DIGI AMERICAS ALLIANCE MEMBERS

CYBERSECURITY MUST HAVE A STATE AGENCY WITH A PRIVATE PARTNERSHIP, CONCLUDES DEBATE - BRAZIL

LN21 - The World Economic Forum (WEF) identifies cybersecurity as one of the top 10 global risks (public sector and private sector). Cyberattacks have doubled globally since the pandemic. Attacks are becoming increasingly sophisticated. The average cost of a data breach for a government institution in 2020 was US$4.441 million (approximately R$24 million). Brazil has a high level of digitalization, but needs to mature in cybersecurity. These are some of the data presented by participants in a public hearing on international risks to digital security, promoted by the Permanent Subcommittee on Cyber Defense, held on Tuesday (9).

R-CIBER DEEPENS THE RELATIONSHIP BETWEEN TELCOS AND DATA CENTER OPERATORS - BRAZIL

Teletime - The approval of the new Cybersecurity Regulation Applied to the Telecommunications Sector (R-Ciber) by Anatel expanded the list of companies that are directly subject to the package's rules framework. But the change in standards also brings changes to the way telecommunications operators relate to data processing and cloud providers. In an interview with TELETIME, the partner in the public law and regulation area at Veirano Advogados, Beatriz França, drew attention to the fact that, with the new text, data center and cloud providers will be required by telecommunications operators (within private contractual relationships between them) to comply with Anatel cybersecurity rules.

GSI/PR JOINS THE AMAZON WEB SERVICES GLOBAL CYBERSECURITY PROGRAM - BRAZIL

Gov.br - The Institutional Security Office of the Presidency of the Republic (GSI/PR) formalized adherence, through the Secretariat of Information and Cybersecurity, to the Global Cybersecurity Program of Amazon Web Services, an international platform that aims to improve security services cybernetics. The partnership allows the exchange of knowledge, the carrying out of joint research and training, in addition to obtaining data on the impacts of cyber incidents on society. The event was attended by the Secretary of Information and Cyber Security (SSIC) of the GSI/PR, Dr. André Molina, the General Coordinator of the Center for Prevention, Treatment and Responses to Government Cyber Incidents(CTIR Gov), Colonel Maier, and Mr. Paulo Cunha, Public Sector Executive in Brazil at AWS together with advisors from SSIC and executives and advisors from AWS. The Term of Adhesion was formally signed, and the respective Work Plan was approved for joint execution at the Government Network Cyber Incident Prevention, Treatment and Response Center (CTIR Gov).

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 12, 2024

ENTITIES PROPOSE NATIONAL CYBERSECURITY POLICY IN MEETING WITH DEPUTIES - BRAZIL

247 - The meeting held this Monday (8) between deputies of the Tax Reform Working Group and representatives of important entities, such as Consad (National Council of Secretaries of State for Administration), CLP (Public Leadership Center), Ibap (Brazilian Institute of Public Administration) and Conseplan (National Council of Secretaries of State for Planning), highlighted the urgent need for a National Defense and Cybersecurity Policy. The meeting emphasized the strategic importance of information security to guarantee national sovereignty. Fabrício Marques, president of Conseplan, highlighted the relevance of the moment: “This is a decisive moment for the future of Brazil. The Tax Reform proposal needs to be clear about the strategic importance of Information Security and Cybersecurity for the country”. Cybersecurity is crucial in an increasingly digital world, especially for a country like Brazil, which leads the digitalization of services and is a frequent target of cyberattacks, he said.

NATIONAL CYBERSECURITY FORUM ADVANCES: TOWARDS BETTER PUBLIC POLICIES - CHILE

Senado - The second meeting of the National Cybersecurity Forum was described as an important milestone, an innovation initiative in the generation of public policies under the Senate that has the participation of experts from the public, private, scientific and military spheres. In the session to monitor the progress of this initiative, Senator Kenneth Pugh, recognized precursor of this forum, together with Senator Ximena Ordenes (who due to force majeure problems could not attend), explained that they already have 452 registered and another 81 professionals are in the process of participating in this organization that will allow concerns to be channeled and promote collaboration in the field of cybersecurity in Chile.

