APARICIONES EN MEDIOS 2019

ENTREVISTAS

Enero 2019

capitalradio

Mayo 2019

“La seguridad y la innovación son los retos clave para un avance real de 5G en Europa”

Ricardo Silva, director de Operaciones de Blue Telecom Consulting.

POR REDACCIÓN COMPUTING | 30 de mayo 2019

Ricardo Silva, COO de BlueTC

¿Cómo se ve desde BlueTC la evolución de 5G?

R. S.: Los despliegues de redes comerciales 5G ya comenzaron en 2018, incluyendo despliegues tanto móviles como fijos inalámbricos. Durante el año 2019 dichos despliegues se van a intensificar y se espera que entorno a medio centenar de redes 5G estén en servicio a finales de este año, con una proporción importante de ellas en Europa.

¿Cuál es el principal reto al que se enfrentan las compañías Telco en el avance de 5G?

R. S.: Uno de los más importantes es el de la seguridad. Las compañías del sector Telco vienen de un universo en el que cada una de ellas utilizaba sus propios protocolos de seguridad. De esta forma, el entorno permanecía bajo control y los posibles incidentes eran poco probables.

Con la llegada de las nuevas generaciones de comunicaciones, la situación cambia drásticamente. Con 5G, las redes evolucionan hacia un modelo de sistemas totalmente distribuido, masivamente escalable y flexible, y que podrá crecer y modificarse con el tiempo. Las nuevas tecnologías que posibilitan 5G, como son SDN, NFV, CUPS (Control Plane User Plane Separation), MEC (Mobile Edge Computing) y Network Slicing abren nuevos escenarios susceptibles de nuevos vectores de ataques maliciosos. Por consiguiente, se rompe con el dominio tradicional de seguridad de los proveedores de servicios y se requerirán nuevas estrategias que tengan una visión holística de sistema, que permita orquestar todo el entorno de seguridad, con estrategias flexibles, con el apoyo de análisis de datos, inteligencia artificial y con la aplicación de políticas automatizadas que permitan cerrar la brecha entre detección de un ataque y su mitigación.

¿Qué otros factores deben tener en cuenta los operadores?

R. S.: La innovación es otro gran desafío. Los operadores deben construir sus propuestas tanto operacionales como comerciales de valor sobre la innovación. Desde el punto de

computing

https://www.computing.es/movilidad/entrevistas/1112234046501/seguridad-y-innovacion-retos-clave-avance-real-de-5g-europa.1.html

Octubre 2019

“Las organizaciones no tienen una estrategia clara al afrontar las tecnologías emergentes”

Por **Redacción Byte TI** - 23 octubre, 2019 0

Miguel Ángel García Matatoros, director general de Blue Teleco

Miguel Ángel García Matatoros, director general de BlueTC

Blue Telecom Consulting (BlueTC) es una consultora que nació en 2005 para dar servicio a compañías del sector Telco. El nuevo entorno digital hace que cualquier producto o servicio tenga que depender de alguna forma de conectividad, lo que ha permitido a BlueTC abrir su campo de acción a sectores tan dispares como Industria, Energía Seguridad o Logística, transformando, al mismo tiempo, un modelo tradicional de consultoría basado en el outsourcing en otra que ofrece valor estratégico para el negocio.

BYOD: cómo pasar de confianza cero a la co total

byte TI

https://revistabyte.es/entrevistas/bluetc-tecnologias-emergentes/

Noviembre 2019

Tecnología

"Las organizaciones no tienen una estrategia clara al afrontar las tecnologías emergentes"

elEconomista.es
13/11/2019 - 20:49

Miguel Ángel García Matatoros, director general de Blue Telecom Consulting

Blue Telecom Consulting (BlueTC) es una consultora que nació en 2005 para dar servicio a compañías del sector Telco. El nuevo entorno digital hace que cualquier producto o servicio tenga que depender de alguna forma de conectividad, lo que ha permitido a BlueTC abrir su campo de acción a sectores tan dispares como Industria, Energía Seguridad o Logística, transformando, al mismo tiempo, un modelo tradicional de consultoría basado en el outsourcing en otra que ofrece valor estratégico para el negocio.

elEconomista.es

https://www.eleconomista.es/tecnologia/noticias/10198661/11/19/Las-organizaciones-no-tienen-una-estrategia-clara-al-afrontar-las-tecnologias-emergentes.html

ENTREVISTAS ▸ MUNDO DIGITAL

"Las organizaciones no tienen una estrategia clara en tecnologías emergentes"

Miguel Ángel García Matatoros, director general de Blue Telecom Consulting.

POR REDACCIÓN COMPUTING | 19 de noviembre 2019

Miguel Ángel García Matatoros, director general de Blue Telecom Consulting

BlueTC comenzó su actividad hace 15 años como consultora especializada en el sector Telco. ¿Cómo ha evolucionado su propuesta desde entonces?

M. Á. G. M.: En el momento en el que comenzamos a operar, las consultoras centraban su negocio en la gestión externa de determinados servicios, de forma que estos servicios dejaban de formar parte de la organización interna del cliente. A pesar de esta tendencia, en Blue Telecom optamos desde el principio por un modelo diferente, con el que fuéramos capaces de inyectar conocimiento a nuestros clientes para que pudieran, de esta forma, enriquecer sus productos y servicios a través de distintas soluciones y tecnologías.

Durante estos años nuestro modelo ha ido ganando madurez, lo que nos ha permitido incrementar de forma progresiva el valor que como consultores podemos aportar a todo tipo de organizaciones.

Con este enfoque hemos logrado que la percepción que tienen las compañías sobre las consultoras como BlueTC sea más positiva. No nos ven como un intermediario que gestiona un servicio genérico, sino como un partner situado en la frontera del desarrollo tecnológico que aporta conocimiento estratégico a su organización.

¿En qué líneas de negocio centra BlueTC su actividad?

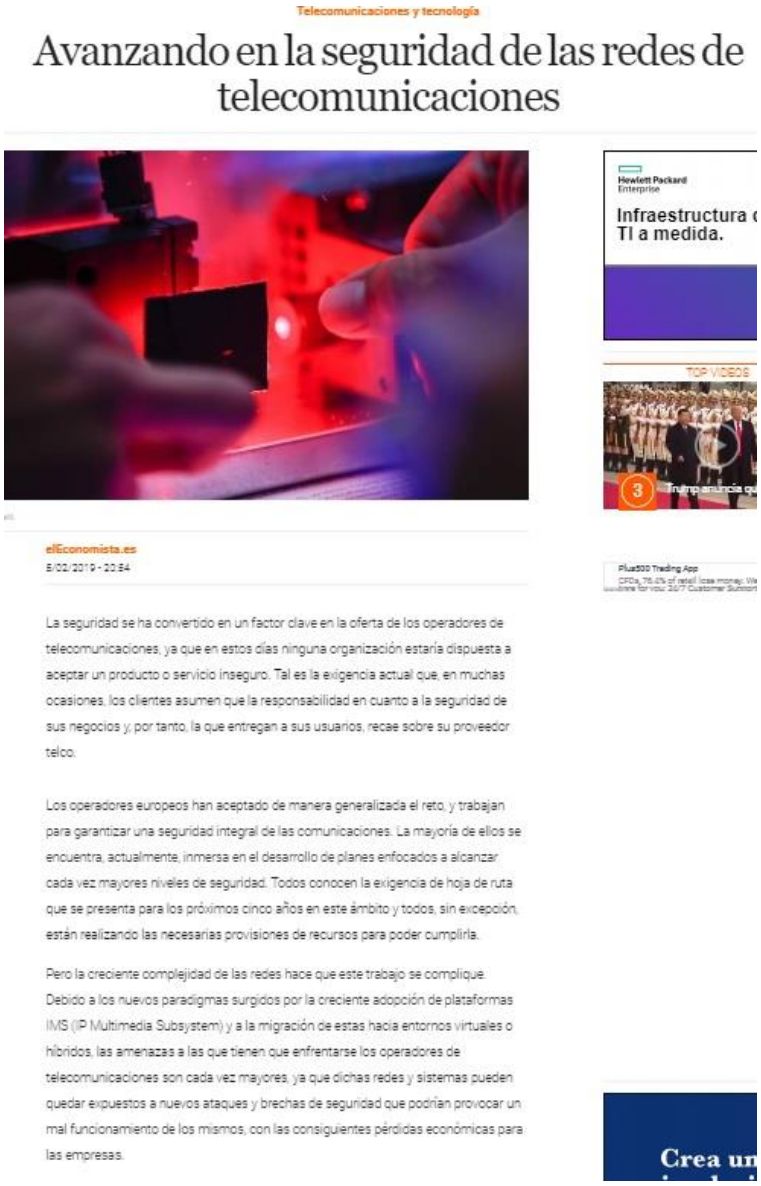
M. Á. G. M.: Blue Telecom centra su actividad en el desarrollo, soporte y operación de sistemas de información enfocados a ofrecer servicios a los usuarios de nuestros clientes, distinguiendo esos sistemas de los de procesos de datos tradicionales, que no ofrecen un servicio directo al usuario. Es decir, nosotros no trabajamos con los sistemas de datos que un operador tiene de sus clientes con el fin de extraerlos o explotarlos, sino que nos centramos en los sistemas que, por ejemplo, ofrecen el servicio de conectividad o de

computing

https://www.computing.es/mundo-digital/entrevistas/1115338046601/organizaciones-no-tienen-estrategia-clara-tecnologias-emergentes.1.html

ARTÍCULOS

Febrero 2019



Telecomunicaciones y tecnología

Avanzando en la seguridad de las redes de telecomunicaciones

elEconomista.es
8/02/2019 - 22:54

La seguridad se ha convertido en un factor clave en la oferta de los operadores de telecomunicaciones, ya que en estos días ninguna organización estaría dispuesta a aceptar un producto o servicio inseguro. Tal es la exigencia actual que, en muchas ocasiones, los clientes asumen que la responsabilidad en cuanto a la seguridad de sus negocios y, por tanto, la que entregan a sus usuarios, recae sobre su proveedor telco.

Los operadores europeos han aceptado de manera generalizada el reto, y trabajan para garantizar una seguridad integral de las comunicaciones. La mayoría de ellos se encuentra, actualmente, inmersa en el desarrollo de planes enfocados a alcanzar cada vez mayores niveles de seguridad. Todos conocen la exigencia de hoja de ruta que se presenta para los próximos cinco años en este ámbito y todos, sin excepción, están realizando las necesarias provisiones de recursos para poder cumplirla.

Pero la creciente complejidad de las redes hace que este trabajo se complique. Debido a los nuevos paradigmas surgidos por la creciente adopción de plataformas IMS (IP Multimedia Subsystem) y a la migración de estas hacia entornos virtuales o híbridos, las amenazas a las que tienen que enfrentarse los operadores de telecomunicaciones son cada vez mayores, ya que dichas redes y sistemas pueden quedar expuestos a nuevos ataques y brechas de seguridad que podrían provocar un mal funcionamiento de los mismos, con las consiguientes pérdidas económicas para las empresas.

elEconomista.es

https://www.eleconomista.es/telecomunicaciones-tecnologia/noticias/9681922/02/19/Avanzando-en-la-seguridad-de-las-redes-de-telecomunicaciones.html

Marzo 2019

Lo que hay que saber antes de iniciar un proyecto de IoT

0 compartido 0 comentarios Suscríbete

Actualizado: 02/03/2019 00:27 horas

Las organizaciones deben apostar por las nuevas tecnologías, como el IoT, pero con cierta cautela y conocimiento.

Nadie duda ya de que la orientación del negocio hacia el entorno digital es un requisito imprescindible para todas las organizaciones con independencia de su tamaño o de su sector de actividad. En este proceso de transformación, las grandes tendencias tecnológicas como Big Data, Machine Learning, Inteligencia Artificial o IoT ocupan un papel protagonista.

Los grandes proveedores de tecnología a nivel global llevan años evangelizando sobre los beneficios que esas propuestas pueden aportar al desarrollo de la actividad comercial. Los analistas, por su parte, publican constantemente nuevas

LO MÁS LEÍDO

1. Del cerebro al ordenador: despega la 'bioelectrónica'
2. Lego: robótica y realidad aumentada para darle una vida a sus ladrillos
3. Netflix sube sus precios en España

Expansión

http://www.expansion.com/economia-digital/protagonistas/2019/03/02/5c45abf1e2704e87a88b460b.html

Mayo 2019

Seguridad e innovación, retos clave para un avance real de 5G

SEGURIDAD

RICARDO SILVA

COO de BlueTC.

20-05-2019

Los despliegues de redes comerciales 5G comenzaron en 2018, incluyendo despliegues tanto móviles como fijos inalámbricos. Durante el año 2019 dichos despliegues se van a intensificar y se espera que en torno a medio centenar de redes 5G estén en servicio a finales de este año, con una proporción importante de ellas en Europa.

Uno de los retos más importantes para el avance de 5G es la **seguridad**. Las compañías del sector Telco vienen de un universo en el que cada una de ellas utilizaba sus propios protocolos de seguridad. De esta forma, el entorno permanecía bajo control y los posibles incidentes eran poco probables.

Con la llegada de las nuevas generaciones de comunicaciones, la situación cambia drásticamente. Con 5G, las redes evolucionan hacia un modelo de sistemas totalmente distribuido, masivamente escalable y flexible, y que podrá crecer y modificarse con el tiempo. Las nuevas tecnologías que posibilitan 5G, como son **SDN, NFV, CUPS(Control Plane User Plane Separation), MEC (Mobile Edge Computing) y Network Slicing** abren nuevos escenarios susceptibles de nuevos vectores de ataques maliciosos. Por consiguiente, se rompe con el dominio tradicional de seguridad de los proveedores de servicios y se requerirán nuevas estrategias que tengan una

R&T REDES&TELECOM

http://www.redestelecom.es/seguridad/opinion/1112033002503/seguridad-innovacion-retos-clave-avance-real-de-5g.1.html

Seguridad e innovación, retos para un avance real de 5G

Por Inma Elizalde - 8 mayo, 2019 297 0

Compartir en Facebook Compartir en Twitter

Los despliegues de redes comerciales 5G comenzaron en 2018, incluyendo despliegues tanto móviles como fijos inalámbricos. Durante el año 2019 dichos despliegues se van a intensificar y se espera que en torno a medio centenar de redes 5G estén en servicio a finales de este año, con una proporción importante de ellas en Europa.

Uno de los retos más importantes para el avance de 5G es la seguridad. Las compañías del sector Telco vienen de un universo en el que cada una de ellas utilizaba sus propios protocolos de seguridad. De esta forma, el entorno permanecía bajo control y los posibles incidentes eran poco probables.

Con la llegada de las nuevas generaciones de comunicaciones, la situación cambia drásticamente. **Con 5G, las redes evolucionan hacia un modelo de sistemas totalmente distribuido, masivamente escalable y flexible, y que podrá crecer y modificarse con el tiempo.** Las nuevas tecnologías que posibilitan 5G, como SDN, NFV, CUPS[1] (Control Plane User Plane Separation), MEC (Mobile Edge Computing) y Network Slicing abren nuevos escenarios susceptibles de nuevos vectores de ataques maliciosos. Por consiguiente, **se rompe con el dominio tradicional de seguridad de los proveedores de servicios y se requerirán nuevas estrategias que tengan una visión holística del sistema**, que permita orquestar todo el entorno de seguridad, con estrategias flexibles, con el apoyo de análisis de datos, inteligencia artificial y con la aplicación de políticas automatizadas que permitan cerrar la brecha entre detección de un ataque y su mitigación.

Información de valor para la toma de decisiones directorTIC.es

https://directortic.es/noticias/seguridad-e-innovacion-retos-avance-real-5g-2019050821532.htm

Con 5G, las redes evolucionan hacia un modelo de sistemas totalmente distribuido

Seguridad e innovación, retos clave para un avance real de 5G

Ricardo Silva, director de Operaciones BlueTC, Blue Telecom Consulting

30/05/2019

Los despliegues de redes comerciales 5G comenzaron en 2018, incluyendo despliegues tanto móviles como fijos inalámbricos. Durante el año 2019 dichos despliegues se van a intensificar y se espera que en torno a medio centenar de redes 5G estén en servicio a finales de este año, con una proporción importante de ellas en Europa.

Uno de los retos más importantes para el avance de 5G es la seguridad. Las compañías del sector Telco vienen de un universo en el que cada una de ellas utilizaba sus propios protocolos de seguridad. De esta forma, el entorno permanecía bajo control y los posibles incidentes eran poco probables.

Con la llegada de las nuevas generaciones de comunicaciones, la situación cambia drásticamente. Con 5G, las redes evolucionan hacia un modelo de sistemas totalmente distribuido, masivamente escalable y flexible, y que podrá crecer y modificarse con el tiempo. Las nuevas tecnologías que posibilitan 5G, como son SDN, NFV, CUPS (Control Plane User Plane Separation), MEC (Mobile Edge Computing) y Network Slicing abren nuevos escenarios susceptibles de nuevos vectores de ataques maliciosos. Por consiguiente, se rompe con el dominio tradicional de seguridad de los proveedores de servicios y se requerirán nuevas estrategias que tengan una visión holística del sistema, que permita orquestar todo el entorno de seguridad, con estrategias flexibles, con el apoyo de análisis de datos, inteligencia artificial y con la aplicación de políticas automatizadas que permitan cerrar la brecha entre detección de un ataque y su mitigación.

Ante la evolución de los estándares los operadores pueden optar por una actitud conservadora, dado que se requieren inversiones considerables que en muchos casos y de manera errónea no se ven como oportunidades de negocio y como un factor diferenciador a la hora de proporcionar servicios seguros e innovadores.

Adicionalmente no hay que perder de vista que las redes 3G son mucho más seguras que las 4G, ya que aún mantienen el parámetro clásico de utilizar protocolos cerrados con los que los hackers lo tienen

Interempresas

https://www.interempresas.net/TIC/Articulos/246560-Seguridad-e-innovacion-retos-clave-para-un-avance-real-de-5G.html

Junio 2019

especial quinta generación de telefonía

La seguridad, un factor clave de las nuevas redes de comunicaciones

Para finales de este año se espera que estén operatibas en torno a un centenar de redes 5G, buena parte de ellas en Europa. El modelo, masivamente escalable y flexible, gana en complejidad

Ricardo Silva
Director de Operaciones BlueTC, Blue Telecom Consulting

Uno de los retos más importantes para el avance de 5G es la seguridad. Las compañías del sector Telco vienen de un universo en el que cada una de ellas utilizaba sus propios protocolos de seguridad. De esta forma, el entorno permanecía bajo control y los posibles incidentes eran poco probables.

Con la llegada de las nuevas generaciones de comunicaciones, la situación cambia drásticamente. Con el 5G, las redes evolucionan hacia un modelo de sistemas totalmente distribuido, masivamente escalable y flexible, y que podrá crecer y modificarse con el tiempo.

Desde el punto de vista comercial, articulando servicios que puedan emocionar a los usuarios y que requieran altas velocidades, muy bajas latencias, amplia cobertura, máxima seguridad y que, por supuesto, las tarifas de dichos servicios sean atractivas. Permitir a los usuarios el acceso a datos 5G ilimitados a un precio asequible es esencial en la nueva era actual de velocidad súper rápida y conectividades con latencias ultra bajas. Evidentemente, el objetivo inicial deberían ser los usuarios centrados en la tecnología.

Tenemos que convertir el 5G en un beneficio real para la sociedad

Si ponemos el foco en países que apuestan rápidamente por las últimas tecnologías, podemos comprobar, por ejemplo, que SK Telecom, un operador de Corea del Sur, acaba de apostar fuerte por sus despliegues en 5G, proporcionando servicios de Realidad Aumentada, Realidad Virtual y *cloud-based game* -juegos de *streaming* basados en la nube-. Y lo hace con máxima seguridad -con tecnologías de criptografía cuántica- y con tarifas, en algunos casos, incluso inferiores a las que se venían aplicando para LTE. El propio director general de SK Telecom reconoció en el día de su lanzamiento que esto marca el comienzo de la era de la Hyper-Innovación que aporta 5G.

Otro operador coreano, KT (Korea Telecom), ha presentado recientemente el primer suscriptor de *Business to Consumer* (B2C) para su red inalámbrica de próxima generación en todo el país, y anteriormente lanzó el servicio de red *business-to-business* (B2B). KT apuesta por la disponibilidad de muy bajas latencias, ya que es fundamental para que los usuarios de 5G puedan disfrutar de servicios que requieren inmersión, como los juegos de *streaming* basados en la nube y AR/VR -realidad

Factoría & Tecnología Digital 4.0

https://kiosco.eleconomista.es/e-paper/viewer.aspx?publication=Digital&date=19_06_2019&tpuid=1205#page/34

Julio 2019

Cómo abordar correctamente un proyecto de Big Data

Por Inma Elizalde - 30 julio, 2019

El analista IDC indica que el mercado del Big Data crece a un ritmo del 12% anual. Esta es una buena noticia, ya que demuestra que las organizaciones están entendiendo los beneficios que pueden aportar este tipo de tecnologías a sus negocios, sobre todo en lo que a seguridad y continuidad de sus operaciones se refiere.

Lo que ya no es tan buena noticia es que en el desarrollo de proyectos concretos que tienen a Big Data como protagonista, las empresas no están logrando establecer una conexión directa de estas herramientas con sus productos y servicios. Es decir, gran parte de las implementaciones de herramientas de Big Data que se están llevando a cabo actualmente no logran dar respuesta a las necesidades reales del negocio.

directorTIC.es

https://directortic.es/destacado/como-abordar-correctamente-un-proyecto-de-big-data-2019073022401.htm

Es una de las grandes tendencias a la hora de emprender el proceso de Transformación Digital

Lo que hay que saber antes de iniciar un proyecto de IoT

Miguel Ángel García Matatoros, director general de Blue Telecom Consulting

16/07/2019

1158

Nadie duda ya de que la orientación del negocio hacia el entorno digital es un requisito imprescindible para todas las organizaciones con independencia de su tamaño o de su sector de actividad. En este proceso de transformación, las grandes tendencias tecnológicas como big data, machine learning, Inteligencia Artificial o IoT ocupan un papel protagonista.

Los grandes proveedores de tecnología a nivel global llevan años evangelizando sobre los beneficios que esas propuestas pueden aportar al desarrollo de la actividad comercial. Los analistas, por su parte, publican constantemente nuevas previsiones de evolución de su implantación. Un caso espectacular es el de Internet de las Cosas (IoT), llegando, según datos de Business Insider, a los 40.000 millones de dispositivos conectados en todo el mundo en 2023.

Está claro que Internet de las Cosas es una de las grandes tendencias en las que apoyarse a la hora de emprender el proceso de Transformación Digital, sin embargo, al iniciar un proyecto relacionado con IoT, las empresas deben ser conscientes que entran en juego distintos factores de los que dependerá el éxito final del mismo. De esta forma, es recomendable contar con toda la información al respecto y buscar el apoyo necesario para entender los distintos paradigmas existentes, algo que facilitará la toma de decisión en lo que puede llegar a ser la estrategia decisiva para el futuro de la organización.

Miguel Ángel García Matatoros, director general de Blue Telecom Consulting.

A grandes rasgos, podemos decir que actualmente existen dos aproximaciones muy diferentes a la realidad de internet de las cosas. Por una parte, el proyecto puede basarse en las plataformas estándar

Interempresas

https://www.interempresas.net/TIC/Articulos/251873-Lo-que-hay-que-saber-antes-de-iniciar-un-proyecto-de-IoT.html

Cómo abordar correctamente un proyecto de Big Data

El analista IDC indica que el mercado del Big Data crece a un ritmo del 12% anual. Esta es una buena noticia, ya que demuestra que las organizaciones están entendiendo los beneficios que pueden aportar este tipo de tecnologías a sus negocios, sobre todo en lo que a seguridad y continuidad de sus operaciones se refiere.

Miguel Ángel García Matatoros,
Director general de Blue Telecom Consulting

Lo que ya no es tan buena noticia es que en el desarrollo de proyectos concretos que tienen a Big Data como protagonista, las empresas no están logrando establecer una conexión directa de estas herramientas con sus productos y servicios. Es decir, gran parte de las implementaciones de herramientas de Big Data que se están llevando a cabo actualmente no logran dar respuesta a las necesidades reales del negocio.

La razón fundamental de esta brecha es una aproximación errónea al Big Data por parte de sus sponsors dentro de la compañía. En muchos casos son los CIOs o los CTOs los que impulsan los proyectos de Big Data dentro de sus organizaciones con el objetivo de sacar todo el partido a los datos que se generan en la empresa. La intención es buena, pero normalmente se olvidan de vincular el proyecto a un objetivo de negocio concreto. En otras ocasiones, el impulsor principal es el CEO, que desea que su organización disponga de las tecnologías más avanzadas, pero normalmente no es capaz de ir más allá de los beneficios que ya le proporcionaban las tecnologías de Data Warehouse que utilizaba hace veinte años. Finalmente, hay una tercera figura, más directamente relacionada con un área de negocio concreta, que sin conocer a fondo las tecnologías disponibles, es capaz de ver claramente cómo su aplicación podría servir para mejorar un proceso determinado.

El compromiso del CEO, la comprensión del CIO o del CTO con respecto a las tecnologías existentes y el conocimiento del negocio del responsable del área, son necesarios para lograr que un proyecto de Big Data deje de centrarse en la tecnología y tenga una conexión directa con los productos y servicios de la empresa, es decir, para que el Big Data deje de ser el fin y se convierta en el medio para alcanzar un objetivo de negocio determinado.

Definir objetivos, elegir la herramienta y ejecutar el proyecto

Antes de plantearse iniciar un proyecto de Big Data, cualquier corporación debería definir unas bases que plasmaran con claridad los objetivos que se plantean con la ejecución del mismo, los datos disponibles en la organización, los conocimientos y capacidades de los profesionales que van a liderarlo o su justificación desde el punto de vista económico y para el negocio.

El siguiente paso sería la elección de la herramienta de Big Data. Hoy en día, existen en el mercado soluciones asequibles y fiables que ya ha sido lo suficientemente probadas. No hay por qué asignar todo el presupuesto de TI a la adquisición de más licencias de las necesarias de las soluciones más caras del mercado o a la contratación de una legión de data scientists para poder analizar los resultados. En la actualidad, Big Data es una opción accesible para la mayoría de las empresas, lo único que hay que averiguar es qué herramienta necesita cada compañía de acuerdo a sus necesidades específicas.

Una vez llevado a cabo el análisis previo y decidida la herramienta, resulta recomendable abordar el proyecto de forma parcial, a través de proyectos más pequeños que permitan ir escalando después. En BlueTC proponemos este sistema básicamente porque presenta unos beneficios claros: se consiguen resultados de forma muy rápida y con una limitada inversión en recursos y tiempo; se logra crear un fundamento sobre el que seguir trabajando y perfeccionando; permite desarrollar competencias específicas; mejora la motivación de los equipos y hace posible demostrar resultados tangibles a la dirección. En BlueTC recomendamos que los esfuerzos económicos iniciales del proyecto de Big Data se centren siempre en buscar la conexión con productos y servicios, evitando desembolsos enormes que agoten el presupuesto y limiten la capacidad de llevar a cabo otros proyectos en el futuro o una actualización de la herramienta de Big Data elegida de acuerdo con el resultado obtenido.

Big Data debe de dejar de ser el trending topic en el que se ha convertido y en el que muchas organizaciones están sin saber muy bien para qué. Pensemos siempre que lo verdaderamente relevante es poder vincular el Big Data a los productos y servicios. Es decir, encontrar una aplicación práctica o un caso de uso concreto que ayude realmente a impulsar el negocio. De nada sirve incorporar la mejor y más cara plataforma de Big Data del mercado si eso no se traduce en una optimización real de las operaciones.•

ComunicacionesHoy

https://www.interempresas.net/Flipbooks/CH/175/html5forpc.html?page=30

Octubre 2019

Consideraciones sobre el análisis de riesgos de ciberseguridad en 5G

SEGURIDAD

RICARDO SILVA

director de Operaciones de BlueTC.

29/10/2019

Ricardo Silva , director de Operaciones de BlueTC.

La Comisión Europea acaba de publicar un informe sobre el **análisis de riesgos de ciberseguridad en redes 5G**. Entre sus conclusiones, destacan distintos aspectos que podrían resultar clave a la hora de ayudar a mejorar la seguridad en las redes 5G. En ese sentido, **Ricardo Silva, director de Operaciones de BlueTC (en la foto)**, identifica dos aspectos que incumben tanto a Proveedores de Servicios Digitales (DSP) como a Fabricantes de Equipos de Telecomunicación (NEV) y que serían los siguientes:

- **"Carencia de suficientes requisitos de seguridad** en los procesos de adquisición de 5G. Esta situación puede responder a la adopción de estrategias inadecuadas en la selección de proveedores o a una falta de priorización de la seguridad sobre otros aspectos en el proceso de adquisición" (capítulo C, punto 2.35, página 21).
- **"Falta de personal especializado** y capacitado para asegurar, monitorizar y mantener redes 5G" (capítulo C, punto 2.35, página 20).

"En el primer punto, además de los requisitos de seguridad específicos para los diferentes activos de la red, es conveniente que el operador, durante el proceso de adquisición, solicite al proveedor la **ejecución de una auditoría de Ciclo de Vida de Desarrollo de Software Seguro** (S-SDLC), que cubra desde evaluaciones de riesgos y modelos de amenazas hasta pruebas de vulnerabilidad y sus resultados. Dicha auditoría debe ser llevada a cabo por

R&T REDES&TELECOM

https://www.redestelecom.es/seguridad/opinion/1114977002503/consideraciones-analisis-de-riesgos-de-ciberseguridad-5g.1.html

Consideraciones sobre el análisis de riesgos de ciberseguridad en 5G

elEconomista.es
29/10/2019 - 20:57

La Comisión Europea acaba de publicar un informe sobre el análisis de riesgos de ciberseguridad en redes 5G. Entre sus conclusiones, destacan distintos aspectos que podrían resultar clave a la hora de ayudar a mejorar la seguridad en las redes 5G. En ese sentido, Ricardo Silva , director de Operaciones de BlueTC, identifica dos aspectos que incumben tanto a Proveedores de Servicios Digitales (DSP) como a Fabricantes de Equipos de Telecomunicación (NEV) y que serían los siguientes:

- "Carencia de suficientes requisitos de seguridad en los procesos de adquisición de 5G. Esta situación puede responder a la adopción de estrategias inadecuadas en la selección de proveedores o a una falta de priorización de la seguridad sobre otros aspectos en el proceso de adquisición" (capítulo C, punto 2.35, página 21).

- "Falta de personal especializado y capacitado para asegurar, monitorizar y mantener redes 5G" (capítulo C, punto 2.35, página 20).

elEconomista.es

https://www.eleconomista.es/telecomunicaciones-tecnologia/noticias/10169241/10/19/Consideraciones-sobre-el-analisis-de-riesgos-de-ciberseguridad-en-5G-.html

Falta de personal especializado y carencia de suficientes requisitos de seguridad en los procesos de adquisición, los dos aspectos principales

Consideraciones sobre el análisis de riesgos de ciberseguridad en 5G

Redacción Interempresas 30/10/2019 582

A partir de un reciente informe publicado por la Comisión Europea, Ricardo Silva, director de Operaciones de Blue Telecom Consulting, identifica dos aspectos que incumben a los Proveedores de Servicios Digitales (DSP) y a los Fabricantes de Equipos de Telecomunicación (NEV) y que podrían resultar clave a la hora de ayudar a mejorar la seguridad en las redes 5G.

La Comisión Europea acaba de publicar un **informe** sobre el análisis de riesgos de ciberseguridad en redes 5G. Entre sus conclusiones, destacan distintos aspectos que podrían resultar clave a la hora de ayudar a mejorar la seguridad en las redes 5G. En ese sentido, Ricardo Silva, director de Operaciones de BlueTC, identifica dos aspectos que incumben tanto a Proveedores de Servicios Digitales (DSP) como a Fabricantes de Equipos de Telecomunicación (NEV) y que serían los siguientes:

- Carencia de suficientes requisitos de seguridad en los procesos de adquisición de 5G. Esta situación puede responder a la adopción de estrategias inadecuadas en la selección de proveedores o a una falta de priorización de la seguridad sobre otros aspectos en el proceso de adquisición (capítulo C, punto 2.35, página 21).
- Falta de personal especializado y capacitado para asegurar, monitorizar y mantener redes 5G (capítulo C, punto 2.35, página 20).

Ricardo Silva, director de Operaciones de Blue Telecom Consulting.

"En el primer punto, además de los requisitos de seguridad específicos para los diferentes activos de la red, es conveniente que el operador, durante el proceso de adquisición, solicite al proveedor la ejecución de una auditoría de Ciclo de Vida de Desarrollo de Software Seguro (S-SDLC), que cubra desde evaluaciones de riesgos y modelos de amenazas hasta pruebas de vulnerabilidad y sus resultados. Dicha auditoría debe ser llevada a cabo por compañías independientes con experiencia en todo lo referente a la seguridad en redes de telecomunicaciones, a fin de que pueda ser capaz de detectar posibles brechas a través de la realización de pruebas de vulnerabilidad".

Interempresas

http://www.interempresas.net/TIC/Articulos/257957-Consideraciones-sobre-el-analisis-de-riesgos-de-ciberseguridad-en-5G.html

Noviembre 2019

Analizando los riesgos en 5G

Por **Olga Romero** - 12 noviembre, 2019

La **Comisión Europea** ha publicado los resultados de un informe en el que analiza los riesgos de ciberseguridad en redes 5G. A raíz de la difusión de dicho estudio, Ricardo Silva, director de operaciones de BlueTC, ha identificado dos puntos que influyen tanto a proveedores de servicios digitales (DSP) como a los fabricantes de equipos de telecomunicaciones (NEV). Ambos aspectos podrían ser clave **para ayudar a mejorar la seguridad de estas redes**.

Ricardo Silva identifica los siguientes puntos. Por un lado "la **carencia de suficientes requisitos de seguridad** en los procesos de adquisición de 5G. Esta situación puede responder a la adopción de estrategias inadecuadas en la selección de proveedores o a una falta de priorización de la seguridad sobre otros aspectos en el proceso de adquisición", ha explicado. Por otro lado, ha destacado que la "**falta de personal especializado** y capacitado para asegurar, monitorizar y mantener redes 5G".

Sobre el primer aspecto, "además de los requisitos de seguridad específicos, el operador debe **solicitar** al proveedor la ejecución de una **auditoría** de Ciclo de Vida de Desarrollo de Software Seguro (S-SDLC), para cubrir desde las evaluaciones de riesgos y modelos de amenazas hasta las pruebas de vulnerabilidad y sus resultados", ha comentado. En este sentido ha indicado que "dicha auditoría debe ser **realizada por compañías independientes**, las cuales tengan experiencia en seguridad en redes de telecomunicaciones".

directorTIC.es

https://directortic.es/seguridad/nuevo-informe-de-riesgos-de-ciberseguridad-en-5g-2019111223000.htm

Consideraciones sobre el análisis de riesgos de ciberseguridad en 5G

A partir de un informe de la Comisión Europea, Ricardo Silva, director de Operaciones de Blue Telecom Consulting, identifica dos aspectos que incumben a los Proveedores de Servicios Digitales (DSP) y a los Fabricantes de Equipos de Telecomunicación (NEV) que podrían mejorar la seguridad en las redes 5G.

05 de noviembre 2019

Ricardo Silva, director de Operaciones de Blue Telecom Consulting

La Comisión Europea acaba de publicar un informe sobre el análisis de riesgos de ciberseguridad en redes 5G. Entre sus conclusiones, destacan distintos aspectos que podrían resultar clave a la hora de ayudar a mejorar la seguridad en las redes 5G. En ese sentido, Ricardo Silva, director de Operaciones de BlueTC, identifica dos aspectos que incumben tanto a Proveedores de Servicios Digitales (DSP) como a Fabricantes de Equipos de Telecomunicación (NEV) y que serían los siguientes:

- "*Carencia de suficientes requisitos de seguridad en los procesos de adquisición de 5G. Esta situación puede responder a la adopción de estrategias inadecuadas en la selección de proveedores o a una falta de priorización de la seguridad sobre otros aspectos en el proceso de adquisición*" (capítulo C, punto 2.35, página 21).

- "*Falta de personal especializado y capacitado para asegurar, monitorizar y mantener redes 5G*" (capítulo C, punto 2.35, página 20).

A partir de aquí, Ricardo Silva expone:

En el primer punto, además de los requisitos de seguridad específicos para los diferentes activos de la red, es conveniente que el operador, durante el proceso de adquisición, solicite al proveedor la ejecución de una auditoría de Ciclo de Vida de Desarrollo de Software Seguro (S-SDLC), que cubra desde evaluaciones de riesgos y modelos de amenazas hasta pruebas de vulnerabilidad y sus resultados. Dicha auditoría debe ser llevada a cabo por compañías independientes con experiencia en todo lo referente a la seguridad en redes de telecomunicaciones, a fin de que pueda ser capaz de detectar posibles brechas a través de la realización de pruebas de vulnerabilidad.

https://www.computing.es/movilidad/opinion/1115061046501/consideraciones-analisis-de-riesgos-de-ciberseguridad-5g.1.html

Consideraciones sobre el análisis de riesgos de ciberseguridad en 5G

Articulo de opinión de Ricardo Silva, director de Operaciones de BlueTC

Por Redacción ERP-Spain.com
Actualizado el 11 de noviembre, 2019 - 17.49hs.

A A

A partir de un reciente informe publicado por la Comisión Europea, Ricardo Silva, director de Operaciones de Blue Telecom Consulting, identifica dos aspectos que incumben a los Proveedores de Servicios Digitales (DSP) y a los Fabricantes de Equipos de Telecomunicación (NEV) y que podrían resultar clave a la hora de ayudar a mejorar la seguridad en las redes 5G.

La Comisión Europea acaba de publicar un **informe** sobre el análisis de riesgos de ciberseguridad en redes 5G. Entre sus conclusiones, destacan distintos aspectos que podrían resultar clave a la hora de ayudar a mejorar la seguridad en las redes 5G. En ese sentido, Ricardo Silva, director de Operaciones de BlueTC, identifica dos aspectos que incumben tanto a Proveedores de Servicios Digitales (DSP) como a Fabricantes de Equipos de Telecomunicación (NEV) y que serían los siguientes:

- "Carencia de suficientes requisitos de seguridad en los procesos de adquisición de 5G. Esta situación puede responder a la adopción de estrategias inadecuadas en la selección de proveedores o a una falta de priorización de la seguridad sobre otros aspectos en el proceso de adquisición" (capítulo C, punto 2.35, página 21).
- "Falta de personal especializado y capacitado para asegurar, monitorizar y mantener redes 5G" (capítulo C, punto 2.35, página 20).

"En el primer punto, además de los requisitos de seguridad específicos para los diferentes activos de la red, es conveniente que el operador, durante el proceso de adquisición, solicite al proveedor la ejecución de una auditoría de Ciclo de Vida de Desarrollo de Software Seguro (S-SDLC), que cubra desde evaluaciones de riesgos y modelos de amenazas hasta pruebas de vulnerabilidad y sus resultados. Dicha auditoría debe ser llevada a cabo por compañías independientes con experiencia en todo lo referente a la seguridad en redes de telecomunicaciones, a fin de que pueda ser capaz de detectar posibles brechas a través de la realización de pruebas de vulnerabilidad".

ERP-LATINO.com ERP-SPAIN.com
Portal en español sobre ERP

https://www.erp-spain.com/articulo/76510/ciberseguridad/todos/consideraciones-sobre-el-analisis-de-riesgos-de-ciberseguridad-en-5g-

Diciembre 2019

El reto de la seguridad en los nuevos sistemas de información

Miguel Ángel García Matatoros,
director general de Blue Telecom Consulting

La tecnología evoluciona y con ella deben avanzar las estrategias de las organizaciones Telco. Las nuevas generaciones de comunicaciones están introduciendo capacidades que los operadores tienen que saber convertir en servicios que supongan un valor añadido para el negocio de sus clientes. Así, con la llegada de 5G, ningún operador puede pretender seguir manteniendo su negocio en la oferta de un servicio de conectividad o de voz similar al que ya tenía con 4G o 3G.

En general, los fabricantes de equipos de red y los consultores han conseguido adaptarse rápidamente a las nuevas opciones tecnológicas, pero a los operadores les está costando más. Tener que pasar en pocos años de gestionar sistemas de circuitos, con los que facilitaban la transmisión de señales analógicas, a otros basados en hardware, que ya incluían procesamiento de la información, para llegar, después, a los sistemas actuales basados en servicios y en software, no está siendo un camino fácil de recorrer.

En el actual entorno digital, los sistemas de información en los que las organizaciones basan sus negocios deben presentar un alto nivel de robustez, a fin de garantizar una óptima calidad de servicio 24x7. Además, estos sistemas ya nunca más trabajarán aislados, sino que tendrán que permanecer en constante conexión con otros y tener la capacidad de procesar, además de los datos que ellos mismos generan, los que les llegan de otras fuentes, no siempre con similares estándares de calidad.

Los nuevos sistemas se apoyan, además, en nuevas técnicas, como son la integración continua y el despliegue continuo (CI/CD), lo que hace que sus funcionalidades, características o prestaciones permanezcan siempre en una constante evolución, a fin de acomodarse a cada demanda particular y de integrar sin interrupción los datos obtenidos por herramientas de inteligencia artificial. Es decir, se ha pasado de disponer de sistemas en los que únicamente se diseñaba la funcionalidad, a entornos de servicio y productos basados por igual en sistemas y en datos, diseñados y operados a la par.

Seguridad integral que abarque diseño, despliegue y operación

Es un hecho que todas las organizaciones, también los operadores de telecomunicaciones, están migrando de un modelo de producto a otro de servicio. Esto supone tener que asumir nuevos retos entorno a la seguridad de los sistemas, que ahora necesitan una seguridad integral que cubra todo su ciclo de vida.

En el pasado, los paradigmas de seguridad se basaban en proteger los datos, los activos y los sistemas propios, pero al cambiar a un modelo de servicio, la seguridad del sistema de un proveedor puede afectar a la de sus clientes o partners. Por ello, la seguridad debe tener en cuenta no solo el diseño del sistema, sino también todo lo relacionado con los conceptos de despliegue y operación.

La primera fase en la seguridad de un sistema moderno se centra en el diseño, alcanzando la certeza de que se está construyendo un software seguro. Para ello, es necesario que el factor seguridad se tenga en cuenta desde las primeras fases del proceso, desde el establecimiento de los requisitos. No solo definiendo correctamente los requisitos funcionales, es decir, lo que tiene que hacer la aplicación, sino definiendo también los requisitos de seguridad. A partir de ahí, hay que seguir trabajando para mantener la seguridad en cada una de las fases de desarrollo, identificando y corrigiendo vulnerabilidades de forma continua y a lo largo de todo el proceso de producción del software. En el nuevo entorno, ya no vale con desarrollar primero la aplicación y luego probarla. Por ello, es conveniente abordar la implantación de un Ciclo de Vida de Desarrollo de Software Seguro (SSDLC), empleando herramientas de prevención y mitigación de vulnerabilidades a lo largo de todo el proceso y abarcando todo el portfolio de aplicaciones de la organización.

En la fase de despliegue, y como consecuencia de la migración de las plataformas IMS hacia entornos virtuales o híbridos que se está experimentando en la actualidad, las redes y sistemas virtuales pueden quedar expuestos a nuevos ataques y brechas de seguridad que podrían provocar un mal funcionamiento de los mismos, con las consiguientes pérdidas económicas para estas empresas. Por ello, llevar a cabo auditorías de red y ser capaces de ejecutar millones de casos de prueba en un corto espacio de tiempo para facilitar el despliegue de una red, resulta fundamental a la hora de detectar, gestionar y eliminar estas posibles amenazas.

Finalmente, es también necesario ocuparse de la seguridad de las operaciones, a través de la implantación de soluciones que se ocupen de monitorizar el sistema en operación, es decir, controlando el uso que se está haciendo del sistema, con el fin de dejar al descubierto los ataques potenciales. En esta fase debemos aprovechar al máximo todo el esfuerzo aplicado a la seguridad anterior a la puesta en producción. Así, por ejemplo, todos los casos de uso cuya seguridad se ha comprobado alrededor de una funcionalidad deben pasar a formar parte de la base operacional de la seguridad, ya que, aunque podamos tener la certeza de que estos casos están protegidos, detectar una concentración de los mismos en la fase de operación puede indicar que la organización está siendo sometida a un ataque, pero con la ventaja de que este aún no ha sido fructífero.•

ComunicacionesHoy

https://www.interempresas.net/Flipbooks/CH/178/html5forpc.html?page=12

Avanzando en la seguridad de las redes de telecomunicaciones

Por Inma Elizalde - 15 diciembre, 2019

77 0

Compartir en Facebook Compartir en Twitter

La seguridad se ha convertido en un factor clave en la oferta de los operadores de telecomunicaciones, ya que en estos días ninguna organización estaría dispuesta a aceptar un producto o servicio inseguro. Tal es la exigencia actual que, en muchas ocasiones, los clientes asumen que la responsabilidad en cuanto a la seguridad de sus negocios y, por tanto, la que entregan a sus usuarios, recae sobre su proveedor telco.

Los operadores europeos han aceptado de manera generalizada el reto, y trabajan para garantizar una seguridad integral de las comunicaciones. La mayoría de ellos se encuentra, actualmente, inmersa en el desarrollo de planes enfocados a alcanzar cada vez mayores niveles de seguridad. Todos conocen la exigencia de hoja de ruta que se presenta para los próximos cinco años en este ámbito y todos, sin excepción, están realizando las necesarias provisiones de recursos para poder cumplirla.

Pero la creciente complejidad de las redes hace que este trabajo se complique. Debido a los nuevos paradigmas surgidos por la creciente adopción de plataformas IMS (IP Multimedia Subsystem) y a la migración de estas hacia entornos virtuales o híbridos, las amenazas a las que tienen que enfrentarse los operadores de telecomunicaciones son cada vez mayores, ya que dichas redes y sistemas pueden quedar expuestos a nuevos ataques y brechas de seguridad que podrían provocar un mal funcionamiento de los mismos, con las consiguientes pérdidas económicas para las empresas.

Información de valor para la toma de decisiones directorTIC.es

https://directortic.es/noticias/avanzando-en-la-seguridad-de-las-redes-de-telecomunicaciones-2019121523350.htm

REPORTAJES

Julio 2019

El dato impulsa el proceso de transformación digital de las instituciones

La transformación digital que ha irrumpido en todos los sectores, industrias y ciudades no sería posible sin los datos. Éstos son los habilitadores de nuevas tecnologías y soluciones. De los datos se derivan los conocimientos empresariales importantes y procesables. De su calidad y correcto análisis depende, entre otros aspectos significativos, la mejor toma de decisiones para el negocio.

Cristina Mínguez

Los datos por sí mismos, más si son masivos, no son nada. Solo cobran valor cuando se procede a su análisis.

El Big Data está provocando que, ante la gran cantidad de datos a almacenar y analizar, "veamos grandes avances en la manera de gestionarlo", comenta Victoria Miravall, Payroll& HCM Product Manager en Wolters Kluwer Tax & Accounting. "La explosión de IoT provoca que la disponibilidad y cantidad de información se genere de forma exponencial, y de ahí que uno de los focos principales en cuanto a avances tecnológicos sea mejorar y agilizar el tiempo de procesamiento de datos, y esto es lo que nos permite una de las grandes tendencias en este sentido como es Edge Computing". En este escenario, para Victoria Miravall, "es necesario pasar a realizar algunos de estos procesos en local, es decir, evitar que el procesamiento de datos se realice en la nube, lo que nos permitirá realizar el análisis de información relevante en tiempo real y no dilatar la toma de decisión a causa del elevado tiempo de procesamiento".

Por su lado, Miguel Ángel García Matatoros, director general de Blue Telecom Consulting, opina que todos los segmentos del sector TI están adoptando sus soluciones para incorporar capacidades relacionadas con las grandes tendencias tecnológicas que están permitiendo la transformación de los negocios. "Sin embargo"-advierte- "creo que intentar analizar la evolución del Big Data y de otras tendencias

ComunicacionesHoy

https://www.interempresas.net/Flipbooks/CH/175/html5forpc.html?page=24

Septiembre 2019

La necesaria transformación digital en la empresa

Por **Manuel Navarro** - 2 septiembre, 2019 0

El debate lo abrió Miguel Ángel García, Director General de Blue TC quien aseguró que "en el germen de la transformación digital debería haber consultoría estratégica para definir cuáles van a ser los usos que le damos a la tecnología y que pueda cambiar la empresa. Además, muchas veces el marco normativo afecta negativamente a la innovación". Por su parte, Diego Martínez, Senior Manager Business Value de Vass consideró que "uno de los puntos clave es el cambio cultural y ver que las empresas puedan afrontar los retos digitales que se nos ponen encima de la mesa. El problema es que las empresas muchas veces no piensan en los objetivos a largo plazo. Hay que aprovechar elementos concretos y no meterse en grandes proyectos sino empezar con pequeños casos de uso y una vez que se tiene la información hay que trabajar mucho para estar preparados para los cambios. En opinión de Miguel Ángel Fiz, Director de Categoría de Sistemas Personales de HP, "los modelos de negocio son un factor clave porque estamos en un mundo en el que las empresas tienen que aprovechar la transformación digital para sacar beneficio y entrar en competencia con otras empresas que surgen de la nada y que ven cuándo es el momento oportuno para lanzarse al negocio. Esto produce que se quieren imitar modelos de negocio de forma errónea, por lo que hay que pensar qué es lo que se quiere y sabiendo dónde se quiere llegar de forma concreta".

byte TI

https://revistabyte.es/actualidad-byte/la-necesaria-transformacion-digital-en-la-empresa/

Diciembre 2019

El ámbito industrial va un paso por detrás del entorno empresarial

Ciberseguridad, un camino de largo recorrido

Cristina Mínguez 02/12/2019

Partiendo de la base de que a seguridad 100% no existe, podemos afirmar que, en general el estado de la ciberseguridad ha mejorado y es moderadamente positivo, si tenemos en cuenta la opinión de los expertos de los principales fabricantes de soluciones de ciberseguridad y empresas proveedoras de servicios consultados. A pesar de ello, y aunque el ritmo de concienciación de las empresas sigue creciendo, desgraciadamente, los presupuestos de ciberseguridad no aumentan al ritmo de otras partidas de TI.

Si en el ámbito empresarial aún queda mucho por hacer, a pesar de los años de labor de los fabricantes de ciberseguridad, el entorno industrial ha empezado recientemente a preocuparse más seriamente por protegerse frente a las ciberamenazas. Los datos del estudio de ciberseguridad industrial 2019 de Kaspersky demuestran que las empresas industriales de todo el mundo están buscando mejorar la protección de sus redes. "De hecho, el 87% de los encuestados admite que la ciberseguridad de sus sistemas industriales y operativos es una prioridad. Sin embargo, para alcanzar el nivel de protección necesario resulta clave invertir en medidas específicas y contar con profesionales altamente cualificados. Además, pese a declararlo prioritario, solo algo más de la mitad de las empresas (57%) dispone del presupuesto asignado a la ciberseguridad industrial", declara Alfonso Ramírez, director general **Kaspersky Iberia**.

En este ámbito industrial, desde la compañía **Mnemo** apuntan que las continuas amenazas a entornos operativos críticos, sobre todo aquellas que han sido eco debido a su impacto social, han sido foco de los expertos y atacantes en estas arquitecturas, y se han tenido que realizar planes de urgencia para su análisis y protección. "En la actualidad es una disciplina que por norma general se encuentra bajo las competencias de ciberseguridad IT, de forma lógica, ya que comparten elementos y fundamentos comunes y ésta última tiene una madurez mucho mayor, pero no es suficiente, son necesarios procesos, tecnologías y profesionales especializados que traten de forma concreta las especificaciones y generen un entorno dedicado con las mayores garantías". Como apuntan, ninguna de estas tres necesidades es fácil de adquirir en la actualidad, es el futuro reto del sector cubrir cada una de ellas en calidad y cantidad suficiente para establecer un ecosistema que podamos denominar seguro".

ComunicacionesHoy

https://www.interempresas.net/TIC/Articulos/260284-El-largo-camino-por-recorrer-aun-en-ciberseguridad.html

https://www.interempresas.net/Flipbooks/CH/178/html5forpc.html?page=06

NOTICIAS

Marzo 2019

Auditado y certificado la seguridad del sistema IMS de uno de los mayores operadores móviles europeos

SEGURIDAD

BlueTC se ha encargado de la auditoría y TÜV TRUST IT de la certificación.

REDACCIÓN REDESTELECOM | 13/03/2019

Blue Telecom Consulting ha llevado a cabo una auditoria de seguridad en uno de los mayores operadores móviles europeos. Esta auditoría se integra dentro del Programa de Calidad, Innovación y Excelencia en el área de IMS (IP Multimedia Core Network Subsystem) del operador.

En un periodo de solo seis semanas, **BlueTC** llevó a cabo más de diez millones de casos de pruebas para comprobar el nivel de seguridad de la red móvil IMS del operador. Más concretamente, se pusieron a prueba tanto un nodo tradicional dedicado como un nodo virtualizado, empleando una librería comprehensiva de ataques y técnicas de penetración conocidos y potenciales. Por su parte, la compañía **TÜV TRUST IT** se encargó de incluir la metodología de pruebas y soluciones en su programa de auditoría y certificación. Las pruebas llevadas a cabo y el corto tiempo de reacción del operador, permitió a esta empresa emitir un certificado que demuestra los niveles de seguridad reales de las redes evaluadas.

