DIGI AMERICAS LATAM CISO

INSIGHTS

OCTOBER 17, 2024

DIGI AMERICAS ALLIANCE MEMBERS

SERGIO MORO DEFENDE CRIAÇÃO DE AGÊNCIA DE CIBERSEGURANÇA NO BRASIL

Senado - Senador Sergio Moro (União-PR) defende a criação de uma agência de cibersegurança no Brasil. Segundo o parlamentar, assim como a sociedade tem migrado para o mundo virtual em diversas áreas, como lazer e finanças, os crimes também estão acompanhando essa tendência. Moro é integrante da Subcomissão Permanente de Defesa Cibernética, vinculada à Comissão de Relações Exteriores e Defesa Nacional, que tem como objetivo monitorar as políticas públicas de defesa cibernética e propor novas medidas para enfrentar os desafios crescentes nesse campo.

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 DA A CONOCER SUS LECCIONES APRENDIDAS Y MEJORAS TECNOLÓGICAS Y EN SEGURIDAD DE LA INFORMACIÓN TRAS CIBERATAQUE DE 2023

Chile Compra - La Dirección ChileCompra y el Equipo de Respuesta ante Incidentes de Seguridad Informática CSIRT del Ministerio del Interior, realizaron este miércoles 16 de octubre un taller de ciberseguridad titulado "un año del ciberataque, lecciones aprendidas y mejoras en la plataforma de Mercado Público". En la actividad participaron 273 asistentes presenciales, a los que se sumaron más de 1.800 vistas a la transmisión del evento que generó gran interés de parte de jefes de informática, equipos de administración y finanzas, encargados de la seguridad de la información de distintas entidades públicas y también proveedores. Expusieron en el evento la Subsecretaria de Hacienda, Heidi Berner; el Coordinador Nacional de Ciberseguridad, Daniel Álvarez y el Director de la Secretaría de Gobierno Digital del Ministerio de Hacienda, José Inostroza. Además de la directora de ChileCompra, Verónica Valle, el Jefe de Seguridad de la información y Ciberseguridad, Paolo Jeldres y el Jefe de División de Tecnología, Cristián Cépedes.

DIGI AMERICAS LATAM CISO

INSIGHTS

OCTOBER 17, 2024

CARABINEROS DE CHILE JUNTO A HACKERS UTILIZAN IA PARA COMBATIR EL CIBERCRIMEN

Madboxpc - Una inédita charla tuvo lugar en la versión 2024 de la 8.8 Computer Security Conference, el primer y más importante encuentro técnico de ciberseguridad en Chile. Por primera vez en sus 14 años de existencia, Carabineros de Chile participó con una divertida y didáctica exposición ante hackers y expertos en ciberseguridad. Con su charla “Proyecto Sitia, Sistema Integrado de Teleprotección con IA”, el Capitán Miguel Ramírez Veas, Jefe de Área Ciberseguridad y Continuidad Operacional TIC, y el Sargento 2do. Darwin Muñoz García, Encargado de Ciberseguridad de la institución, conquistaron al público asistente, y destacaron la oportunidad de compartir en la 8.8 con personas tan apasionadas como ellos por la ciberseguridad.

¿AGENCIA DE CIBERSEGURIDAD PARA ‘CENSURAR LAS REDES SOCIALES’? - COLOMBIA

El Tiempo - En días pasados se vivió una de tantas discusiones plagadas de consideraciones políticas coyunturales alrededor de un tema estructural y necesario para el país: contar con una agencia de ciberseguridad que eleve las capacidades del Estado y la sociedad de defenderse y prevenir riesgos y ataques digitales. Una discusión dejó en claro la visión tan cortica y básica que tenemos como sociedad sobre temas relevantes de país. Vimos ‘geniales conclusiones’, incluso de denotados colegas, como que “el gobierno Petro va a censurar las redes sociales” con esa norma. Me produce genuino pesar gastar renglones de este valioso espacio para discernir alrededor de semejante tontería, básicamente porque partir de la pobreza del odio político para analizar la realidad es un muro infranqueable que deja, del otro lado, y en este caso, los argumentos técnicos, científicos y socioeconómicos que sostienen la necesidad de contar con ese marco normativo de ciberseguridad.

ATAQUES CIBERNÉTICOS COSTARON MÁS DE $500.000 MILLONES AL SECTOR FINANCIERO EN 2023 - COLOMBIA

La República - En el acto de instalación del 17° Congreso de Seguridad, Amenazas cibernéticas, Fraude y Experiencia, el presidente de Asobancaria, Jonathan Malagón, inició su intervención mencionando el cambio que existía hace 10 años en el sector financiero. "Hace una década, 55% de las transacciones se hacían en canales físicos, 80% de la consulta de saldo se hacía en cajeros automáticos". "Hoy, tan solo 21% de las transacciones se hacen por canales físicos, hay aproximadamente 23 millones menos de cheques en circulación y 0% de las tarjetas cuentan solo con banda magnética de protección", añadió el presidente. Sin embargo, aunque los casos de clonación de tarjetas redujeron 86%, los de fleteo 49% y los de hurto en oficinas bancarias 30%, “en 2023 hubo 407.000 casos de fraude a través de Internet y esto le costó al sector más de $500.000 millones”, comentó el dirigente.

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.

DIGI AMERICAS LATAM CISO

INSIGHTS

OCTOBER 17, 2024

PARAGUAY | MITIC Y EL CONSEJO DE CIBERSEGURIDAD DE EUA ACUERDAN FORTALECIMIENTO EN CIBERSEGURIDAD A TRAVÉS DE MEMORÁNDUM DE ENTENDIMIENTO

DPL News - En un paso significativo para el Paraguay en materia de ciberseguridad, el Ministerio de Tecnologías de la Información y Comunicación (Mitic) y el Consejo de Ciberseguridad de los Emiratos Árabes Unidos firmaron en la ciudad de Dubai, un Memorándum de Entendimiento (MOU) para colaborar en áreas clave relacionadas con la seguridad de la información. El acuerdo fue firmado por el Ministro del Mitic Gustavo Villate, y el Dr. Mohammed Hamad Al Kuwaiti, Jefe de Ciberseguridad del Gobierno de los Emiratos Árabes Unidos, para establecer un marco de cooperación en varios aspectos esenciales para la protección digital de ambos países.

EL GOBIERNO BONAERENSE ORGANIZA EL FORO PROVINCIAL DE CIBERSEGURIDAD - ARGENTINA

La Capital MDP - La temática de la ciberseguridad ha cobrado una creciente relevancia en la medida en que organismos públicos, empresas y personas tienen la necesidad de proteger enormes cantidades de datos y flujos de información digital. Del 15 al 17 de octubre, este será el eje central de debate del Foro Provincial de Ciberseguridad organizado por la Subsecretaría de Gobierno Digital del Ministerio de Gobierno de la Provincia de 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.

DIGI AMERICAS LATAM CISO

INSIGHTS

OCTOBER 17, 2024

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.