DIGI AMERICAS ALLIANCE MEMBERS

LEAK OF BANKING DATA INCREASES CONCERN ABOUT FRAUD AND SCAMS IN BRAZIL

AJN - Leakage of bank data is a growing concern among Brazilians, especially with the increase in fraud and scams. Although the General Data Protection Law (LGPD) was implemented in 2020, there is still no specific legislation that addresses the damage caused by these incidents, making it difficult for victims to obtain compensation. As explained by lawyer and law professor at Universidade Tiradentes (Unit), Clara Machado, the LGPD does not differentiate between types of leaked data. "When a leak occurs, the company or financial institution can be fined, with penalties ranging from 2% to 10% of revenue, limited to 50 million reais, as stipulated by the LGPD", he explains.

AIR FORCE CYBER DEFENSE CENTER ACTIVATED – BRAZIL

Air & Naval Defense - On the morning of this Thursday (11/07), the military ceremony to activate the structure of the Aeronautics Cyber Defense Center (CDCAER) took place on the premises of the Air Force Command (COMAER), in Brasília (DF).), with Colonel Silvio Roberto Assunção de Oliveira Filho appointed to be the first Chief. The event marks a significant advance in COMAER's cybersecurity strategy.
The CDCAER was created to manage, execute and control all activities related to cyber defense within the scope of the Air Force. Subordinated directly to the Air Force Information Technology Directorate (DTI), the Center is part of the Military Cyber Defense System, whose central body is the Cyber Defense Command.

RESOLUTION ON THE 5G CYBERSECURITY DECREE IS IN THE NOTIFICATION PHASE

CRHoy - The resolution on the process related to the cybersecurity regulation for 5G networks is in the notification phase. "The TACA was consulted and they indicate that in this file the resolution is in the notification phase to the parties," reported the Press Office of the Judiciary after consulting this medium. The case refers to file 24-001014-1027-CA-4, which is being processed in the Contentious Administrative Court (TCA). It has to do with the precautionary measure that temporarily nullifies the scope of Executive Decree 44196-MSP-SMALL.

BLINKEN ANNOUNCES SUMMIT OF LEADERS IN COSTA RICA THAT WOULD ADDRESS SEMICONDUCTOR ISSUE

CRHoy - US Secretary of State Antony J. Blinken announced this Wednesday that next year a leaders' summit would be held in Costa Rica in which the issue of the local semiconductor industry would be addressed. The announcement was made at the ministerial session of the countries of the Alliance for Economic Prosperity in the Americas (APEP), which among other things seeks to create opportunities for members to explore collaborative ways to strengthen the microchip supply chain, through the development of skilled labor capacity. Regarding the possible issues to be discussed in the activity, the United States Embassy indicated that "it is still too early to have established the agenda for the 2025 summit, but the announcements from Washington D.C. explain the general priorities of APEP."

MILEI APPOINTS BITCOIN EXPERT AS CYBERSECURITY DIRECTOR – ARGENTINA

Crypto Trends - In a bold move, Argentine President Javier Milei has appointed Ariel Waissbein, a renowned Bitcoin technology expert, as the new director of the Federal Cybersecurity Agency (AFC). This appointment underlines the Milei government's intention to strengthen the protection of the country's critical IT infrastructure by incorporating advanced knowledge in cryptography and computer security. Ariel Waissbein is not an unknown name in the world of computer security and cryptography. With over 20 years of cybersecurity experience and a strong background in mathematics, Waissbein has worked as a consultant for prominent companies such as CoinFabrik and BitTrap, which specialize in the decentralized finance (DeFi) environment.

CYBERSECURITY: CURRENT CHALLENGES IN DATA PROTECTION – CHILE

La Tercera - With billions of cyberattacks a year, Chile faces a constant threat in the digital world. The implementation of cybersecurity policies, the promotion of the Framework Law and the creation of the ANCI are important steps, but the lack of trained professionals and the need to improve infrastructure are critical challenges. At the recent AWS re:Inforce 2024 event in Philadelphia, the importance of fostering a transversal culture of digital prevention and public-private collaboration was highlighted as key to strengthening cybersecurity.

CERTAL WILL TRAIN JUDGES ON CYBERSECURITY AFTER AGREEMENT – PARAGUAY

Judicial - The Association of Judges of Paraguay AJP, in collaboration with the Center for Studies in Regulation and Telecommunications CERTAL, signed a cooperation agreement that includes the training and updating of judges on critical issues such as piracy and cybersecurity. This agreement seeks to strengthen the response capacity of magistrates in these complex and current crimes such as crimes perpetrated online, as well as cases referring to the violation of intellectual property.

