Cybercrime Digest

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

1-15 November 2018

Source: France Diplomatie

Date: 12 Nov 2018

Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace

"On 12 November at the UNESCO Internet Governance Forum (IGF), President Emmanuel Macron launched the Paris Call for Trust and Security in Cyberspace. This high-level declaration on developing common principles for securing cyberspace has already received the backing of many States, as well as private companies and civil society organizations. […] In order to respect people's rights and protect them online as they do in the physical world, States must work together, but also collaborate with private-sector partners, the world of research and civil society. "[...] We recognize that the threat of cyber criminality requires more effort to improve the security of the products we use, to strengthen our defenses against criminals and to promote cooperation among all stakeholders, within and across national borders, and that the Budapest Convention on Cybercrime is a key tool in this regard. [...]"." More than 50 States, 90 NGOs and academia and 130 corporations and groups have endorsed the Paris Call. READ MORE [French Version]

RELATED ARTICLES

France Diplomatie, Paris Call for Trust and Security in Cyberspace, 12 Nov 2018

List of Supporters of the Paris Call for Trust and Security in Cyberspace, 12 Nov 2018

Source: United Nations General Assembly

Date: 13 Nov 2018

United Nations, Third Committee Approves 11 Drafts amid Heated Debate over Death Penalty Moratorium, Use of Mercenaries, Efforts to End Cybercrime

"[…] The Committee considered a draft resolution titled, "Countering the use of information and communications technologies for criminal purposes". The representative of the Russian Federation, introducing the draft, said it addresses a contemporary global threat. As no substantive discussions on cybercrime were under way, this initiative would create such an opportunity and he suggested that the Russian Federation could host the first discussion on preventing cybercrime during the Assembly's seventy-fourth session. […] The representative of United States expressed profound disappointment that the Russian Federation is pressing forward with its initiative and paying lip service to building consensus. This draft resolution has a singular clear objective of politicizing the topic and undermining the ability of law enforcement. There is no consensus around a new cyber treaty. Drawing attention to a cyberattack by the Russian Federation, she wondered why delegates would "put the fox in charge of the henhouse" and said the United States would vote "no" on the draft resolution. […] The Committee then approved the draft resolution." READ MORE

RELATED ARTICLES

Council on Foreign Relations, The UN Doubles Its Workload on Cyber Norms, And Not Everyone Is Pleased, 15 Nov 2018

Source: European Union Agency for Fundamental Rights

Date: 12 Nov 2018

Towards a legal handbook on cybercrime and fundamental rights

"The EU Fundamental Rights Agency and the Council of Europe are jointly organising a cybercrime experts meeting in Bucharest that will take place from 15 to 16 November. EU Agencies such as Europol, Eurojust, as well as the Council of Europe's cybercrime division and other relevant experts will define the scope and features of a future handbook on European law relating to cybercrime and fundamental rights that has been requested by the European Parliament. […] The handbook should be available in the second half of 2020, first in English then in other EU languages." READ MORE

Source: Seneweb

Date: 13 Nov 2018

Sénégal, es magistrats à l'école de cybercriminalité et la preuve électronique

"La deuxième formation judiciaire régionale sur la cybercriminalité et la preuve électronique pour les pays de la Cedeao et la Mauritanie a démarré, ce lundi, à Dakar. Elle est organisée par le Conseil de l'Europe dans le cadre du projet Glacy+ et en coopération avec le Bureau des télécommunications et des technologies de l'information de la Cedeao. Cette formation judiciaire avancée regroupe des magistrats en provenance du Bénin, du Burkina Faso, de Cabo Verde, de Côte d'Ivoire, de Guinée, de Guinée Bissau, du Mali, du Sénégal, du Togo et de la Mauritanie. Cette semaine, les bénéficiaires vont approfondir leurs connaissances acquises tout en les exercer travers des exemples pratiques. […] Au total, des magistrats formés par les deux cours seront de 60 personnes. La cérémonie d'ouverture de cette formation est présidée par le ministre de la Justice, Ismaïla Madior Fall." READ MORE

