ISSN: 2718-6245

OBSERVATORIO ARGENTINO DEL CIBERESPACIO

Director del Proyecto: BM (R) Alejandro Moresi
Codirector: TC (R) Ing Carlos Amaya
Editora: Bib Alejandra Castillo

ISSN: 2718-6245
http://www.esgcffaa.edu.ar/esp/oac-boletines.php

AÑO 3 N° 26
Agosto 2020

OAC Boletín de Agosto 2020

""La información y la guerra psicológica vendrán sobre todas las formas y métodos de operaciones en las guerras futuras para lograr la superioridad en la tropa, el control de armas, erosionar la moral el espíritu psicológico del personal de las fuerzas armadas y la población del enemigo. En efecto, la guerra de información y las operaciones psicológicas son las bases para la victoria."

S. G. Chekinov and S. A. Bogdanov
Pronosticando la naturaleza y contenido de las guerras futuras

Tabla de Contenidos

El **Observatorio Argentino del Ciberespacio** (**OAC**), micro-sitio de la **Escuela Superior de Guerra Conjunta**
URL: http://www.esgcffaa.edu.ar/esp/oac-boletines.php,.
Es un esfuerzo posible por el financiamiento que el observatorio recibe de la **Universidad de la Defensa Nacional**, a través de los programas UNDEFI y se encuentra inserto en la **Antena Territorial de Defensa y Seguridad** de la Secretaría de Ciencia y Tecnología de la Nación y es administrado por el **Centro de Estudios de Prospectiva Tecnológica Militar "Grl Mosconi" de la Facultad de Ingeniería del Ejército Argentino**
Nuestro objetivo se reafirma en la intención de llevar a la comunidad ciberespacial distintas perspectivas de este nuevo ámbito operacional, aportando novedades reportes e informes que permitan a la comunidad educativa y a la sociedad en general conocer más acerca del mismo

ESTRATEGIA

Monitor Mundial de Residuos electrónicos

La organización Mundial de Telecomunicaciones presentó La tercera edición del Global E-waste Monitor 2020, lanzada en julio de 2020 por Global E-waste Statistics Partnership , proporciona una visión integral para abordar el desafío global de los desechos electrónicos. Se reportó un récord de 53.6 millones de toneladas métricas (Mt) de desechos electrónicos (productos desechados como una batería o enchufes así como computadoras y teléfonos móviles) generados en todo el mundo en 2019, un aumento de 9.2 Mt en cinco años. Aquí, les presentamos un mapa interactivo del problema

https://globalewaste.org/map/

La innovación compromete a los usuarios a un mayor control estatal

En este artículo los expertos en Internet hablan acerca de las industrias de comunicaciones y redes de alta tecnología de China están proponiendo una gran cantidad de capacidades futuras por venir si los vendedores se unen a compañías como Huawei y ZTE. Pero estas nuevas tecnologías, una vez instaladas, conducirían a sus usuarios por un camino cerrado y abierto al control del gobierno chino

https://www.afcea.org/content/technology-innovation-defines-china%E2%80%99s-internet-grab?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=uc5u6

CIBERDEFENSA

Retener los RRHH, una clave sin descifrar en 2 ambientes operacionales

Más que nada, marcar la diferencia y permanecer en la misión son las claves para la retención.

“Lo que es realmente interesante es que el Recurso Humano que estamos obteniendo de Estados Unidos nunca ha sido más relevante". "Los especialistas nativos que están llegando al ejército hoy son exactamente los guerreros que necesitamos para el futuro. Se trata más de descubrir cómo liberar el talento y la capacidad que hay dentro de ellos que de enseñarles cosas". Así se expresaron los principales líderes del U.S. Space Command y del U.S. Cyber Command.

https://www.defense.gov/Explore/News/Article/Article/2037131/making-a-difference-fuels-retention-in-space-cyber-commands/

Israel , en alerta por ataques al sistema de potabilización de agua

Dos ataques cibernéticos han afectado las instalaciones de gestión del agua de Israel, tuvieron lugar el mes pasado, en junio, y no causaron ningún daño a las organizaciones atacadas. El primer ataque fue sobre las bombas de agua agrícolas en la parte superior de Galilea, mientras que el segundo se centró sobre las bombas de agua en la provincia central de Mateh Yehuda.

https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/

Reduciendo el riesgo de ataque vía IoT

Algunos aspectos para reducir el impacto de ciberataque sobre Internet de las Cosas (IoT), un término muy amplio que implica el uso de computadoras simples, que incluyen una gran cantidad de productos electrónicos de consumo, como marcos de fotos conectados a Internet o altavoces inteligentes que realizan un número limitado de funciones. Pero el término también incluye dispositivos que se utilizan con fines comerciales, como sistemas de automatización de edificios, termostatos o controles de escaleras mecánicas, y dispositivos de automatización de oficinas, como monitores conectados a Internet en salas de conferencias. Todos estos dispositivos "simples" tienen una cosa en común: crean nuevas superficies de riesgo para la red en la que residen.

