Cybercrime Digest

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

16-30 April 2017

Source: Agenda de Prensa

Date: 24 Apr 2017

Chile accede al Convenio de Budapest sobre la Ciberdelincuencia

"Chile se convirtió hoy en el tercer país de América Latina en acceder al Convenio de Budapest sobre Ciberdelincuencia, el único tratado internacional en esta materia, al depositar el instrumento de adhesión a este tratado internacional en la sede del Consejo de Europa en Estrasburgo. El tratado, que fue abierto a la firma en Budapest (Hungría) el 23 de noviembre de 2001, entrará en vigor con respecto a Chile el 1 de agosto de 2017. El convenio vincula ya a 54 Estados, incluyendo a la República Dominicana, Panamá y Chile en América Latina. Otros países latinoamericanos que han sido invitados a adherirse son Argentina, México, Colombia, Perú, Costa Rica y Paraguay." READ MORE

RELATED ARTICLES

Council of Europe, Accession by Chile to the Budapest Convention, 20 Apr 2017

Source: Council of Europe/ European Union

Date: 27 Apr 2017

Cybercrime@EAP III and iPROCEEDS: investigating cybercrime and its financial gain

"A novel initiative comprising 12 countries from the Eastern Partnership Region, South-eastern Europe and Turkey was launched today in Tbilisi, Georgia through a Cybercrime Coordination and Partnership Exercise to explore and establish closer links between professional communities of cybercrime investigators, cybersecurity players, financial intelligence/investigation officers and the private sector. The exercise is organised by the Cybercrime Programme Office of the Council of Europe, through the two joint projects of European Union and the Council of Europe – Cybercrime@EAP III and iPROCEEDS – in close cooperation with Data Exchange Agency of the Ministry of Justice of Georgia, in Tbilisi, Georgia from 24 to 28 of April 2017. The simulation exercise aims at addressing the problems of coordination and cooperation in the most practical way and will require the participants to detect cyber security incidents against critical infrastructure, apply digital forensics skills, detect and handle suspicious financial transactions and money laundering and recover data through international cooperation channels." READ MORE

Source: European Commission

Date: 25 Apr 2017

Law Enforcement Challenges in the Online Context

"Talking about the challenges that law enforcement authorities face in obtaining quickly e-evidence in the context of criminal investigations is crucial. It is key to efficiently fight cybercrime, to fight also terrorism and to solve all kinds of criminal investigations. This is the reason why it is a priority under the European Agenda for Security that the Commission adopted. Our traditional investigation tools are not always fit for the fast pace of the digital world we live in. Such tools are often considered to be outdated, slow and burdensome – especially when faced with modern day challenges associated with the cloud." READ MORE

Source: Europol

Date: 18 Apr 2017

Global action tackles distribution of child sexual exploitation images via Whatsapp

"Europol and INTERPOL have supported the Spanish National Police on Operation Tantalio, a complex investigation targeting the distribution of child sexual exploitation material through darknet platforms and Whatsapp. So far 39 suspects were arrested in Europe and South America. Specialists in combating child sexual exploitation from the Spanish National Police, Europol and INTERPOL worked through action days at the headquarters of the Spanish National Police Headquarters on 28-29 March. The arrests and house searches conducted led to the seizure of hundreds of devices containing several terabytes of child sexual exploitation material." READ MORE

Source: INTERPOL

Date: 21 Apr 2017

INTERPOL-led cybercrime operation across ASEAN unites public and private sectors

"An INTERPOL-led operation targeting cybercrime across the ASEAN region has resulted in the identification of nearly 9,000 Command and Control (C2) servers and hundreds of compromised websites, including government portals. The operation, run out of the INTERPOL Global Complex for Innovation (IGCI), brought together investigators from Indonesia, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam to share information on specific cybercrime situations in each country. Additional cyber intelligence was also provided by China." READ MORE

Source: La Nacion

Date: 24 Apr 2017

La Argentina busca adherir a un tratado internacional de lucha contra el cibercrimen

