Información de valor para la toma de decisiones

directorTIC

editorial

AÑO XIII - Nº 166

Julio/Agosto 2015 - 0,01 Euros

<TU WEB SOLUCIONES>

Compañía de posicionamiento y análisis S.L.

Soluciones MARKETING 3.0

Lead Targeting

¿Cómo conseguir contactos con la calidad que necesito, en el momento oportuno y verdaderamente interesados en mi proyecto?

Tu herramienta para conseguir leads.

Inbound marketing

¿Cómo convertirme en la respuesta a las necesidades de mis clientes y que acudan a informarse a mi web de una forma natural?

Ayuda a tu web a ser mejor comercial.

Influence Marketing

¿Cómo despertar la necesidad en un futuro cliente, asesorar desde el inicio del proceso de compra y ser el referente de mi sector?

Crea tus leads en el momento óptimo.

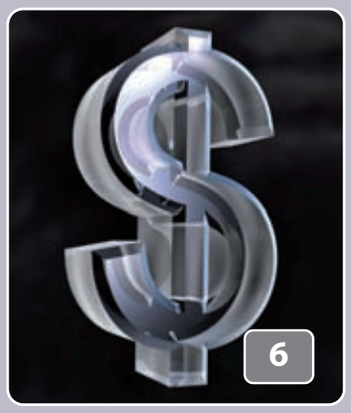
91 308 85 66 • info@tuwebsoluciones.com

Información de valor para la toma de decisiones

directorTIC

AÑO XIII - Nº 166 Julio/Agosto 2015

Big data, el camino para convertirse en millonario



6

Unit4 ofrecerá ERP autónomo para organizaciones

18

El CIO tiene que superar varios retos en materia de seguridad

8

La red inalámbrica, el elemento más vulnerable de la infraestructura TI

32

Proyectos

14 Ibermática renueva los equipos de la Diputación Foral de Álava

16 Fujitsu investigará junto a la FIBHCSC la fusión avanzada del conocimiento

Soluciones

28 Ahorrar en telecomunicaciones con Infocom

Informes

31 PandaLabs detecta 225.000 nuevas muestras diarias de malware

Editorial

Parece que en estas fechas todos estamos más contentos, cansados también, pero muy animados porque, por fin, llegan las ansiadas vacaciones.

Es hora de descansar, reponer fuerzas, cargar pilas y cambiar de aires para enfrentar el "nuevo curso" con más ganas. Es el momento en que la creatividad aumenta hasta niveles fuera de lo normal y surgen las ideas de los grandes proyectos que comenzarán en septiembre. Es tiempo de estar en familia, divertirnos en la playa, aprovechar para hacer deporte y para hacer todo aquello, para lo que no tenemos tiempo a lo largo del año. El único problema es que, después, necesitaremos otras vacaciones, de las propias vacaciones, pero no nos importa porque: ¡por fin es verano!

Desde nuestra redacción queremos desearos un feliz verano y os esperamos de nuevo en septiembre con muchas novedades.

directorTIC
Información de valor para la toma de decisiones

redactora jefe:
Isis Vecino ▪ isis@taieditorial.es

redacción y colaboradores:
Rosa Martín ▪ rmartin@taieditorial.es
Inma Elizalde ▪ inma@taieditorial.es

publicidad:
David Rico ▪ david@taieditorial.es
Virginia Alcalde ▪ virginia@taieditorial.es

producción: Marta Arias ▪ marta@taieditorial.es

edita:
T.A.I. Editorial, S.A.
(Técnicos Asesores Informáticos Editorial, S.A.)
www.taieditorial.es
Ctra. Fuencarral a Alcobendas Km.14.500
28108 ALCOBENDAS (Madrid)
tel. 902 30 40 33 / 91 661 61 02
fax: 91 661 29 28
e-mail: correo@taieditorial.es

miembro de: AEEPP FIPP FEDERACION INTERNACIONAL DE LA PRENSA PERIODICA

distribución Publigarma, S.A.
Papiro, 5-7
FUENLABRADA
tel.: 91 621 43 00
fax: 91 621 43 01

depósito legal TO.221-00
ISSN 2341-1511

Queda prohibida la reproducción total o parcial de los originales de esta publicación sin autorización por escrito.
No nos hacemos responsables de las opiniones emitidas por nuestros colaboradores y anunciantes.

Impreso en papel ecológico

De conformidad con lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, consiento que mis datos sean incorporados a un fichero responsabilidad del GRUPO TAI EDITORIAL y que sean tratados con la finalidad de mantener, desarrollar y controlar la relación contractual y negocial, así como para remitirle información sobre productos y servicios relacionados con su sector de actividad.

Asimismo declaro haber sido informado sobre la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición dirigiéndome a GRUPO TAI EDITORIAL en Carretera Fuencarral a Alcobendas Km. 14,5, 28108 Madrid o bien remitiendo un mensaje a la dirección de correo electrónico correo@tai.es.

Del mismo modo consiento que mis datos puedan ser comunicados a las empresas del GRUPO TAI EDITORIAL para su tratamiento con la finalidad anteriormente indicada, permitiendo así la gestión y operación unitaria del Grupo.

T.A.I. editorial
www.taieditorial.es

PUBLICACIONES EN PAPEL
Para tiendas, fabricantes, distribuidores, mayoristas, importadores, resellers...etc

tai sectores
Para los gerentes de la pyme
PYMES

Newsbook
Negocios en informática
Para los directores de T.I. de grandes cuentas y midmarket
directorTIC

DOMINIOS | CORREO | HOSTING | TIENDAS ONLINE | **SERVIDORES**

NUEVA GENERACIÓN
1&1 SERVIDOR CLOUD

¡PRUÉBALO 1 MES GRATIS!

Después, desde 9,99 €/mes.*

Powered by intel Cloud Technology

ELEGIDO SERVICIO DE ATENCIÓN AL CLIENTE DEL AÑO 2015

Con la garantía de ser atendido por los mejores profesionales.

FÁCIL DE USAR. 100% CLOUD.

El nuevo 1&1 Servidor Cloud te ofrece la combinación perfecta entre el rendimiento de un hardware dedicado y la flexibilidad de la nube.

FLEXIBLE Y ASEQUIBLE

Configuración a medida

- SSD, RAM y CPU configurables de manera independiente y flexible. Adaptables a todo tipo de necesidades
- **Nuevo:** tarifas preconfiguradas listas para contratar

Transparencia de costes

- Facturación por minutos
- Facturas detalladas para un control y una planificación de costes eficiente
- Sin compromiso mínimo de permanencia

FÁCIL Y SEGURO

1&1 Cloud Panel

- Interfaz innovadora y potente con administración inteligente

Seguridad

- Firewall integrado para proteger tu servidor de ataques
- Backups y snapshots para evitar pérdidas de datos
- Los centros de datos de 1&1 se encuentran entre los más seguros de Europa

TODO INCLUIDO

Máximo rendimiento

- Tráfico ilimitado
- Tu servidor listo en 55 segundos
- SSD Premium con capacidad virtualmente ilimitada
- Redes privadas, API profesional, balanceadores, firewall y muchas más capacidades configurables
- Incluye aplicaciones listas para usar como WordPress, Drupal™ y Magento®

1 PRUEBA DE 30 DÍAS

1 CLIC CAMBIO DE TARIFA

1 LLAMADA SOPORTE EXPERTO

91 136 00 00

1&1

1and1.es

* 1&1 Servidor Cloud un mes de prueba gratis. Después, desde 9,99 €/mes (12,09 €, 21% IVA incl.). Sin coste por alta de servicio ni compromiso de permanencia.
Servicio de Atención al Cliente del año: 200 tests de Mystery Shopper realizados por Gesfutur XXI y 2.000 entrevistas online realizadas por TNS entre mayo y agosto de 2014.
Windows es una marca registrada de Microsoft Corporation en Estados Unidos y en otros países. Linux es una marca registrada de Linus Trovalds en Estados Unidos y otros países.
Intel y el logotipo Intel son marcas comerciales de Intel Corporation en los Estados Unidos y en otros países.

Big Data...

...el camino para convertirse en millonario

En la lista de los más ricos del planeta de 2015 se han colado caras nuevas, lo curioso es que provienen de una de las tecnologías de moda: el *big data*.

Si echamos un vistazo al pasado reciente, podemos asegurar que, sobre todo en España, las grandes ideas han surgido de las necesidades más básicas y más simples. Las grandes fortunas han surgido de ponerle un palo a un caramelo o de una buena idea para una saga de libros, entre otras muchas ideas sencillas que han supuesto para sus creadores el pasaporte a la cumbre de los multimillonarios. Ahora, la forma en que unos pocos han percibido la recopilación, la interpretación y el uso de los datos masivos les ha llevado a construir verdaderos imperios y aquí os dejamos los ejemplos de algunos de ellos.

Vicent Viola, Virtu Financial (59 años)

Virtu Financial es una de las empresas más grandes de comercio electrónico de alta frecuencia y de creación de mercado de empresas. Virtu ejecuta diversas estrategias de negociación en renta variable, renta fija, divisas y materias primas a través de numerosas bolsas de valores y otros mercados. Opera en más de 25 sitios a nivel mundial, incluyendo la bolsa de New York y la Chicago.
Fue fundada por Vicent Viola, ex-presidente de la New York Mercantile Exchange en 2008 y desarrolló sus propios algoritmos de negociación en base a los principios del *big data*. El año pasado, la compañía anunció que solo había sufrido un día de pérdida en cinco años y se cree que Viola cuenta con un patrimonio neto de mil setecientos millones de dólares.

Reed Hastings, Netflix (54 años)

Netflix es una empresa estadounidense, fundada en 1997 en California, que propor-

ciona, mediante una tarifa plana mensual, *streaming* multimedia de películas y series de televisión bajo demanda a través de Internet y de DVD por correo. Comenzó su servicio basado en suscripción en 1999 y para el año 2009, Netflix estaba ofreciendo una colección de 100.000 títulos en DVD y había superado los 10 millones de suscriptores. A día de hoy cuenta con más de 55 millones de suscriptores y su éxito se debe a la anticipación de sus fundadores, Reed Hastings y Marc Randolph, que comenzaron vendiendo DVDs por correo y aprendieron a utilizar el *big data* para dar a cada usuario lo que quería.

Predecir lo que su usuario va a querer ver a continuación es el objetivo principal de la estrategia de datos de esta compañía y para ello se han empleado equipos de aficionados a las películas que buscan entre todos los contenidos de cine y televisión y los etiquetan según sus temáticas. Netflix también está invirtiendo en organizar concursos, con premios millonarios, para aquellos que sean capaces de descubrirles los algoritmos que hacen posible predecir con mayor precisión los hábitos de su audiencia.

A día de hoy Reed Hastings tiene una fortuna aproximada de mil millones de dólares y también forma parte del consejo de administración de Facebook.

Alexander Karp, Palantir (47 años)

Karp tuvo la ayuda de la CIA con la construcción de Palantir, que utiliza algoritmos de *big data* para combatir a los terroristas y el fraude financiero de todo el mundo. Su principal cliente es el gobierno de Estados Unidos, que utiliza su software para predecir todo, desde la colocación de bombas en las carreteras a las transacciones fraudulentas. Aunque gran parte de su trabajo continúa siendo alto secreto, se sabe que sus rutinas para detectar patrones y anomalías en los datos que indican actividad sospechosa o fraudulenta se derivan de la tecnología desarrollada por Paypal. De hecho,Peter Thiel, co-fundador del servicio de pago en línea, también es co-fundador en Palantir.

La compañía fue fundada en 2004 como empresa privada especializada en análisis de datos y es conocida por dos proyectos en particular: Palantir Gotham y Palantir Metropolis.

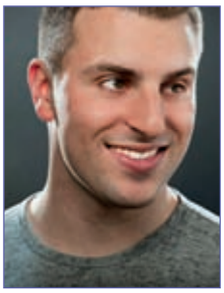
Inicialmente se concentra en la seguridad y la lucha contra el terrorismo para clientes gubernamentales, una idea que ha supuesto a Alexander Karp conseguir una fortuna que ronda mil doscientos millones de dólares.

Travis Kalanick, Uber (38 años)

Uber es una empresa que proporciona a sus clientes una red de transporte a través de una App. Esta aplicación conecta a los usuarios que necesitan un medio de transporte con conductores de vehículos registrados en su servicio, los cuales ofrecen un servicio de transporte. La empresa organiza recogidas en decenas de ciudades de todo el mundo, tiene su sede en San Francisco y fue fundada por Travis Kalanick y Garrett Camp en 2009.

En esta caso sus fundadores utilizaron el *big data* como medio para distribuir la red alternativa de transporte y así conseguir que, zonas que no estaban bien comunicadas, mejorasen notablemente. Realizando un análisis en profundidad de las ciudades a las que sirve, se centran en las zonas peor atendidas para procurar enlaces con autobuses o trenes. También monitorean los viajes de los usuarios para predecir las demandas y asignar recursos que les permitan llegar a su destino.

Travis Kalanick, es uno de los recién llegados a la lista de Forbes y cuenta con un patrimonio neto de cinco mil trescientos millones de dólares.



