DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 26, 2024

DIGI AMERICAS ALLIANCE MEMBERS

PRELIMINARY POST INCIDENT REVIEW - CROWDSTRIKE

CrowdStrike - On Friday, July 19, 2024 at 04:09 UTC, as part of regular operations, CrowdStrike released a content configuration update for the Windows sensor to gather telemetry on possible novel threat techniques. These updates are a regular part of the dynamic protection mechanisms of the Falcon platform. The problematic Rapid Response Content configuration update resulted in a Windows system crash. Systems in scope include Windows hosts running sensor version 7.11 and above that were online between Friday, July 19, 2024 04:09 UTC and Friday, July 19, 2024 05:27 UTC and received the update. Mac and Linux hosts were not impacted. The defect in the content update was reverted on Friday, July 19, 2024 at 05:27 UTC. Systems coming online after this time, or that did not connect during the window, were not impacted.

GLOBAL IT OUTAGE: THE CYBER RESILIENCE ALARM HEARD AROUND THE WORLD

WEF - Last week, one of the largest IT outages in history disrupted businesses and governments around the world. The incident, which affected 8.5 million Microsoft Windows devices, led to widespread disruptions of airlines, banks, broadcasters, healthcare providers, retail payment terminals and cash machines globally. The cost of the outage is estimated to top $1 billion. The disruption was caused by a flawed update to a cloud-based security software of CrowdStrike, one of the global top cybersecurity companies. The update to the Falcon software triggered a malfunction that disabled parts of the computer systems and software like Microsoft Windows. Three days after the incident, CrowdStrike reported that a significant number of the devices are back online and operational.

PM DE SP APREENDE UNIDADE MÓVEL DE CIBERCRIME - BRASIL

CISO Advisor - A Polícia Militar de São Paulo descobriu, em uma ação de patrulha na Capital, um veículo equipado com um “stingray” improvisado: um stingray é um equipamento portátil que transmite um sinal de rede celular, fazendo com que aparlhos celulares das proximidades se conectem a ele como se estivessem se conectando a uma antenas de ERB (estações rádio-base) de uma operadora de telecomunicações. A detenção aconteceu na noite do dia 23 de Julho, terça-feira desta semana, na avenida Professor Luiz Ignácio Anhaia Mello, na zona Leste. O veículo era um Jeep Renegade branco, que foi parado porque despertou suspeitas entre os policiais ao trafegar com as luzes apagadas.

ESPERIDIÃO AMIN DESTACA AUDIÊNCIA PÚBLICA SOBRE SEGURANÇA CIBERNÉTICA - BRASIL

Senado - O senador Esperidião Amin (PP-SC) destacou, em pronunciamento nesta terça-feira (16), audiência pública realizada pela Subcomissão Permanente de Defesa Cibernética (CREDC), na semana passada, para debater os riscos internacionais em segurança cibernética e a importância de uma agência nacional de segurança digital no Brasil. O parlamentar, que é presidente do colegiado, ressaltou que o Fórum Econômico Mundial estima que os crimes cibernéticos estão afetando mais de 10% do produto interno bruto (PIB) dos países do Ocidente.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 26, 2024

ADVIERTEN LIBERACIÓN DE “INFORMACIÓN SENSIBLE” DE BASE DE DATOS DE CIUDADANOS BOLIVIANOS

El Deber - La página Hacking Bolivia advirtió que un “actor de amenazas” está liberando la base de datos de ciudadanos bolivianos que contiene “información sensible” y que podría ser utilizado por estafadores digitales. Además, esta misma cuenta aseguró que hubo 'posibles accesos no autorizados' a sistemas y servicios gubernamentales. Un experto explicó que existen riesgos para un ciudadano común si es que acceden a su información privada y personal.

