2013-07-18

CiberNoticias # 10

SCProgress

www.scprogress.com

ÍNDICE

1. La colaboración Público-Privada en ciberseguridad……..03
2. La ciberseguridad, elemento clave en las nuevas ciudades inteligentes……..04
3. Servicios secretos rusos vuelven a las máquinas de escribir……06
4. ¿Cómo se pinchan cables de fibra óptica?……07
5. Equipo UTM Serie NG de Cyberoam……11
6. España, un mercado de crecimiento para Avira……12

Noticia # 01: La colaboración Público-Privada en ciberseguridad.

La gestión de los riesgos, las amenazas y el desarrollo de la capacidad de reacción ante una alerta temprana se demuestra como estratégica en el mantenimiento de la integridad tanto de individuos, como de empresas y Estados. La colaboración Público-Privada es reconocida por todos como la única vía de abordar esta situación.

Aunque hace un año se aprobó la Estrategia Española de Seguridad y estamos a la espera de inminente publicación de la Estrategia Española de Ciberseguridad, el mundo no deja de avanzar de una forma acelerada y el análisis de los acontecimientos nos hace modificar nuestras percepciones y los modelos con los que tradicionalmente habíamos entendido la realidad.

La crisis económica, los conflictos sociales, los nuevos escenarios de guerra económica, las situaciones de nuevos espacios de confrontación... son parte sustancial de nuestra vida diaria. Pero, del mismo modo, aparecen nuevas oportunidades que permiten comprender por qué las grandes crisis proporcionan nuevas vías de expresión del ser humano permitiéndonos elaborar nuevas construcciones de entendimiento de nuestro presente y de nuestro futuro.

Hablar de ciberseguridad, en estos últimos trece años, ha sido la prédica de la anticipación de una revolución tecnológica que iba aparejada a un nuevo modelo de cambio social. La tecnología de internet ha proporcionado un nuevo paradigma de la comunicación social, rompiendo las dimensiones clásicas del espacio y el tiempo. La tecnología que posibilita este cambio también permite que se desarrollen capacidades que generan amenazas, para las que, ni Estados ni empresas ni individuos estábamos preparados. Por ello, esa labor de comprensión del nuevo entorno necesita nuevas herramientas de estudio, de formación y de colaboración entre todos los agentes sociales, tanto públicos como privados.

Fuente: Segu-info.com

Noticia # 02: La ciberseguridad, elemento clave en las nuevas ciudades inteligentes.

En todo el mundo se está acentuando el hecho de que la mayoría de la población se concentre en entornos urbanos según los últimos informes de la ONU. En Europa, por ejemplo, el 75% de sus habitantes residen en ciudades.

Esta tendencia hace que sea necesario realizar un cambio del modelo actual de cara a conseguir entornos más eficientes y sostenibles mediante una correcta gestión de recursos.

El modelo Smart City obliga a que todos los elementos que conforman la ciudad evolucionen hacia plataformas inteligentes que interactúen entre sí para lograr una gestión eficiente. Así pues, las Smart Cities serán ciudades instrumentadas en las que existirá una red compleja de sensores accesibles, a través de los cuales se recabará información crucial para el funcionamiento y la toma de decisiones.

En este marco toma fuerza la utilización de las TIC como mecanismo que proporcione la modernización de las infraestructuras permitiendo la integración de los sistemas de información, la mejora de procesos internos, el ahorro en costes de operación y la disminución en los tiempos de respuesta en la ejecución de tareas.

Entre las herramientas que componen la estructura de las ciudades inteligentes, la más importante y compleja es la Smart Grid que proporciona la inteligencia necesaria para mejorar la administración de recursos y migrar de una gestión de la oferta eléctrica a una gestión de la demanda a través de la señalización en tiempo real de tarifas a los consumidores finales.

Una de sus grandes ventajas es la posibilidad de consultar los datos de consumo mediante dispositivos inteligentes que disponen de capacidades de tele medida, cuya principal función es recolectar valores de consumo de cualquier servicio que se pueda dar a un grupo de ciudadanos (electricidad, agua, gas...) de forma remota y enviarlos al distribuidor, que se encargará de hacerlos disponibles para las empresas comercializadoras y los clientes. La implantación de la tele medida pretende aumentar la eficiencia energética para el año 2020 reduciendo un 20% las emisiones de gases de efecto invernadero, un 20% el consumo de energía primaria y elevando otro 20% la utilización de las energías renovables. Además, sustituye al modelo actual de lectura manual de contadores, permitiendo lecturas periódicas con mayor frecuencia. Incluso va a permitir a los usuarios conocer al instante el consumo energético de sus hogares.

Los futuros electrodomésticos inteligentes también harán uso de esta información para funcionar en los periodos de menor coste para el usuario, siempre que su tarea pueda ser pospuesta como en lavadoras o lavavajillas.

Por contrapartida, es necesario resaltar que la inclusión de las TIC en el concepto de Smart City supone adquirir las amenazas potenciales y riesgos de seguridad asociados a este tipo de tecnologías, por lo que la seguridad inteligente debe ser tenida en cuenta como producto básico. Dicha seguridad inteligente debe incluir componentes de seguridad urbana y componentes de seguridad de la infraestructura que salvaguarde la economía y el desarrollo de la ciudad (redes eléctricas, transporte público, sistemas de distribución de aguas o servicios de emergencias) y de ese modo evitar que se suma en el caos.

Fuente: Blog seguridad.

Noticia # 03: Servicios secretos rusos vuelven a las máquinas de escribir.

Los servicios de secretos rusos están volviendo a apostar con fuerza por las máquinas de escribir para proteger informaciones extremadamente secretas del espionaje informático, asegura hoy el diario "Isvestiya".

Según el diario, el Servicio Federal de Protección (FSO), considerado responsable de la seguridad del presidente y del gobierno,

Las revelaciones sobre espionaje cibernético ponen nerviosos también a los servicios secretos. Los rusos optan por protegerse y operar "a la antigua".

hizo un encargo de 20 máquinas de escribir, ya que pretende escribir y archivar en papel en lugar de en soportes electrónicos la información especialmente controvertida.

El portavoz del servicio secreto FSO, Serguei Devyatov, dijo a la agencia de noticias Itar-Tass que también se siguen utilizando antiguas conexiones telefónicas a prueba de escuchas para conversaciones secretas entre las cúpulas de los países. (dpa).

Fuente: http://www.dw.de

Noticia # 04: ¿Cómo se pinchan cables de fibra óptica?

Casi todos los países del mundo esperan que sus servicios de inteligencia evalúen la telecomunicación internacional. Por ello, cuando las líneas de telecomunicación atraviesan las fronteras de un país, los proveedores son obligados a facilitar la interfaz de sus cables de fibra óptica a las autoridades gubernamentales respectivas.

Tempora puede acceder legalmente a las informaciones que corren por territorio británico. Sin embargo, los cables de fibra óptica también se pueden pinchar clandestinamente, sin el consentimiento del proveedor.

Enormes cantidades de datos viajan alrededor del mundo a través de cables de fibra óptica. Para hackear esos datos, los cables son pinchados regularmente. A veces de forma legal, otras veces clandestinamente.

Un cable de tierra está compuesto por 144 fibras ópticas. Cables submarinos contienen, como máximo, ocho fibras. En un primer paso, los datos electrónicos son transformados con láser en pulsos de luz ultracortos. Estos pulsos representan los dígitos cero y uno con los que se codifica la información digital. Al final de la fibra óptica se encuentra un fotodiodo que vuelve a generar impulsos eléctricos a partir de los pulsos de luz.

Fuente: http://www.dw.de

El punto débil de los cables de fibra óptica.

El arte está en filtrar las informaciones relevantes.

Aproximadamente diez mil millones de estos pulsos de luz corren por una sola fibra óptica por segundo. Así, cada fibra puede transmitir una cantidad de datos de entre 1,2 a cinco gigabyte por segundo.

No obstante, estas informaciones no llegan muy lejos, como explica Klaus-Dieter Langer, del Instituto Frauenhofer de Berlín: "Una fibra óptica no es completamente transparente, sino que tiene un amortiguamiento natural. Un vidrio grueso tampoco deja pasar la misma cantidad de luz que un vidrio delgado."

Por ello, las señales de los cables de fibra óptica tienen que ser reforzadas cada 80 kilómetros, y esto sucede por medio de un regenerador. Sin embargo, los regeneradores también son el punto débil de los cables. Allí pueden ser pinchados fácilmente, porque las fibras ya no vienen juntas, sino que cada una tiene que ser reforzada por separado.

Fuente: http://www.dw.de

El reto consiste en evaluar la enorme cantidad de datos

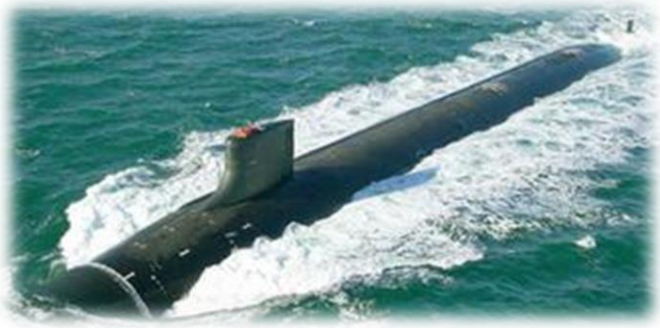
"Si se logra desviar luz de una fibra óptica, basta un cierto porcentaje para detectar y transformar los datos. No es tan fácil preparar una fibra para pincharla, pero solo se trata de un obstáculo técnico."

Sin embargo, añade Klaus-Dieter Langer, el proveedor puede detectar el intento de pinchaje. Para ello, se necesitan instrumentos de medición muy sensibles, y las líneas tendrían que ser vigiladas constantemente. Entonces se podría notar que la señal disminuye de repente.

Después de ser intervenida la fibra óptica, el mayor reto consiste en evaluar la enorme cantidad de datos. "Una fibra, con un rendimiento del 50 por ciento, proporciona datos de un tamaño de diez terabyte por hora. Pero, como el espacio de almacenamiento no es ilimitado, el arte está en filtrar en un lapso de una hora las informaciones relevantes", señala Langer.

Fuente: http://www.dw.de

¿También se pinchan cables submarinos?



¿El submarino estadounidense Jimmy Carter pincha cables submarinos?

Muchos datos, además, primero tienen que ser decodificados, por lo que es necesario almacenarlos temporalmente. Los servicios secretos tienen que proceder de forma muy selectiva para no perderse en el laberinto de datos. Por eso, Klaus-Dieter Langer cree que los agentes secretos solo pinchan algunas fibras ópticas de ciertos proveedores de interés.

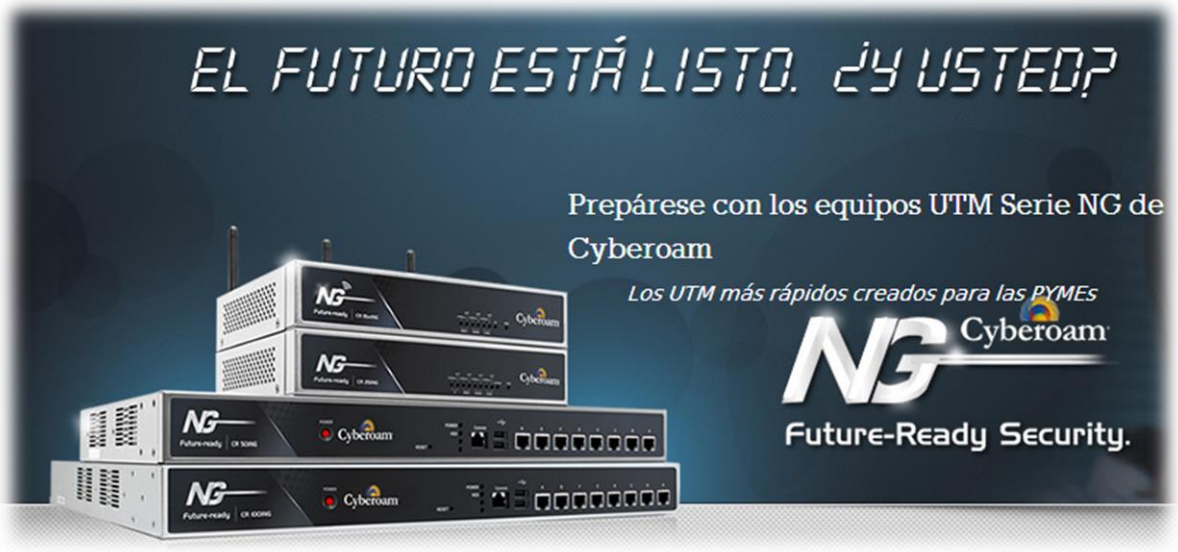
¿Y qué hay detrás de las especulaciones de que el submarino estadounidense Jimmy Carter pinche cables de fibra óptica en el fondo del mar?

