DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 10, 2025

DIGI AMERICAS ALLIANCE MEMBERS

aws Batuta Apple CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks we hack your software

Google kriptos LUMU netskope paloalto NETWORKS Resecurity

Schneider Electric SISAP Sistemas Aplicativos Telefónica tenable Trellix TREND MICRO

HACKER ATTACK: WHAT WE KNOW ABOUT THE SCAM THAT DIVERTED R$541 MILLION - BRAZIL

CNN Brasil - A hacker attack carried out this week against C&M Software resulted in the embezzlement of R$541 million from the payment institution BMP. To date, a man identified as João Nazareno Roque has been arrested on suspicion of involvement in what the São Paulo Civil Police consider "the largest cyberattack against financial institutions in the country." According to João Roque, the hacker attack reportedly began in March while leaving a bar in Jaraguá, a neighborhood in the West Zone of São Paulo. The suspect, in a statement to the police, said he was approached by another man who allegedly stated that he wanted to learn about the systems of C&M Software, where João worked.

MINISTRY OF DEFENSE LAUNCHES NEW STRATEGY TO COMBAT CYBERCRIME: THIS IS WHAT IT'S ALL ABOUT - COLOMBIA

Caracol Radio - In a context where digitalization has boosted productivity in both the public and private sectors, Colombia faces new and complex challenges in cybersecurity. So much so that, although cybercrimes have decreased by 16% this year, there have been 24,959 cybercrimes nationwide.
However, the Ministry of Defense announced that since 2011, when CONPES document 3701 was issued, the country has embarked on an institutional path toward protecting the digital environment in the defense sector.

MITIC AND THE SENATE DISCUSSED ACTIONS TO STRENGTHEN CYBERSECURITY - PARAGUAY

dplnews - Minister Gustavo Villate and the technical team of the Ministry of Information and Communication Technologies (Mitic) met with members of the Senate's governing board to discuss cybersecurity issues and ongoing efforts in this area. One of the points shared was strengthening the culture of digital protection, such as the use of strong passwords, considering that most cyber incidents in recent months originated from weak passwords or outdated systems.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 10, 2025

FROM HACKING TO LAWLESS CYBERSECURITY STRATEGY - PARAGUAY

abc - Constant cyberattacks have exposed the weakness of the governmental digital environment in which even President Santiago Peña was violated, while the country evolves in an environment of technological transformation without regulations and laws to protect and enhance the Paraguayan digital ecosystem. The National Cybersecurity Strategy 2025-2028 confidentially presented at the Lopez Palace, after the hacking of the President of the Republic's X social network account, seeks to stop the constant siege of the digital ecosystem violated on several occasions, even ironically against the minister responsible for public policies in this sector.

WITH THE LAMBARÉ HACK, THE NUMBER OF PUBLIC ENTITIES ATTACKED BY CYBERCRIMINALS RISES TO 32 - PARAGUAY

Breaking News - The Municipality of Lambaré and the National Directorate of Public Procurement (DNCP) have joined the list of public entities hacked by the cybercriminal group CyberTeam. Both were attacked in the afternoon and evening hours of Wednesday. This was reported by the group itself through its X account @cyberteam2009. In both cases, this group mocked cybersecurity. Regarding Lambaré, they posted the following: “Guess who fell again? Password? lambare2010.” While Villate was talking about security, the CyberTeam was already online, reading emails and choosing a wallpaper.

CYBERCRIME 2025: ARTIFICIAL INTELLIGENCE, HACKTIVISM, AND THE COLLAPSE OF THE DIGITAL PERIMETER

Infobae - During the first half of 2025, the global cybersecurity landscape became more critical, more complex, and deeply cross-cutting. The sustained growth of cybercrime, driven by emerging technologies and geopolitical tensions, challenges the response capacity of governments, businesses, and users. The healthcare sector, for the first time this year, becomes a target seeking to affect the public in highly sensitive matters, putting pressure on the industry like never before. Personal data, medical records, and medical examinations are the order of the day; nearly 39% of threats come from mobile platforms using phishing techniques. It's not just about data; we're talking about operational difficulties, disclosed treatments, and violated confidentiality. The impact is physical, emotional, and financial.

LACK OF CYBERSECURITY: DIGITAL FRAUD, A SERIOUS PROBLEM FOR INTERNET USERS

Diaro de Yucatan - "The evolution of fraudsters in the digital age is no longer the common fraudster who sold you mirrors on the street. They have now become more sophisticated with new technologies, and the way they obtain information is through cyber fraud, which should not be confused with cyberattacks," warned Rafael Cortez Melecio, national president of the Council of Entrepreneurs in Technology, Innovation and Communications (Cetic). Cyberattacks, according to Cortez Melecio, involve a hacker penetrating systems exposed to the Internet to obtain information, and this is largely due to a lack of cybersecurity culture.

SECURITY COALITION URGES CONGRESS TO RENEW 2015 CISA LAW - USA

Cybersecurity Dive - Congress must reauthorize a cybersecurity threat information sharing law before it expires in October, a group of leading technology companies told lawmakers on Monday. The 2015 Cybersecurity Information Sharing Act “has enabled rapid dissemination of actionable threat intelligence to protect networks before an incident occurs, more coordinated responses to cyber incidents; and improved situational awareness across multiple sectors,” the Hacking Policy Council said in a letter to House and Senate homeland-security committee leaders.

QANTAS CONFIRMS PERSONAL DATA OF OVER A MILLION CUSTOMERS LEAKED IN BREACH - AUSTRALIA

Reuters - Australia's Qantas Airways (QAN.AX), opens new tab said on Wednesday more than a million customers had their phone number, birth date or home address accessed in one of the country's biggest cyber breaches in years. The airline operator said that another four million customers had just their name and email address taken during the hack.

SCATTERED SPIDER POSES SERIOUS RISK TO SEVERAL HUNDRED MAJOR COMPANIES

Cybersecurity Dive - The cybercrime group Scattered Spider’s tactics put a group of roughly 300 major companies at heightened risk of attack, according to a new report from security firm CyberCube. The 287 firms represent approximately 2% of organizations with revenues above $500 million, according to CyberCube’s analysis of more than 15,000 companies in key global markets. The analysis covers eight regions, including the U.S., the U.K., Canada, Australia, Germany, France, Japan and Singapore.

NEED TO DEVELOP OT CYBERSECURITY PROGRAMS TO BRIDGE IT AND ENGINEERING CULTURES, DEFEND FROM CYBER THREATS

Industrial Cyber - Mature OT cybersecurity programs span beyond perimeter defenses, with an emphasis on deep visibility, continuous risk assessment, and strong governance reflecting the unique conditions and needs of OT (operational technology) environments. The roadmap accounts for legacy systems, scattered industrial installations, multilayer network segmentation, secure remote access to the plant, and asset inventories that are up to date, even as critical equipment ages. But most industrial companies are still stuck using legacy risk models designed for the way our systems used to be, rather than the way they are today. The question remains, however, is most, if not all, of the installed base is not hardened for modern threats, including ransomware, nation-state, and supply chain compromise, and leaves critical industrial environments at risk.

CYBERSECURITY COMPLIANCE: THE COSTS, RISKS AND RACE TO CERTIFICATION

Forbes - For companies in the defense industrial base, Cybersecurity Maturity Model Certification will soon be a prerequisite for doing business. And as CMMC compliance rollout deadlines loom, the Department of Defense isn’t mincing words. “CMMC started under Trump 1,” said Katie Arrington, performing the duties of the DoD Chief Information Officer and a key architect of the program. “It will finish and be implemented under Trump 2.” She made these comments in a keynote at the AFCEA International TechNet Cyber convention in May.