RELATED ARTICLES

France 24, À Dakar, une école pour renforcer la lutte contre la cybercriminalité en Afrique, 7 Nov 2018

Source: Daily FT

Date: 8 Nov 2018

Sri Lanka, AG stresses on importance of cyber security for socio-economic growth

"Attorney General Jayantha Jayasuriya PC yesterday said successfully facing the growing cybersecurity challenge is key to safeguarding socioeconomic prosperity in the country. The importance of cybersecurity, challenges towards it and some of the measures taken so far were highlighted by Jayasuriya in his address after inaugurating the 11th National Cyber Security Week 2019 organised by SL-CERT and ICTA […]. He said the value of global cyber security incidents in 2015 was $ 590 billion and estimated to be $ 2.1 trillion, a fourfold increase. […] In that context he commended the SL-CERT (Computer Emergency Readiness Team) for its pioneering initiative in enhancing awareness of cyber security in the country as part of its core role of being the focal point for cybersecurity in Sri Lanka. […] He said following the enactment of the Computer Crime Act in 2007, based on the Budapest Cyber Crime Convention, the ICTA and SLCERT worked very closely and tirelessly for eight years to make Sri Lankathe first country in South Asia in the Budapest Convention in 2016. Being a State party to the Budapest Convention, Sri Lanka has created legal and policy framework to meet the challenges associated with cybercrime, he added." READ MORE

Source: Institut Supérieur de la Magistrature de Tunisie

Date: 14 Nov 2018

Tunisie, formation judiciaire en matière de cybercriminalité et preuve électronique

"L'Institut Supérieur de la Magistrature de Tunisie a organisé du 12 au 14 novembre 2018 une session de formation au profit de 24 magistrats des différents tribunaux de la république sur le sujet « la cybercriminalité et la preuve électronique ». Les magistrats participants bénéficieront au début de l'année 2019 d'une deuxième session plus approfondie sur le même sujet. Cette session est l'une des différentes activités programmées dans le cadre du projet Cyber-Sud qui est un projet conjoint de l'Union européenne et du Conseil de l'Europe. Le projet contribue à la prévention et au contrôle de la cybercriminalité et d'autres infractions impliquant la preuve électronique, en conformité aux normes internationales de protection des droits de l'homme et au respect de l'État de droit ainsi qu'aux bonnes pratiques. Ce projet concerne outre la Tunisie, l'Algérie, la Jordanie, le Liban et le Maroc." READ MORE

Source: ENISA

Date: 7 Nov 2018

EU cybersecurity organisations agree on 2019 roadmap

"On 6 November 2018, following a meeting at working level, the four Principals of the Memorandum of Understanding between ENISA, the European Defence Agency (EDA), Europol and the CERT-EU, met at CERT-EU's premises. The purpose of the meeting was to update each other on relevant developments and assess the progress made under the MoU […] and to agree on a roadmap for 2019. The initial focus will be on working closer in the areas of training and cyber exercises, building the cooperation capacity and improve the exchange of information on respective projects." READ MORE

Source: Europol

Date: 9 Nov 2018

Europol and Eurojust strive to improve access to cross-border electronic evidence.

"The SIRIUS conference 2018 took place on 6-7 November at Europol's headquarters in The Hague. This two-day event gathered over 200 judicial and law enforcement authorities from 40 countries, as well as representatives from Airbnb, Apple, Facebook, Google and PayPal, to address issues and challenges encountered when conducting Internet-based investigations. […] SIRIUS is an innovative project that includes an interactive knowledge-sharing platform accessible to judicial and law enforcement authorities, and aims to produce and disseminate trainings and digests to improve EU-US cooperation in cross-border access to electronic evidence." READ MORE

Source: The Irish TImes

Date: 1 Nov 2018

Brexit 'will not impact' UK-EU co-operation on cybersecurity

"Brexit will not have an impact on the levels of co-operation between the UK and the EU on cybersecurity, according to the head of Britain's National Cyber Security Centre. "This is the ultimate global issue, this is an issue that transcends borders," said the centre's chief executive, Ciaran Martin. "In terms of post an EU exit, we've clear instruction from the cabinet to cooperate unconditionally on European security. We're leading the way on things like electoral security in Europe […], and if you look pragmatically at cybersecurity as an issue very little of what we can do at the National Cyber Security centre is dependent on EU competences and EU law." READ MORE