Brian Chesky, Airbnb (33 años)

Cuentan los rumores que el CEO y co-fundador de Airbnb no ha tenido casa propia hasta el año 2010, pero no se ha tratado de un problema económico, sino que, al parecer, estuvo utilizando su propio servicio que conecta a viajeros con propietarios de viviendas dispuestos a alquilarlas durante una temporada.

Airbnb fue fundada en 2008 por Brian Chesky, Joe Gebbia y Nathan Blecharczyk en San Francisco y actualmente se hacen 24 millones de reservas en 34.000 ciudades. La compañía recoge a diario medio petabyte de información sobre hábitos de viaje y días festivos, lo que les permite inscribir a los propietarios en los destinos más populares y en las horas puntas.

Esta idea le ha supuesto a Brian y a sus compañeros la nada desdeñable fortuna de mil novecientos millones de dólares cada uno.

Evan Spiegel y Bobby Murphy, SNAPCHAT (24 y 26 años)

Son los recién llegados a la lista Forbes más jóvenes, con tan solo 24 y 25 años. Se conocieron cuando estudiaban en la Universidad de Stanford y en 2013 rechazaron una oferta de 3000 millones de dólares que Facebook les ofrecía por su aplicación. La decisión resultó ser un acierto ya que la compañía tardó apenas un mes en ser valorada en 19 mil millones de dólares.

Snapchat es una aplicación que permite a los usuarios tomar fotografías, grabar vídeos, añadir textos y dibujos y mandarlos a una lista de contactos limitada. Estos vídeos y fotografías se conocen como "Snaps" y los usuarios pueden controlar el tiempo durante el que estos serán visibles, de 1 a 10 segundos de duración. Transcurrido este tiempo las imágenes desaparecerán de la pantalla del destinatario y serán borradas del servidor de Snapchat.

Aunque había un montón de aplicaciones de mensajería y fotografía, Spiegel y Murphy fueron los primeros en percatarse de que no todo el mundo - por alguna razón desconocida - quería que esas fotos permaneciesen en los teléfonos de sus destinatarios y el éxito fue rotundo, lo que les ha supuesto entrar en la lista Forbes con una fortuna de mil quinientos millones de dólares cada uno.

Isis Vecino

El CIO tiene que superar varios retos en **materia de seguridad**

El CIO debería formarse más, emplear más tiempo y un mayor presupuesto en seguridad, así como elaborar un mejor plan holístico, mientras se espera que la seguridad siga siendo la prioridad número uno de los departamentos de tecnología de la información. Así lo afirmaban Mario García, director general de Check Point; Ángel Victoria, director comercial de G Data; Alberto Arbizu, responsable de *cloud* y *networking* de Citrix y Ricardo Maté, director general de F5 Networks Iberia en el desayuno sobre seguridad organizado por la revista directorTIC.

Inma Elizalde

Aunque la seguridad es uno de los aspectos en los que todas las empresas siguen invirtiendo, es mucho el trabajo que queda por hacer. Así opina Mario García, director general de Check Point, ya que "todavía no estamos preparados para el tipo de amenazas y ataques que están llegando y que están tan de moda". Una afirmación que viene avalada por un contundente dato: a nivel mundial, el número de empresas preparadas para estos retos no llega al 1 %. Por ello, Ángel Victoria, director comercial de G Data, opina que las empresas tienen que realizar una evaluación continua en este largo reto en el que las amenazas son cada vez más complejas y sofisticadas y van persiguiendo objetivos muy concretos. ¿El problema? Además de la insuficiente preparación para abordar esto por parte de las compañías, el bajo presupuesto invertido para hacerlo. Todo ello junto a otros factores que están potenciando las amenazas o las inversiones en esta área: por un lado la implantación de políticas de movilidad, destaca Alberto Arbizu, responsable de *cloud* y *networking* de Citrix y por otro, no solo a nivel empresarial sino de todos los gobiernos, los ciberataques que están cambiando de manera decisiva la manera de ver la seguridad.

Por su parte Ricardo Maté, director general de F5 Networks Iberia hace referencia al cambio del paradigma de la aplicación dentro de un centro de procesos de datos. "Y es que por un lado están la aparición y el despliegue masivo de dispositivos móviles o Internet de las Cosas, que va a poner millones de dispositivos conectados a través de redes IP, dispositivos que de alguna manera hay que proteger. Por otro lado el despliegue de aplicaciones dentro de la nube, con políticas de seguridad que, en muchos casos, son distintas a las que se tienen dentro de los centros de datos propios y esto hace que se mire todo de una manera diferente a la que se veía hasta ahora, desde el punto de vista de seguridad". Y es que, en su opinión, los modelos tradicionales ya no valen. "A veces es más sencillo desplegar políticas de seguridad para acometer proyectos en todas estas áreas pero para la pyme es un reto prácticamente inabarcable. Las grandes compañías, como disponen de presupuestos mucho mayores, pueden permitirse poner en marcha planes de seguridad que cuenten con una cobertura mayor pero eso no significa que tenga resuelta toda su problemática. En algunos casos creen que están protegidos y que no les va a pasar nada pero cuando sufren un ataque se dan cuenta de que no tenían los mecanismos de seguridad adecuados.

El papel del CIO ante la seguridad

Algunas empresas no tienen un responsable de seguridad, por lo que es el CIO el que tiene que ocuparse de la misma. Sin embargo, los asistentes al debate consideran que estos tienen que evolucionar en gran medida en esta materia, aunque también son de la opinión de que la persona de seguridad no debería depender del CIO en ningún caso ya que el objetivo de la gente de informática es mantener la operatividad delos sistemas, mientras el responsable de seguridad tiene que mantener los sistemas seguros y muchas veces estos objetivos pueden llegar a chocar. Por esta razón el CIO que no tiene

"En las empresas hay que hacer un plan holístico viendo qué es lo que se quiere hacer, cómo y dónde quieres llegar en tu estrategia de seguridad "

un CISO tiene que asumir una responsabilidad mucho más grande y tiene que ser él quien ordene no lanzar servicios que no sean seguros, buscando asesoramiento en las empresas y fabricantes para apoyarse y ver cómo sacan adelante dicho servicio.

Y es que, tal y como manifiesta Ángel Victoria, "los CIOs tienen tanto por abarcar dentro de las empresas que son más reactivos que proactivos en temas de seguridad, por lo que van a remolque".

Otro reto importante que tienen que asumir, según Ricardo Maté, es el de la formación. Un elemento que deberían considerar como crítico, formándose ellos en primer lugar para poder conocer los riesgos existentes, formar a su equipo y a sus empleados, con el fin de evitar riesgos.

Mario García también hace alusión a la falta de concienciación de las personas, al tiempo que recuerda que no se puede sacar un servicio al mercado que no sea seguro.

Y es que tal y como los expertos sostienen, "la empresa tiene que ser consciente de que deben trasladar al empleado ciertas prácticas de uso, siendo ellas quienes propongan las medidas cuando se entra a trabajar en una compañía".

¿Hasta qué punto se utilizan mal los dispositivos móviles?

Los ponentes al debate hicieron alusión a la gran cantidad de riesgos que puede conllevar hacer un mal uso de los dispositivos móviles. ¿Algunos ejemplos? El hecho de no tener un sistema de autentificación avanzado que permita, desde cualquier dispositivo móvil, entrar en tus aplicaciones pone en riesgo a las empresas. El hecho de que en tus dispositivos móviles o en tu propio ordenador de pantalla no tengas un sistema en el que cada determinado tiempo no debas hacer tu autentificación puede permitir que en un momento dado vayas a tomar un café, dejes tu ordenador, tableta o móvil a disposición de cualquier persona y accedan a tus aplicaciones. "Los dispositivos móviles, de alguna manera, son un tema tabú para la mayoría de los CIOs porque son conscientes de que es un elemento muy crítico y peligroso para esas aplicaciones", observa Ricardo Maté, aunque apunta que no se puede prohibir a los empleados y clientes que accedan a tus aplicaciones con dichos dispositivos, por lo que tienes que darles los mecanismos de seguridad para proteger el acceso a las aplicaciones que tienes con esos dispositivos". Para ello hay tecnologías que permiten garantizar un nivel muy elevado de seguridad, sostiene.

Aplicaciones

¿De qué tipo de aplicaciones estaríamos hablando? De todo tipo, responde Mario García, quien recuerda que Check Point es una empresa de origen israelí que lleva la seguridad muy dentro y sin embargo cuentan con una política de BYOD. "Eso no implica que dispongamos de aplicaciones que existen en la nube que son terceras a nosotros. ¿Puedo acceder a ellas desde mi dispositivo móvil? Sí pero con un procedimiento de

Mario García, director general de Check Point

seguridad. Hay que proveer de las herramientas y forzar a su cumplimiento", propone.

Desde Citrix, Alberto Arbizu responde que muchas veces no somos conscientes de lo que hacemos en materia de seguridad cuando, por poner un ejemplo, subimos nuestras fotos a Dropbox y no sabemos que al hacerlo, aunque podemos disponer de esa información, la propietaria de la misma pasa a ser Dropbox.

Ángel Victoria pone el énfasis en materia de movilidad, donde se ha creado la figura del *chief movility manager*, una nueva figura que está sumando informaciones de la parte de sistemas, del director de seguridad, del de comunicación, de RR.HH., aunque falta otro factor: el de la legalidad. Hay que aunarlo todo e intentar consensuarlo, dice. "Un reto importante porque hace años la seguridad tenía diferentes capas, estaba compartimentada de alguna manera y hoy en día es justo lo contrario", especifica.

El impacto

Tampoco debemos olvidar la diferenciación que debemos realizar entre el impacto económico que tienen determinado tipo de ataques o de información frente al impacto de imagen. El impacto económico que hay en la mayoría de los casos es bajo pero desde el punto de vista de imagen es muy alto porque como entidad deberíamos preocuparnos más en garantizar y transmitir una seguridad hacia los usuarios, el eslabón más débil.

Los ponentes también hicieron referencia a las Administraciones Públicas quienes, en su opinión deberían jugar un papel muy importante en esta protección porque son garantes de una gran cantidad de información confidencial de los ciudadanos. "Garantizan un sistema de acceso seguro pero no que el que esté tecleando esa información seas tú y que esa información no vaya a un ciberdelincuente", dicen.

¿Qué pedirían a las Administraciones en cuanto a la regulación de los datos?

En este sentido lo tienen claro ya que como desde F5 Networks manifiesta su representante, "hay una Ley de Protección de datos que es muy exigente con respecto a qué información se puede publicar o cómo se publica. La legislación existe, otra cosa es qué hacen las empresas y los organismos públicos para protegerla. Requiere por un lado la concienciación, la planificación, la puesta en marcha de determinadas acciones para proteger esos datos y no en todas las empresas u organismos se lleva esto a cabo". "En estos momentos se empiezan a desplegar muchas aplicaciones en la nube", prosigue, "y

"En Citrix hemos optado por la política de alianzas frente a las nuevas amenazasl"

muchas de ellas las despliegan departamentos de empresas que están fuera del control de IT, fuera del control de las políticas de seguridad de la empresa, por lo tenemos que ver cómo somos capaces de implantar una misma política de seguridad cuando contratas aplicaciones fuera de tu entorno. Cómo estableces mecanismos de autentificación para acceder a esas aplicaciones que están fuera de tu entorno protegido".

Esto es muy interesante, reconocen desde G Data, "porque puedes regirte en cuanto a leyes europeas, que pueden ser muy estrictas en cuanto a privacidad pero por otro lado puedes estar usando servicios de otros países donde la NSA —Agencia de Seguridad Nacional— ha tenido mucho poder en cuanto a saltarse cualquier tipo de privacidad".

Y es que como Maté dice, "muchos de los servicios *cloud* que se están dando están establecidos fuera de España y en algunos casos fuera de Europa. La normativa que rige dentro de ese centro de datos donde se da el servicio *cloud* no tiene porqué ser la misma que se da en otros lugares. Y es muy curioso porque algunos SLAs tienen un nivel de servicio muy bajo, por lo que las empresas deberían regular que no se contrata ningún servicio *cloud* si no pasa por un departamento de seguridad que verifique que cumple con unos estándares mínimos de seguridad y que esos proveedores *cloud*, a su vez, cumplen con los estándares que se han definido".

Un elemento fundamental en este sentido es para Ángel Victoria la encriptación de los datos, algo que no ocurre ni con Dropbox ni con WhatssApp. "Nosotros hemos sacado una aplicación de mensajería instantánea y proporcionamos herramientas que un departamento TI pueda probar sin problemas porque permiten la encriptación".

¿Qué tipo de herramientas son las que más demandan las empresas?

Hay de todo, responde Mario García, pero hay que hacer un plan holístico de seguridad viendo qué es lo que se quiere hacer, cómo y dónde quieres llegar en tu estrategia de seguridad. Una vez que tienes claro esto, tendrás que decidir cuáles son las adecuadas porque no te hacen falta todas las tecnología en todas partes. Hay que adecuar las protecciones al uso y a la utilidad que se hace de cada una de ellas. Y a partir de ahí ver si vas a contratar un servicio en la nube y cuál, qué SLA me están dando, dónde va a poner los datos esta empresa... Tenemos que ser conscientes de que la información es dinero y que el uso de la información tiene unas normas y pensar cómo vamos a permitir el acceso a la información y desde dónde vamos a acceder a ella. La falta de estas medidas lleva a ataques", recuerda. Es más, dice que lo ideal sería sentarse con un director de seguridad o un responsable de informática y preguntarle por las aplicaciones que tiene, dónde las tiene, cómo las va a securizar... para tomar decisiones.

