Cybercrime Digest

Source: Council of Europe

Date: 17 Mar 2017

Ratification by Monaco and signature by San Marino of the Budapest Convention on Cybercrime

"Today, Monaco deposited the instrument of ratification and San Marino signed the Budapest Convention on Cybercrime. With the signature of San Marino, 46 out of 47 Member States of the Council of Europe have either signed or ratified the Budapest Convention. In total, 53 States are now Parties and another 16 States have either signed or been invited to accede. Monaco also deposited the instrument of ratification to the Protocol on Xenophobia and Racism. 29 States are now Party to the Protocol." READ MORE

Source: Presidencia de la República de Costa Rica

Date: 23 Mar 2017

Expertos discuten sobre los retos y oportunidades para Costa Rica en materia de Ciberdelincuencia

"En el marco de la aprobación en primer debate del Convenio Europeo sobre Ciberdelincuencia, representantes del Consejo de Europa y de la Organización de Estados Americanos (OEA), discutieron junto a autoridades locales y expertos nacionales sobre los retos y oportunidades que tiene el país en esta materia. […] El Consejo de Europa y la Organización de Estados Americanos (OEA), se han preocupado por encontrar respuestas conjuntas para enfrentar conductas que la mayoría de las veces no encuentran reacción en los ordenamientos jurídicos latinoamericanos, o se encontraban reguladas en forma insuficiente. La Vicepresidenta de la República, Ana Helena Chacón Echeverría, destacó que "como Gobierno de la República, consideramos que a nuestro país le resulta de especial interés acogerse al Convenio sobre la Ciberdelincuencia." READ MORE

RELATED LINKS

CR Hoy, Experto urge aprobar acuerdo contra delitos informáticos, 21 Mar 2017

A. M. Costa Rica Archives, Cybercrime bill may get final approval, 24 Mar 2017

Source: Voces por la Justicia

Date: 22 Mar 2017

Encuentro sobre delitos informáticos en busca de avances en Argentina

"El ministro de Justicia y Derechos Humanos de la Nación, Germán Garavano, encabezó el "Encuentro con el Consejo de Europa en Materia de Delitos Informáticos". El objetivo fue evaluar acciones conjuntas a fin de conseguir la adhesión de la Argentina al Convenio de Budapest, el único tratado de cooperación internacional vigente sobre delitos informáticos, que ya ha sido ratificado por 52 naciones. El 16 de marzo de este año el presidente de la Nación, Mauricio Macri, envió al Congreso el Proyecto de Ley de Adhesión a la Convención de Budapest." READ MORE

RELATED LINKS

International Association of Privacy Professionals, Argentina's Data Sovereignty Bill, 21 Mar 2017

Ghana to set up national cyber security council

Source: Asempa News

Date: 30 Mar 2017

"The Minister of Communications, Mrs Ursula Owusu-Ekuful, disclosed the government's plan when she addressed the opening of a three-day international workshop on criminal justice statistics on cyber-crime and electronic evidence in Accra yesterday. The workshop is being hosted by the National Communications Authority (NCA), in collaboration with the Council of Europe and the European Union, under the auspices of the Global Action on Cybercrime Extended Project, also konwn as GLACY+. […] Mrs Owusu-Ekuful said the Ministry of Communications would work with the Ministry of Justice and Attorney-General to engage Parliament to ratify the Budapest Convention to facilitate the successful prosecution of cross-border ICT crimes. The Budapest Convention is a global arrangement which prioritises a common criminal policy aimed at protecting countries against cyber-crime by adopting appropriate legislation and fostering international cooperation." READ MORE

RELATED LINKS

Ghana News, Government to allocate funds to fight Cybercrime, 29 Mar 2017

Dutch Parliament Website Hit by Ransomware Attack

Source: SoftPedia

Date: 30 Mar 2017

"According to local publication NL Times, hackers targeted the lower house of the parliament, the Tweede Kamer. Hackers managed to encrypt some files before being stopped. While the parliament spokesperson decided to not reveal anything about the attack, a Dutch parliamentarian tweeted about ransomware hitting the government computer system." READ MORE