https://www.afcea.org/content/four-steps-reduce-iot-risk?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=rc5u6

CIBERGUERRA

Documento de Interés (breve informe)

La guerra cibernética de Putin: el Estado de Rusia en el quinto dominio

En este documento el Dr. Andrew Foxall, examina en resumen cuestiones como: **(1)** Acontecimientos en los últimos dos años, entre ellos la anexión de Crimea y la intervención militar en Siria, han demostrado que Rusia ha vuelto a una política exterior agresiva. Las capacidades que Rusia ha demostrado durante este período han tomado desprevenido a Occidente. **(2)** El enfoque distintivo de Rusia en la guerra en Ucrania ha resaltado la capacidad del Kremlin para la guerra de la información. No hay nada fundamentalmente nuevo sobre las técnicas y métodos empleados por Rusia, con la guerra cibernética la Internet ha facilitado más los objetivos de la guerra de información. **(3)** Durante la última década, Rusia ha demostrado una mayor capacidad de guerra cibernética y una creciente voluntad de usarlos para una variedad de propósitos, incluso para descartar y distorsionar información; desorientar a los estados nacionales y distraer o apoyar actividades militares convencionales. El empleo de hackers no formalmente pertenecientes al estado ruso, para atacar estados-nación, plantas industriales, instituciones financieras, departamentos gubernamentales, medios de comunicación y otros objetivos occidentales. **(4)** Mostraron habilidad para combinar la guerra cibernética con la guerra convencional. En su guerra con Georgia, en 2008, las ofensivas terrestres de Rusia fueron acompañadas por ataques cibernéticos generalizados a sitios web del gobierno. En su guerra con Ucrania, desde 2014, la guerra híbrida de Rusia incluyó ataques cibernéticos no solo en sitios web gubernamentales y de medios, sino también en energía infraestructura. **(5)** La tendencia de emplear la guerra cibernética de Rusia en igual relación que con la guerra convencional, ha desarrollado capacidades agresivas permiten constituir una amenaza en curso para los países occidentales deben planificar la amenaza de subversión y desestabilización. Occidente debería adoptar un enfoque más duro para la guerra cibernética; invertir recursos en recopilación de inteligencia, abordando las debilidades que facilitan las actividades del Kremlin, y financiar un programa educativo para la seguridad de Internet

https://www.stratcomcoe.org/afoxall-putins-cyberwar-russias-statecraft-fifth-domain

Como mide sus resultados el Ciber-Comando de los EE.UU.

A lo largo de estas misiones, los líderes han aprendido que deben ser flexibles, ya sea en tácticas, estructura de equipos o las capacidades que necesitan o desarrollan. Cuando examinan si una operación determinada o incluso cuando una estrategia ha tenido éxito, no están analizando las métricas, sino los resultados.

https://www.c4isrnet.com/cyber/2020/07/10/cyber-commands-measure-of-success-outcomes/

Ejercicio Cyber Flag 19-1

Un ejercicio cibernético de una semana diseñado para mejorar la preparación para ataques cibernéticos y para forjar alianzas entre quienes serían convocados durante un evento del mundo real para mantener a los actores maliciosos fuera de la infraestructura cibernética crítica. Esta edición del ejercicio consistió en frustrar los ataques maliciosos y las intrusiones en una red de Sistemas de Control Industrial / Control de Supervisión y Adquisición de Datos creada específicamente para el ejercicio para simular un caso basado en instalaciones portuarias.

https://www.defense.gov/Explore/News/Article/Article/1896846/cyber-flag-exercise-focuses-on-partnerships/

CIBERCONFIANZA

Los grupos de trabajo para el futuro de Internet

Si bien el crecimiento de Internet a veces parece caótico, existen grupos que trabajan en la investigación de protocolos, aplicaciones, arquitectura y tecnología, así el grupo de trabajo de investigación de Internet (IRTF) se centra en cuestiones de investigación a más largo plazo relacionadas con Internet, mientras que la organización paralela, el Grupo de trabajo de ingeniería de Internet (IETF), se centra en los problemas a corto plazo de ingeniería y elaboración de normas. En este link también encontrará información sobre el Grupo de Investigación de: (1) Cryto, (2) investigación de redes, (3) investigación de infraestructuras de Internet descentralizadas, (4) Consideraciones sobre el protocolo de derechos humanos, (5) Congestión de internet, (6) Redes centradas en la información. Y muchos más

https://irtf.org/

EE.UU: hace recomendaciones a sus Agencias sobre el uso de videoconferencias

Es una guía destinada al asesoramiento y apoyo a las agencias federales para incorporar seguridad cibernética al adoptar o expandir el uso de software de videoconferencia y herramientas de colaboración en línea. La guía también incluye sugerencias para las personas que usan estas herramientas para organizar y asistir a reuniones, información que es particularmente crítica a medida que las agencias transmiten cada vez más debates sensibles sobre estas plataformas.