"Los CIOs tienen tanto por abarcar dentro de las empresas que son más reactivos que proactivos en temas de seguridad, por lo que van a remolque"

Alberto Arbizu, responsable de cloud y networking de Citrix

El pago por uso

Al contrario que en otros sectores, el pago por uso todavía es algo emergente en la seguridad, confiesan los directivos. "Cada cliente tiene unas necesidades diferentes de otros. A unos les viene bien el pago por uso, a otros tenerlo en propiedad... cada uno tiene sus propios requisitos, su propia particularidad y hay que saber afrontar cada una de las cosas. Y en muchos casos son complementarios. Lo que hay que aceptar es que hay espacio para todas las herramientas. En el plan de seguridad hay que tener en cuenta dónde vamos a poner esa aplicación y qué voy a hacer con ella, pensando asimismo en la vida de la misma porque hoy la podemos tener en local, más adelante en una cloud privada, otro día híbrida... teniendo en cuenta cómo va a evolucionar la seguridad, quién va a acceder y cómo va a acceder a esos datos. Con ese plan en mente podremos tener la libertad de mover esas aplicaciones, ser más flexibles... porque la seguridad no tiene que venderse como un freno a la hora de hacer las cosas, tiene que

Ángel Victoria, director comercial de G Data

Ricardo Maté, director general de F5 Networks Iberia

ser un facilitador para hacerlas. Para hacer algo en la nube tiene que ser seguro, si no no lo podría hacer", argumenta el director general de Check Point.

Y es que como recuerda el director general de F5 Networks Iberia, "muchas empresas no contemplan soluciones de seguridad porque no han tenido, o creen no haber tenido ataques. Incluso hay vulnerabilidades que son públicas pero todavía no se han resuelto dentro de las empresas", advierte. Por ello, el director comercial de G Data aconseja proporcionar herramientas que gestionen estas vulnerabilidades. "Hay que empezar por lo básico e ir construyendo un entorno de seguridad adecuado pero muchas veces por el camino se quedan las prácticas más simples" "Crear un manual de seguridad que sea entendible por parte de todos los empleados", añade García.

¿Desafíos para los fabricantes?

Y entre los desafíos para los fabricantes la explosión brutal de *malware* y la profesionalización de los ataques, y por lo tanto ser capaces de proveer de herramientas para que las empresas puedan defenderse de lo conocido y de lo desconocido o intentar estar por delante de las potenciales amenazas y ataques, por poner algunos ejemplos. En algunos casos, como en el de Citrix, han optado por la política de alianzas frente a las nuevas amenazas, integrar tecnologías de otras compañías dentro de sus soluciones porque, tal y como reconoce Alberto Arbizu, responsable de *cloud* y *networking* de la compañía, no se puede ser perfecto y saber de todo.

¿Soluciones complejas?

¿En qué medida se están reduciendo la complejidad en las soluciones de seguridad? No mucho, a juzgar por las palabras de los presentes que comentan que aunque intentan suministrar herramientas que hagan la vida más sencilla, detrás hay una complejidad y se necesitan expertos que sepan gestionar las soluciones que hay detrás. Y es que las soluciones tienen que ser muy ajustables, por lo que requieren de cierto grado de complejidad.

Sin embargo las empresas no les piden herramientas a medida sino customizarlas, reconoce Ángel Victoria, director comercial de G Data. "Hay que darles una solución a medida en el sentido de que no hay dos empresas iguales, especifica Mario García, director general de Check Point.

"Los dispositivos móviles son un tema tabú para la mayoría de los CIOs"

Nuevas amenazas

El ciberterrorismo es un negocio suculento para muchos, un negocio que no para... Entre los nuevos ataques que están surgiendo en los entornos de la virtualización y el *cloud computing* figuran los ataques de denegación de servicio y los accesos a la información "porque en el momento en el que publicas diferentes aplicaciones en diferentes proveedores y permites al usuario que utilice su clave y su *password* fuera del control de la empresa, alude Arbizu, "existe un riesgo. El departamento de IT de la empresa debe tener un sistema de identidades dentro de su control que sea el que defina las políticas de autenticación y que establezca el túnel seguro desde tu sistema de autentificación con el proveedor de aplicación en la nube".

Y todo ello sin olvidar que otra de las cosas que más se buscan es comprometer el PC o el dispositivo de una persona para ganar acceso desde ese punto de trabajo a través de un móvil, un PC fijo o un portátil o Mac. Ganar acceso a todos los sistemas y servicios de empresa, por lo que una de las áreas de desarrollo más grande en seguridad es cómo voy a conseguir que esos PCs no se comprometan, si alguien los compromete cómo voy a averiguar que están comprometidos, cómo impedir que esa información salga hacia afuera y cuáles son las herramientas para que cada día sea más difícil.

Presupuestos

Y, aunque los presupuestos en esta materia se mantienen más o menos estables, Ricardo Maté dice que algunas grandes empresas están empezando a tener un poco más de presupuesto para inversión, lo cual afecta a la seguridad, aunque otras empresas siguen con una congelación de los mismos. Mientras Mario García considera que las empresas de seguridad "están cogiendo más tarta del presupuesto de IT" porque las empresas son conscientes de que tiene que actualizar su seguridad, analizando lo que se gasta. Dentro de la seguridad ¿el mayor crecimiento de dónde viene? De la movilidad, el BYOD, el *cloud computing*... todos ellos por partes iguales, afirman al unísono los ponentes, aunque reconocen que el BYOD es el que más está por explotar porque las empresas no están tomando las medidas adecuadas para protegerse.

En cuanto a las predicciones pasan por que la seguridad va a seguir siendo la prioridad número uno de los departamentos de tecnología de la información y de los departamentos de seguridad y por desgracia vamos a seguir viendo cada vez más ataques sofisticados, más difíciles de proteger y defender y al final las empresas tienen que dotarse de los mecanismos para conseguir esa protección.

Para ver todos los vídeos de la mesa escanea este código

SAPIMSA potencia la seguridad del correo electrónico con Email Protection de **Retarus**

El mundo SAP requiere de un equipo humano y tecnológico preparado y adaptado a las necesidades del futuro. SAPIMSA, empresa española que cuenta con el máximo prestigio como proveedor de servicios del ecosistema SAP, ha apostado por Email Protection de Retarus, una solución de ecomunicación de próxima generación cuya implantación le ha permitido mejorar los servicios de seguridad de su correo electrónico.

SAPIMSA es un proveedor de servicios que, desde el año 1990, centra su dedicación en exclusiva al entorno y herramientas SAP, lo que supone que su equipo profesional se considere como uno de los que más experiencia tiene dentro de este complicado ecosistema. Desde entonces, la empresa ha obtenido múltiples reconocimientos por parte de sus clientes, para los que ha desarrollado proyectos de gran complejidad.

Aplicando los principios de una mejora continua y apoyada en la calidad de la gestión, SAPIMSA posee distintas certificaciones que cualifican a su equipo humano y entidad. Entre ellas, la certificación ISO 9001:2000, que asegura un servicio de alta calidad, sujeto al seguimiento y evaluación necesarios. Además, la empresa española lleva a cabo certificaciones continuas de su equipo humano en ITIL e ISO 20000, aplicando de esta forma en sus proyectos los más altos estándares del mercado, todo lo cual le ha permitido ser *partner* destacado SAP y entidad destacada en el mercado.

SAPIMSA, en su política de mejora y evolución tecnológica continua, se propuso mejorar los servicios de seguridad en el correo electrónico, que hasta ese momento desarrollaba a través de un *appliance in house*.

Mayor seguridad en el correo electrónico

El objetivo de la compañía pasaba por mejorar los servicios de seguridad en su correo electrónico y, para ello, necesitaba disponer de una solución completa que mejorara la velocidad de las actualizaciones de las listas de virus y spam y que, al mismo tiempo, permitiera una gran reducción de los costes operacionales, apostando por Email Protection de Retarus.

"La implementación de la solución fue muy rápida, ya que aproximadamente un 95 % del esfuerzo recayó en el lado de Retarus. Por nuestra parte, sólo tuvimos que desviar el tráfico entrante a la infraestructura de Retarus y, durante un par de semanas, llevar a cabo una prueba de concepto. Mientras se llevaba a cabo la última prueba se añadieron más dominios de SAPIMSA y, finalmente, se pasó a la fase de producción. Todo el proceso fue sencillo, rápido, eficaz y transparente. Todo un éxito", afirmaba Juan Carlos Álvarez, socio y director de informática de SAPIMSA.

Una vez finalizada la implantación de Email Protection, Retarus llevó a cabo una completa formación al administrador del servicio, completando la entrega y, por tanto, el proyecto de implantación, sin que fuera necesario llevar a cabo algún cambio sustancial, configuración o modificación de los estándares de seguridad propios de SAPIMSA.

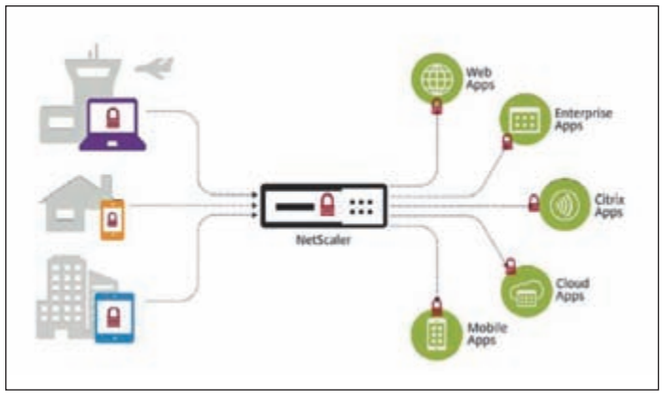
"Para Retarus, la implantación de E-mail Protection en SAPIMSA ha sido una prueba más de cómo una solución de e-comunicación de próxima generación puede llevarse a cabo en muy poco tiempo y, sobre todo, sin afectar lo más mínimo la operativa de negocio. Hemos sido una compañía pionera a la hora de ofrecer soluciones *cloud* de ecomunicación para el ecosistema SAP, y por ello empresas del prestigio de SAPIMSA han optado por Retarus", concluía Andrés García, *country manager* de Retarus Ibérica.

Retarus
Tel.: 91 414 95 00

Las nuevas demandas en los Accesos a las Aplicaciones e Infraestructuras: un punto de inflexión en la seguridad para las empresas

Con el "boom" de la Consumerización de las TI y la implantación de políticas de (BYOD), la proliferación de los dispositivos móviles - todos con servicios de datos de alta velocidad -, ha roto cualquier tipo de previsión. Prácticamente todos los usuarios son susceptibles de tener un "acceso remoto listo" a demanda. Todo lo que se necesita es una solución que sea compatible con todos los dispositivos y la capacidad de prestar el acceso adecuado conforme a las políticas de protección de datos.

La demanda de lo que los usuarios para acceder a cualquier tipo de aplicación, independientemente de si esta se encuentre en el Data Center o en la Cloud; además de los recursos compartidos de red, aplicaciones web, SaaS y aplicaciones móviles, hacen que las organizaciones demanden de manera urgente un único punto de acceso a la información de manera segura.
En Citrix, hemos recogido todas estas necesidades por parte de los usuarios; y lo hemos reflejado en la nueva funcionalidad Citrix Unified Gateway, facilitando:



1.- Múltiples modos de conexión, asegurando la cobertura para el conjunto más amplio de usuarios y situaciones de acceso. A través un modo de acceso "sin cliente", que requiere nada más que un navegador, permitiendo un acceso rápido a cualquier tipo de recurso y aplicación.
Cualquier usuario, se puede descargar el software de cliente Citrix Receiver - el cliente de acceso universal de Citrix, complementando el acceso a XenDesktop y XenApp -, o el NetScaler con Unified Gateway Plug-in.

2.- SmartAccess para la gestión y control de las políticas de acceso. Permite a los administradores restringir o ampliar el grado del acceso provisionado inicialmente, para alinearse con el nivel de confianza de cada sesión de acceso. Si el dispositivo de un usuario es menos de confianza, como un quiosco del aeropuerto, entonces el acceso puede ser limitado a los recursos de acceso. Sin embargo, si el usuario está en casa en un ordenador portátil corporativo, entonces la política puede dinámicamente permitir el acceso a todas las aplicaciones y servicios.
Además, NetScaler con el Unified Access Gateway, soporta cualquier tipo de plataforma basada en MacOS y Windows, en el caso de portátiles y dispositivos con iOS, Android o Linux OS.

3.- Una única URL para cualquier Aplicación, Dispositivo o Dato.

- **Single Sign On (SSO)** para asegurar un único acceso seguro para aplicaciones SaaS y Web2.0, consolidando todos los accesos en una única solución y proporcionando un importante ahorro en costes.

Protección de extremo a extremo

- **Control basado en Identidad:** NetScaler Unified Gateway se puede utilizar como un proveedor de identidad SAML 2.0 para controlar el acceso a los recursos dentro de un DC o en una nube. NetScaler concede al usuario el acceso - sólo tras la validación de la identidad del mismo -, al conjunto de recursos que tenga autorización. Además de esto, NetScaler soporta diversos mecanismos de autenticación como autenticación local, RADIUS, LDAP, TACACS, Certificados Digitales, NTLM y Constrained Delegation de Kerberos.