CIBERATAQUE PARALIZÓ LOS SISTEMAS DE UNA MUNICIPALIDAD DE LA COSTA DEL RÍO URUGUAY

El Entrerios - La Intendencia de Paysandú sufrió en la tarde de este miércoles un ciberataque que inactivó buena parte de las operaciones que realiza habitualmente utilizando redes y servicios de Internet. Desde el municipio lo calificaron como “un incidente de ciberseguridad que afecta el normal funcionamiento de sus sistemas”, los que todavía no han están funcionando normalmente.El secretario general de la Intendencia, Fermín Farinha, confirmó que “se está trabajando conjuntamente con CERTuy”, el Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay, conformado por especialistas en ciberseguridad, de la Agencia de Gobierno Electrónico y Sociedad de la Información del Conocimiento (Agesic).

EN UNA SEMANA LA RED DE CIBERCRIMEN DE LA POLICÍA INTERVINO EN CERCA DE 50 CASOS - ARGENTINA

El Territorio - Recientemente la Policía de Misiones puso en funcionamiento una red de 30 agentes especializados en Cibercrimen, quienes están trabajando en las 15 Unidades Regionales. Desde su inicio han recibido numerosas solicitudes de asesoramiento por parte de vecinos, así como de entidades privadas y públicas, sobre medidas para evitar estafas y ciberdelitos. La formación de los efectivos, brindada por la Dirección de Cibercrimen, se centró en el abordaje de los delitos informáticos más comunes, tales como estafas, hacking, phishing, grooming, preservación y secuestro de dispositivos, así como extracciones de secuencias fílmicas en domicilios y comercios para el análisis probatorio judicial.

PCM REALIZÓ PRIMER SIMULACRO INTERNACIONAL DE ATAQUES CIBERNÉTICOS CON 102 ENTIDADES PÚBLICAS Y PRIVADAS - PERÚ

Gob.pe - La Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno y Transformación Digital, realizó el Primer Simulacro Internacional de Ataques Cibernéticos para reforzar las capacidades de seguridad digital de las entidades públicas y privadas del país. Durante cuatro horas seguidas, se conectaron en simultáneo 364 especialistas de 102 entidades, quienes se enfrentaron a una serie de simulaciones de ataques en diferentes escenarios digitales diseñados por el Centro Nacional de Seguridad Digital, para observar las acciones de los equipos de respuesta ante incidentes de seguridad digital.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 26, 2024

GUARDIA NACIONAL INAUGURA JORNADA DE CIBERSEGURIDAD 2024 “INTERNET SEGURO PARA TODAS Y TODOS” - MÉXICO

Gob.MX - Con el objetivo de concientizar y sensibilizar a la sociedad sobre la importancia del uso responsable de las tecnologías de la información, así como de promover la cultura de la denuncia de los delitos en el entorno digital, la Guardia Nacional, a través de la Dirección General Científica, inauguró la Jornada de Ciberseguridad 2024 “Internet seguro para todas y todos”. Se trata de un esfuerzo conjunto entre autoridades e instituciones del servicio público y privado, además de organismos de la sociedad civil, vinculados con el uso de las nuevas tecnologías, quienes llevan a cabo una serie de conferencias, paneles y entrevistas, orientadas a prevenir y enfrentar los nuevos delitos en materia de seguridad cibernética, tales como fraudes en el comercio electrónico, usurpación de identidad, acoso sexual en línea o trata de personas, entre otros.

IMPULSAN CIBERSEGURIDAD EN EMPRESAS E INSTITUCIONES EN GUANAJUATO - MÉXICO

Mexico Industry - Durante el primer trimestre de 2024, México experimentó un aumento del 28 por ciento en ciberataques comparado con el mismo periodo de 2023, según Check Point Research. Ante estos retos, IDEA GTO y las empresas ho1a Innovación y MetroCarrier de Megacable a través de una alianza brindarán herramientas, conocimiento y estrategias de ciberseguridad para empresas e instituciones con el objetivo de fomentar la cultura de seguridad digital que garantice la protección de su información, redes y sistemas, ante los riesgos y amenazas del entorno.