CONTROVERSIAL HACKTIVISTS WOULD HAVE CAUSED CENSORSHIP OF TELEGRAM IN EL SALVADOR

Global Voices - The president of El Salvador, Nayib Bukele, has become the face of technological progress in Central America, despite relentless cyberattacks against Salvadoran public institutions that have put the data of millions of citizens at risk. In 2021, Bukele impressed international viewers when he made Bitcoin legal currency in El Salvador, and in 2024 he announced the inauguration of a new Google office in the country, promising to digitize the education and health sectors. However, there has been no public acknowledgment of more than a dozen data breaches against public infrastructure between April and June 2024.

UNITY IS STRENGTH: LATAM WOMEN'S CYBERSECURITY GROUPS

Heraldo de México - Cybersecurity, a crucial field for all organizations, faces complex and multidimensional challenges that require diverse perspectives and skills. In this area, women have demonstrated a unique and valuable approach to addressing these challenges; However, the gender gap in this sector remains a reality in Latin America, where women represent only a small fraction of the workforce, which limits the potential and diversity of perspectives in this important area.

AN APATHY OF CYBERSECURITY CONCERNS – T&T

Newsday - FOR JUST over a month, the website of the Guyana Cricket Board has been quite visibly defaced by hackers who demanded US$1,000 in Bitcoin. The defacement took the form of a warning and demand, stating partly, "Your company was hacked due to major security issues and your documents, contracts, work correspondence ended up in our possession, we would love to forget this incident but we cannot, so your business partners should not suffer because of your negligence to security."

CISA PUBLISHES RESILIENCE-PLANNING PLAYBOOK FOR CRITICAL INFRASTRUCTURE

StateScoop - The Cybersecurity and Infrastructure Security Agency on Wednesday published a supplemental manual to its infrastructure resilience planning framework, which provides guidance on how local governments and the private sector can work together to improve the security and resilience of the nation's critical infrastructure. The new playbook includes processes and table top exercises to help public and private sectors minimize the impact of cyberattacks on their communities, reduce the risk of disruption to critical services and keep system restoration costs low.

RANSOMWARE ATTACKS ARE HITTING ENERGY, OIL AND GAS SECTORS ESPECIALLY HARD, REPORT FINDS

StateScoop - Ransomware attacks are hitting energy and oil and gas sectors harder, costing utilities more in recovery time and funding as victims appear increasingly willing to pay ransom demands, according to a new report from the cybersecurity firm Sophos. The report looks at ransomware impacts to critical infrastructure organizations and is based on more than 200 responses from a wider survey of 5,000 cybersecurity and IT leaders taken in January and February. Sophos said that the ransomware attack rate appears to be falling globally, but researchers found that recovery times for energy, oil and natural gas, and utilities have been steadily increasing since at least 2022.

THE NEXT FRONT IN U.S.-CHINA TECH BATTLE? UNDERWATER CABLES THAT POWER THE GLOBAL INTERNET

CNBC - U.S.-Chinese tensions surrounding technology have have sunk to sea lows. Subsea cables hit the headlines earlier this year after four out of 15 critical submarine cables in the Red Sea were cut amid attacks by Yemen's Iran-backed Houthi rebels on Israeli U.S., and U.K. ships. Public awareness of submarine cables has grown as a result — and these networks of cables are becoming a new source of strain in international relations, amid heating geopolitical engagements between the U.S. and China.

THE RISE OF SMART CONTRACTS AND STRATEGIES FOR MITIGATING CYBER AND LEGAL RISKS

WEF - Imagine a world where contracts are executed seamlessly without human intervention, reducing costs and enhancing efficiency across industries – from finance to real estate. This is the promise of smart contracts, self-executing agreements embedded in blockchain technology. However, the rapid adoption of this revolutionary technology comes with significant risks. In 2016, a coding flaw in the Decentralized Autonomous Organization (DAO) smart contract on the Ethereum platform led to a theft of $50 million worth of ether, illustrating the potential vulnerabilities.

DIGITAL SAFETY: ARE YOU USING ONE OF THE WORLD'S MOST POPULAR PASSWORDS?

WEF - What makes a terrible online password? Something simple, short and predictable. Astonishingly, those are also the characteristics of the world's most common online password, which is 123456, according to online password management company NordPass. NordPass also calls 123456 the worst password, because as well as being used over 4.5 million times, it takes less than a second for hackers to crack – like the rest of the top 20 most popular online passwords.