DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 20, 2024

DIGI AMERICAS ALLIANCE MEMBERS

COSTA RICA: THEY RECOGNIZE A LACK OF ADVISORS TO LEGISLATE CYBERSECURITY, DATA PRIVACY OR 5G

TyN - The deputy and president of the Science and Technology Commission, Johanna Obando, as well as the secretary of that same commission, José Pablo Sibaja, recognize the lack of expert technology personnel in the Legislative Assembly to advise the deputations, which are the in charge of legislating on topics such as cybersecurity, data privacy, technological development, infrastructure, among others. This was indicated during an event organized by the Costa Rican Union of Chambers and Associations of the Private Business Sector (Uccaep) on the morning of this Tuesday, June 18.

GSI: WITHOUT NEW AGENCY, COUNTRY LOST 14% OF ITS GDP DUE TO LACK OF INFORMATION SECURITY - BRAZIL

Digital Capital - Brazil may have lost around R$1.5 trillion in 2023 to cyberattacks, which represents 14% of the GDP recorded last year and was R$10.5 trillion. These figures were obtained by projecting the same percentage presented at the World Economic Forum, which set the losses generated in the global economy due to cybersecurity problems at 14% of global GDP (US$10.5 trillion). In a more conservative estimate, made by Accenture, this loss reached R$500 billion. The assessment was made by GSI Special Advisor, Marcelo Malagutti, when defending the creation of the National Cybersecurity Agency (ANCiber), during a webinar by Fundação Getúlio Vargas on the topic: “Cybersecurity in Brazil: how to build a strategy and an agency?”.

ARMY PUBLISHES NOTICE AND SEEKS RESOURCES TO CREATE CYBER GUARDIAN 6.0 - BRAZIL

Digital Convergence - The Cyber Defense Command wants public and private partners to organize and enable the exercise of cyber warfare against critical infrastructures, Cyber Guardian 6.0. A public call receives suggestions and proposals for one month. The Cyber Guardian aims to create a realistic environment where participating critical infrastructures need to protect their Information Technology systems from cyber attacks, contributing to the growth of Brazil's cyber resilience, through the collaborative action of the Armed Forces, partner bodies and of the country's main critical infrastructures, adopting constructive and virtual simulation techniques.

BANXICO REPORTS ON TWO CYBERATTACKS SO FAR IN 2024 - MEXICO

Informador - The Bank of Mexico (Banxico) reported that during the first half of 2024, two significant cyber incidents were recorded against two financial institutions. Last March, a Popular Financial Society (Sofipo), whose name was not disclosed, suffered a computer breach in its transfer service. Although cybercriminals attacked the electronic transfer service it provides, customers were not harmed, he said.

DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 20, 2024

THIS IS HOW THEY ARE SCAMMING WITH A FALSE EPM WEBSITE; SIGNS TO IDENTIFY THE ORIGINAL PORTAL - COLOMBIA

Semana - Cybercriminals are increasingly finding new ways to trick users and steal from them through various tricks, such as identity theft. A recent case involves Empresas Públicas de Medellín (EPM), who last Friday, June 14, reported in a statement that their website had been a victim of impersonation. This platform is crucial for citizens to pay their bills. According to the statement, the criminals would have modified the legitimate address of the company, “facturaweb.epm.com.co”, redirecting customers to a bank account controlled by third parties through the fraudulent URL “facturaepm.com.co”.

SENATOR PUGH IS HONORED FOR HIS CONTRIBUTION TO COMMON STRATEGIES FOR CYBERSECURITY - CHILE

Senado - Romania has a responsibility to coordinate the 27 European states to develop cybersecurity competencies. Along these lines, the government of that country recognized the work of Senator Kenneth Pugh in building diplomatic ties between both countries, and in developing common strategies for cybersecurity, thus facilitating investments between Chile and Romania. The distinction was awarded by the President of Romania, Klaus Werner Iohannis through his representative in Chile, the ambassador, Floricel Mocanu. The ceremony, held at the Embassy headquarters, was also attended by the president of the Senate, José García Ruminot and Senator José Miguel Insulza.

U. OF CHILE WILL SHARE CYBERSECURITY TOOLS WITH THE CHILEAN RESEARCH AND EDUCATION NETWORK (REUNA)

UChile - The Vice-Rector of Information Technologies, through the Information Security Office (OSI), signed a cooperation agreement with the Chilean Research and Education Network (REUNA), a platform made up of more than 40 universities, research centers of excellence and international astronomical groups present in our country. The agreement will make automated vulnerability monitoring tools available to all universities and partner institutions of this Network. In this way, it will contribute to carrying out preventive analyses, through proofs of concept, with the aim of early identifying possible computer security incidents.