Source: Dawn

Date: 6 Nov 2018

'Almost all' Pakistani banks hacked in security breach, says FIA cybercrime head

"In a shocking revelation, the head of the Federal Investigation Agency's (FIA) cybercrime wing has said data from "almost all" Pakistani banks was stolen in a recent security breach". According to a recent report we have received, data from almost all Pakistani banks has been reportedly hacked," FIA Cybercrimes Director retired Capt Mohammad Shoaib told Geo News on Tuesday. When pressed to clarify, the official said data from "most of the banks" operating in the country had been compromised. Speaking to DawnNewsTV, Shoaib said hackers based outside Pakistan had breached the security systems of several local banks. "The hackers have stolen large amounts of money from people's accounts," he added. […] He said the FIA has written to all banks, and a meeting of the banks' heads and security managements is being called. The meeting will look into ways the security infrastructure of banks can be bolstered. […] It wasn't immediately clear when exactly the security breach took place. According to Shoaib, more than 100 cases are being investigated by the agency in connection with the breach." READ MORE

Source: Ministerio del Interior y Seguridad Pùblica

Date: 13 Nov 2018

Chile, Vicepresidente asiste a inicio del debate de nueva Ley de Delitos Informáticos

"El Delegado Presidencial de Ciberseguridad, Jorge Atton, expuso a los senadores de la Comisión de Seguridad Pública los principales aspectos de la normativa propuesta para poner a Chile a la vanguardia en la persecución de acciones delictuales en el espacio digital. "Tenemos que tener una capacidad igual o mayor para anticiparnos a esos ataques", sentenció el Presidente de la República al firmar el proyecto de Ley de Delitos Informáticos el pasado 25 de octubre. El debate de la iniciativa comenzó este martes en el Senado, por lo que el Vicepresidente Andrés Chadwick asistió a la exposición realizada por el Delegado Presidencial para la Ciberseguridad, Jorge Atton. Con la tramitación de esta normativa se da cumplimiento a las disposiciones de la Política Nacional de Ciberseguridad (2017-2022), que cuenta entre sus medidas con "la actualización de nuestra legislación en materia de delitos informáticos"." READ MORE

Source: The Sydney Morning Herald

Date: 6 Nov 2018

Twitter suspends 1.2 million accounts for terrorism in two years

"Social media giant Twitter suspended 1,210,357 accounts for promoting terrorism between August 2015 and the end of 2017. […] The suspensions represent just a fraction of the website's active user base – about 330 million at the start of 2018. […] Australia's Home Affairs Minister Peter Dutton, who attended the meeting, said the "incredible" number highlighted just how much more work social media companies had to do to combat terrorism. […] "Those companies also have a specific obligation - to engage with and assist law enforcement organisations - particularly where encrypted messages or services are being used to carry messages conveyed and used in the planning of a terrorist attack or other serious criminal enterprise"." READ MORE

RELATED ARTICLES

Reuters, Twitter deletes over 10,000 accounts that sought to discourage U.S. voting, 8 Nov 2018

Source: El Espectador

Date: 2 Nov 2018

¿Puede un "hacker" dejar sin luz a Colombia?

"Según un informe presentado por la también empresa de seguridad informática Kaspersky Lab, dentro de sus registros de ataques a sistemas de control industrial, es decir, los computadores presentes en las infraestructuras críticas, América Latina es la sexta región que más registra eventos en esta materia. Cerca del 46 % de todos los equipos reportaron por lo menos una de estas amenazas durante el primer semestre de 2018. "Lo importante es empezar a hablar de estos temas, porque cada quien puede decir que fueron casos que pasaron en Ucrania y Polonia, y que no van a llegar al país. En la región, de a poco se ha empezado a trabajar. Con el Convenio de Budapest se busca que los países que se adhieran al mismo puedan empezar a tener una infraestructura de ciberseguridad para prevenir estos ataques", afirmó Camilo Gutiérrez, jefe de laboratorio de investigación de ESET Latinoamérica. " READ MORE

Source: ZD Net

Date: 2 Nov 2018

Giant ransomware bundle threatens to make malware attacks easier for crooks

"Some of the most potent forms of ransomware of 2018 are being offered for sale in a cut-price bundle deal on the dark web that also contains one of the most dangerous forms of file-encrypting malware to terrorise organisations this year. SamSam is part of the 23 ransomware bundle -- significant because previously it's only been deployed by a highly specialised group. Other well-known forms of ransomware available in the $750 '2018 ransomware pack' include Magniber, Satan, CryBrazil, XiaoBa, and more. The pack has been uncovered by researchers at cyber security firm Sixgill who describe it as an "extraordinarily rare finding"." READ MORE

Source: Reuters

Date: 2 Nov 2018

Vietnam releases cybersecurity draft decree

"Vietnam on Friday released a long-waited draft decree on guidelines to implement a cybersecurity law that global technology companies and rights groups have said could undermine development and stifle innovation. The draft required firms providing a range of services, including email or social media, to set up offices in Vietnam if they collect or analyze data, let their users conduct anti-state actions or cyber attack, and if they fail to remove content deemed anti-state, fake, slandering or inciting violence. Facebook and Google, both of which are widely used in Vietnam and serve as the main platforms for dissidents, do not have local offices or local data storage facilities and have pushed back on the localization requirements. Legislators approved the law in June, overriding strong objections from tech companies, rights groups and Western governments including the United States." READ MORE

Latest reports

- ICMEC, Studies in Child Protection: Sexual Extortion and Non Consensual Pornography, October 2018
- Global Commission on the Stability of Cyberspace, Norm Package Singapore, 8 Nov 2018
- Access Now, Human Rights in the age of Artificial Intelligence, November 2018
- World Economic Forum, Regional Risks for Doing Business 2018, November 2018

Upcoming events

- 14-16 November, Colombo, Sri Lanka - In Country workshops on data protection and INTERPOL, GLACY+
- 15 November 2018, Beirut, Lebanon – Round table on cybersecurity, CyberSouth
- 16 November 2018, Beirut, Lebanon – Awareness meeting on Budapest Convention, CyberSouth
- 15-16 November, Bucharest, Romania - Human Rights Workshop with the Fundamental Rights Agency, GLACY+
- 18 November 2018, Amman, Jordan – Awareness meeting on Budapest Convention vs gap analysis, CyberSouth
- 19 – 20 November 2018, Tunis, Tunisia – Study visit to DGST and garde nationale, CyberSouth
- 19 – 21 November, Port Louis, Mauritius - In Country workshops on data protection, GLACY+
- 19 – 22 November 2018, Amman, Jordan – Basic Judicial Training, CyberSouth
- 19 – 23 November, Manila, Philippines - Regional delivery of Introductory Course on cybercrime and electronic evidence for Judges and prosecutors, GLACY+
- 20 – 22 November 2018, Tbilisi, Georgia – Cybersecurity Capacity Maturity Model for Nations (CMM), Cybercrime@EAP2018
- 21 – 24 November, Ankara, Turkey - Second Delivery of the Introductory Training Module on Cybercrime, Electronic, Evidence and Online Crime Proceeds, iPROCEEDS
- 26 November 2018, Strasbourg, France – Steering committee, CyberSouth
- 27 – 29 November 2018, Strasbourg, France – 20th Plenary Meeting of the Cybercrime Convention Committee, Cybercrime@EAP2018
- 27-30 November, Strasbourg, France - Participation in the T-CY20, Protocol Drafting Plenary & GLACY+ Steering Committee, iPROCEEDS, GLACY+, Cybercrime@EAP2018, CyberSouth
- 29 November 2018, Beirut, Lebanon – Anti-Cybercrime Forum, CyberSouth

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