FE DE ERRATAS 2do Boletín OAC

Un error involuntario en la redacción y edición de este segundo boletín del OAC, ha provocado la necesidad de reenviar a nuestros apreciados suscriptores una nueva edición que anula la anterior.

Rogamos sepan disculpar.

CIBERCONFIANZA

ACERCA DE LA PRIVACIDAD DE LOS DATOS

Como se prepara Google

El año pasado, Google asumió el compromiso de cumplir con el nuevo Reglamento General de Protección de Datos (GDPR) de Europa, para todos los servicios que brinda en la Unión Europea.

Han estado trabajando con mucho esfuerzo en la implementación durante más de dieciocho meses antes de que entre en vigor la nueva ley.

Aquí se presenta una actualización de algunos de los pasos claves que han tomado.

https://www.blog.google/topics/public-policy/our-preparations-europes-new-data-protection-law/

Como se prepara Apple

Los escándalos recientes han revelado la cantidad de datos que recopilan varias compañías tecnológicas. Los usuarios de Android, especialmente han tenido una llamada de atención con respecto al alcance del seguimiento de la ubicación y a la recopilación de datos que estaba llevando a cabo Google y Facebook.

¿Pero cuántos datos dan los usuarios de iPhone a Apple?. ZDnet realizó una investigación y descubrió que, si bien Apple alberga una gran cantidad de datos sobre usted, se trata principalmente de metadatos en lugar de contenido real.

https://www.nextgov.com/analytics-data/2018/05/how-much-data-does-apple-have-you-heres-how-find-out/148251/

EL BIG DATA ROMPERÁ LAS ESTADÍSTICAS EN MATERIA DE EMPLEO

2018 se presenta como un año apasionante desde el punto de vista de la tecnología y la extracción de ideas valiosas acerca de los datos que generamos en el día a día.

https://retina.elpais.com/retina/2018/01/16/tendencias/1516082670_295394.html

¿POR QUÉ ATACAN LOS HACKERS?

Más allá de los beneficios económicos que puede dejar esta actividad delictiva, los hackers tienen razones tan fuertes como la política o tan humanas como estar enojados.

http://www.elfinanciero.com.mx/tech/los-motivos-de-los-hackers.html

---

CIBERDEFENSA

UNA FORMA DE HACERSE DE RRHH PARA LA CIBERDEFENSA

Uno de los aspectos más importantes en el tema de ciberdefensa es la captación y fidelización de RRHH, aquí publicamos una solución que ha encontrado España, para incrementar sus fuerzas de ciberdefensa. Es esto una fuerza adicional encubierta o solo un directorio de quienes son los que saben sobre el tema**?**.

http://www.abc.es/espana/abci-espana-fichara-2000-hackers-y-expertos-civiles-contra-ciberamenazas-201801140302_noticia.html

https://bitlifemedia.com/2017/10/la-ciber-reserva-no-es-mas-que-una-libreta-de-direcciones-angel-gomez-de-agreda/

CIBERGUERRA

OPERACIONES CIBERNÉTICAS DE ESCALA

En febrero de 2016 W.J.HENNIGAN, publicó que los comandantes estadounidenses montaron una ofensiva cibernética contra el Estado Islámico en Siria, la operación más importante desde que se estableció el comando de ciberdefensa en 2009. La misma consistió en el despliegue de hackers militares contra las redes de computadoras y teléfonos celulares del grupo extremista.

El asalto digital, fue lanzado desde Fort Meade en Maryland y marcó la primera gran integración del Comando Cibernético de EE.UU.

Funcionarios del Pentágono describieron el creciente rol del Comando Cibernético como parte de un "cambio estratégico" de la defensa cibernética a la ciberofensiva como una nueva herramienta para el combate y la lucha antiterrorista.

El objetivo fue "sobrecargar sus redes" e "interrumpir su capacidad de comando y control de las fuerzas" con jamming y otras ciberherramientas.

http://www.latimes.com/nation/la-fg-isis-cyber-20160228-story.html

LA INTELIGENCIA ARTIFICIAL (AI) Y LAS ARMAS DE HACKEO

El experto de la Universidad de Ben-Gurion (BGU) Bracha Shapira, hablando con The Jerusalem Post después de su presentación en el Foro Económico Mundial de Davos, dijo que los ciberataques que usan IA "están ganando ... su participación es más fácil ... las cosas no son buenas en este momento".

Las técnicas de defensa cibernética de AI podrían utilizarse para la detección inteligente de ataques. El aprendizaje automático supervisado puede clasificar entre patrones buenos y malos si "existen suficientes datos para aprender esos patrones y poder identificar nuevos ataques que se desvían del patrón normal", dijo.

Además, "cada programa deja huellas únicas en el ciberespacio que pueden rastrearse y aprenderse. Los programas maliciosos tendrían un patrón diferente del comportamiento normal, ya que deben actuar de manera diferente para lograr sus objetivos ", explicó.

A diferencia de los analistas humanos más inteligentes, Shapira dijo que la defensa cibernética aplicando **AI** puede ir más allá de un simple diagnóstico de un ataque, para observar "todas las capas de tráfico cibernético en la red ... no solo una capa ... puede mirar la línea de tiempo y utiliza algoritmos potentes para procesar toda la información ".

http: //www.jpost .com / Israel-Noticias / Inteligencia artificial-ciber-hacking-arms-race-at-throttle-539886

¿ATAQUES CIBERNÉTICOS DEVASTADORES PUEDEN ¿PROVOCAR EL EMPLEO DE ARMAS NUCLEARES?

