Cybercrime Digest

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

16 – 31 December 2020

Source: European Commission

Date: 16 Dec 2020

The EU's Cybersecurity Strategy for the Digital Decade

"The EU continues to support third countries that wish to accede to the Council of Europe Budapest Convention on Cybercrime, and work to finalise the Second Additional Protocol to the Budapest Convention that includes measures and safeguards to improve international cooperation between law enforcement and judicial authorities, as well as between authorities and service providers in other countries, and for which the Commission participates in the negotiations on behalf of the EU. The current initiative for a new legal instrument on cybercrime at UN level risks to amplify divisions and slow down much needed national reforms and related capacity building efforts, potentially hindering effective international cooperation against cybercrime: the EU does not see a need for any new legal instrument on cybercrime at UN level. The EU continues to engage in the multilateral exchanges on cybercrime to ensure the respect of human rights and fundamental freedoms, through inclusiveness, transparency, and taking into account available expertise, with the goal of delivering added value for all." READ MORE

RELATED ARTICLES

European Commission, New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient, 16 Dec 2020

European Commission, Proposal for directive on measures for high common level of cybersecurity across the Union (NIS2 Directive), 16 December 2020

Source: Europol

Date:18 Dec 2020

Europol and the European Commission inaugurate new decryption platform for law enforcement investigations

"This week Europol launched an innovative decryption platform, developed in close cooperation with the European Commission's Joint Research Centre. It will significantly increase Europol's capability to decrypt information lawfully obtained in criminal investigations. The launch of the new decryption platform marks a milestone in the fight against organised crime and terrorism in Europe. In full respect of fundamental rights and without limiting or weakening encryption, this initiative will be available to national law enforcement authorities of all Member States to help keep societies and citizens safe and secure." READ MORE

Source: Council of Europe

Date: 17 Dec 2020

CyberEast: Webinar on Cybersecurity and Human Rights

"Bringing together experts from Croatia, Estonia and Germany, the Webinar explored the issues of necessary regulation for human rights in cyberspace, finding the right balance by linking to practice under Article 15 of the Budapest Convention on Cybercrime, and the role of private entities in ensuring these rights and freedoms. Impact of COVID-19 on the situation with safeguards and guarantees was another highlight of discussions during the event." READ MORE

Source: Council of Europe

Date: 23 Dec 2020

Cyberattack on the website of the European Court of Human Rights

"Following the delivery of the Selahattin Demirtas v. Turkey (No. 2) judgment on December 22, the website of the European Court of Human Rights was the subject of a large-scale cyberattack which has made it temporarily inaccessible. The Court strongly deplores this serious incident. The competent services are currently making every effort to remedy the situation as soon as possible." READ MORE

RELATED ARTICLES

Brussels Times, European Court of Human Rights hit by cyber attack, 23 December 2020

Source: Independent

Date: 30 Dec 2020

Ireland, new powers will allow Gardaí to demand computer passwords

The "Department of Justice officials are preparing a piece of legislation to implement a recommendation by the Commission on the Future of Policing in Ireland to codify police powers of search, arrest and detention. Officials say that, as part of the police powers bill, the inclusion of a provision giving gardaí the right to seek computer passwords is being considered. It is hoped this will fast-track the gardaí's ability to access materials on devices." READ MORE

Source: National Crime Agency

Date: 25 Dec 2020

UK, 21 arrests in nationwide cyber crackdown

"The operation, which ran over the past five weeks, was coordinated by the National Crime Agency and involved cybercrime teams from across the Team Cyber UK network. Those targeted were customers of WeLeakInfo, a site that hosted 12 billion stolen credentials from over 10,000 data breaches before it was taken down in January 2020 following an NCA investigation. Cyber criminals paid for access to the site in order to download personal data for use in further criminality, including cyber attacks and fraud offences." READ MORE

Source: Council of Europe

Date: 22 Dec 2020

Pilot Training on Online Child Sexual Exploitation and Abuse for criminal justice sector in Ukraine

"The new training on online child sexual exploitation and abuse (OCSEA) for judges, prosecutors, and the national police in Ukraine, which was prepared by the EndOCSEA@Europe Project, was piloted on 8-11 December 2020 in Ukraine in cooperation with the CyberEast Project of the Council of Europe Cybercrime Office in Bucharest (C-PROC) and the project on Combatting Violence against Children in Ukraine (Phase II) of Children's Rights Division. The Council of Europe independent experts who designed the content of the module, Rajka Vlahovic, Mark Cameron and Maria Andriani Kostopoulu led a series of four practical sessions with local and active stakeholders in this area. The training was very successful in achieving its main objectives to give a practical and tailor-made overview of relevant international standards and procedures, in particular the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Abuse (The Lanzarote Convention) and the Council of Europe Convention on Cybercrime (The Budapest Convention) in light of the current situation in Ukraine and by using relevant examples from several countries presented in case studies and reinforced through practical exercises." READ MORE

Source: Reuters

Date: 15 Dec 2020

Moderna COVID-19 vaccine documents accessed in EMA cyberattack

"Moderna Inc said on Monday it was informed by the European Medicines Agency (EMA) certain documents related to pre-submission talks of its COVID-19 vaccine candidate were unlawfully accessed in a cyberattack on the medicines regulator. The EMA, which assesses medicines and vaccines for the European Union, said earlier this month that it had been targeted in a cyberattack, which also gave hackers access to documents related to the development of the Pfizer Inc and BioNTech COVID-19 vaccine. Moderna said its submission to the EMA did not include any information identifying individual study participants and there is no information at present that any participants had been identified in any way." READ MORE

RELATED ARTICLES

European Medicines Agency, Cyberattack on EMA - update 3, 22 Dec 2020

Source: The Guardian

Date: 19 Dec 2020

What we know – and still don't – about the worst-ever US government cyber-attack

"Nearly a week after the US government announced that multiple federal agencies had been targeted by a sweeping cyber-attack, the full scope and consequences of the suspected Russian hack remain unknown. Key federal agencies, from the Department of Homeland Security to the agency that oversees America's nuclear weapons arsenal, were reportedly targeted, as were powerful tech and security companies including Microsoft. Investigators are still trying to determine what information the hackers may have stolen, and what they could do with it. […] Here's a look at what we know, and what we still don't, about the worst-ever cyber-attack on US federal agencies." READ MORE

RELATED ARTICLES

CyberScoop, How the Russian hacking group Cozy Bear, suspected in the SolarWinds breach, plays the long game, 18 Dec 2020

Cybersecurity and Infrastructure Security Agency, Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations, 17 Dec 2020

Source: Reuters

Date: 16 Dec 2020

Suspected Chinese hackers stole camera footage from African Union

"As diplomats gathered at the African Union's headquarters earlier this year to prepare for its annual leaders' summit, employees of the international organization made a disturbing discovery. Acting on a tip from Japanese cyber researchers, the African Union's (AU) technology staffers discovered that a group of suspected Chinese hackers had rigged a cluster of servers in the basement of an administrative annex to quietly siphon surveillance videos from across the AU's sprawling campus in Addis Ababa, Ethiopia's capital. The security breach was carried out by a Chinese hacking group nicknamed "Bronze President," according to a five-page internal memo reviewed by Reuters. It said the affected cameras covered "AU offices, parking areas, corridors, and meeting rooms."" READ MORE

Source: Europol

Date: 22 Dec 2020

Cybercriminals' favourite VPN taken down in global action

"The virtual private network (VPN) Safe-Inet used by the world's foremost cybercriminals has been taken down yesterday in a coordinated law enforcement action led by the German Reutlingen Police Headquarters together with Europol and law enforcement agencies from around the world. The Safe-Inet service was shut down and its infrastructure seized in Germany, the Netherlands, Switzerland, France and the United States. The servers were taken down, and a splash page prepared by Europol was put up online after the domain seizures. This coordinated takedown was carried out in the framework of the European Multidisciplinary Platform Against Criminal Threats (EMPACT). Active for over a decade, Safe-Inet was being used by some of the world's biggest cybercriminals, such as the ransomware operators responsible for ransomware, E-skimming breaches and other forms of serious cybercrime." READ MORE

Source: Cyberjustice

Date: 18 Dec 2020

Bucarest, nouvelle capitale européenne de la cybersécurité

"La proposition de création d'un Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité est apparue dans un contexte de transformation des technologies numériques comme une réponse au nombre croissant de cybermenaces et attaques ayant lieu sur le territoire européen. […] La Roumanie a déjà prouvé son attachement aux normes de cybersécurité au niveau international : à la suite d'une offre du Gouvernement roumain, le Comité des Ministres du Conseil de l'Europe a décidé la création en 2013 d'un Bureau du Conseil de l'Europe sur la cybercriminalité (C-PROC), siégeant à Bucarest. Sa mission essentielle vise le renforcement de la capacité des systèmes juridiques dans le but de répondre aux défis posés par la cybercriminalité et aux preuves sous format électronique, veillant au respect des normes prévues par la Convention de Budapest." READ MORE

Source: El Peruano

Date: 30 Dec 2020

Peru, Crean la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional

"La Fiscalía de la Nación dispuso conformar una Comisión encargada de evaluar técnicamente la creación de un Piloto de Fiscalía Especializada o Unidad Especializada en Ciberdelincuencia, la cual estuvo integrada por diversos fiscales y funcionarios de la institución. Para el cumplimiento de este objetivo de la comisión se recibió asistencia técnica de la Unión Europea (Programa El PAcCTO) y la Embajada de Estados Unidos. Mediante Informe de fecha 21 de diciembre de 2020 emitido por la Comisión antes señalada se analiza entre otros, la tipología de lucha contra la ciberdelincuencia en diversos países, tipos penales con mayor incidencia delictiva en el Ministerio Público y Policía Nacional del Perú, distritos fiscales con mayor incidencia en delitos informáticos; concluyéndose en la necesidad de la creación de una Unidad Especializada o Fiscalía Superior Coordinadora en Ciberdelincuencia del Ministerio Público, y recomendándose la organización funcional de la citada unidad, la misma que dependerá administrativamente y funcionalmente de la Fiscalía de la Nación." READ MORE

Source: Senado de la República

Date: 20 Dec 2020

Mexico, urgen a la SRE concluir la adhesión al Convenio sobre Ciberdelincuencia

"Ante el crecimiento de los delitos digitales, entre ellos la pornografía infantil, la senadora Josefina Vázquez Mota urgió a la Secretaría de Relaciones Exteriores (SER) a que lleve a cabo las acciones necesarias para que el Estado Mexicano se adhiera al Convenio de Budapest sobre ciberdelincuencia y a su protocolo adicional. Mediante un punto de acuerdo, la legisladora de Acción Nacional consideró que es muy importante reactivar y retomar las negociaciones con Europa, para concluir el trámite de adhesión que México solicitó hace 13 años. Indicó que la violencia sexual contra niñas, niños y adolescentes, en todas sus vertientes, entre ellas la pornografía infantil, ha crecido enormemente a partir de la expansión de las tecnologías de la información." READ MORE

Source: Portal do Governo de São Paulo

Date: 18 Dec 2020

Brazil, Governo do Estado inaugura Divisão de Crimes Cibernéticos

"O Governador João Doria inaugurou, nesta sexta-feira (18), a Divisão de Crimes Cibernéticos (DCCIBER), uma superestrutura para combater os crimes cometidos por meios eletrônicos. A solenidade aconteceu virtualmente, diretamente do Palácio dos Bandeirantes e da sede da nova divisão. "Inaugurada em tempo recorde, é a mais moderna e eficiente delegacia de crimes cibernéticos no Brasil. Ela já é a maior, a mais equipada e agora a mais bem instalada", afirmou o Governador." READ MORE

Source: The Verge

Date: 16 Dec 2020

Twitter says it will start removing COVID-19 vaccine misinformation

"Twitter announced Wednesday that it will remove tweets making false or misleading claims about COVID-19 vaccinations. Any tweets claiming that vaccines "intentionally cause harm to control populations" or invoke conspiracy theories will be subject to removal, according to Twitter's blog post. Tweets falsely suggesting that COVID-19 doesn't exist or espouse "widely debunked" claims may also be removed. Enforcement of the new policy will begin next week." READ MORE

Source: Government of Samoa

Date: 23 Dec 2020

The Pacific Cyber Security Operational Network (PacSON) launches its Website

"The Pacific Cyber Security Operational Network has now officially launched its online website which will provide assistance in communicating and sharing the work and information resources the network through its members seek to provide. It was established in 2017, the Pacific Cyber Security Operational Network (PaCSON) is a commitment by the Australian Government to assist the Indo-Pacific region to develop capacities that address cyber threats, strengthen cybersecurity, and combat cybercrime through the Cyber Cooperation Program. The increasing internet connectivity presents significant opportunities in the Pacific region but also exposes users to increased threats from cybercriminals. To combat this threat, PaCSON was established to foster regional cooperation and collaboration and to ultimately protect the Pacific region's respective information infrastructures and constituents." READ MORE

Latest reports

- ENISA, ENISA welcomes the EU Cybersecurity Strategy and Agency's proposed tasks, 22 Dec 2020
- ENISA, Cybersecurity in the Maritime Sector: ENISA Releases New Guidelines for Navigating Cyber Risk, 17 Dec 2020
- ENISA, Launch of New Ad-hoc Working Group on European Cybersecurity Skills Framework, 18 December 2020
- Computer Law and Security Review, Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action', to be published in April 2021
- MDPI, Cybersecurity Policy and the Legislative Context of the Water and Wastewater Sector in South Africa, 30 Dec 2020
- Europol, Annual Review, 16 Dec 2020
- AlSur, Comentarios al Segundo Protocolo Adicional del Convenio de Budapest sobre Ciberdelincuencia, 15 Dec 2020
- Securelist, Kaspersky Security Bulletin 2020. Statistics, 15 Dec 2020
- McAfee, The Hidden Costs of Cybercrime on Government, 21 Dec 2020

Upcoming events

- 7 January, C-PROC, (on-line), African DPA Network Series of Regional Webinars (3rd workshop), GLACY+
- 14-15 January, Azerbaijan (on-line), Workshop on online fraud, crime proceeds and reporting mechanisms, CyberEast
- Kosovo*: Assessment of investigation and collection/ handling of electronic evidence under the respective domestic legislation, desk review - iPROCEEDS-2
- Turkey: Assessment of investigation and collection/ handling of electronic evidence under the respective domestic legislation, desk review - iPROCEEDS-2