La evolución de las redes de conmutación a tráfico basado en redes IP ha traído consigo la aparición de un mayor número de variables relacionadas con el núcleo de la red, lo cual implica más complejidad. Los **Session Border Controllers** (SBC) presentan limitaciones y vulnerabilidades inherentes, lo que requiere llevar a cabo pruebas cada vez más cuidadosas en las redes IMS. La nueva normativa europea sobre la protección de datos personales y la estricta

R&T REDES&TELECOM

http://www.redestelecom.es/seguridad/noticias/1110832002503/auditado-y-certificado-seguridad-del-sistema-ims-de-uno-de-mayores-operadores-moviles-europeos.1.html

BlueTC audita la seguridad de las operadoras

aruba 360 secure fabric nuevas redes de comunicaciones

Blue Telecom Consulting, BlueTC, ha llevado a cabo una auditoría de seguridad en uno de los mayores operadores móviles europeos. Esta auditoría se integra dentro del Programa de Calidad, Innovación y Excelencia en el área de IMS (IP Multimedia Core Network Subsystem) del operador.

En un periodo de solo seis semanas, BlueTC llevó a cabo más de diez millones de casos de pruebas para comprobar el nivel de seguridad de la red móvil IMS del operador. Más concretamente, se pusieron a prueba tanto un nodo tradicional dedicado como un nodo virtualizado, empleando una librería comprehensiva de ataques y técnicas de penetración conocidos y potenciales. Por su parte, la compañía TÜV TRUST IT se encargó de incluir la metodología de pruebas y soluciones en su programa de auditoría y certificación. Las pruebas llevadas a cabo y el corto tiempo de reacción del operador, permitió a esta empresa emitir un certificado que demuestra los niveles de seguridad reales de las redes evaluadas.

BlueTC llevó a cabo más de diez millones de casos de pruebas para comprobar el nivel de seguridad de la red móvil IMS del operador

La evolución de las redes de conmutación a tráfico basado en redes IP ha traído consigo la aparición de un mayor número de variables relacionadas con el núcleo de la red, lo cual implica más complejidad. Los Session Border Controllers (SBC) presentan limitaciones y vulnerabilidades inherentes, lo que requiere llevar a cabo pruebas cada vez más cuidadosas en las redes IMS. La nueva normativa europea sobre la protección

BYOD: cómo pasar de la confianza cero a la conf total

10 noviembre, 2019

Los entornos laborale día ya no están contro rígidos perímetros de A...

Leer más

Los retos de seguridad mundo orientado a la movilidad

10 noviembre, 2019

Una de las principales preocupaciones de los es la necesidad de ga las...

Leer más

https://www.revistabyte.es/actualidad-byte/bluetc-seguridad-de-las-operadoras/

BlueTC audita y TÜV TRUST IT certifica la seguridad del sistema IMS de uno de los mayores operadores móviles europeos

14 Marzo 2019

Blue Telecom Consulting (BlueTC) ha llevado a cabo una auditoria de seguridad en uno de los mayores operadores móviles europeos. Esta auditoría se integra dentro del Programa de Calidad, Innovación y Excelencia en el área de IMS (IP Multimedia Core Network Subsystem) del operador..

En un periodo de solo seis semanas, BlueTC llevó a cabo más de **diez millones de casos de pruebas** para comprobar el nivel de seguridad de la **red móvil IMS** del operador. Más concretamente, se pusieron a prueba tanto un nodo tradicional dedicado como un nodo virtualizado, empleando una librería comprehensiva de ataques y técnicas de penetración conocidos y potenciales. Por su parte, la compañía TÜV TRUST IT se encargó de incluir la metodología de pruebas y soluciones en su programa de **auditoría y certificación.** Las pruebas llevadas a cabo y el corto tiempo de reacción del operador, permitió a esta empresa emitir un certificado que demuestra los niveles de seguridad reales de las redes evaluadas.

La evolución de las redes de conmutación a tráfico basado en redes IP ha traído consigo la aparición de un mayor número de variables relacionadas con el núcleo de la red, lo cual implica más complejidad. Los Session Border Controllers (SBC) presentan limitaciones y vulnerabilidades inherentes, lo que requiere llevar a cabo pruebas cada vez más cuidadosas en las redes IMS. La nueva **normativa europea sobre la protección de datos personales** y la estricta legislación respecto a la seguridad de las infraestructuras de telecomunicaciones han provocado que los grandes operadores comiencen a contratar los servicios de consultoras especializadas para que auditen la seguridad de sus redes.

Una visión muy detallada

En este proyecto, las baterías de pruebas ejecutadas fueron más allá de lo que los estándares internacionales exigen, alcanzando una **nueva marca de buenas prácticas** en cuanto al número y alcance de los casos de pruebas. Si normalmente un operador realiza unos miles de casos de prueba, la solución ofrecida por BlueTC es capaz de llevar a cabo millones en un periodo de tiempo muy corto. Esto permite al operador disponer de una visión muy detallada sobre el comportamiento de sus nodos con respecto al tráfico SIP, el tipo de amenazas a las que la red está expuesta (tanto VoLTE como los accesos de interconexión IMS), su gravedad y las causas. El informe de auditoría resalta las causas más probables y las medidas aplicables, lo que permite al operador facilitar información a sus proveedores con la que poder mejorar sus productos.

techWEEK.es

http://www.techweek.es/seguridad/noticias/1019678004801/bluetc-audita-tuv-trust-it-certifica.1.html
www.itseguridad.es/auditoria/noticias/1019678043905/bluetc-audita-seguridad-sistema.1.html
http://www.itcio.es/telecomunicaciones/noticias/1019678015702/bluetc-audita-seguridad-sistema.1.html

BlueTC audita y TÜV TRUST IT certifica la seguridad del sistema IMS de uno de los mayores operadores móviles europeos

elEconomista.es
15/03/2019 - 20:47

Blue Telecom Consulting (BlueTC®) ha llevado a cabo una auditoría de seguridad en uno de los mayores operadores móviles europeos. Esta auditoría se integra dentro del Programa de Calidad, Innovación y Excelencia en el área de IMS (IP Multimedia Core Network Subsystem) del operador.

En un periodo de solo seis semanas, BlueTC llevó a cabo más de diez millones de casos de pruebas para comprobar el nivel de seguridad de la red móvil IMS del operador. Más concretamente, se pusieron a prueba tanto un nodo tradicional dedicado como un nodo virtualizado, empleando una librería comprehensiva de ataques y técnicas de penetración conocidos y potenciales. Por su parte, la compañía TÜV TRUST IT se encargó de incluir la metodología de pruebas y soluciones en su programa de auditoría y certificación. Las pruebas llevadas a cabo y el corto tiempo de reacción del operador, permitió a esta empresa emitir un certificado que demuestra los niveles de seguridad reales de las redes evaluadas.

La evolución de las redes de conmutación a tráfico basado en redes IP ha traído consigo la aparición de un mayor número de variables relacionadas con el núcleo de la red, lo cual implica más complejidad. Los Session Border Controllers (SBC) presentan limitaciones y vulnerabilidades inherentes, lo que requiere llevar a cabo pruebas cada vez más cuidadosas en las redes IMS. La nueva normativa europea sobre la protección de datos personales y la estricta legislación respecto a la seguridad de las infraestructuras de telecomunicaciones han provocado que los grandes operadores comiencen a contratar los servicios de consultoras especializadas para que auditen la seguridad de sus redes.

elEconomista.es

http://www.eleconomista.es/telecomunicaciones-tecnologia/noticias/9764038/03/19/BlueTC-audita-y-TUV-TRUST-IT-certifica-la-seguridad-del-sistema-IMS-de-uno-de-los-mayores-operadores-moviles-europeos.html