokeswoman Le Thi Thu Hang told Reuters in a comment on Wednesday's letter. "The ratification of the cybersecurity law is aimed at creating a safe and healthy cyberspace," Hang said in a written statement in response to a request for comment. That would protect the legitimate rights and interests of organizations and individuals online, and ensure national security as well as social order and safety, she added. " READ MORE

Source: La Nacion

Date: 29 Jul 2018

Les autorités financières marocaines s'inquiètent de la recrudescence des cyber-risques

"Les autorités financières marocaines s'inquiètent de la recrudescence du cyber-risque au sein du système financier. […] Pour le cas du Maroc, les autorités financières se sont attelé sur le sujet depuis 2017 en élaborant «une feuille de route pour la surveillance du cyber-risque au sein du système financier et ce, en tenant compte du dispositif national existant». En effet, un dispositif de cybersécurité a été mis en place au plan national à travers notamment la création du Comité stratégique pour la sécurité des systèmes d'information et l'institution de la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) relevant du Département de la Défense Nationale Marocaine. Selon le rapport de la stabilité financière, le principal objectif de cette feuille de route est de «convenir d'un cadre de référence commun et harmonisé entres les trois régulateurs pour la surveillance de ce risque, tout en veillant à une bonne coordination inter-autorités et à l'égard des autres parties prenantes (DGSSI, Agence de Développement du Digital, instances internationales)»." READ MORE

Source: UpGuard

Date: 20 Jul 2018

How a Robotics Vendor Exposed Confidential Data for Major Manufacturing Companies

"Sensitive documents for over a hundred manufacturing companies were exposed on a publicly accessible server belonging to Level One Robotics, "an engineering service provider specialized in automation process and assembly for original equipment manufacturers, Tier 1 automotive suppliers as well as our end users." Among the companies with data exposed in the incident are divisions of VW, Chrysler, Ford, Toyota, GM, Tesla and ThyssenKrupp. The 157 gigabytes of exposed data include over 10 years of assembly line schematics, factory floor plans and layouts, robotic configurations and documentation, ID badge request forms, VPN access request forms, and ironically, non-disclosure agreements, detailing the sensitivity of the exposed information. Not all types of information were discovered for all customers, but each customer contained some data of these kinds." READ MORE

Source: Reuters

Date: 24 Jul 2018

Singapore disconnects healthcare computers from the Internet after cyber attack

"Singapore has disconnected computers from the internet at public healthcare centers to prevent cyberattacks of the kind that caused its worst breach of personal data, a government official said on Tuesday. Singapore started to cut web access for civil servants in 2016 to guard against cyberattacks, but stopped short of including public healthcare institutions. Officials may still surf the web using separate personal or agency-issued devices. In the most recent attack in June, hackers stole particulars of more than 1.5 million patients, including the prime minister's drug prescriptions, in what the government has called "a deliberate, targeted and well-planned cyberattack"." READ MORE

RELATED ARTICLES

Ministry of Health of Singapore, SingHealth's IT System Target of Cyberattack, 20 Jul 2018

Source: La Nacion

Date: 29 Jul 2018

Chile, Gobierno enviará al Congreso tres proyectos de ley en materia de ciberseguridad

"Tras los episodios de fraude en los bancos, el Ejecutivo enviará al Congreso tres proyectos de ley con suma urgencia, los cuales no sólo establecerán nuevos delitos en materia de ciberseguridad, sino que además obligarán a las entidades a entregar información sobre los incidentes que puedan haberlos afectado. "Con estos dos últimos episodios hemos demostrado debilidad. Me preocupa que hoy no tengamos una legislación que nos permita saber cuáles son los delitos informáticos, cuáles son las penas asociadas, cuál es el marco de ciberseguridad", reconoció a Reportajes el subsecretario del Interior, Rodrigo Ubilla. Antes del 26 de agosto, aseguró, se enviará al Parlamento el proyecto de ley de modernización de delitos informáticos, que modificará la ley vigente desde 1993, cuando en Chile no existía internet." READ MORE

Source: Kaieteur News

Date: 22 Jul 2018

Guyana, Cybercrime Bill lacks provision for international cooperation

"Former Minister of Culture, Youth and Sport, Dr. Frank Anthony, has expressed the view that the Cybercrime Bill passed Friday evening in the National Assembly should have included a clause on how Guyana will work with the international community. […] He noted that most of its provisions have their genesis in the 2001 Budapest Convention on Cybercrime. […] According to Dr. Anthony, 'the Government to its discredit' has made two fundamental changes. Firstly, they dropped the section dealing with international cooperation and secondly, they added the section dealing with sedition." READ MORE

Latest reports

- Alexander Seger, Enhanced cooperation on cybercrime: a case for a protocol to the Budapest Convention, 16 Jul 2018
- Council of Europe, GLACY+: 2018/AO/45 - Call for tenders - 31 August 2018 - Provision of event organisation services in Addis Ababa, Ethiopia, 1 August 2018
- Council of Europe, Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment, adopted on 4 Jul 2018
- The Library of Congress, Regulation of Cryptocurrency Around the World, June 2018
- American Chamber of Commerce to the European Union, European Commission proposals on cross-border access to electronic evidence - Our Position, 3 Jul 2018
- Center for Strategic and International Studies, Low-Hanging Fruit – Evidence-Based Solutions to the Digital Evidence Challenge, July 2018
- University College London, You are your Metadata: Identification and Obfuscation of Social Media Users, 30 Jul 2018
- ICANN, Data Protection/Privacy Update: Key GDPR WHOIS Updates and Next Steps, 27 Jul 2018

Upcoming events

- 1-3 August, Port Louis, Mauritius – Special residential programme on cybercrime and electronic evidence for the Supreme Court Justices, GLACY+
- 13-17 August, Manila, Philippines – ECTEG Course, Cybercrime and digital forensics specialized training for law enforcement officers, GLACY+

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime