Cybercrime Digest

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

16-31 July 2020

Source: European Commission

Date: 24 Jul 2020

EU Security Union Strategy: connecting the dots in a new security ecosystem

"Today, the European Commission sets out a new EU Security Union Strategy for the period 2020 to 2025, focusing on priority areas where the EU can bring value to support Member States in fostering security for all those living in Europe. From combatting terrorism and organised crime, to preventing and detecting hybrid threats and increasing the resilience of our critical infrastructure, to promoting cybersecurity and fostering research and innovation, the strategy lays out the tools and measures to be developed over the next 5 years to ensure security in our physical and digital environment. [...] Cybercrime is a global challenge where effective international cooperation is necessary. The EU supports the Council of Europe's Budapest Convention on cybercrime, which is an effective, well-established framework that allows all countries to identify what systems and communication channels they need to put in place to be able to work effectively with each other." READ MORE

RELATED ARTICLES

European Commission, Communication on the EU Security Union Strategy, 24 Jul 2020

European Commission, Delivering on a Security Union: initiatives to fight child sexual abuse, drugs and illegal firearms, 24 Jul 2020

Source: Council of the European Union

Date: 30 Jul 2020

EU imposes the first ever sanctions against cyber-attacks

"The Council today decided to impose restrictive measures against six individuals and three entities responsible for or involved in various cyber-attacks. These include the attempted cyber-attack against the OPCW (Organisation for the Prohibition of Chemical Weapons) and those publicly known as 'WannaCry', 'NotPetya', and 'Operation Cloud Hopper'. The sanctions imposed include a travel ban and an asset freeze. In addition, EU persons and entities are forbidden from making funds available to those listed. Sanctions are one of the options available in the EU's cyber diplomacy toolbox to prevent, deter and respond to malicious cyber activities directed against the EU or its member states, and today is the first time the EU has used this tool." READ MORE

Source: Council of Europe

Date: 22 Jul 2020

C-PROC Webinars conclude the first batch with EU/CoE series on cybercrime for LATAM and the Caribbean

The first batch of C-PROC cybercrime webinars ended with two sessions dedicated to the Latin American and Caribbean Regions on 20 and 22 July 2020, organized by the EU Cyber Direct and the GLACY+ Projects in the framework of the joint EU/ CoE initiative "Cybercrime and Criminal Justice in the Cyberspace". Such webinars were aimed at facilitating the sharing of experience between criminal justice practitioners, who are to be the beneficiaries of a future UN treaty on cybercrime, and foreign policy experts, who will be involved in the negotiation of this treaty. Additional information, including presentations and recordings, can be retrieved on the dedicated website. New webinars will be organized after the summer break. READ MORE

Source: Council of Europe

Date: 17 Jul 2020

New series of online meetings was launched by the Council of Europe, CARICOM IMPACS and the U.S. Department of Justice

"The first of a series of activities organized by the Caribbean Community Implementation Agency for Crime and Security (CARICOM IMPACS) and the Council of Europe's Octopus Project on Cybercrime, together with the US Department of Justice, took place online between 16-17 July 2020. The activity is part of a programme of meetings and workshops that will happen between July 2020 and March 2021 and it is addressed to authorities responsible for cybercrime legislation (such as Ministries of Justice, Interior or Telecommunications, Attorney General's Offices, or Parliaments) from CARICOM Members States: Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Grenada, Guyana, Haiti, Jamaica, Montserrat, Saint Lucia, St Kitts and Nevis, St Vincent and the Grenadines, Suriname, Trinidad and Tobago. The aim of this programme is to have an assessment of legislation in place and to make recommendations for further reform of domestic legislations on cybercrime and electronic evidence in CARICOM Member States. The assessments, as well as the recommendations, together with the experience shared and knowledge gained should permit authorities in charge to pursue the further strengthening of their legislation. This should furthermore permit States of the region to assess the option of accession to the Budapest Convention on Cybercrime." READ MORE

RELATED ARICLES

Antigua Observer, RSS boss calls for region to harmonise cybercrime laws, 29 Jul 2020

Source: Council of Europe

Date: 29 Jul 2020

CyberSouth: Regional workshop on legislation and international cooperation in cybercrime and electronic evidence

"CyberSouth project organised a regional online workshop on legislation and international cooperation in cybercrime and electronic evidence, on the 29th of July 2020. The event gathered around 60 participants from the Ministry of Justice, International legal departments, Public Ministry and Police forces of priority countries as well as experts from France and the United States of America. The aim of this regional workshop was to introduce to the countries the international standards on cybercrime legislation and legal instruments for international cooperation and assess whether their legislation is in line. The workshop was also an opportunity for the countries to present their legislative tools and procedures for conducting cybercrime investigations, collection of e-evidence and best practices on the international cooperation." READ MORE

Source: Europol

Date: 27 Jul 2020

No More Ransom: how 4 millions victims of ransomware have fought back against hackers

"While the world is in the grip of a coronavirus outbreak, another virus is quietly wreaking havoc. Although this virus has been around for years, its cases have been rising alarmingly in the past few months and has brought critical activities such as hospitals and governments to a standstill. This virus is ransomware, but a free scheme called No More Ransom is helping victims fight back without paying the hackers. Celebrating its fourth anniversary this month, the No More Ransom decryption tool repository has registered since its launch over 4.2 million visitors from 188 countries and has stopped an estimated $ 632 million in ransom demands from ending up in criminals' pockets. […] You can consult all the key figures in our dedicated infographic." READ MORE

Source: Afrique IT News

Date: 17 Jul 2020

Le Burkina Faso et le Bénin s'arment face à la cybercriminalité

"Débuté le 15 juillet, un atelier de formation sur la protection des données voit en ce moment la participation d'une soixantaine de cadres béninois et burkinabés. Ce sont des experts en cybercriminalité, fonctionnaires de police et magistrats réunis jusqu'au 17 juillet autour de la thématique. L'atelier s'inscrit dans le cadre du projet « Action Globale sur la Cybercriminalité Elargie » de l'Union européenne et du Conseil de l'Europe. Ce projet vise le renforcement des capacités des Etats à travers le monde à mettre en application les lois sur la cybercriminalité et les preuves électroniques. Il a également pour but de favoriser la coopération internationale sur ces questions." READ MORE

RELATED ARICLES

Gouvernement de la République du Benin, Lutte contre la cybercriminalité au Bénin : L'ANSSI renforce les capacités des acteurs de la chaîne judiciaire, 16 Jul 2020

Source: 24 Heurs au Benin

Date: 30 Jul 2020

Bénin: La Convention sur la cybercriminalité transmise au parlement

"Le gouvernement a décidé ce mercredi 29 juillet 2020 en Conseil des ministres, de la transmission à l'Assemblée nationale pour autorisation de ratification, de la Convention sur la cybercriminalité adoptée à Budapest en Hongrie, le 23 novembre 2001, et de son protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, adopté à Strasbourg en France, le 28 janvier 2003. Selon le Conseil des ministres, cette convention vise à harmoniser les éléments d'infraction ayant trait au droit pénal matériel national et les dispositions connexes en matière de cybercriminalité ; à fournir au droit pénal procédural national, les pouvoirs nécessaires à l'instruction et à la poursuite d'infractions de cette nature ainsi que d'autres infractions commises au moyen d'un système informatique ou dans le cadre desquelles des preuves existent sous forme électronique ; et à mettre en place un régime rapide et efficace de coopération internationale." READ MORE

Source: Ministère des postes, télécommunications et économique numérique du Congo

Date: 29 Jul 2020

Cybercriminalité : Vers la conformité de la législation congolaise aux conventions de Budapest et de Malabo

"La question de la conformité du cadre juridique sur la cybercriminalité de la République du Congo au regard de la Convention de Budapest du Conseil de l'Europe sur la cybercriminalité et de la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo), a figuré au cœur de l'atelier tripartite de restitution, entre le gouvernement congolais et l'Union Européenne et Conseil de l'Europe en charge en la matière, tenu par visioconférence, ce mercredi 29 juillet 2020, à Brazzaville. Le gouvernement congolais a été représenté à cette rencontre par les ministres Léon Juste Ibombo, des postes, télécommunications et économique numérique et Aimé Wilfrid Bininga, de la justice, des droits humains et de la protection des peuples autochtones." READ MORE

RELATED ARTICLES

Agence d'Information d'Afrique Centrale, Cybercriminalité : le Congo veut adapter sa législation aux normes internationales, 29 Jul 2020

Source: Council of Europe

Date: July 2020

CyberEast Interview: On Gender Misbalance in the Field of Cybercrime and Cybersecurity and the Work of the CERT-GOV-MD in Moldova

"The human factors remain the key issue in cybersecurity around the world. From an increasingly complex landscape, cybersecurity has always boiled down to the people, the process and the technology – three elements that we are putting together to maintain a cybersecure environment. We are not implementing only technology, but we are addressing the human element as well. In the end, I think the ultimate determinant of success in cybersecurity is the implementation of the right process, which is the bridge between people and technology. […] Now tech and cybersecurity is the place to be. So why does it seem as if women, who make up 51 percent of the world's population, cannot manage to break into the most exciting field of human endeavour on the planet today? I must admit there is a community of women in cyber; however, we are failing to bring more women into cybersecurity in the first place and unfortunately the number of women in cybersecurity is dropping every year." READ MORE

Source: Presidencia da Republica do Brasil

Date: 24 Jul 2020

Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética

"O Brasil foi convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética em dezembro de 2019. O convite terá validade por três anos. A adesão proporcionará às autoridades brasileiras acesso mais ágil a provas eletrônicas sob jurisdição estrangeira, além de tornar a cooperação jurídica internacional voltada à perseguição penal dos crimes cibernéticos mais efetiva. Nesta semana, foi enviado ao Congresso Nacional texto da Convenção com fins de adesão brasileira ao instrumento." READ MORE

Source: EU Neighbours

Date: 28 Jul 2020

Tunisia : EU-funded CyberSouth helps develop course on cybercrime and electronic evidence for magistrates

"The working group in charge of developing the basic course on cybercrime and electronic evidence dedicated to magistrates held its second online meeting on 15-16 July. The event took place in the framework of the EU-funded CyberSouth project and with the support of the Council of Europe. The Tunisian delegates have worked together with the international expert to align the national requirements with the international standards on cybercrime and e-evidence." READ MORE

Source: Daily Observer

Date: 16 Jul 2020

Liberia, Gov't to Get First Cyber Crime Forensic Lab

"After several months of negotiation and participation in several workshops and conferences by technicians from the government through the Ministry of Posts and Telecommunications (MOPT), the EU and ECOWAS have finally agreed to set up a Cyber Crime Forensic Lab in Liberia. Computer or cyber forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it." READ MORE

Source: U.S. Department of Justice

Date: 22 Jul 2020

Man Admits Operating Unlicensed ATM Network that Laundered Millions of Dollars of Bitcoin and Cash for Criminals' Benefit

"A Yorba Linda man has agreed to plead guilty to federal criminal charges that he operated an illegal virtual-currency money services business that exchanged up to $25 million – including on behalf of criminals – through in-person transactions and a network of Bitcoin ATM-type kiosks. […] Using the moniker "Superman29," Mohammad advertised his business online to buy and sell Bitcoin throughout Southern California, in transactions up to $25,000. In a typical transaction, he met clients at a public location and exchanged currency for them. Mohammad generally did not inquire as to the source of the clients' funds and on many occasions he knew the funds were the proceeds of criminal activity. Mohammad admitted that he knew at least one Herocoin client was engaged in illegal activity on the dark web." READ MORE

Source: Bleeping Computer

Date: 24 Jul 2020

Garmin outage caused by confirmed WastedLocker ransomware attack

"Wearable device maker Garmin shut down some of its connected services and call centers on Thursday following what the company called a worldwide outage, now confirmed to be caused by a WastedLocker ransomware attack. […] While Garmin didn't mention it in their outage alert, multiple flyGarmin services used by aircraft pilots are also down, including the flyGarmin website and mobile app, Connext Services (weather, CMC, and position reports) and Garmin Pilot Apps (Flight plan filing unless connected to FltPlan, account syncing, and database concierge)." READ MORE

Source: Observatorio GUatemalteco de Delitos Informaticos

Date: 22 Jul 2020

Guatemala, grupo de hacktivistas efectuan ciberataques a instituciones nacionales

"El grupo portugués CyberTeam , en asociación con el perfil despiadado de Angelic , llevó a cabo ataques contra objetivos de alto perfil en Portugal y Guatemala. Todos los ataques tenían una connotación hacktivista, acompañada de mensajes a las autoridades públicas de ambos países. Es una demostración de compromiso entre grupos con diferentes orígenes y perfiles, pero con convergencia ideológica. Por medio de un video difundido en su canal en youtube, anonymousGt manifiesta su malestar por una serie de situaciones que afectan al País bajo la pandemia que vivimos y la crisis social que esta afectando a los guatemaltecos." READ MORE

Source: The Cyber Peace Institute

Date: 14 Jul 2020

Hackers Trick Humanitarian Non-profit into Big Wire Transfers

"Organizations working to defend fundamental human rights and freedoms are among the most vulnerable to cyberattacks. The attacks not only impact the targeted entity, but the vulnerable communities that they serve. When these organizations suffer financial loss or a data breach as a result of a cyberattack, the organization must divert resources to address the attack — meaning that they may be unable to provide critical services and protection to the regular citizens affected by violence or armed conflicts, or whose livelihoods depend on these organizations. Even more, these organizations may hold highly sensitive data related to the communities they serve; a breach of this data may itself put lives directly at risk." READ MORE

Latest reports

- Council of Europe, Cybercrime and COVID19 webpage, updated weekly
- European Data Protection Board, Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 24 Jul 2020
- UNODC, Sixth session of the Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime, Statements, presentations and supporting documents, 29 Jul 2020
- European Union, Council of Europe, Cybercrime and Criminal Justice in Cyberspace - Latin American and Caribbean Region – Video Recording, 20 Jul 2020
- European Parliament Think Tank, Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights, 15 Jul 2020
- Banco Interamericano de Desarrollo, Organización de los Estados Americanos, Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe, July 2020
- Europol, Online Jihadist Propaganda: 2019 in Review, 28 Jul 2020
- Lawful evidence cOllecting & Continuity plAtfoRm Development (LOCARD) Project, Public Deliverables, updated in July 2020
- ENISA, A billion user hours lost in EU telecoms due to security incidents in 2019, 23 Jul 2020
- ENISA, ENISA Strategy - A Trusted and Cyber Secure Europe, 17 Jul 2020
- LUISS University, The persistence of Online Black-Markets: an investigation on the generativity of digital infrastructures operating under adverse conditions, 13 Jul 2020
- India Corporate Law, Section 65B of the Indian Evidence Act, 1872: Requirements for admissibility of electronic evidence revisited by the Supreme Court, 27 Jul 2020

Upcoming events

Due to the COVID-19 pandemic outbreak and the countermeasures applied by most of the countries worldwide, in-country activities of the C-PROC capacity building initiatives foreseen in the month of August have been rescheduled to a later date.

- 3-5 August, First meeting of adaptation of the Judicial Training Manual into national Lebanese curricula, CyberSouth
- 7 August, Desk Study, Review of cybercrime legislation for Papua New Guinea, GLACY+
- By 15 August, Desk Study: Judicial Training Systems and Capabilities, CyberSouth
- By 15 August, Desk Study: Report with recommendations for priority countries on financial investigations for online crime proceeds, CyberSouth
- By 15 August, Desk research: Assessment of compliance of procedural law frameworks in line with Articles 16 to 21 Budapest Convention and related legislation (including data protection), Bosnia and Herzegovina iPROCEEDS-2
- By 15 August, Desk Study, INTERPOL, Guide for Developing Cybercrime and E-evidence Training Strategy for Law Enforcement, GLACY+
- By 15 August, Desk Research: C-PROC, Desk research: Assessment of compliance of procedural law frameworks in line with Articles 16 to 21 Budapest Convention and related legislation (including data protection), Turkey iPROCEEDS-2
- By 15 August, Support participation in long-distance specialised master programme (nomination and selection of candidates) iPROCEEDS-2