MUJERES DE COLOMBIA PODRÁN CAPACITARSE GRATIS EN INTELIGENCIA ARTIFICIAL Y CIBERSEGURIDAD - MINTIC

MINTIC - El Ministerio TIC promueve la participación del género femenino en la industria tecnológica, de ahí que en alianza con la comunidad Hacker Girls, lance el programa 'Women Training Series', que brindará espacios de formación, conexión y potenciará mejores oportunidades laborales para 1.000 mujeres que podrán capacitarse gratis en Inteligencia Artificial y Ciberseguridad. "Estamos trabajando por incentivar la participación de las mujeres en el sector tecnológico y cerrar la brecha de género. Es por ello que, con la iniciativa Hacker Girls, apoyamos los espacios de educación y las oportunidades laborales en áreas asociadas a las tecnología de la información. Extendemos una invitación muy especial a todas las mujeres de Colombia para que se capaciten en estos temas, los cuales cada vez toman más relevancia", manifestó el ministro TIC, Mauricio Lizcano

ORGANIZACIONES DE DERECHOS HUMANOS ALERTAN SOBRE LOS RIESGOS DEL TRATADO SOBRE CIBERCRIMEN A SER DISCUTIDA EN LA ONU

Derechos Digitales - Organizaciones de derechos humanos, derechos digitales y libertad de prensa se reunieron este 24 de julio con medios de comunicación para abordar los riesgos del tratado de la ONU sobre Cibercrimen. El tratado presenta serios riesgos para el ejercicio de los derechos humanos y la igualdad de género, así lo señalaron las y los expertos, Tirana Hassan, directora ejecutiva de Human Rights Watch, Paloma Lara-Castro, coordinadora de políticas públicas de Derechos Digitales, Katitza Rodriguez, directora de política de Privacidad Global de Electronic Frontier Foundation y Khadija Patel, presidenta del Instituto Internacional de Prensa.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 26, 2024

NASA'S SCIENCE MISSION SPACECRAFT ARE AT RISK FROM HACKERS, BUT A NEW LAW COULD HELP PROTECT THEM

The Conversation - Nasa's missions are some of the most technologically advanced and critically important endeavours. From the Mars Rover explorations to the Artemis missions to the Moon, the space agency's projects push the boundaries of science and technology. However, these missions are also prime targets for cyber-attacks. In a bold move to counter the escalating threat of these attacks, US congressmen Maxwell Alejandro Frost and Don Beyer have proposed the Spacecraft Cybersecurity Act. If passed, the legislation would mandate the US space agency Nasa to overhaul the way it procures and builds its spacecraft.

THE NEED FOR A STRATEGIC APPROACH TO DISINFORMATION AND AI-DRIVEN THREATS

Rusi - Recent changes in governments across NATO countries – with the potential for more in the near future – have unfolded as several countries commit to increased levels of defence spending. UK Prime Minister Keir Starmer went even further by declaring his government's intention to reach a 2.5% commitment and announcing plans to publish a 2025 strategic defence review. The shift in support of defence spending is driven in part by concerns that a potential second Trump presidency will lead to a US retreat from NATO countries that fail to meet the 2% GDP defence spending threshold. Additionally, the current threat of kinetic warfare on the European continent – unprecedented since the Second World War – has compelled many European countries to enhance their military capabilities and bolster their defence institutions more broadly. This includes investing in modern, more technology-enabled capability, boosting weapons production, and launching extensive armed forces recruitment programmes.

RUSSIA'S CYBER CAMPAIGN SHIFTS TO UKRAINE'S FRONTLINES

Rusi - With the main thrust of Russia's anticipated summer offensive underway, it is an opportune moment to take stock of the significant and underappreciated changes that have taken hold in Moscow's approach to cyber operations in Ukraine. Much Western analysis to date has fixated on Russia's highly visible opening cyber offensive, the merits of its approach, and the potential for a renewed destructive campaign of a similar nature against Ukrainian critical infrastructure. This focus is misplaced, however, and has anchored Western understanding of the war's cyber dimensions to Russia's countervalue strategy to amass societal pressure via the widespread sabotage of computer networks – an approach that has not seen primacy since the invasion's first year when assumptions about a short war still guided Russia's theory of victory.