"El Senado acaba de emitir dictamen favorable y la Argentina está, así, un paso más cerca de sumarse a la Convención de Budapest, el primer tratado supranacional sobre delitos informáticos. Este tratado busca estandarizar las legislaciones nacionales y los protocolos y técnicas de investigación para posibilitar e impulsar la cooperación internacional en temas como las estafas informáticas, la distribución de pornografía infantil, las infracciones vinculadas a la propiedad intelectual y los atentados contra la integridad del sistema. […] El proyecto de adhesión -con reserva de los artículos que no sean compatibles con el Código Penal vigente- será votado ahora por el pleno de la Cámara alta. El Ministerio de Justicia de la Nación postula dos motivos principales: la cooperación internacional en materia de delitos informáticos y el establecimiento de protocolos estandarizados para la obtención de pruebas digitales." READ MORE

RELATED ARTICLES

Mondaq, Argentina: Budapest Convention on Cybercrime, 27 Apr 2017

Source: U.S. Department of State

Date: 27 Apr 2017

U.S.-Argentina Partnership on Cyber Policy

"[…] The Governments of the United States and Argentina acknowledge the importance of cyber policy cooperation and express our intent to strengthen our engagement on cyber issues bilaterally, regionally, and globally. […] The U.S. and Argentina further intend to launch an intergovernmental, bilateral Cyber Policy Working Group to facilitate improved cooperation. This group can serve as a policy-level channel for identifying cyber issues of mutual concern and developing joint initiatives." READ MORE

Source: 7sur7

Date: 28 Apr 2017

La Belgique se dote d'un "cyberplan national d'urgence"

"Le Conseil des ministres a donné vendredi son feu vert au tout premier "cyberplan national d'urgence" et avalisé un accord avec l'Otan permettant l'envoi d'équipes spécialisées en cas de cyberattaques. C'est le Centre pour la Cybersécurité Belgique (CCB) qui a élaboré ce cyberplan national d'urgence en collaboration avec le Centre de coordination et de crise du gouvernement, dans le cadre de sa mission de gestion de crise en cas de cyberincident, a expliqué le cabinet du Premier ministre Charles Michel dans un communiqué. Le plan en question prévoit une structure de réponse aux cybercrises et aux cyberincidents qui requièrent une coordination et une gestion au niveau national." READ MORE

RELATED ARTICLES

Belga, Il n'y a jamais eu autant de "cyber-incidents" en Belgique, 28 Apr 2017

Source: TelecomPaper

Date: 27 Apr 2017

Switzerland commissions new 5-year cybersecurity plan

"Switzerland has successfully completed its national cybersecurity plan for the period 2012-2017 and a new plan will be drawn up for the next five years, the Federal Council announced. The first national strategy for the protection of Switzerland against cyber risks (NCS) has completed 15 of its 16 measures, according to the latest annual report adopted by the council. An assessment of the progress to date found that the strategic orientation of the NCS was "correctly selected and the decentralised but closely coordinated implementation of the NCS works well overall", the council said in a statement." READ MORE

Source: Associated Press

Date: 29 Apr 2017

Turkish court formally blocks access to Wikipedia

"In a move that social media users called censorship, a Turkish court on Saturday blocked access to Wikipedia, the free online encyclopedia, enforcing an earlier restriction by Turkey's telecommunications watchdog. The Information and Communication Technologies Authority (BTK) said an Ankara court ordered Saturday that a "protection measure" related to suspected internet crimes be applied to Wikipedia. Such measures are used to block access to pages or entire websites to protect "national security and public order." READ MORE

Source: ESET

Date: 22 Apr 2017

US court hits Russian PoS hacker with record 27 year jail sentence

"For four years, between October 2009 and October 2013, Roman Valeryevich Seleznev hacked into retail POS systems, installing malware that stole payment card details from purchasers, and selling the data to the criminal underworld. Many of the 32-year-old Russian's victims were small businesses[…]. In all, more than 500 American businesses and 3,700 financial institutions are said to have fallen victim to malware planted by Seleznev. Evidence was presented that Seleznev hacks sent stolen credit card data from infected point-of-sale systems to servers under his control." READ MORE

Source: SC Magazine UK

Date: 21 Apr 2017

Kenya set to pass cyber-crime bill as east Africa seeks legal harmony

"The Kenya government is set to pass the Computer and Cybercrime Bill into law after its approval by cabinet as east African countries push for regional harmonisation of cyber-crime laws. The bill is set to be tabled in parliament for debate and then go to a vote within the next few weeks. After that, it is expected to be signed by the president before the end of the year. The Computer and Cybercrime Bill 2016 was approved by the Kenyan cabinet chaired by President Uhuru Kenyatta as part of its ongoing efforts to challenge cyber-crime in the east African community." READ MORE