https://www.cisa.gov/publication/cybersecurity-recommendations-federal-agencies-using-video-conferencing

CIBERSEGURIDAD

Índice de Inteligencia de Amenazas 2020 de X-Force IBM

La inteligencia de amenazas accionable puede ayudar a su organización a asignar recursos, comprender amenazas relevantes y reforzar su estrategia de seguridad. El índice anual de inteligencia de amenazas IBM X-Force® arroja luz sobre los mayores riesgos cibernéticos que enfrentan las organizaciones hoy en día, con datos recopilados durante el año pasado. Obtenga nuevas ideas sobre las tendencias que configuran el panorama de amenazas, que incluyen: (1) 8.500 millones de registros violados en 2019, dando a los atacantes acceso a más credenciales robadas. Asegurar las credenciales y los controles de acceso es más importante que nunca. (2) 150,000 vulnerabilidades reveladas hasta la fecha. Contrarestar vulnerabilidades sigue siendo un problema para muchas organizaciones. (3) Los ataques de ransomware aumentaron un 67% en el cuarto trimestre de 2019. Los actores de amenazas están innovando con un nuevo código de ransomware para ataques destructivos. (4) Los ataques de tecnología operativa (OT) aumentaron 2.000% año tras año. Los actores de amenazas continúan cambiando su vista para atacar vectores que incluyen IoT, OT y sistemas industriales y médicos conectados. (5) Los ataques de la industria minorista aumentaron. La industria número dos después de los servicios financieros, el comercio minorista, fue el objetivo de los

datos de la tarjeta de pago y los valiosos datos del programa de lealtad. (6) América del Norte, el mayor objetivo geográfico. Asia, Europa, Medio Oriente y América del Sur siguieron a América del Norte en número de ataques. El informe está disponible en :

https://www.ibm.com/security/data-breach/threat-intelligence

Las medidas de resiliencia para COVID 19 en el Mundo

La Plataforma de la Red Global de Resiliencia ha desarrollado un mapa interactivo donde podemos ver las medidas que cada Estado toma para formular políticas y compartir información, ver qué iniciativas y medidas se han introducido en todo el mundo, debatir e intercambiar entre pares acerca de experiencias, iniciativas en curso, medidas normativas y normativas innovadoras para ayudar a que las comunidades permanezcan conectadas, aprovechando el potencial de las TIC durante esta crisis y recuperación a medio y largo plazo de COVID19.

https://reg4covid.itu.int/

Los viejos lenguajes y los programas vigentes un desafío no considerado

El artículo expone el problema en este caso con el lenguaje COBOL y los millones de líneas de código vigentes en muchos sistemas bancarios y de la administración pública sin RR.HH. para su mantenimiento y la migración es un desafío pendiente

https://www.ticbeat.com/tecnologias/nueva-jersey-busca-programadores-cobol/

CIBERFORENSIA

Informes de la Agencia de Ciberseguridad e Infraestructuras de los EE.UU

En esta área hemos incorporado los informes semanales que proporciona la CISA (Cybersecurity & Infrastructure Security Agency) de los EE.UU., estos boletines proporciona un resumen de las nuevas vulnerabilidades que han sido registradas por la Base de Datos de Vulnerabilidad (NVD) del Instituto Nacional de Estándares y Tecnología (NIST) .

Semana de 6 de julio: https://us-cert.cisa.gov/ncas/bulletins/sb20-195

Semana del 13 de Julio: https://us-cert.cisa.gov/ncas/alerts/aa20-195a

Semana del 20 de julio: https://us-cert.cisa.gov/ncas/bulletins/sb20-209

Semana del 29 de Julio: https://us-cert.cisa.gov/ncas/bulletins/sb20-209

AGENDA de INTERÉS

Cursos y Seminarios en Línea

- 18 de Agosto a distancia: Comienza la **Diplomatura en Gestión de la Ciberseguridad** en la Escuela Superior de Guerra Conjunta http://www.esgcffaa.edu.ar/esp/actividades-detalle.php?id=222, inscripciones a cursoextension.esgc@gmail.com
- 1 al 5 de agosto; evento virtual de Black Hat información: https://www.blackhat.com/us-20/briefings/schedule/index.html
- 22 al 25 de Septiembre 2020;: Tactical Edge Conferencias de Ciberseguridad https://tacticaledge.co/archive_2018_es.html
- Conversando Cyberseguridad todos los sábados a las 1630 https://tacticaledge.co/conversando_cyberseguridad.html

Sitio web:
http://www.esgcffaa.edu.ar/esp/oac-boletines.php
Nuestra dirección postal es:
* | Luis María Campos 480 - CABA - República Argentina |
* Nuestro correo electrónico:
*|observatorioargentinodelciberespacio@conjunta.undef.edu.ar | *