CYBERCRIME: CRIMES AGAINST MINORS AND ILLICIT ACCESS TO SOCIAL NETWORKS CONCENTRATE INVESTIGATIONS BY THE PDI - CHILE

Diario Concepcion - A call for attention was made by the Investigative Police (PDI), due to the high number of arrests, produced from last year to date, related to crimes against minors, using access to the internet and social networks as a means to access girls, boys and adolescents. This was stated by the head of the Cybercrime Investigative Brigade in the Region, subprefect Andrés Contreras, in the context of the institution's 91st anniversary. “From last year to date, the number of arrests we have for this type of crime is close to 40 arrests. We still have ongoing investigations regarding that crime,” the officer indicated.

NIC CHILE REPORTS INCIDENT IN CLIENT USER ACCOUNTS

NIC - NIC Chile informs that we have detected the occurrence of a cybersecurity incident that has affected the accounts of some of our users during July 3, 2024. In this situation, our initial evaluation indicates that an attacker took advantage of the weakness of some passwords of our clients' user accounts, gaining unauthorized access to them and in some cases modifying the information associated with their DNS servers. We continue to analyze the incident to establish a definitive diagnosis.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 12, 2024

ITAÚ REPORTS CYBERSECURITY INCIDENT THAT COULD AFFECT RAPPICARD CLIENTS - CHILE

La Tercera - This Thursday Itaú reported in a statement a cybersecurity incident that could affect the personal data of RappiCard clients of said bank. As the entity made clear to its users, this exposure would only be for this specific product. The bank emphasized that the reported problem would only involve the exposure of identification and contact data, and completely ruled out that transactional data or access credentials to the RappiCard had been compromised.

ECUADOR AND THE EUROPEAN UNION REINFORCE THEIR SECURITY COOPERATION

EEAS - Ecuador and the European Union in Ecuador have taken significant steps in their joint work to combat organized crime. Through a series of recent initiatives, both partners seek to strengthen cooperation in key areas such as: the fight against drug trafficking and organized crime, crime and cybersecurity. Proof of this commitment is the recent inauguration of the “Europol Unit of the National Police of Ecuador” whose opening responds to the signing of a bilateral agreement in October 2023 to establish diplomatic and police relations. Since European ports are one of the main destinations for drugs coming from Ecuador, the Unit will be able to have a direct link with the National Police for the exchange of information and execution of operations coordinated with the EU to improve the fight against organized crime. transnational.

COSTA RICA REAFFIRMS COMMITMENT TO THE IMPLEMENTATION OF 5G TECHNOLOGY

Summa - This Wednesday the Government of Costa Rica reaffirmed its commitment to the security and privacy of citizens in the implementation of 5G technology, despite facing legal actions that seek to stop the advancement of this important technology. Since August 2023, the Government has promoted executive decree N°44196-MSP-MICITT that seeks to balance the benefits of 5G connectivity with the cybersecurity measures necessary to protect companies and users. However, this decree has been the subject of legal challenges by various entities, including an equipment manufacturing company and the ICE Internal Workers Front union.

CYBERSECURITY SERVICES IN THE COUNTRY GROW 13% AND GENERATE $19 MILLION - COSTA RICA

CRHoy - Cybersecurity services in Costa Rica reach a growth of 13% so far in 2024. This is the data from the Frost Radar report from Frost & Sullivan, which indicates the increase in the percentage compared to last year, with revenues of $19 million. According to Marcelo Ruiz, consulting director of the research firm in the field of technology and innovation, Costa Rica is the country with the most ransomware attacks in Central America, however, since the massive attacks of 2022, it has increased Greater awareness about the importance of cybersecurity in both the private and public sectors. According to the report, one of the main positive aspects that stand out at the national level is that there is a National Cybersecurity Plan with the support of the Organization of American States (OAS), in addition to the technical cooperation agreements with Honduras , Panama, Dominican Republic, Israel and resources with the United States and Spain.

ACTIONS TO MAKE COLOMBIA A POWER IN CYBERSECURITY

La República - Working from the regions to connect Colombia is a Government purpose. And if we talk about cybersecurity, if we do not build digital security that begins in the territories, it will not be possible to achieve a real transformation. Hence, achieving true articulation of all sectors and areas of knowledge is essential to achieve total protection in the digital environment.