- **Análisis End Point:** para verificar la identidad de la propiedad corporativa de los dispositivos y determinar si cumplen con las políticas corporativas de seguridad, como por ejemplo tener operativo y actualizado de antivirus y software de firewall personal. Para dispositivos que no cumplan estas comprobaciones, el acceso puede estar restringido a la remediación de las zonas definidas en el que los usuarios pueden obtener las herramientas necesarias para dar cumplimiento a lo dispuesto.

- **Accesos Clásicos SSL y MicroVPN (dispositivos móviles):** Todas las sesiones están protegidos por las normas de interceptación de cifrado SSL/TLS. Con VPN SSL, el túnel se puede utilizar para proporcionar acceso a un amplio conjunto de recursos, y/o acceso total a la red. Alternativamente, los administradores dispondrán de la solución innovadora de MicroVPN en XenMobile, que permite definir el túnel por aplicación, entre el servidor de apps. Móviles y el dispositivo, reduciendo el impacto a nivel de seguridad de los dispositivos que se encuentran en una situación comprometida.

- **Split Tunneling:** esta funcionalidad, hace que los clientes tengan acceso a otra red mientras se están conectando a un entorno protegido (eliminando así una potencial de pérdida de datos). Con esta funcionalidad, los usuarios pueden ser bloqueados para acceder directamente a la Internet, pero podrán obtener acceso a determinados servicios de subred local del cliente (por ejemplo, impresión y archivos compartidos).

- **Limpieza de la caché del navegador:** todos los objetos almacenados en la caché local del browser, pueden ser borrados después de cada sesión.

- **Monitorización y Troubleshooting con Web/HDX Insight**: Con NetScaler Insight Center, los administradores también tendrán visibilidad de extremo a extremo de todo el tráfico web y tráfico ICA. Los informes dan visibilidad sobrelos usuarios, escritorios y aplicaciones, por ejemplo, sobre el ancho de banda consumido, las sesiones activas, o latencia para el usuario, el round-trip para el servidor y vuelta los tiempos de respuesta para XenDesktop y XenApp en las sesiones de acceso remoto.
Proporcionando información en Tiempo Real, también permite mostrar el histórico de los datos en los accesos, para ayudar a los administradores de TI sobre ¿Qué escritorios alojados (o aplicaciones web) se utilizan más? o el nivel de señal de rendimiento para añadir más capacidad al servidor, etc.

Conclusiones

Manteniendo el equilibrio entre la necesidad de una única dirección URL/Portal de acceso para los usuarios y la necesidad de un único punto de control para los administradores de TI, Citrix NetScaler Unified Gateway, cubre todas las nuevas necesidades de todos accesos remotos para las Empresas u Organizaciones.
Con Unified Gateway, Citrix permite a los usuarios obtener una alta granularidad de acceso a todas las aplicaciones, escritorios, datos y otros recursos que necesiten donde quieran, cuando quieran y desde cualquier tipo de dispositivo desde el que quieran acceder. Al mismo tiempo, los administradores de aplicaciones, dispondrán del control granular necesario y mayores capacidades de protección, para mantener el cumplimiento de las normas y asegurar los más altos niveles de seguridad en toda la empresa, desde cualquier dispositivo/sistema operativo. Con NetScaler Unified Gateway, todos los usuarios estarán protegidos en una sola plataforma unificada significa que ahora pueden consolidar el conjunto heterogéneo de soluciones anteriormente comentadas para cumplir con todas las necesidades en los accesos remotos seguros. El resultado es menos complejidad y menos costes.

Ibermática renueva los equipos de la Diputación Foral de Álava

La Diputación Foral de Álava ya cuenta con un parque de ordenadores totalmente renovado. A lo largo de algo más de cuatro meses Ibermática se ha encargado de sustituir hasta 1.212 equipos de sobremesa y portátiles, así como de migrar su sistema operativo a Windows 7 64 bits con Internet Explorer 11 y Office 2010. Todo ello bajo las pautas marcadas por el Centro de Cálculo de Álava y en estrecha colaboración con su equipo técnico. Con la nueva plataforma informática la entidad foral podrá responder de forma más ágil a las cada vez mayores necesidades que van surgiendo en sus distintos ámbitos de actuación.

El Centro de Cálculo de Álava (CCASA), encargado de prestar los servicios que garanticen la consecución de la visión estratégica de los sistemas de información de la Diputación Foral en el entorno de las tecnologías de la información y comunicaciones, adjudicó a Ibermática hace algunos meses un contrato para renovar todo su parque de equipos informáticos de puesto de trabajo. El objetivo, contar con una plataforma con mayores prestaciones, tanto a nivel del hardware como del software, acordes con unas necesidades que crecen permanentemente en el tiempo.

La migración ha incluido tanto la renovación del hardware de PC como el paso al sistema operativo Windows 7 64 bits con Internet Explorer 11 y Office 2010. Todo el proceso ha sido altamente automatizado, dando como resultado puestos más estandarizados y configuraciones más rigurosas. En esta línea, también se ha automatizado la instalación de aplicaciones (hasta 118 comerciales y 229 internas), cuya implementación podrá realizarse a partir de ahora de forma desatendida.

Con el apoyo tecnológico de Ibermática, sustituye 1.212 equipos y los migra a Windows 7

Además, se ha aprovechado la renovación de los puestos para la integración del PC con el sistema de Telefonía de la Entidad Foral, y se ha impulsado un ambicioso plan de comunicación y formación, con un grado de asistencia a los cursos presenciales de entorno al 80 %.

Con todo, se ha conseguido racionalizar el parque informático, permitiendo una estandarización del puesto de trabajo, así como dotar a los profesionales de la Diputación Foral de un método de gestión y distribución automática de aplicaciones al puesto ofimático. Todo ello ha requerido organizar una importante estructura de *backstage* técnica y humana para resolver con agilidad las incidencias registradas durante el proceso.

En este sentido, cabe destacar que el impacto del cambio en el usuario ha sido mínimo. Y es que la solución técnica de este proyecto y los procesos de despliegue necesarios para poder distribuirla en todos los puestos corporativos de la Diputación y CCASA se ha realizado de manera automatizada, sin intervención del usuario y manteniendo la información y configuración del antiguo sistema.

Además, la migración se ha realizado mediante técnicas de USMT (User State Migration Tools) que también han permitido la automatización de los procesos de copia y configuraciones del puesto de usuario al nuevo puesto Windows 7, así como el apoyo sobre la plataforma SCCM 2012 de la Diputación para la distribución automática de los aplicativos del puesto.

Ibermática
Tel.: 943 413 500

Cómo detener ciberataques en 5 pasos

Ninguna compañía de alto nivel está hoy en día a salvo de sufrir un ciberataque. Los expertos, a menudo, explicando esta circunstancia de un modo alegórico, comparan la situación que sufren las empresas con los patos a los que se dispara en un puesto de tiro en una feria. El ejemplo ilustra una realidad: todas las empresas se hallan en el punto de mira y son susceptibles de sufrir el disparo de un cibercriminal en algún momento, la cuestión es sencillamente cuándo.

En el mismo momento en que se sufre un incidente de seguridad que causa una fuga de datos se producen perjuicios económicos con costes tanto directos como indirectos. Los costes directos incluyen las investigaciones forenses, notificación a los afectados, remediación y multas reglamentarias - y estos son bastante costosos. La próxima legislación en materia de seguridad de la información y protección de datos de la UE podría castigar los incumplimientos con enormes multas de hasta el 5% de la facturación anual global de una empresa, o 100.000 euros.

Mario García, director general de Check Point para España y Portugal

Sin embargo, los costes indirectos, aunque menos tangibles, pueden ser aún más elevados. La marca corporativa y la reputación reciben un duro golpe que provoca daños a largo plazo - y, a su vez impacta directamente en el equipo ejecutivo. No obstante, no sólo se trata de conocer los datos y riesgos en materia de ciberseguridad, sino de entender exactamente cuáles son esos riesgos para cada compañía y cómo responder a ellos.

Simplificando al máximo, el riesgo para la seguridad de la información puede ser evaluado como una combinación de tres factores: activos, vulnerabilidades y amenazas. Hay cinco pasos clave que se pueden implementar para ayudar a su empresa a minimizar su exposición al riesgo, y mantener sus equipos fuera de la línea de fuego.

Primer paso: Evaluación

Llevar a cabo una revisión completa y objetiva de su entorno actual es la primera etapa en la construcción de una base sólida de seguridad. La evaluación debería valorar el perfil de riesgo de la empresa y la aproximación a la seguridad en todas las áreas, desde donde se almacenan y procesan los datos, a la red de arquitectura e infraestructura de seguridad, capacidad de monitorización y preparación de respuesta a incidentes.

Segundo paso: Segmentación

Después de una evaluación completa, el siguiente paso es segmentar la red de modo que las organizaciones puedan detener los ataques de alta velocidad conteniendo la infección antes de que se extienda a través de límites departamentales.

Tercer paso: Agregar controles de seguridad

Consiste en implementar controles para proteger los datos, los activos de negocio y operaciones, mientras que se refuerza la aplicación de las normas y estándares de la industria. Los métodos de ataque modernos exigen una prevención frente a amenazas en múltiples capas y tecnologías como la emulación de amenazas o 'sandboxing' que pueden ser de gran ayuda. Estas capas deben trabajar de manera conjunta para detectar, anunciar y detener los intentos de ataque, impulsadas por la inteligencia de amenazas en tiempo real.

Cuarto paso: Monitorización

La monitorización es un elemento crítico de seguridad para salvaguardar la red. El aumento de la visibilidad por la monitorización continua alerta a las organizaciones de cuando un ataque se está iniciando.

Quinto paso: Elaborar planes de respuesta a incidentes

Una respuesta efectiva ante incidentes es la que puede detectar un ataque antes de que tenga la oportunidad de causar problemas. Para garantizar la recuperación de desastres y la continuidad del negocio, las organizaciones necesitan trazar escenarios y formular un plan para mantener el negocio en marcha, incluso cuando se sufra un ataque.

En conclusión, es fundamental entender que, a pesar de que los ataques hayan aumentado en sofisticación y complejidad técnica, las organizaciones no están indefensas. Si bien es inevitable que una empresa concreta vaya a ser el blanco de un atacante, cómo se planifique y cómo se prepare marcará una gran diferencia en el resultado, para que en definitiva, no sea una presa tan fácil de disparar.

Fujitsu investigará junto a la **FIBHCSC** la fusión avanzada del conocimiento

Fujitsu Laboratories of Europe y Fujitsu en España han anunciado hoy un acuerdo de colaboración de investigación estratégica con la Fundación para la Investigación Biomédica del Hospital Clínico San Carlos (FIBHCSC). Fujitsu trabajará en estrecha colaboración con esta Fundación en varios proyectos de investigación, todo ello dentro de un objetivo a largo plazo de crear un sistema sanitario de valor añadido que ayude a la toma de decisiones clínicas a través de la provisión de servicios integrados mediante la informática sanitaria.

El acuerdo marco se basa en un satisfactorio proyecto de prueba de concepto inicial, desarrollado entre Fujitsu y FIBHCSC, que será presentado en el Fujitsu Innovation Gathering, el encuentro anual sobre innovación de Fujitsu Laboratories que se celebrará el 9 de Junio en IFEMA Madrid, de forma simultánea con el "Fujitsu World Tour 2015", el gran evento anual de la compañía en España.

"Estamos muy contectos de trabajar con la FIBHCSC para conseguir estos objetivos estratégicos a largo plazo. Esta colaboración está estrechamente alineada con la misión de Fujitsu Laboratories para transformar la tecnología en soluciones innovadoras que beneficien a la sociedad y mejoren la vida de los ciudadanos. También es un ejemplo de cómo la innovación abierta puede aplicarse para acelerar los procesos, consiguiendo resultados rápidos para resolver problemas del mundo real. Con respecto a la primera colaboración, el proyecto tecnológico sobre la salud mental, estamos deseando extenderlo, con el objetivo de cubrir de manera eventual todas las áreas clínicas a través de múltiples perspectivas departamentales, tales como gerentes, médicos y pacientes. Mediante el establecimiento de un sistema centrado en el valor, el objetivo es permitir la toma de decisiones basadas en evidencias para la prestación de servicios de salud integrados", aseguraba el Dr. Adel Rouz, vicepresidente ejecutivo de Fujitsu Laboratories of Europe.

El primer trabajo que se esta desarrollando se ocupa de cuestiones de salud mental, mediante el análisis de datos para identificar patrones y ayudar a las decisiones clínicas. Ha sido seleccionada esta especialidad debido a su fuerte impacto tanto a nivel social, como en los recursos sanitarios.

"Estamos en constante búsqueda para identificar nuevas formas de mejorar la manera en la que tratamos la enfermedad mental, que es muy representativa en los países desarrollados. Tenemos acceso a una gran cantidad de datos, pero es difícil extraer información significativa que nos ayude a

mejorar la calidad de los cuidados que ofrecemos. En este proyecto se aplica un enfoque completamente nuevo, utilizando la tecnología para extraer y visualizar una amplia gama de información útil que puede dar pistas sobre el comportamiento de nuestros pacientes. Es un importante paso adelante y estamos trabajando en estrecha colaboración con Fujitsu para convertir estos resultados iniciales, en unos servicios sanitarios inegrados más amplios en el futuro ", explicaba Julio Mayol Martínez, director de innovación del FIBHCSC.