U.K. Tells WhatsApp to Open Up to Intelligence Services

Source: Bloomberg

Date: 26 Mar 2017

"U.K. Home Secretary Amber Rudd said Facebook Inc.'s WhatsApp messaging system should open its encryption to security services and urged online companies to be more aggressive in shutting down sites exploited by terrorists. After newspapers disclosed that Khalid Masood, who killed four people in London last week, had used WhatsApp shortly before he began his attack, Rudd identified the company as needing to do more to help fight terrorism." READ MORE

'Turkish' hackers threaten to reset hundreds of millions of iCloud accounts

Source: Motherboard

Date: 22 Mar 2017

"A hacker or group of hackers is apparently trying to extort Apple over alleged access to a large cache of iCloud and other Apple email accounts. The hackers, who identified themselves as 'Turkish Crime Family', demanded $75,000 in Bitcoin or Ethereum, another increasingly popular crypto-currency, or $100,000 worth of iTunes gift cards in exchange for deleting the alleged cache of data. […] According to one of the emails in the accessed account, the hackers claim to have access to over 300 million Apple email accounts, including those use @icloud and @me domains." READ MORE

RELATED ARTICLES

Forbes, Apple Responds to Hacker's Threat to Wipe Hundreds of Millions of iPhones, 22 Mar 2017

Source: Reuters

Date: 17 Mar 2017

G20 to jointly combat cyberattacks against global banks in the wake of Bangladesh Bank hack

"The world's biggest economies will pledge to jointly fight cyber attacks on the global banking system, one of the biggest coordinated efforts yet to protect lenders since an $81 million heist of the Bangladesh central bank's account last year. Meeting in the German resort town of Baden-Baden, G20 finance chiefs will agree to fight attacks regardless of their origin and promise cross-border cooperation to maintain financial stability, according to a draft document seen by Reuters." READ MORE

Source: The Daily Star

Date: 28 Mar 2017

Bangladesh and the Convention on Cybercrime

"[…] Bangladesh has already enacted certain laws to deal with crimes relating to computer and information technology. To combat cybercrimes properly, it needs to have up-to-date laws and legal mechanisms to investigate and prosecute cyber criminals. […] At the international level, the Convention on the Cybercrime, 2003 is the first and still the only convention, which seeks to address internet, and computer related crimes by securing international cooperation among member states and harmonising national laws on cybercrimes and improving investigative techniques. […] Ratifying this Convention will help the country to improve and harmonise the national legislations relating to cybercrimes with the international standard and will facilitate Bangladesh and its authorities to have easy access to international authorities to deal with cybercrimes effectively and confidently." READ MORE

Source: ZD Net

Date: 27 Mar 2017

APAC accounted for majority of botnet detections globally

"Asia-Pacific is proving to be a haven for botnets, accounting for more than half of all detections worldwide, but remains somewhat unscathed from ad fraud, adware, and ransomware. Three countries in the region were among the top five locations for botnet detections, led globally by the Philippines, according to a report by Malwarebytes, which assessed data from nearly 1 billion malware detections between June and November 2016, across some 100 million Windows and Android devices in 200 countries. The report focused on six threat types: ransomware, ad fraud malware, Android malware, botnets, banking Trojans, and adware. Botnet detections in the Philippines were nearly four times more than that in Indonesia, which was ranked second on the global list." READ MORE

Source: Open Gov Asia

Date: 29 Mar 2017

Implementation of New Zealand government's Cyber Security Action Plan

"The New Zealand government has released its first Annual Report on the implementation of Cyber Security Strategy, Action Plan and National Plan to Address Cybercrime, launched in December 2015. […] During 2017, the government will consider the requirements for accession to the Budapest Convention on cybercrime. NZ Police is considering participation in key international cybercrime units such as European Cybercrime Centre within Europol and International Cybercrime Coordination Cell within the FBI." READ MORE

Source: ZD Net

Date: 27 Mar 2017

Developing Papua New Guinea's Cybercrime Policy: Local Contexts, Global Best Practice

"Last August the Papua New Guinean government passed the Cybercrime Act into law. […] Coincidentally, however, the law was introduced at a time when the government faced significant criticism online, raising concerns the act is simply government censorship under the pretence of security. […] Taking the initiative to legislate against cybercrime is an important first step from the PNG government. However, there are areas where PNG can strengthen its approach to cybersecurity. With persistent concerns about censorship hovering over the policy, further definition around certain articles is needed to prevent exploitation and cyber censorship." READ MORE