Peter Franck, portavoz del "Chaos Computer Club", no descarta esta posibilidad. A través de la comunicación radiotelegráfica normal, señala, los datos prefiltrados podrían ser enviados a una base. Otra posibilidad sería depositar un aparato en el fondo del mar que registre las informaciones, y recogerlo más tarde.

Según Franck, los cables submarinos son de gran interés para los servicios secretos, ya que gran parte de la comunicación internacional pasa por ellos. Así, en los siete mares, las fibras ópticas submarinas podrían ser pinchadas por servicios de espionaje.

Fuente: http://www.dw.de

Noticia # 05: Equipo UTM Serie NG de Cyberoam.



"Los UTM más rápidos creados para las PYMES"

Funciones:

- Firewall.
- VPN.
- Intrusion Detection & Prevention.
- Gateway Level Anti-virus for Mails, Website, File Transfers.
- Gateway level Anti-spam.
- Content Identification & Filtering.
- Bandwidth Management for Applications & Services.
- Load Balancing & Failover Facilities'.
- Soluciones para redes corporativas y SOHO (small office & home office).

Noticia # 06: España, un mercado de crecimiento para Avira.

"Avira, que busca potenciar su programa de afiliados, está desarrollando una estrategia de venta multicanal de sus soluciones de seguridad en España".

España se ha convertido en uno de los mercados estratégicos de crecimiento de negocio de este 2013 para Avira. Así lo ha asegurado la empresa alemana, que ha detectado una gran oportunidad en el consumo español de software de seguridad. España, asegura Avira, es el líder europeo en penetrabilidad y crecimiento en el área de los smartphones y ha registrado en 2012 datos espectaculares de crecimiento de usuarios multidispositivo, tanto en el entorno personal como laboral, que están siempre conectados. Avira, con 1'8 millones de usuarios en España de su producto de descarga gratuita y 100 millones en todo el mundo, basará su crecimiento en el mercado español en la expansión de su red de ventas hacia el retail y hacia un aumento significativo de su red de distribuidores asociados, con un perfil orientado a la pequeña y mediana empresa, hasta llegar a 100 el primer año. La multinacional experta en seguridad entra con esta estrategia en una nueva fase de crecimiento en el mercado nacional.

Cornelia Lehle, Directora Partner Business Global de Avira, "España como mercado encaja perfectamente en nuestra estrategia de crecimiento". El año pasado el crecimeitno de Avira en nuestro país fue del 30%, "y pensamos que es un país con un enorme potencial tanto en consumo, especialmente en doméstico y pymes, como en la posibilidad de incrementar los acuerdos con distribuidores locales", prosigue Lehle.

Avira dispone de un importante programa de socios para el canal de distribución que aporta a los asociados diversos servicios y ventajas competitivas más allá del soporte técnico personalizado, como la Partner Academy, o multitud de material de apoyo comercial y de marketing, entre otros servicios.

Tests independientes y análisis tecnológicos coinciden en calificar Avira como el software antivirus y antimalware más rápido, eficaz y preciso del mercado. Siendo una de las soluciones de seguridad más populares del mundo, registra un promedio de 192 instalaciones de su software cada minuto, explica la compañía.

Fuente: www.channelbiz.es