La investigación se centra en la fusión avanzada del conocimiento y su tratamiento informático

En concreto, el trabajo que se está implementando, se centra en la realización de un análisis avanzado, con el objetivo de despejar incógnitas sobre enfermedades mentales a partir de un análisis de los datos en multiples facetas y así, apoyar la toma de decisiones clínicas. Por ejemplo, la plataforma utiliza *open data* para revelar correlaciones ocultas, identifica los patrones de asistencia de los enfermos a través de silos de datos clínicos heterogéneos y establece perfiles demográficos de los pacientes con trastornos de salud mental. También proporciona análisis exploratorios de conjuntos de datos complejos, ofreciendo información a través de una visualización rica e interactiva, que lleva a lograr entender mejor los datos en las diferentes fuentes consultadas.

"Estamos encantados de reforzar la relación entre Fujitsu y FIBHCSC con este acuerdo marco de colaboración en investigación y ya estamos viendo nuevas áreas de innovación. El proyecto de salud mental es el primer componente de un programa más amplio, con el objetivo de que, gracias a la aplicación de la tecnología, se pueda crear una solución sanitaria verdaderamente integrada. Nuestro objetivo es lograr soluciones que beneficien la sociedad y contribuyan a nuestro desarrollo y al de nuestros clientes, y esta asociación, ya en marcha, es una clara muestra de ello", afirmaba Ángeles Delgado, directora general de Fujitsu en España.

En la actualidad, también se está trabajando en un segundo proyecto, que se basa en la mejora de la rapidez y eficiencia en la detección del cáncer, utilizando la tecnología de registro de imágenes médicas de Fujitsu para la comparación de los cambios temporales de los nódulos. Esta tecnología tiene el potencial para incrementar la precisión y eficiencia de los radiólogos para la valoración de la evolución de los tumores, que de esta manera, podría ayudar en la detección más rápida de esta enfermedad, consiguiendo una precisión de imágenes mucho mayor que con sistemas anteriores, según test realizados en casos de enfermedades pulmonares.

Fujitsu
Tel.: 91 784 90 00

Unit4 ofrecerá ERP autónomo para organizaciones

Unit4, líder de rápido crecimiento en software empresarial, ha anunciado una colaboración estratégica con Microsoft que llevará al mercado la creación de aplicaciones de negocio y ERPs autónomos para organizaciones centradas en las personas.

Unit4 utilizará la tecnología inteligente de componentes de la plataforma PaaS de Azure y las soluciones de Microsoft Office, incluyendo el análisis predictivo, el aprendizaje automático, el análisis de flujo de eventos y el procesamiento de eventos complejos. Combinado con la People Platform de Unit4, la colaboración incrementará la velocidad de la innovación y conseguirá que los clientes se beneficien de un nuevo enfoque para la informática empresarial.

Convirtiendo en realidad el ERP autónomo

Para cumplir con la promesa de un ERP autónomo, Unit4 y Microsoft establecerán un equipo de desarrollo para asegurar que las innovaciones en Azure y Office se apliquen, cuanto antes, en la plataforma People Platform de Unit4. La información contextual se derivará mediante la combinación de los datos de negocio dentro de las aplicaciones de Unit4 con la información relevante de Office 365, Office Delve, correo electrónico, calendario, Yammer y más. Esto permitirá ofrecer un valor de negocio sin precedentes.

Las aplicaciones empresariales de Unit4, combinadas con Microsoft Azure, acelerarán la creación de un software de negocios autónomo

Las empresas de servicios profesionales serán capaces de combinar el análisis de datos históricos con el análisis predictivo para obtener información valiosa con la que decidir qué proyectos merecen su interés. Las organizaciones del sector público mejorarán la detección del fraude en los pagos de facturas, con el reconocimiento de patrones avanzados y el aprendizaje automático. Las ONGs tendrán la capacidad de hacer coincidir las campañas de donación, con los patrones de donación y con los donantes-objetivo de una manera más eficaz. Para lograr esta visión, los sistemas ERP requieren de datos de alta calidad y del acceso para completarlos. El ERP tradicional proporciona a los usuarios formularios en blanco no intuitivos y pide introducir todos los datos requeridos, lo que lleva a la entrada de datos no intuitiva, a los errores y a la frustración.

El ERP autónomo simplifica, en gran medida, la recopilación de datos mediante la utilización de tecnologías clave tales como el análisis predictivo para proporcionar a los usuarios información significativa contextual. Dicha información facilita la entrada de datos intuitiva basada en formularios prerellenados y en preguntas de validación sí-no basadas en el contexto. Ello ofrece una gran experiencia de usuario en todos los dispositivos, desde el ordenador de sobremesa al teléfono móvil.

Unit4
Tel.: 902 100 893

Más información sobre este proyecto

Movilidad, securizada y gestionada para sobrevivir al fenómeno BYOD

Uno de los retos más importantes del CIO es adaptar su compañía a la forma de trabajar de sus empleados y esto es inevitable cuando hemos llegado a un momento en que todos queremos trabajar de la misma forma en que vivimos. Estamos hablando de movilidad y del popular BYOD *(Bring Your Own Devcie)*, es decir, del uso que hacemos de nuestros móviles personales como herramienta de trabajo. Una circunstancia que ha dejado de ser una tendencia para convertirse en una realidad a la que, más pronto que tarde, se enfrentan todas las empresas. Afecta directamente a su productividad, normalmente mejorándola, aunque para que esto sea siempre así, esa movilidad debe estar securizada y gestionada. La "estrategia móvil" debe, por tanto, protagonizar su propio capítulo en la política de seguridad de las organizaciones.

Ángel Victoria, director comercial G DATA

Las empresas, con independencia de su tamaño o facturación, se han convertido en el objetivo más lucrativo de la industria del cibercrimen y sus dispositivos móviles constituyen uno de sus puntos débiles más reconocidos. El perímetro de la red se difumina y se hace móvil, tanto que podemos decir que viaja en el bolsillo de cada empleado y, en consecuencia, se multiplica el número de puertas que debemos blindar y proteger. No podemos afrontar el desafío que supone securizar los dispositivos móviles cuando surgen los problemas. Prevenir, cuando hablamos de seguridad, es más sencillo que remediar.

Se hace esencial proteger estos *smartphones* y tabletas que se conectan a nuestra red corporativa, tanto si son propiedad de la empresa como si funcionan en "régimen BYOD". Llegados a este punto, proteger esta "movilidad empresarial" no resulta complicado, basta con una solución de seguridad que incorpore un módulo MDM (*Mobile Device Management*).

Todas las soluciones empresariales de G DATA lo incorporan de serie y, además de proteger el terminal, como es lógico, permite la administración centralizada de los *smartphones* y tabletas que usan los empleados de su empresa, tal y como ha venido haciendo dese siempre con el resto de los ordenadores, portátiles y servidores que forman parte de la infraestructura TI de la compañía.

Es decir, desde la misma consola que utiliza para la gestión de los tradicionales clientes fijos, podrá programar escaneados, bloquear apps maliciosas o recibir alertas, en caso de terminales infectados. Además, su sistema antirrobo permite borrar la información almacenada en el terminal en caso de pérdida o robo del dispositivo.

Hemos comprobado muchas veces que lo que no se puede gestionar, no se puede proteger con eficacia. Ignorar la seguridad de los dispositivos móviles, o no incluirlos en las políticas de seguridad empresarial, implica obviar una realidad que está transformando la forma de funcionar de las empresas, así como trasladar la responsabilidad de su seguridad al propio empleado, con todo lo que esto significa. Si es algo que nunca haríamos con el ordenador que descansa en nuestra oficina, ¿por qué hacerlo con el dispositivo móvil?

Planificación de costes en tiempo real

Desde siempre, una de las tareas de todas las direcciones financieras, ha sido la de realizar el presupuesto y la planificación. Es una tarea fundamental, ya que una correcta planificación adelanta necesidades de financiación, nos da información acerca de la rentabilidad de nuestros clientes y productos y contribuye a un correcto gobierno de nuestras organizaciones.

En los últimos tiempos el entorno cambiante en las empresas, con un aumento de la presión regulatoria, una mayor dificultad de encontrar fuentes de financiación y la necesidad de alinear operaciones de negocio con la estrategia corporativa, hacen que el proceso de planificación deba ser más efectivo que nunca. Afortunadamente, las herramientas que tenemos disponibles también han tenido una gran evolución y nos permiten obtener, tratar y mostrar toda la información de una manera precisa, en cualquier momento y lugar donde nos encontremos y sobre todo, en cualquier dispositivo. Todo ello nos permite construir modelos, en base a los datos que nos interesa analizar, llegando a niveles de detalle muy bajo, para tomar decisiones y realizar acciones basadas en información en tiempo real.

Lo primero que nos tenemos que plantear es para qué planificamos exactamente. Eso nos dará la definición de nuestro modelo y de qué situaciones afectan a mi negocio, obteniendo las variables más importantes de las que depende y las que nos permitirán obtener distintos resultados en función de cambios en esas variables. Una primera aproximación de qué información podemos obtener, dependiendo de qué modelo de planificación construyamos puede ser la siguiente:

Con el *reporting* actual de cualquier herramienta sabremos qué pasó, comparado con los datos reales que vamos obteniendo de nuestros transaccionales. Si ya realizamos un *reporting Ad-hoc* podremos analizar cuántas veces se dio una situación, en qué momento exacto, en que área o producto. Si construimos informes de *Drill down* sabremos exactamente dónde se encuentra el problema y al añadir alertas a nuestros informes nos avisarán de qué acciones se deben tomar, lo que nos permitirá reaccionar rápidamente a cualquier variación respecto a los resultados esperados. Además, tener la posibilidad de realizar simulaciones nos permitirá adaptarnos de antemano a distintas situaciones, teniendo en cuenta que ya hemos analizado qué podría pasar si modificásemos ciertas variables de nuestro presupuesto. También realizando modelos que incluyan *forecasting* tendremos información sobre qué le pasaría a una tendencia continua, recalculando en tiempo real los datos que esperábamos obtener o podríamos construir modelos predictivos que nos aportarán información basada en algoritmos sobre qué pasará si suceden ciertas condiciones con patrones predeterminados.

El enfoque tradicional era la construcción de una planificación estratégica con metas y planes - a tres o cinco años - con una revisión de los planes anuales y adecuación de los objetivos a la situación en ese momento. Este enfoque estático ha funcionado durante mucho tiempo, pero ya no es válido actualmente. Ahora, deberemos realizar una planificación estratégica en tiempo real, con esto seguiremos planificando con un horizonte plurianual, pero las acciones se han de poder llevar a cabo en tiempo real. Para eso deberemos tener herramientas que nos permitan disponer de la información precisa para incorporarla a nuestros cuadros de mando en tiempo real e, incluso, adelantarnos a posibles situaciones que tendremos en el futuro. Las mayores diferencias que existen entre el enfoque tradicional y el nuevo enfoque de planificación en tiempo real serán, por un lado, que el enfoque tradicional es eficiente y cumple la misión de aportar una planificación que dirija las decisiones a tomar en el futuro, mientras que la planificación en tiempo real permite optimizar las decisiones ya que se toman en un espacio de tiempo más corto. Por otra parte, en el enfoque tradicional se descubría un desvío respecto a una meta y se respondía con el objetivo de reconducir la situación y con una planificación en tiempo real predeciremos ese desvío, lo que nos permitirá realizar acciones antes de que se produzca.

No solo existen diferencias en la manera de analizar la información por parte de ambos enfoques, sino también en las personas que participan en él. En el enfoque tradicional mucho todo es más centralizado, mientras que la planificación en tiempo real permite a cada departamento realizar su propio análisis a la vez que se realiza una planificación global.

¿Cómo nos ayudan las herramientas de planificación a alcanzar los objetivos?

Todos los grandes proveedores de software empresarial han entendido que deben tener en sus *portfolios* herramientas analíticas, lo que permitirá que sus clientes extraigan el mayor partido a sus sistemas transaccionales y de información. Estas herramientas aportan la posibilidad de configurar distintos escenarios con los que realizar simulaciones, tienen la capacidad de realizar cálculos complejos en tiempos razonables, se integran con herramientas ofimáticas que nos permiten realizar análisis de los datos y con sistemas transaccionales para disponer de información en tiempo real. Además también se integran con sistemas calidad, seguridad e integridad del dato, asegurando así, que todas las personas trabajan con la misma versión de los mismos y facilitando los flujos de trabajo, en los que los distintos participantes llevan a cabo su parte del plan, permitiendo controles y aprobaciones.

En nuestras manos está extender la cultura de disponer de una información precisa, en cualquier momento y en cualquier dispositivo.

José Luis Fernández
EPM manager de Techedge España

El escudo de los CIO: concienciación y formación del equipo de trabajo

Cuando se trata de seguridad informática empresarial, los trabajadores solemos ser el eslabón más débil de la cadena, ese del que se aprovechan los ciberdelincuentes para tratar de sacar provecho. Según el informe de Gartner de 2014, el 80 % de los incidentes informáticos están causados por fallos humanos. La estadística no deja lugar a dudas, tampoco cuando asegura que estos sucesos pueden disminuir hasta en un 90 % cuando los empleados cuentan con formación.

Este es uno de los principales objetivos que se plantean los CIOs hoy en día. Muchos de ellos cuentan con presupuestos millonarios que les permiten invertir en lo último en tecnología para sus empresas, pero esto no es bastante si se tiene en cuenta que un virus enviado por correo, un malware que sobrevive en un pendrive o un spyware oculto tras una inocente presentación, pueden dar al traste con el sistema informático al completo y destrozar, de paso, la reputación de la compañía atacada.

En este punto, el CIO se encuentra en una complicada encrucijada: por un lado maneja una importante cantidad de dinero para conseguir la máxima seguridad informática posible y, por otro, se ve incapaz de inculcar a sus empleados el nivel de compromiso adecuado para que estos tomen conciencia de que se trata de un problema corporativo que afecta a todos los trabajadores sin importar su cargo en la empresa.

Alfonso Ramírez, director general de Kaspersky Lab Iberia

En este sentido, muchos CIOs apuestan por los cursos de formación que permitan a todos los miembros de la compañía conocer cuáles son los riesgos a los que se enfrentan en materia de seguridad y qué hacer para no caer en comportamientos inadecuados que puedan poner en peligro todo el sistema. Sin embargo, aquí suelen chocar con un escollo que, muchas veces, se vuelve insalvable: los cursos de formación suelen ser demasiado largos y técnicos y, las personas, sin la motivación necesaria, suelen recaer en sus conductas pasados los primeros días tras la formación.

La clave está, por tanto, en encontrar un modo de informar y formar a todo el organigrama de la empresa de un modo ameno pero eficaz para influir en las actuaciones de las personas en cuanto a seguridad IT. Con este objetivo ha nacido Kaspersky Cyber Safety Game, una iniciativa pensada para concienciar a todos los miembros de una compañía, no solo sobre cuáles son las conductas de riesgo o inadecuadas, sino también con ejemplos de buenas prácticas y modelos a imitar.

El proyecto cuenta con una plataforma online adaptable a cada empresa que quiera saber su nivel de seguridad, una carga de correos electrónicos para el empleado simulando ciberamenazas en la plataforma, formación para los administradores… De este modo, mediante técnicas activas de aprendizaje, juegos y motivación, el proyecto consigue que todos los miembros de una compañía sepan reconocer las amenazas, las ponga en común y establezca un vínculo corporativo. Lo esencial es que impere la idea de que si todo el mundo tiene cuidado con la ciberseguridad, es imprescindible que uno mismo también lo haga.

Gracias a este curso, el CIO será capaz de realizar pequeñas pruebas a sus empleados y analizar cuál es su nivel de conciencia ante el peligro y su grado de compromiso y, fundamentalmente, contará con una herramienta que le permitirá contar con un aliado en materia de seguridad.

Diario de las frustraciones de un CIO: Internet de las cosas

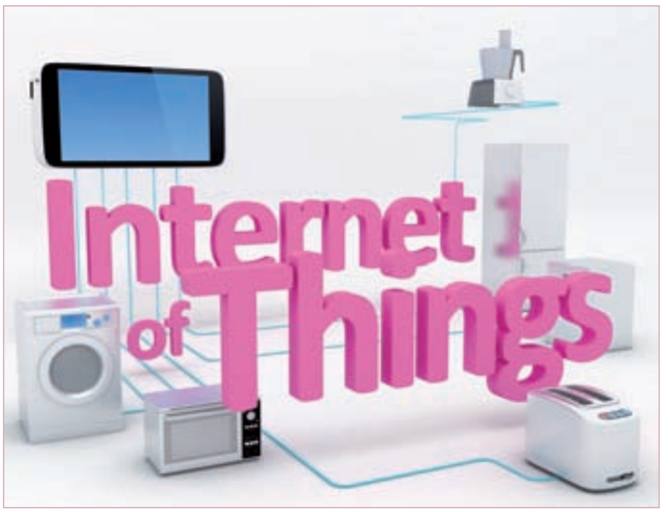
Hola de nuevo, soy Pepe. Algunos ya me recordareis de otras frustraciones como la de la Juventud, divino tesoro. Pero hoy he dejado a un lado a mis compañeros más benjamines para centrarme en una preocupación que nos atañe a todos. Y con "todos" me refiero a todos los CIOs, todos los compañeros de la empresa e, incluso, a todos los usuarios de tecnología.

Lo que me está quitando el sueño es el IoT… Tres puñeteras letras que me tienen sin pegar ojo... IoT (Internet of Things). El Internet de las cosas… ¿Qué cosas? ¿Cuántas cosas más pueden tener Internet en nuestras vidas? ¿Cuántas cosas más me van a estar controlando sin que yo me entere? Esto es como vivir en una película de policías, pero siendo yo el mafioso al que todos vigilan.

Ahora resulta que un informe de Gartner prevé la aparición de 26 mil millones de nuevos aparatos con Internet de aquí a las Juegos Olímpicos de Tokio (2020). Solo son 5 años... ¡Claro que habrá 26 mil millones de nuevos aparatos!

Entre tabletas, teléfonos, portátiles la cosa está fácil, pero... ¡Ah! No, esperad... Están excluidas las tabletas, los teléfonos y los PCs... eso quiere decir que lo que va a tener Internet es la bombilla de casa que ahora se va a encender por WiFi, o el frigorífico que me va a estar dando la vara con que tengo que ir a la compra, o la maquinilla de afeitar que a saber qué se le ocurre decirme por las mañanas y os aseguro que como se pase me vuelvo a la brocha y la cuchilla de toda la vida.

El caso es que ya nos están amenazando —a los CIOs— con que nos vayamos preparando para lo que viene. ¿No es suficiente con que mi tostador me de los buenos días o que descubra que mi perro se está echando la siesta en mi cama gracias a su localizador GPS instalado en el collar?



Se ve que no...

Creo que además pretenden que, desde nuestros puestos de trabajo, controlemos cómo interactúan nuestros clientes con estas nuevas "cosas" que se han convertido en inteligentes.

Y digo yo... ¿esto no es entrometerse —un poquito— en la vida de los demás? Y si la gente lo permite... ¿Qué nuevas legislaciones van a "parir" nuestros señores políticos? La verdad sea dicha, tienen tanta idea de tecnologías como de hacer acrobacias con un avión de juguete...

¿Vamos a poder adaptarnos a todo? ¿Vamos a ser capaces de asegurar nuestro entorno para que los ciberma-los no entren en nuestra casa a través de la chimenea electrónica, tipo Papá Noel?

No señores no... esto está tomando tintes muy negros para nosotros... vamos a vivir un estrés continuo —más del habitual quiero decir— porque ahora la estúpida máquina de café va a saber qué tomo cada mañana y todos los días me sacará el mismo café con leche. ¡¿Y SI YO LO QUERÍA CORTADO?! ¿¿¿Eh, Eh??? ¡¿Me vas a leer la mente?!

Perdón, me he venido muy arriba...

Sin embargo, lo que más me preocupa es la repentina psicosis que va a generar en mi empresa que un hacker pueda acceder a la condenada maquinita. Eso quiere decir que, a partir de ahora, este trasto que tengo enfrente mientras escribo, va a necesitar *firewalls*, antivirus y de todo.

Pues aunque parezca mentira... ¡A mí, personalmente, me hace ilusión lo del hacker!

Tranquilos, que hay una explicación. No soy pro-ciberataques, pero si que soy de la generación de Pulgarcito, de TBO, de Olé...

¡Y aquí me tenéis, vigilando día y noche la insulsa maquinita! Esperando que, de una vez por todas, deje de ser un trasto aburrido y surjan de ella dos ojillos tras unas gafas de culo de vaso sujetas a una prominente nariz. Sí señores, estoy esperando al amo del camuflaje, al soberano del disimulo, al rey del disfraz a ese hacker que se haga pasar por una inofensiva máquina de café. ¡Sí, estoy esperando a Mortadelo disfrazado de cafetera!

José
Frustrated chief information officer

Más información sobre este proyecto

Tráfico SSL: ¿Cómo y por qué descifrarlo?

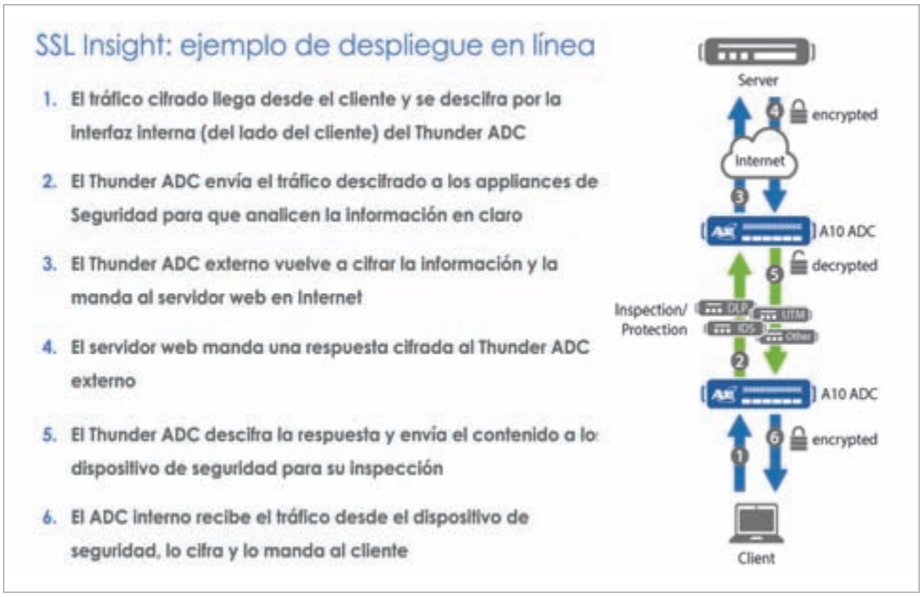
Si bien la adopción de SSL ha sido muy bien recibida: la encriptación mejora la confidencialidad y la integridad de la información, el uso que están dando los hackers de este protocolo que permite la conexión cifrada para eludir las defensas corporativas está levantando ampollas.

Según Gartner, "menos del 20% de las organizaciones que cuenta con algún dispositivo de seguridad, tipo firewall, IPS o UTM es capaz de descifrar el tráfico SSL entrante o saliente". Esto significa que los hackers pueden evadir más del 80% de las defensas de seguridad de red de las empresas, simplemente realizando ataques por tunelización en tráfico encriptado.

Ante este panorama, en el que las empresas se enfrentan a una mayor presión para cifrar el tráfico de aplicaciones y mantener sus datos a salvo de espías, se hace necesario adoptar una medida eficaz. SSL representa casi un tercio del tráfico empresarial, y con más aplicaciones soportando claves SSL de 2048 bits y 4096 bits, las organizaciones ya no pueden negar lo evidente. Analizar el tráfico SSL es un requerimiento ineludible, y para ello una plataforma de inspección SSL dedicada parece ser la mejor opción.

Ahora bien, antes de decantarse por una u otra, las empresas deben tener en cuenta que existe en el mercado un amplio rango de productos de seguridad para analizar y proteger datos y usuarios: firewalls, Sistemas de Prevención de Intrusiones (IPS), soluciones dirigidas a la Prevención de Pérdida de Datos (DLP), investigación forense o plataformas de prevención de amenazas avanzadas, entre otras. Desafortunadamente, muchos de estos productos de seguridad no pueden inspeccionar el tráfico SSL, exponiendo a las organizaciones a ataques y fugas de datos. Algunas plataformas lo soportan, pero con equipos de rango high-end, y con importantes impactos en el rendimiento.

Una plataforma de inspección SSL efectiva debe asegurar criterios como rendimiento, cumplimiento, disponibilidad y gestión de claves SSL, además de ser capaz de interoperar con un conjunto diverso de productos de seguridad de múltiples proveedores (para descifrar el trafico una sola vez), y respetar -no descifrar- el tráfico regulado o sensible.



No más Amenazas ocultas en el tráfico cifrado

Aunque los dispositivos de seguridad dedicados pueden inspeccionar y analizar el tráfico de red, raramente están diseñados para descifrar tráfico SSL a altas velocidades. De hecho, algunos productos de seguridad no incorporan dicha capacidad.

La funcionalidad de interceptación de tráfico SSL Insight de los ADCs Thunder elimina el punto ciego impuesto por el cifrado SSL, y descarga las tareas de cifrado y descifrado, de uso intensivo de CPU, fuera de los dispositivos de seguridad, mejorando el rendimiento de las aplicaciones y la experiencia de usuario.

A10 ha validado sus productos A10 Thunder Series con los de los principales proveedores de seguridad dentro de la Alianza de Seguridad de A10, permitiendo a las organizaciones resolver los principales desafíos sobre seguridad con soluciones integradas y probadas.

De esta forma, lo equipos A10 Thunder Series son capaces de ofrecer una visibilidad sin precedentes del tráfico SSL, para detectar las amenazas avanzadas; permiten la autenticación, ofreciendo seguridad federada y single sign-on; mientras aseguran la protección y gestión automatizada de certificados SSL, e inteligencia de amenaza y de URL para una toma de decisiones más eficaz.

Alain Karioty,
VP ventas para Iberia y Latinoamérica

Diario de las frustraciones de un CIO: Seguridad

Hola… Soy Pepe, pero no pienso escribir mis apellidos, ni mi edad, ni dónde vivo o cuántos años tengo. Espero que lo comprendáis, es un problema de seguridad. El otro día comprendí lo importante que es dejar de dar datos personales a diestro y siniestro y cuidar un poquito más lo que hacemos en Internet.

Esta nueva psicosis me viene porque el otro día estaba viendo un debate sobre seguridad —que por cierto recomiendo que veáis, porque es realmente interesante— donde un fabricante de Check Point sugirió que no se nos ocurriría dejar un fajo de billetes a la vista de todos, encima de una mesa y en mita de una tienda atestada de gente, pero sí que se nos ocurre levantarnos del ordenador dejando la página de nuestra oficina bancaria virtual abierta mientras vamos a sacarnos un café. Es más, en este debate también pusieron un ejemplo real: en un canal de televisión conocido estaban hablando de la importancia de la seguridad, cuando enfocaron a la pantalla de un compañero en la que se podía ver perfectamente su nombre de usuario y contraseña, supongo que la que se organizó después fue como para tomarse pastillas para los nervios.

No me quiero imaginar el disgusto de ese pobre CIO al que habrán llamado para pedir responsabilidades y yo me pregunto… ¿qué culpa tenemos nosotros de tener compañeros un pelín despistados? Pues aunque me duela reconocerlo, un poquito de culpa sí tenemos, pero solo un poquito.

Tenemos que tratar de hacer comprender a nuestros CEOs, y al resto de nuestros compañeros, que no somos Sherlock Holmes y no podemos pasarnos el día averiguando si alguien ha instalado algo indebido o se ha descargado una App que nos va a traer problemas. ¿Tan complicado es preguntar si pueden instalar un programa en el ordenador? En lugar de eso, luego vienen lamentándose de que tenemos un virus y yo tengo que aguantar a los tres informáticos quejándose, pero con razón (todo sea dicho de paso).

No estamos concienciados de la seguridad y, hace unos días, ya mencionaba que el futuro que nos depara el IoT va a ser como un película de la mafia en la que todos espían y vigilan al pez gordo, pero esta vez el pez gordo va a estar desayunando y el frigorífico va a saber lo que hemos comido.

Y digo yo… ¡si no le interesa a mi frigorífico lo qué he desayunado esta mañana, tampoco le interesa a un *hacker*! Pero lo preocupante es que van a intentar entrar en mi frigorífico, igual que intentan entrar en el ordenador de la empresa.

¿Qué para qué? Pues ahora mismo no se me ocurre, pero seguro que ellos ya tienen una idea y que además les va a ser rentable. Así que… amigos míos… hay que comenzar a pensar en lo que compartimos por Internet, tener en cuenta que no merece la pena descargarse todo lo que vemos, ni dar nuestros datos a cualquiera, porque si andas un poco lento te roban hasta la foto del DNI.

De hecho, tengo un buen amigo que os puede asegurar que ha aprendido la lección. Cualquiera podemos caer en las garras de un fraude y aún más si todavía no nos hemos tomado el café. Este ha sido el caso de mi compañero, que estaba vendiendo una cosa de segunda mano y le llamaron interesándose por el producto a primera hora de la mañana. El pobre, que aún no se había tomado el café, ni estaba todo lo alerta que debería haber estado, aceptó hacer una transferencia entre tarjetas, ya que el comprador le aseguró que no tenía otro medio de pago. Algo desconcertado, le dio el número de su tarjeta al comprador para que este le hiciese la transferencia, pero evidentemente, no solo valía con eso… el estafador necesitaba los tres números que aparecen en la parte posterior de la tarjeta y ,simplemente, los pidió. Menos mal que mi compañero se dio cuenta a tiempo y se negó a darle los números, de lo contrario ahora mismo no habría visto un duro de su sueldo.

El estafador —al verse pillado— colgó de inmediato, pero este pequeño intento frustrado ha supuesto una tarjeta bloqueada, para mi compañero, durante más de una semana.

Así que cuidado, porque los ladrones están detrás de las cosa más cotidianas y muchos robos ocurren, precisamente, por descuido. Supongo que a nadie se le ocurriría gritar en mitad de la carnicería que te vas todo el mes de agosto de vacaciones y que tu casa se va a quedar vacía, entonces…¿ por qué publicarlo en las redes sociales?

La seguridad empieza por tener un poco de lógica y un poquito de discreción en nuestro día a día, porque sino luego ocurren los desastres. A ver, ahora, a cuántos os quedan ganas de subir al Facebook las fotos de las maletas en la puerta de casa diciendo que os vais de vacaciones ¡Un poquito de por favor, hombre!

José
Frustrated chief information officer

Más información sobre este proyecto

¡DISTRIBUIDOR!

Defiéndete de la competencia. Utiliza la plataforma del profesional TIC para mejorar tus compras

entra en

Mayoristastai.es

1 DATE DE ALTA GRATUITAMENTE

2 SOLICITA TUS PEDIDOS Y CONSULTAS A TODO EL CANAL

3 RECIBE EN TU E-MAIL LAS CONTESTACIONES DE TODOS LOS MAYORISTAS Y SUBMAYORISTAS

Ofrece una compra inteligente mediante las solicitudes y el acceso a servicios exclusivos

Mayoristastai.es, la herramienta que marca la diferencia con tu competencia

Mayoristastai.es, la plataforma gratuita, que conecta al distribuidor y al profesional TI con los mayoristas más destacados del canal, hace balance de su actividad de los últimos meses. En este período ha logrado la confianza de 500 profesionales que ya se han registrado para conseguir las mejores condiciones de compra del mercado a través de las más de 150 solicitudes que se han cursado a través del *site*.

Mayoristastai.es sigue apostando por aportar a la tienda o profesional TI una herramienta para ser más competitivo y realizar una compra más efectiva. La plataforma, además de facilitar la búsqueda de información de producto, gracias a su renovado diseño que permite consultar todas las referencias actuales de producto gracias a las 80.000 fichas técnicas, que están homologadas internacionalmente, ofrece la posibilidad de cursar solicitudes a todos los mayoristas registrados. Esta opción es una ventaja para diferenciarse de la competencia actual, que no está restringida al canal profesional, ya que en los últimos años se ha producido la entrada de otros agentes de otros ámbitos en la distri-

El acceso a los servicios exclusivos está reservado a los usuarios registrados e identificados

bución de soluciones de informática como son las grandes superficies no especializadas o los vendedores *on-line*.
Para marcar la diferencia con estos nuevos competidores y evitar que sigan desapareciendo tiendas y distribuidores tradicionales de informática Mayoristastai.es ofrece una opción de compra inteligente mediante las solicitudes y el acceso a servicios exclusivos.

¿Por qué registrase?

Mayoristastai es una herramienta para el negocio diseñada para el profesional de TI, ya que el registro evita que la opción de cursar solicitudes las pueda cursar el usuario no profesional. El proceso de registro es simple y rápido. Sólo tiene que cumplimentar una serie de datos requeridos para que el administrador de la plataforma los compruebe y curse el alta que se envía por e-mail para comenzar a utilizar la web.

La posibilidad de enviar solicitudes a los mayoristas que forman parte de la plataforma con el fin de obtener información sobre las condiciones de venta es la ventaja competitiva que el usuario tiene en relación a su competencia. Con la solicitud podrá obtener el mejor precio, conocer los plazos de entrega, servicios técnicos y todos los datos que necesite para establecer una relación comercial con todos los mayoristas registrados en la web.
A través de la solicitud podrá realizar su propia comparativa y mantener una relación directa y personaliza sin intermediarios y en tiempo real con el mayorista que desee e incluso conocer y acceder a nuevos proveedores. Esta relación le permitirá agilizar el trabajo ya que evita consultar varias web de mayoristas, tener varias opciones a la hora de comprar y realizar otros trámites. El contacto es rápido y sin intermediarios.
La plataforma está en continua evolución y crecimiento como avalan los datos de su eficacia. Desde su lanzamiento ha conseguido más de 4.000 referencias vistas al mes por los usuarios registrados; ha facilitado la descarga de más de 300 listas de precios proporcionadas por los mayoristas. Y el ratio de visualización no ha dejado de crecer con más de 20.000 páginas al mes servidas.

La plataforma impulsa el negocio TI de manera neutral

Esta cifras muestran solo los inicios de la plataforma porque se sigue trabajando para ampliar el número tanto de mayoristas como de ofertas y servicios exclusivos con el fin de que el profesional tenga en un único site la mejor herramienta comercial con la garantía de la confidencialidad de sus solicitudes, la independencia de la herramienta y el mejor tiempo de respuesta desde los mayoristas.

¿Cómo se usa?

El diseño, intuitivo y rápido, permite acceder de manera muy sencilla a sus servicios y ventajas en un clic. En la página principal se muestran los tres botones principales: buscador de producto, solicitud de precio o información y servicios exclusivos.
Al pulsar el botón del buscador se accede a la página donde se encuentran todas las categorías de producto y las 80.000 fichas técnicas. El usuario puede buscar por nombre de producto y por código o si lo prefiere por marca, categoría o subcategoría. También puede buscar por los mayorista activos en la plataforma que comercializan el producto o marca que busca; o que está más próximo a su ubicación geográfica. Y puede realizar la solicitud de información o de precio directamente desde el producto.
Si el usuario sabe lo que necesita y no tiene necesidad de realizar una búsqueda primero, puede acceder directamente al botón de solicitud, identificarse y proceder a enviar la solicitud. Si el usuario entra aquí por primera vez también puede registrarse, ya que e imprescindible para cursar las solicitudes.
El usuario también puede disfrutar de los servicios exclusivos a los que se accede directamente al pulsar el tercer botón de la página principal. Estos servicios, a día de hoy, permiten el acceso a listas de precios y ofertas exclusivas de los mayoristas activos en la plataforma.

Ahorrar en telecomunicaciones con Infocom

Teamnet es una consultora cuyo objetivo es mejorar los resultado empresariales a corto plazo. La compañía apuesta por el I+D+i y está desarrollando soluciones de gestión de costes empresariales en diferentes aspectos como las telecomunicaciones, la energía, materias primas, etc.

Isis Vecino

A lo largo de estos años las empresas se han visto obligadas a controlar de forma exhaustiva sus gastos, con el objetivo de llegar a reducirlos. De esta forma, Teamnet ha desarrollado una práctica solución que ayuda a las empresas a gestionar el gasto en telecomunicaciones, tanto de voz como de datos.

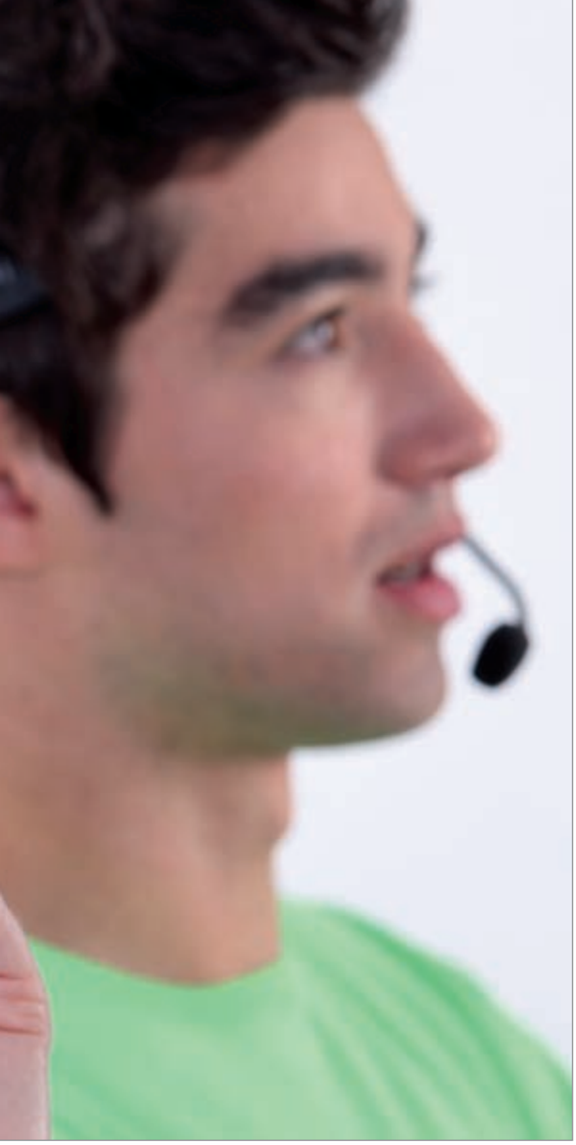
Javier Cid de Quevedo, CEO de Teamnet, explica en esta entrevista en qué consiste su solución.

"El Telecom Expense Management (TEM) es un servicio que TEAMNET presta como solución para la gestión eficiente del gasto en partidas tan complejas y voluminosas como las de telecomunicaciones, es decir, las que están relacionadas con el consumo de voz —fijo y móvil— y datos. La solución que gestiona esta partida y automatiza los servicios TEM es INFOCOM, una herramienta innovadora financiada por el CDTI que ya está testada en grandes corporaciones", explica Javier Cid.