RELATED ARTICLES

Daily Nation, Hackers stalk Kenyan firms as race to go online peaks, 18 Apr 2017

Source: Bulawayo

Date: 18 Apr 2017

Cyber Bill to be enacted before elections in Zimbabwe

"Consultations around the Cyber Bills are at an advanced stage and the ICT ministry will soon be tabling them before Cabinet, said ICT Minister Mandiwanzira. "We do not want this process to be viewed as an attempt to curtail people's freedoms during the elections period and as such we will seek to conclude the process as soon as possible". Although the Bill, which critics say grants government access into citizens' lives, is viewed with suspicion by many, ICT Minister said people are free to make their contributions before it is taken to Cabinet and eventually Parliament where it will be passed into law." READ MORE

Source: All Africa

Date: 1 May 2017

Rwanda: creating the National Cyber Security Authority is Vital

"Just last week, the Chamber of Deputies passed the draft law establishing the National Cyber Security Authority (NCSA) and determining its responsibilities, organisation and functioning. This stride is in consonance with the implementation of existing national cyber security policy. As well, the Penal Code envisages cybercrimes or computer-related offences though it needs to be reviewed to accommodate the current trend of cybercrime. Once the Bill establishing the National Cyber Security Authority is signed into law, it will generally safeguard private and government information and infrastructure against online crimes and cyber-attacks." READ MORE

Source: IAPS Dialogues

Date: 21 Apr 2017

The Philippines and Cyber Leadership: A Potential Leader

"Despite the nascent state of its cyber security, the recent initiatives by the Philippine government provide a unique opportunity to play an increasingly influential role with respect to domestic and regional cyber security concerns. Its proposal in 2016 for the establishment of a cyber security working group would allow its concerns to be discussed amongst its peers and with other established cyber powers. Closer to home, the establishment of the Department of Information and Communication Technologies (DICT) in conjunction with the draft National Cybersecurity Plan 2022 (NCP 2022) better equips the government to meet the complex demands of this emergent and increasingly crucial domain." READ MORE

Source: Actu24

Date: 26 Apr 2017

L'importance du projet Glacy dans la lutte contre la cybercriminalité au Sénégal

"GLACY est un programme de renforcement des capacités qui vise à renforcer les différentes institutions, judiciaires et des forces d'ordre dans la lutte contre la cybercriminalité et la preuve électronique. Ce renforcement des capacités peut se faire grâce à la formation des juges, procureurs, agents de police, Gendarmerie et autres institutions de police et judiciaires à faire un meilleur usage des principes établis dans la Convention de Budapest. Avec le projet GLACY, le Conseil de l'Europe contribue à l'élaboration ou révision de la législation sur la cybercriminalité, contribue pour aider sur la façon investiguer sur la cybercriminalité et la façon de gérer les éléments de preuve électroniques." READ MORE

Latest reports

- European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, Committee on Civil Liberties Justice and Home Affairs (LIBE), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, April 2017
- Europol – R. Wainwright, F.J. Cilluffo, Responding to Cybercrime at Scale: Operation Avalanche – A Case Study, March 2017
- Center for Cyber Security, The cyber threat against Denmark, February 2017
- National Crime Agency UK, Pathways into Cyber Crime, 21 Apr 2017
- MELANI CH, 24th semi-annual report, 20 Apr 2017
- IBM X-Force, A Magnet for Cybercrime: Financial Services Sector, 27 Apr 2017
- G Data, 8,400 new Android malware samples every day, 27 Apr 2017

Upcoming events

- 2 – 5 May 2017, Minsk, Belarus – Training Programme on International Cooperation, including multinational ISPs, for the Eastern Partnership Region, EAP II/EAP III
- 2 – 5 May 2017, The Hague, the Netherlands – Review meeting of the Empact Dark Web and Virtual Currencies Training at Europol, GLACY+, iPROCEEDS
- 3 – 5 May 2017, Yerevan, Armenia – Workshop on the draft Criminal Procedure Code (cybercrime and electronic evidence) – compliance with the Convention, EAP III
- 10 – 12 May 2017 – Baku, Azerbaijan – Workshop on Law reform to comply with the Budapest Convention, EAP III
- 15 – 16 May 2017, Bucharest, Romania – Brainstorming meeting for the general update of the basic and advanced training materials for judges, prosecutors and public defenders, GLACY+

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime