INSIGHTS
SEPTEMBER 27, 2024

CYBERSECURITY UNDER DISCUSSION: DEBATE HIGHLIGHTS RISKS OF ATTACKS AND CHALLENGES FOR BRAZIL

Senate - Losses are estimated at over US$10 trillion. In Brazil, and across the world, internet pirates are on the loose, looking for easy targets to manipulate data. The Senate has a Permanent Subcommittee on Cyber Defense. And this week's Em Discussão program features a debate on the topic. The public hearing brought together industry experts.

NUCLEP RECEIVES ABIN AND ADVANCES IN CYBER PROTECTION AND NATIONAL DEFENSE – BRAZIL

Defense in Focus - On Monday (23), NUCLEP took a significant step towards improving its cybersecurity and data protection by receiving representatives from the Brazilian Intelligence Agency (ABIN). During a visit marked by the exchange of strategic information, NUCLEP President Carlos Henrique Silva Seixas highlighted the importance of collaboration to strengthen the defense of Brazil's nuclear and industrial sector. The meeting also opened up new possibilities for partnerships between the institutions, which is crucial for the protection of sensitive technologies.

EMBRATEL REINFORCES FOCUS ON CYBERSECURITY FOR THE PUBLIC SECTOR – BRAZIL

Tele.Síntese - With the increase in digital threats and the growing need for data protection in the public sector, Embratel has intensified its investments in cybersecurity and technological infrastructure. In 2023, the company allocated R$9 billion to expand its network and develop new solutions for its customers, mainly for governments and city halls. At Inovatic 2024, promoted by Tele.Síntese, Ana Lucia Domiquili, Embratel's government sales director, stated that the company is focused on providing services that go beyond connectivity. Thus, presenting an offering that includes cloud, IoT and data insights.

NATEL DETERMINES MEASURES TO COMBAT FRAUD AND TELEPHONE SCAMS – BRAZIL

Agência Brasil - The National Telecommunications Agency (Anatel) determined this Monday (23) a set of measures for telecommunications service providers with the aim of preventing the use of telephone calls to commit scams and fraud. The regulatory agency clarifies that the determined measures aim to guarantee the transparency and traceability of telephone calls and correspond to a response to the update of methods used by fraudsters and complementary actions to other provisions already implemented by Anatel and in progress.

CYBERSECURITY EXPERTS MEET IN PERU TO STOP CYBERATTACKS IN THE REGION

Andina - Within the framework of the Regional Cyberdrill for the Americas, an event that seeks to strengthen cybersecurity in the region and that is being held in our country with national and international experts, today the exercises of simulations of cyberattacks and responses began. For this start, the technicians of the International Telecommunication Union (ITU) and the company FIRST designed a series of interactive simulations, where the teams made up of the participants competed against each other by completing tasks and roles. All this with the purpose of putting into practice the knowledge acquired during the previous days.

ECU 911 SOCIAL NETWORK HACKED – ECUADOR

El Comercio - On the night of Wednesday, September 18, 2024, cybercriminals hacked one of the social media accounts of ECU 911, as detailed by the entity. The official statement reported that the attackers breached the account of X, belonging to the Zonal Coordination 5-8. ECU 911 condemned the attack and assured that it will file a complaint with the State Attorney General's Office. In addition, the Integrated Security Service (ECU 911) explained that cybercriminals accessed X's account of the Zonal Coordination 5-8.

THE ICT MINISTRY STRENGTHENS DIGITAL SECURITY IN PUBLIC ENTITIES WITH THE UPDATE OF THE INFORMATION SECURITY AND PRIVACY MODEL – COLOMBIA

MINTIC - Given the growing risk of digital security incidents faced by public entities, the ICT Ministry has intensified its commitment to protecting IT assets and ensuring continuity in the provision of services to citizens. Aware of the digital vulnerability of State institutions, the ICT Ministry has developed policies and strategies that seek to ensure the safe and efficient use of information and communications technologies (ICT).

COLOMBIA AND THE UNITED STATES CHAMBER OF COMMERCE SIGN AN AGREEMENT TO PROMOTE TECHNOLOGICAL DEVELOPMENT IN THE COUNTRY

BNAmericas - Within the framework of the UN Future Summit taking place in New York, the ICT Ministry and the United States Chamber of Commerce signed a Memorandum of Understanding (MoU) that marks a new chapter of collaboration between the parties at the technology level. The agreement seeks to promote the recognition of experiences and best practices, to address key challenges focused on different areas, such as the digital economy, connectivity, artificial intelligence regulation and digital education. An alliance that continues to contribute to the digital transformation of Colombia and supports efforts to make the country a Digital Power.

U.S. EMBASSY SPONSORS STRATEGIC WORKSHOP ON CYBERSECURITY WITH INTERNATIONAL EXPERTS - PARAGUAY

US Embassy - International experts from the William J. Perry Center for Hemispheric Defense Studies of the United States of America held the Strategic Cybersecurity Workshop at the Metropolitan University of Asunción (UMA) on September 24 and 25, 2024, in order to promote a dialogue between different sectors of Paraguayan society, to strengthen, together with international experts, digital defense and face current and future cyber challenges. This workshop, organized with the support of the UMA, fostered a collaborative environment focused on cybersecurity issues, generating debates among representatives of ministries, the security sector, the financial sector, academia and other related institutions in Paraguay.

WHAT IS THE PACT OF THE FUTURE: THE 56 ACTIONS PROPOSED BY THE UN AND THE POINTS REJECTED BY MILEI'S GOVERNMENT

Infobae - "Argentina will be a Beacon of Freedom." With that definition, the government of Javier Milei celebrated last night having been the only country that decided to leave the "Pact of the Future", an agreement approved in the United Nations General Assembly with the support of 193 countries, which established commitments to reform international institutions and implement 56 actions and more than 100 proposals for change to guarantee growth, equality and guarantee social, political and economic rights for present and future generations. It also included an extensive chapter called "Digital Pact", which raises the need to regulate social networks, technology companies and artificial intelligence.

GLOBAL CYBERSECURITY INDEX - ITU

ITU - The Global Cybersecurity Index (GCI) is a trusted reference that measures the commitment of countries to cybersecurity at a global level – to raise awareness of the importance and different dimensions of the issue. As cybersecurity has a broad field of application, cutting across many industries and various sectors, each country's level of development or engagement is assessed along five pillars – (i) Legal Measures, (ii) Technical Measures, (iii) Organizational Measures, (iv) Capacity Development, and (v) Cooperation – and then aggregated into an overall score.

IN WAR AND SOCIETY, LARGE LANGUAGE MODELS ARE WHAT WE MAKE OF THEM

War on the Rocks - Prophecy and alarmism about AI are both overblown. No technology is a panacea or poses a risk independent of the people and institutions surrounding its use. Adapting algorithms to support strategic analysis requires studying the people, culture, and bureaucracy as much as it does model performance. War on the Rocks has been at the center of emerging debates about the roles, missions, and even ethics and morality of the growing integration of AI into the military. Every day, articles emerge highlighting either the game-changing possibilities of generative AI models or the perils associated with them. This trend is particularly acute with respect to large language models that synthesize large volumes of data to generate prompt-based responses that every reader has probably already played with, if not used in a professional setting.

MITIGATING AI-GENERATED DISINFORMATION: A CYBER COLLABORATIVE FRAMEWORK FOR G7 GOVERNANCE

Global Solutions - In an increasingly multipolar and conflict-prone world, witnessing the rise of artificial intelligence(AI), this paper explores the disruptive potential of AI-generated disinformation, a growing threatto global peace and security. The advance of generative AI tools able to rapidly produce convincing"synthetic disinformation", such as large language models (LLMs), has exponentially amplified thereach and impact of foreign information manipulation and interference (FIMI) wielded by bothstate actors and non-state actors alike. Against this challenge, the G7 countries have shownproactive leadership in recognising and addressing the threat posed by AI and disinformation, lveraging resources and expertise to develop innovative strategies. Still, the lack of uniformityin regulatory approaches and policies across G7 nations, as well as the compartmentalisationbetween cyber policies and counter-disinformation responses, has resulted in fragmentedsolutions that are now insufficient. This paper argues that tackling AI-generated disinformationwith a cyber-security approach not only offers an effective framework for G7 action but alsopaves the way for broader AI and cyber regulation milestones, leveraging the G7's role as normsetter in peace, security and global governance.

WIFI SUSPENDED AT BIG UK TRAIN STATIONS AFTER 'CYBERSECURITY INCIDENT'

The Guardian - Wifi networks at a number of train stations across the UK have been suspended after a "cybersecurity incident". Nineteen stations including London Euston, Manchester Piccadilly and Birmingham New Street had their wifi services suspended on Wednesday night after the incident. They were still down on Thursday. The Manchester Evening News reported that passengers accessing the wifi at Piccadilly station were directed to a webpage titled "We love you, Europe", which contained Islamophobic messages and details of several terrorist attacks that have taken place in the UK and in Europe.