ONE YEAR AFTER ITS LAUNCH, THE WORK OF THE CYBERCRIME DIRECTORATE STANDS OUT

Diario de Democracia - Authorities from the Buenos Aires Ministry of Security, the judiciary, police chiefs and the Municipality of Junín met at the Cybercrime Investigations Directorate of the Northern Region Division, located in the Villa del Parque neighborhood, on the first anniversary of its creation and implementation. There, the work of the department was highlighted and they agreed in defining it as "fundamental for the investigation of computer criminal acts." It is worth remembering that Junín has been the first city in the province of Buenos Aires to have a police office dedicated to the investigation of crimes. IT; which was a result of the articulation of actions promoted by the Municipality, the police forces and the Justice for prevention.

THE CNCS: THE GOVERNMENT BODY THAT MONITORS DOMINICAN CYBERSPACE

Gob.do - Cybersecurity and cyberspace are terms that continue to be used very frequently in the Dominican Republic due to the advancement and continuous use of technology in multiple facets of daily life; For the executive director of the National Cybersecurity Center (CNCS), General PN Juan Gabriel Gautreaux Martínez, these two statements group together the measures and protocols used to protect digital assets. When invited to the MAPTV program, Gautreaux Martínez highlighted that the CNCS, an entity chaired by the Ministry of the Presidency, is the government body responsible for ensuring that these protocols and measures are complied with in the country.

CYBERCRIME REORGANIZES IN THE FACE OF POLICE HARASSMENT

Expansion - Cyberattacks have declined this year thanks to large-scale police operations, leading online criminal groups to organize themselves, even launching physical threats, according to experts. 2023 was a record year, both in the number of attacks and the amount extorted from victims. "In the first four months of 2024, the number of publicly reported incidents related to ransomware (blackmail programs) has decreased compared to the first four months of 2023," Allan Liska, cybersecurity expert at Recorded Future, told AFP.

THE RISKS OF A LAST-MINUTE CYBERCRIME TREATY PROTOCOL

Global Initiative - One idea now gaining support among countries seeking a broad scope of crimes in the convention (a bloc led by Russia) is to begin a process of drafting a protocol to the convention – a supplementary agreement that would add a list of ‘additional crimes’ to the original treaty – even though the text of the convention itself is not yet final. Drawing comparisons to the negotiation process of the UN Convention against Transnational Organized Crime (UNTOC), the paper highlights crucial differences in political, practical, and legal contexts.

BUSINESSES ARE HARVESTING OUR BIOMETRIC DATA. THE PUBLIC NEEDS ASSURANCES ON SECURITY

The Conversation - Imagine walking through a bustling railway station. You're in a hurry, weaving through the crowd, unaware that cameras are not just watching you but also recognising you. These days, our biometric data is valuable to businesses for security purposes, to enhance customer experience or to improve their own efficiency. Biometrics, are unique physical or behavioural traits, and are part of our everyday lives. Among these, facial recognition is the most common. Facial recognition technology stems from a branch of AI called computer vision and is akin to giving sight to computers. The technology scans images or videos from devices including CCTV cameras and picks out faces.

AI-POWERED SUPER SOLDIERS ARE MORE THAN JUST A PIPE DREAM

Wired - The day is slowly turning into night, and the American special operators are growing concerned. They are deployed to a densely populated urban center in a politically volatile region, and local activity has grown increasingly frenetic in recent days, the roads and markets overflowing with more than the normal bustle of city life. Intelligence suggests the threat level in the city is high, but the specifics are vague, and the team needs to maintain a low profile—a firefight could bring known hostile elements down upon them. To assess potential threats, the Americans decide to take a more cautious approach. Eschewing conspicuous tactical gear in favor of blending in with potential crowds, an operator steps out into the neighborhood's main thoroughfare to see what he can see.

WHITE HOUSE WANTS TO BOOST CYBER FUNDS FOR FISCAL 2026

Cyberscoop - The White House wants federal agencies to ask for more money that would be used to improve the nation's cyber defenses, per a memo sent to agency heads Wednesday. In the document, Office of Management and Budget Director Shalanda Young and National Cyber Director Harry Coker Jr. directed agencies to review and align incoming budget requests to fit the Biden administration's national cyber strategy and implementation plan. The White House's ask fits with its directive that federal agencies move toward fully mature zero-trust architectures. Agencies will submit an updated zero-trust implementation plan to the OMB and ONCD within 120 days following the memo's release, and be on target by the end of fiscal 2026, the memo states.