Durante décadas, los estadounidenses han amenazado con el uso de armas nucleares contra sus enemigos en circunstancias muy limitadas, como respuesta al uso de armas biológicas contra su país. Pero un nuevo documento incluiría también intentos de destruir una infraestructura de gran envergadura, como la red eléctrica o las comunicaciones de un país, las que serían más vulnerable a las armas cibernéticas.

El borrador del documento, llamado Nuclear Posture Review, fue escrito en el Pentágono y está siendo revisado por la Casa Blanca (1)

(1) https://www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html

El riesgo de ciberataque en los sistemas de armas nucleares es "relativamente alto". La falta de personal calificado y la lentitud del cambio institucional expone las capacidades del Reino Unido y de los EE.UU.(2)

(2) https://www.theguardian.com/technology/2018 / jan / 11 / cyber-attack-risk-on-nuclear-weapons-systems-relativamente-high-thinktank

EVOLUCIÓN EN LA BATALLA DE LAS AMENZAS CIBERNÉTICAS

En la conferencia de Tel Aviv, el ex director de la CIA David Petraeus, dice que las amenazas cibernéticas están creciendo y los estados están perdiendo la batalla, se dijo también que el "invierno" de las amenazas cibernéticas está por llegar.

Ese es el mensaje que los expertos en seguridad cibernética, tanto israelíes como estadounidenses, presentaron en una conferencia de tecnología cibernética en Tel Aviv, los que definieron 2017 como el peor año para los ataques cibernéticos a nivel mundial, y el 2018 parece ser incluso peor

https://www.timesofisrael.com/winter-of-cyber-threats-is-coming-experts-warn/

TABLERO GLOBAL INTEGRADO PARA CIBERGUERRA

Lockheed anticipa su respuesta a la búsqueda de una herramienta para coordinar los efectos cibernéticos en los dominios terrestres, aéreo, marítimo y espacial. Llamado "Henosis", de la palabra griega *unidad*, el nuevo tablero digital de Lockheed Martin está destinado a dar a los comandantes una única dirección para la defensa cibernética y la ofensiva en tiempo real contra objetivos terrestres, marítimos, aéreos y espaciales.

http://www.defenseone.com/technology/2018/03/lockheed-martin-desarrolla-integrated-dashboard-wage-cyber-warfare/146419/?oref=defenseone_today_nl

---

CIBERSEGURIDAD

LA ERA DE LA INTERNET DE LAS COSAS (IoT) 2018

La Internet de las cosas se está consolidando como una de las innovaciones más transformadoras de nuestro tiempo. Partiendo de un concepto simple, como todos los dispositivos conectados a la red para que la tarjeta envíe y reciba datos que se conviertan en activos independientes de forma independiente, esta tecnología gana fuerza a la medida que más y más elementos se añaden al sistema y se vuelven "Inteligentes".

Cada día nuevos objetos interactúan con la red, según datos de la consultora Gartner, en el año 2020 unos 20.000 millones de dispositivos formarán parte de **IoT**. Desde sistemas integrales para el hogar hasta coches sin conductor, el espectro completo entre lo ordinario y lo extraordinario disponible en **IoT** en los próximos años.

https://www.pandasecurity.com/spain/mediacenter/mobile-news/iot-ciberseguridad-vigilancia/

¿DESAPARECERÍA LA WEB CERT.ORG, CENTRO DE RESPUESTA ANTE INCIDENTES INFORMÁTICOS?

La organización cert.org, creada bajo el amparo de DARPA hace casi 30 años (comenzó en 1988), como consecuencia de la aparición del gusano Morris, fue creada bajo el concepto de un centro de ayuda para esas instituciones y usuarios afectados por incidencias de seguridad.

https://www.riskbasedsecurity.com/2018/ 02 / rip-cert-org-you-will-be-missed /

DOCUMENTOSDE INTERES

EL FUTURO DE LA GUERRA POLÍTICA: RUSIA, EL OESTE Y LA LLEGADA DE LA COMPETENCIA DIGITAL GLOBAL

En este interesante y extenso artículo de ALINA POLYAKOVA y SPENCER P. BOYER brindan su punto de vista respecto de la guerra política del Kremlin contra los países democráticos la que habría evolucionado de abierta a actividades de influencia encubierta.

En el trabajo mencionado, ubican a Rusia como pionera en el empleo de herramientas asimétricas para el siglo XXI, incluyendo dentro de las mismas los ataques cibernéticos y las campañas de desinformación, estas herramientas ya estarían siendo superadas.

Los avances tecnológicos en inteligencia artificial (IA), automatización y aprendizaje automático, combinados con la disponibilidad de grandes volúmenes de datos, conforman el escenario para una nueva guerra política con conflictos sofisticados, económicos y altamente impactantes

https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf?_cldee=YW1vcmVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-c72ddabb9af8e711812870106fa6f4a1-5552093f48bb4f0eb1b574cd1f289ede&esid=8b740730-ef21- e811-8128-70106faac331 & urlid = 20