Source: IT Web Security

Date: 15 Mar 2017

Data breaches remain unreported by South African organisations

"[…] Dr Jabu Mtsweni, research group leader for cyber defence at the CSIR, says the looming legislative change in South Africa is also driving increased cyber-security awareness and culture in the business environment and government. "We see that the cyber crime and cyber security bill recently tabled in Parliament has the potential to stimulate and build a robust cyber-security posture in South Africa. However, these efforts might be hampered by the delays in actually putting the legislation into action." He adds that data breaches and general cyber attacks continue to remain unreported by organisations due to fear of reputational damage and suchlike in SA and that this trend is creating a "false sense of security" and the incorrect perception that SA in not badly affected by cyber attacks." READ MORE

Source: IDG

Date: 29 Mar 2017

Latin America begins to acknowledge the serious threats of cybercrime

"[…] Mexico has been criticised in the past for having a lack of plan in place for dealing with cyber threats. In 2007, Mexico was invited to sign the Budapest Convention on Cybercrime, the world's first international treaty addressing cybercrime, drawn up by the Council of Europe. A number of non-European countries have been invited to do so since it was inaugurated in 2001. Ten years on, Mexico has yet to sign or ratify the agreement. Reasons for this include Mexico's legislative process being unable to adhere to the provisions. Other Latin American nations that have yet to sign the Convention include Argentina, Chile, Colombia, Paraguay, and Peru." READ MORE

Source: Malware Bytes

Date: 23 Mar 2017

Saudi Arabia hit with cyberespionage spearphishing campaign

"A new spear phishing campaign is targeting Saudi Arabia governmental organizations. The attack originates from a phishing email containing a Word document in Arabic language. If the victim opens it up, it will not only infect their system but send the same phishing document to other contacts via their Outlook inbox. At least a dozen Saudi agencies were targeted. This email-borne attack leverages social engineering to trick users into executing code via a Macro." READ MORE

Latest reports

- The National Security Podcast, Cyberspace -- Breaking down the impact it has on your data and your safety, Mar 2017
- UNODC, Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime, Annotated Provisional Agenda, Mar 2017
- European Payments Council, 2016 Payment Threats Trends Report, 20 Mar 2017
- FFA UK, Financial fraud data for 2016, 30 Mar 2017
- Nokia, Threat Intelligence Report – 2H 2016, 27 Mar 2017
- Kaspersky, The cost of launching a DDoS attack, 23 Mar 2017
- Genalto, 2016 Breach Live Index, Mar 2017
- A. Osula, Remote search and seizure of extraterritorial data in Estonia, Mar 2017

Upcoming events

- 31 March – 2 April, Colombo, Sri Lanka - Introductory Judicial training on cybercrime and electronic evidence for prosecutors, GLACY+
- 3-4 April, Ankara, Turkey - Workshop on inter-agency and international cooperation for search, seizure and confiscation of online crime proceeds, iPROCEEDS
- 3-6 April, Chisinau, Moldova - Training for judges, prosecutors and investigators on presentation and handling of electronic evidence, EAP II/III
- 3-7 April, Accra, Ghana - Introductory ToT on cybercrime and electronic evidence for judges and prosecutors and adaptation of materials to the local context, GLACY+
- 5-7 April, Bridgetown, Barbados - Participation in INTERPOL's 3rd Americas Working Group on Cybercrime for Heads of Units, GLACY+
- 6-7 April, Kyiv, Ukraine - Workshop on Law reform around the topics of cybercrime procedures and public-private cooperation, EAP III
- 10 April, Belgrade, Serbia - Meeting to support existing public/private initiatives or establish such mechanisms at domestic level, iPROCEEDS
- 10-13 April, Vienna, Austria - Participation in the 3rd meeting of the UN Intergovernmental Expert Group on Cybercrime, GLACY+ / iPROCEEDS / EAP II
- 10-13 April, Kyiv, Ukraine - Training of judicial, prosecutorial and investigative authorities on the use of tools for executing requests under the Budapest Convention, EAP II/III

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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime