DIGI AMERICAS ALLIANCE MEMBERS

SUBCOMMITTEE TO HEAR ARMY CYBER DEFENSE COMMANDER - BRAZIL

Senate - Brazil was one of the countries most targeted by cyberattacks in 2023, according to data from digital security companies. On Wednesday (30), starting at 2 pm, the Permanent Subcommittee on Cyber Defense (CREDC) will discuss the relationship between national security and cyber defense with General Alan Denilson Lima Costa, head of the Cyber Defense Center (CDCiber) of the Ministry of Defense. Cyber defense is one of the missions of the Armed Forces. CDCiber began operating in 2012, two years after its creation by the Army Command. Today, the Navy and the Air Force also have their own cyber defense centers.

FIESP JOINS THE FEDERAL POLICE IN THE FIGHT AGAINST CYBERCRIME - BRAZIL

Metropoles - The Federation of Industries of the State of São Paulo (Fiesp) will enter into a technical cooperation agreement with the Federal Police to help not only in the repression of cybercrimes, but also in the exchange of intelligence. The information was released this Tuesday (10/29) during the 6th Congress on Cybersecurity, Data Protection and AI Governance. According to Otávio Margonari Russo, director of Cybercrimes at the Federal Police, the agreement has been under discussion for a year and a half to give effect to what he believes “is the best way to prevent and also repress cybercrimes”.

INTERBANK ACKNOWLEDGES THAT ITS CLIENTS' DATA WAS EXPOSED BY A THIRD PARTY

RPP - Through social media, Interbank and Plin users reported failures in both applications, which prevented them from making monetary transactions. In response to RPP's query about the incidents on the platform, the bank responded as follows: "At Interbank, the security of our clients is our top priority. We have identified that some data from a group of clients has been exposed by a third party without our authorization. In light of this situation, we have implemented additional security measures, including special monitoring of both the operations and the information of our clients," it reads at the beginning.

URUGUAY LAUNCHES NEW REGULATIONS AND PREPARES TO LAUNCH ITS NATIONAL CYBERSECURITY STRATEGY

Telesemana - In the days when Uruguay is finalizing the details of its National Cybersecurity Strategy (ENC) 2024-2030, it is launching legislation that classifies the crime of cybercrime and establishes international ties. The initiative is part of a regional context in which the country is a prominent player, according to the International Telecommunication Union (ITU). A few weeks ago, Uruguay announced its Law 20.327, which, made up of 11 articles to prevent and suppress cybercrime in Uruguay, classifies cybercrime and creates a database of cybercriminals.

GOVERNMENT TO CREATE A STATE CYBERSECURITY AGENCY - EL SALVADOR

The Minister of Justice and Security, Gustavo Villatoro, asked the Legislative Assembly to approve a “Cybersecurity and Information Security Law” to regulate, monitor and supervise cybersecurity and security measures of “information held by public institutions.” The project establishes the creation of a State Cybersecurity Agency (ACE), whose general director and legal representative would be appointed by the President of the Republic. The bill was delivered on October 15 to the Legislative Operations Management of the Legislative Assembly but was not received until Wednesday, October 30 by the plenary, which passed it to the National Security Commission, which was convened for next Monday at 2:00 p.m.

CYBERSECURITY CHALLENGES ARE ANALYZED TO RESPOND TO POSSIBLE CRISES IN THE COUNTRY'S CRITICAL INFRASTRUCTURE - CHILE

Mining Report - National and international experts met to analyze the challenges of crisis management in the face of possible cyberattacks on the country's critical infrastructure, especially considering the strategic importance of the electrical sector in Chile and the world. This was the central theme of the II International Conference on Cybersecurity and Critical Electrical Infrastructure: Crisis management before a cyberattack, organized by the National Electrical Coordinator, the Faculty of Sciences and Engineering of the Adolfo Ibáñez University, the Anacleto Angelini UC Innovation Center and USACH Training.

RECORDING: DEFINING CYBER WAR: THE IMPACT OF INSURANCE ON CYBER NORMS

RUSI - Global cyber security and governance are at a critical juncture. Efforts to develop the rules, norms and values of cyberspace reflect shifting international power dynamics and competing political visions of what and who cyber security is for. Debates over concepts like ‘responsible cyber behaviour’ or ‘cyber war’ are not only shaped by states but also the private sector. As an example, in August 2022, the cyber insurance market Lloyd’s issued guidance to underwriters that they should exclude losses from cyber war and state-backed cyber attacks that significantly impair the ability of a state to function. Global cyber security rules, definitions and norms are – rightly or wrongly – increasingly seen as being central to the financial future of the cyber insurance market.

3 KEY FACTORS TO MAKE YOUR CYBERSECURITY TRAINING A SUCCESS

WEF - The digital economy continues to evolve at a rapid pace, bringing new technologies, such as AI to every individual and industry around the globe. While AI benefits our society in numerous ways – from transforming sectors such as healthcare and education – cybercriminals are rapidly taking advantage of these tools. Threat actors are harnessing technologies, including AI, to augment the volume and velocity of their attacks, making it inevitable that enterprises will fall victim to a cyberattack. Nearly 90% of organizations experienced one or more cyber incidents last year.

AI COULD EMPOWER AND PROLIFERATE SOCIAL ENGINEERING CYBERATTACKS

WEF - Generative AI (GenAI) and Large Language Models (LLM) in particular, have taken the world by storm. The technology has shown tremendous potential to automate various day-to-day tasks, ranging from basic IT helpdesk requests to sophisticated user behaviour analysis. This task automation is typically carried out by AI agents — autonomous software that is designed to perform tasks and execute actions. Notably, businesses across industries are increasingly adopting AI tools to increase efficiency and reduce costs. However, the rise of AI models has also led to the emergence of new cyberattacks that effectively utilize it, known as AI-based attacks. These attacks are characterized by being automated, adaptive and tailored to their targets. The rise of these attacks opens a new arena in cybersecurity and is changing the cybersecurity landscape. In fact, MITRE has introduced the MITRE ATLAS framework as an extension of the widely used MITRE ATT&CK framework to address the adversarial tactics in AI systems.