THE NATIONAL CYBERSECURITY STRATEGY THAT THE GOVERNMENT IS WORKING ON, WHAT WILL IT ENTAIL AND HOW WILL CYBERCRIME BE COMBATED? - URUGUAY

El Pais - Cybersecurity threats are becoming more dangerous, more sophisticated, more recurring and closer to each company and person. “We should all think that we were hacked or that we will be hacked at some point,” say experts on the subject. Given this context, the Uruguayan government is working on its National Cybersecurity Strategy (ENC), which incorporates “investigation agents” outside the popular radar, unifies a vision of the State and focuses on people. The creation of the ENC is part of the Digital Uruguay 2025 Agenda presented by the Agency for Electronic Government and Information and Knowledge Society (Agesic), which seeks to mitigate cybersecurity risks and guarantee the availability of critical information assets.

DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 20, 2024

THE ARMED FORCES CONTINUE TO COLLABORATE WITH NATIONAL CYBERSECURITY - URUGUAY

Gub.uy - In the month of June, experts from the United States Department of Defense (SOUTHCOM & Connecticut National Guard) hold exhibitions for the civil-military public, referring to cybersecurity. In this instance, the Defense Staff summoned those responsible for Cybersecurity of State Infrastructures to attend a presentation by the United States Department of Defense (SOUTHCOM & Connecticut National Guard) consisting of presentations by experts from Areas of Threat Intelligence, International Deployment of Major Incident Response Groups and implementation and best practices of a Cybersecurity Operations Center (SOC).

BANCO BISA PROVIDES TOOLS IN FAVOR OF BUSINESS CYBERSECURITY - BOLIVIA

Fides - “Information Security in companies” is an initiative based on education, awareness and collaboration of Banco BISA and focuses on strengthening collective resilience against cyber threats through meetings with specialists. In this context, regional events were held in La Paz, Cochabamba and Santa Cruz in which representatives of companies and representatives of the BISA specialized in the computer field participated. The main objective of these events was to highlight the importance of cybersecurity in the context of the growing use of digital services and channels in Bolivia.

CISA LEADS FIRST TABLETOP EXERCISE FOR AI CYBERSECURITY

CyberScoop - Looking to build its incident response muscles before artificial intelligence becomes an even greater threat, the federal government on Thursday held its first tabletop for the burgeoning technology, bringing in partners from across the country and abroad for the exercise. The Cybersecurity and Infrastructure Security Agency led the tabletop under the Joint Cyber Defense Collaborative, the operational arm of the cyber defense agency that is focused on working with industry, alongside 50 AI experts from 15 companies and several international cyber defense agencies.

FBI TAKES DOWN ARMY OF ‘ZOMBIE’ COMPUTERS. HERE WHAT TO KNOW

WEF - In late May 2024, the US Federal Bureau of Investigation made an arrest in a case it described at something “ripped from a screenplay”. The operation took down a botnet that had infected millions of computers with malware in nearly 200 countries. Selling access to this network enabled crimes, including billions of dollars of financial fraud, identity theft, bomb threats and access to child exploitation materials around the world. The alleged operator used the proceeds to buy fast cars, luxury watches and properties in multiple countries. The service, known as “911 S5”, is thought to have been the world’s biggest-ever example of a botnet. And it comes as the share of web traffic caused by harmful bots is rising year-on-year.

DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 20, 2024

STATEMENT FROM NATIONAL SECURITY ADVISOR JAKE SULLIVAN ON THE GLOBAL EFFORT TOSTRENGTHEN THE CYBERSECURITY OF ENERGY SUPPLY CHAINS

The White House - Energy systems around the world face continuous cyber attacks and are vulnerable to disruption. As new digital clean energy technologies are integrated, we must ensure they are cyber secure to prevent destruction or disruption in services. This is a global issue and at the G7 Leaders' Summit in Apulia, President Biden and G7 leaders committed to taking critical action to strengthen the cybersecurity of the global supply chain of key technologies used to manage and operate electricity, oil, and natural gas systems across the world. The G7 will work to establish a collective cybersecurity framework for operational technologies for both manufacturers and operators. This builds on the White House Council on Supply Chain Resilience's work to strengthen supply chains critical to America's economic and national security. It also builds upon the efforts of the U.S. Department of Energy (DOE) and Idaho National Laboratory which have brought tremendous expertise to bear in securing operational technologies to date.

THE NEW FRONT IN CHINA'S CYBER CAMPAIGN AGAINST AMERICA

The Economist - The island of Guam, a tiny American territory that lies more than 6,000km west of Hawaii, has long known that it would take a battering in any Sino-American war. The island's expanding airfields and ports serve as springboards for American ships, subs and bombers. In the opening hours of a conflict, these would be subject to wave after wave of Chinese missiles. But an advance party of attackers seems to have lurked quietly within Guam's infrastructure for years. In mid-2021 a Chinese hacking group—later dubbed Volt Typhoon—burrowed deep inside the island's communication systems. The intrusions had no obvious utility for espionage. They were intended, as America's government would later conclude, for "disruptive or destructive cyber-attacks against…critical infrastructure in the event of a major crisis or conflict". Sabotage, in short.