DIGI AMERICAS LATAM CISO

INSIGHTS

OCTOBER 17, 2024

DIGI AMERICAS ALLIANCE MEMBERS

aws Apple CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks Google GRUPO RADICAL LUMU METABASE Q netskope paloalto NETWORKS Resecurity Santander Schneider Electric SISAP Sistemas Aplicativos Telefónica tenable Trellix TREND MICRO

SERGIO MORO DEFENDS CREATION OF CYBERSECURITY AGENCY IN BRAZIL

Senate - Senator Sergio Moro (União-PR) advocates the creation of a cybersecurity agency in Brazil. According to the parliamentarian, just as society has migrated to the virtual world in several areas, such as leisure and finance, crimes are also following this trend. Moro is a member of the Permanent Subcommittee on Cyber Defense, linked to the Committee on Foreign Affairs and National Defense, which aims to monitor public cyber defense policies and propose new measures to face the growing challenges in this area.

BRAZIL'S FEDERAL POLICE ARREST ALLEGED NATIONAL PUBLIC DATA HACKER

Cyberscoop - The Federal Police of Brazil on Wednesday arrested a person allegedly responsible for a series of audacious data breaches targeting large international companies and U.S. government entities. The suspect, who is known in the cybercrime underground as USDoD or EquationCorp, is allegedly the person responsible for a breach of the online background check and fraud prevention service National Public Data, exposing personal information and Social Security numbers of millions of Americans. Brazilian authorities also say the suspect is responsible for compromising the FBI's InfraGard — a portal used by American law enforcement to share critical threat information. The Brazilian police did not name the suspect. In August, Brazilian tech publication Tecmundo reported that CrowdStrike had given a report to Brazilian police naming a 33-year-old "Luan "B.G." as the person responsible for breaching National Public Data. Shortly thereafter, a "Luan" told HackRead that CrowdStrike had doxxed him and claimed responsibility for the breach.

CHILECOMPRA REVEALS ITS LESSONS LEARNED AND TECHNOLOGICAL AND INFORMATION SECURITY IMPROVEMENTS AFTER THE 2023 CYBERATTACK

Chile Compra - The ChileCompra Directorate and the Computer Security Incident Response Team (CSIRT) of the Ministry of the Interior held a cybersecurity workshop on Wednesday, October 16, entitled "one year of cyberattacks, lessons learned and improvements to the Mercado Público platform." 273 attendees participated in the activity, in addition to more than 1,800 views of the event broadcast, which generated great interest from IT managers, administration and finance teams, information security managers from various public entities, and also suppliers. The event was attended by the Undersecretary of Finance, Heidi Berner; the National Coordinator of Cybersecurity, Daniel Álvarez and the Director of the Digital Government Secretariat of the Ministry of Finance, José Inostroza. In addition to the director of ChileCompra, Verónica Valle, the Head of Information Security and Cybersecurity, Paolo Jeldres and the Head of the Technology Division, Cristián Cépedes.

CHILEAN POLICE AND HACKERS USE AI TO COMBAT CYBERCRIME

Madboxpc - An unprecedented talk took place at the 2024 version of the 8.8 Computer Security Conference, the first and most important technical cybersecurity meeting in Chile. For the first time in its 14 years of existence, Carabineros de Chile participated with a fun and educational presentation to hackers and cybersecurity experts. With their talk “Sitia Project, Integrated Teleprotection System with AI”, Captain Miguel Ramírez Veas, Head of the Cybersecurity and ICT Operational Continuity Area, and 2nd Sergeant Darwin Muñoz García, Head of Cybersecurity for the institution, won over the audience, and highlighted the opportunity to share at 8.8 with people as passionate as they are about cybersecurity.

CYBERSECURITY AGENCY TO ‘CENSOR SOCIAL MEDIA’? - COLOMBIA

El Tiempo - In recent days, there was one of many discussions full of political considerations around a structural and necessary issue for the country: having a cybersecurity agency that increases the capacities of the State and society to defend themselves and prevent risks and digital attacks. A discussion made clear the very short and basic vision that we have as a society on relevant issues for the country. We saw 'brilliant conclusions', even from renowned colleagues, such as that "the Petro government is going to censor social networks" with this norm. It makes me genuinely sad to spend lines of this valuable space to discern around such nonsense, basically because starting from the poverty of political hatred to analyze reality is an insurmountable wall that leaves, on the other side, and in this case, the technical, scientific and socioeconomic arguments that support the need to have this regulatory framework for cybersecurity.

CYBERATTACKS COST THE FINANCIAL SECTOR MORE THAN $500 BILLION IN 2023 - COLOMBIA

La República - At the opening ceremony of the 17th Congress on Security, Cyber Threats, Fraud and Experience, the president of Asobancaria, Jonathan Malagón, began his speech by mentioning the change that existed 10 years ago in the financial sector. "A decade ago, 55% of transactions were made through physical channels, 80% of balance inquiries were made at ATMs." "Today, only 21% of transactions are made through physical channels, there are approximately 23 million fewer checks in circulation and 0% of cards have only a magnetic stripe for protection," added the president. However, although cases of card cloning were reduced by 86%, those of fleteo by 49% and those of theft in bank offices by 30%, "in 2023 there were 407,000 cases of fraud through the Internet and this cost the sector more than $500,000 million," said the leader.

PANAMA UPDATES ITS CYBERCRIME LEGISLATION TO ALIGN WITH THE CONVENTION ON CYBERCRIME

COE - On 10 October 2024, the National Assembly of Panama approved several provisions on cybercrime and electronic evidence, including for amending the Criminal Code, the Code of Criminal Procedure and Law 11 of 2015 on international legal assistance in criminal matters. The Council of Europe (Cybercrime Programme Office) supported over the past months the Public Ministry’s drafting team, leading the legal reform process, including with a set of public consultation workshops on 21-22 August.

PARAGUAY | MITIC AND THE US CYBERSECURITY COUNCIL AGREE TO STRENGTHEN CYBERSECURITY THROUGH A MEMORANDUM OF UNDERSTANDING

DPL News - In a significant step for Paraguay in cybersecurity, the Ministry of Information and Communication Technologies (Mitic) and the Cybersecurity Council of the United Arab Emirates signed a Memorandum of Understanding (MOU) in Dubai to collaborate in key areas related to information security. The agreement was signed by Mitic Minister Gustavo Villate, and Dr. Mohammed Hamad Al Kuwaiti, Head of Cybersecurity for the Government of the United Arab Emirates, to establish a framework for cooperation in several essential aspects for the digital protection of both countries.

THE BUENOS AIRES GOVERNMENT ORGANIZES THE PROVINCIAL CYBERSECURITY FORUM - ARGENTINA

La Capital MDP - The topic of cybersecurity has become increasingly important as public bodies, companies and individuals need to protect huge amounts of data and digital information flows. From October 15 to 17, this will be the central topic of debate at the Provincial Cybersecurity Forum organized by the Undersecretariat of Digital Government of the Ministry of Government of the Province of Buenos Aires.

WEF REPORT | NAVIGATING CYBER RESILIENCE IN THE AGE OF EMERGING TECHNOLOGIES: COLLABORATIVE SOLUTIONS FOR COMPLEX CHALLENGES

WEF - As society moves further into the digital age, emerging technologies offer new opportunities for growth and efficiency. However, such advances bring a significant increase in cybersecurity risks, requiring a fundamental shift in approach. This white paper explores the risks and opportunities associated with emerging technologies, presenting data-driven insights and recommendations for enhancing cyber resilience. The paper outlines a numbers of practical actions for leaders in government, industry and academia to support them in creating a resilient and sustainable cyberspace. It emphasizes the need for a proactive, collaborative approach that integrates security, resilience, sustainability and quantifiable risk measurement into all aspects of technology development and deployment. Real-world case studies provide insights into how emerging technologies can be effectively integrated into broader cybersecurity frameworks while managing the associated risks, helping to build a secure digital future.

5 CYBERSECURITY RISKS POSED BY EMERGING TECHNOLOGY – AND HOW WE CAN DEFEND AGAINST THEM

WEF - The advance of digital technology is fundamentally transforming industries, economies and the values on which our societies are built. A new report from the World Economic Forum highlights the enormous opportunities emerging technologies offer, including artificial intelligence (AI), quantum computing, biotechnologies and the Internet of Things (IoT). But the optimism of the report, Navigating Cyber Resilience in the Age of Emerging Technologies, is tempered with a warning. As these advanced technologies take on ever more critical functions – often central to national security – a new level of cyber resilience will be required to protect them from attacks by bad actors.

US FEDERAL GOVERNMENT IS TARGET OF TELECOM CYBERATTACK

Global Data - Intelligence leaked this summer that state-sponsored threat actors connected to China breached US Federal government resources via major telecom providers’ networks. Last week, it was revealed by several journalism sources including the Wall Street Journal that the target of the activity was federal government communications related to court-ordered network wiretapping applications that the hackers accessed through AT&T, Lumen, and Verizon’s networks.