¿Qué ventajas y beneficios aporta este tipo de servicio a una gran empresa?

INFOCOM permite, a las grandes organizaciones e instituciones, detectar errores y sobrecostes en su factura de telecomunicaciones, tanto de datos, como de voz y móvil. Las grandes empresas evitan, así, el gasto de cientos de miles de euros en las cuentas anuales. Sin embargo, para gestionar los gastos en telecomunicaciones es necesario realizar una serie de controles y análisis, que de hacerse de forma manual supondrían mucho tiempo y esfuerzo. Por este motivo, INFOCOM se encarga de estas tareas de forma automatizada y eficiente.

Esta solución detecta —retarificando el 100 % de los CDR´s, cuotas y descuentos— los errores existentes en la facturas de servicios de telecomunicaciones que, según estudios, se sitúan entre el 7 % y 14 % del gasto. Además, controla el inventario de terminales, líneas y servicios que están siendo facturadas, gestiona la relación con las operadoras, analiza el uso y el consumo —con detalle de recursos infrautilizados o mal



utilizados— que puede llegar a un ahorro del 10 %, reparte el coste por unidades funcionales o centros de coste, define y gestiona las políticas de BYOD y analiza la información histórica para la correcta negociación de nuevos acuerdos comerciales

¿Por qué considera que un CIO debería implantar esta solución?

El ahorro medio anual en los gastos de telecomunicaciones que están consiguiendo grandes compañías e instituciones públicas desde que instalaron INFOCOM 2014, es de entre un 10 % y un 30 %. El motivo es que esta herramienta permite una gestión centralizada del todo el gasto de telecomunicaciones de fijo, móvil y datos de una organización, independientemente de los operadores con las que se trabaje o de los países implicados. Además, genera ahorro en la propia organización mediante la identificación de errores de facturación o la definición de políticas que inhiban el consumo no profesional y facilita y mejora la gestión de la relación con las operadoras al disponer de información veraz y contrastada, eliminando así dependencias de estos proveedores que suelen ser estratégicos.

¿Es necesario algún tipo de software o hardware para incorporar esta solución a la empresa?

La solución INFOCOM es una herramienta web (*cloud/OnPremise*), multilenguaje y multicomercializadora, que se compone de dos módulos, el analítico y el de gestión, desarrollados en tecnología Microsoft. Esta herramienta busca la flexibilidad y la sencillez, ya que puede ser utilizada por el cliente de forma autónoma, o por operadas mediante el servicio especializado en telecomunicaciones de TEAMNET. INFOCOM automatiza gran parte de las tareas necesarias para el control del gasto empresarial, lo que consigue mejorar la eficiencia y fiabilidad de los procesos.

INFOCOM permite detectar errores y sobrecostes en la factura de telecomunicaciones

¿Cómo se instalaría esta solución en una empresa?

Para que la compañía interesada utilice INFOCOM, solo es necesario que aporte al equipo de Teamnet el acuerdo marco firmado con las operadoras, los ficheros de facturación y el inventario disponible en la organización, con todo esto se procede a la carga de información para activar la herramienta.

Sin embargo, si la instalación se realiza en los servidos del cliente, será necesario disponer de un sistema operativo Microsoft Windows Server 2012 R2 standard con IIS activado, una base de datos Microsoft SQL Server 2012 versión Business Intelligence de *open license* y un *framework* 4.5 de Microsoft.

Javier Cid de Quevedo, CEO de Teamnet

¿Cómo funciona la solución?

El acceso a INFOCOM se puede realizar a través de Internet o de la red local desde cualquier dispositivo, pues se trata de una solución web.

La plataforma permite al usuario, de forma sencilla y automatizada, la refacturación del 100 % de los tráficos, cuotas y descuentos, que permite la identificación de errores en el precio de las llamadas realizadas, errores en la aplicación de dichas cuotas y descuentos, en las fechas de inicio y fin de los servicios contratados, incluso el reconocimiento de servicios activos que nunca son utilizados, pero siguen siendo facturados.

Por otro lado, también permite funcionalidades como la identificación de opciones de ahorro en la contratación, inhibición del consumo innecesario —gasto fuera del horario de trabajo, por ejemplo— el reparto de los costes por Centro de Coste (CECO) o el seguimiento presupuestario mediante informes, que aportan información muy valiosa de cara a la gestión eficiente del gasto en telecomunicaciones.

INFOCOM consta de dos módulos, el de gestión que permite capturar y procesar la información sobre los precios acordados con los operadoras, las facturas, el inventario de los terminales y líneas; y el analítico, que analiza la información anterior, cruzando dinámicamente varias dimensiones con tecnología de análisis multidimensional (OLAP - procesamiento analítico en línea On-Line Analytical Processing). Así, con esta herramienta, el usuario puede conocer de forma automática el consumo mensual de las líneas de su área de responsabilidad, el desglose del consumo por origen (operador, empresa, área, departamento y usuario), la evolución mensual del consumo

y costes medios mensuales por líneas, un análisis de patrones de consumo, ranking y detalle de las llamadas más largas y de mayor coste o, por ejemplo, un análisis y detalle de las llamadas fuera del horario laboral.

¿Qué mejoras se han implantado desde la versión de 2012 a la de 2014?

La versión INFOCOM 2014 ofrece otra serie de ventajas, como la capacidad de hacer comprobaciones simultáneas de múltiples acuerdos marco con diferentes operadoras nacionales o internacionales, acceso y uso multiempresa para el caso de *holdings* o grupos empresariales, varios perfiles de usuario o carga masiva de inventarios, entre otras. Además, la plataforma es multilenguaje y es capaz de leer los contenidos de facturación en todos los idiomas, con alfabeto latino y cirílico, algo muy útil en el caso de contratos con operadoras internacionales. También es escalable, ya que horizontalmente incorpora nuevas funcionalidades y verticalmente tiene mayor capacidad de proceso. En cuanto a la seguridad, incorpora mejoras en cuanto a confidencialidad, *firewalls* y seguridad en IIS.

¿Desde TEAMNET se aporta formación a los trabajadores de la empresa en la que se implementa esta solución?

> Con la instalación de INFOCOM el ahorro medio anual en los gastos de telecomunicaciones es de entre un 10 y un 30 %

INFOCOM es una herramienta consolidada que busca la flexibilidad y la sencillez, ya que puede ser utilizada por el cliente de forma autónoma u operada por el servicio especializado en TEM —telecomunicaciones— de TEAMNET. Así, en los casos en que se considere necesario, el equipo técnico de TEAMNET puede dar soporte al homólogo de cada compañía e, incluso, puede externalizarse para que el equipo de TEAMNET se encargue del control y seguimiento.

¿Qué tipo de conocimiento es necesarios para llevar a cabo el análisis de los datos?

El material entregado a cada compañía está totalmente adaptado para que su personal técnico pueda interpretar fácil y rápidamente los resultados y así se optimicen los procesos internos para generar ahorro en la factura. Dicho esto, el responsable de la gestión de los gastos en telecomuncaciones, deberá tener unos conocimientos mínimos sobre la contratación de servicios de telecomunicaciones. Si los usuarios son simplemente consumidores de la información no se requiere de conocimientos especiales.

Teamnet
Tel.: 91 436 24 85

PandaLabs detecta 225.000 nuevas muestras diarias de *malware*

PandaLabs ha detectado —solo en el primer trimestre de este año— más de 225.000 nuevas muestras del *malware* al día. Esta cifra récord supone un aumento de cerca de un 40 % con respecto al mismo periodo de 2014 y también es superior a la media registrada en todo el año pasado que se situaba en torno a los 205.000 nuevos ejemplares diarios. Algunos días se han llegado a registrar picos que superan las 500.000 muestras diarias.

PandaLabs ha detectado —solo en el primer trimestre de este año— más de 225.000 nuevas muestras del *malware* al día. Esta cifra récord supone un aumento de cerca de un 40 % con respecto al mismo periodo de 2014 y también es superior a la media registrada en todo el año pasado que se situaba en torno a los 205.000 nuevos ejemplares diarios. Algunos días se han llegado a registrar picos que superan las 500.000 muestras diarias.

La importancia de la seguridad está en alza y esto se hace cada día más notable. A diario se han dado picos que superan las 500.000 muestras de *malware* y, de estas, 225.000 son completamente nuevas. Además, durante este primer trimestre han aparecido variantes de *malware* conocidos que han sido modificados para tratar de evitar su detección por parte de los laboratorios de antivirus. En este sentido, la creación de troyanos siguen siendo el tipo más común de *malware* (un 72 % pertenece a este grupo) y, además, es la principal fuente de infección entre los usuarios, ya que el 76 % de ellos se ha infectado por esta vía.

Cryptolocker: el rey de los ataques

Durante los inicios de 2015, los ataques a través de *ransomware*, especialmente en su variante Cryptolocker, han sido los más destacados. En este trimestre, PandaLabs ha observado cómo los criminales han seguido explotando esta vía, tratando de obtener beneficio de las empresas a través del robo de información valiosa. Este ha sido precisamente el caso de diez compañías petrolíferas, dedicadas al transporte marítimo y entre las que se encuentra una organización española. De hecho, Panda Security acaba de denunciar, bajo la denominación de "Operación Oil Tancker: la Amenaza Fantasma", cómo estas empresas han sido víctimas del robo de información.

"En este caso la particularidad ha sido que no han infectado a través de *malware* si no a través de archivos que se ejecutan de manera recurrente", explicaba Luis Corrons, director técnico de PandaLabs en Panda Security.

Otros métodos de ataque que se han popularizado durante este trimestre son los que tienen su origen en las redes sociales, con especial repercusión en Facebook, donde comenzaron a lanzarse supuestas campañas publicitarias que regalaban tarjetas promocionales para empresas conocidas. Este ha sido el caso de ZARA, que ha comenzado el trimestre con importante ataque en el que se empleaba como gancho las tarjetas regalo de la firma de ropa por valor de 500 euros. En muy poco tiempo, más de5.000 personas se habían suscrito al evento y se habían enviado 124.000 invitaciones.

Los móviles también han sido objetivo de los cibercriminales, aunque la mayoría de las infecciones continúan produciéndose en teléfonos con sistema operativo Android y el método más utilizado este trimestre ha sido vía SMS.

España, por encima de la media en infecciones

El ratio de infecciones a nivel mundial ha sido de un 36 %, seis puntos más que en el mismo periodo de 2014. España sigue situándose por encima de la media con un 38 % de ordenadores infectados, aunque continúa siendo China el país a la cabeza de este ranking con un 48 % de infecciones. Le siguen Turquía (43 %) y Perú (42 %).

Entre los países con menor índice de infección se encuentran principalmente los europeos. De hecho, Noruega (22 %) lidera el top 10 de países con menos infecciones. Se sitúan también por debajo de la media países como Dinamarca (28 %), Finlandia (28 %), Estados Unidos (34 %) y Venezuela (33 %), entre otros.

"No debemos olvidar que los ciberdelincuentes se mueven por un motivo clave: conseguir dinero. Y en paralelo, nuestra vida es cada vez más digital, por lo que también estamos más expuestos a ser víctimas de un ataque. A lo largo del año, seguiremos viendo ataques que secuestren el ordenador, y ataques a través de redes sociales y dispositivos móviles", concluía Luis Corrons.

Panda Security
Tel.: 902 243 651

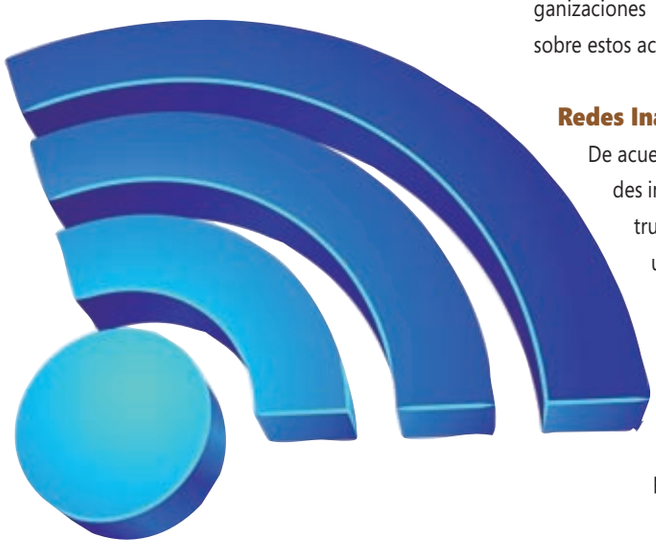
Más información sobre este informe

La red inalámbrica, el elemento más vulnerable de la infraestructura TI

Los decisores de TI consideran que las redes inalámbricas son el elemento más vulnerable de la infraestructura de TI, según el nuevo estudio de Fortinet, compañía líder en soluciones de ciberseguridad de alto rendimiento. Casi la mitad de los encuestados españoles (47 %) clasificó a las redes inalámbricas como las más expuestas desde el punto de vista de la seguridad, en contraste con el 32% que considera que es la red principal.

El estudio también revela que la insuficiente seguridad inalámbrica es una preocupación para casi todos los CIOs encuestados (92 % a nivel mundial, 89 % en España), un dato que no sorprende si tenemos en cuenta que más de un tercio de las redes inalámbricas empresariales para empleados internos, carecen de una de las funciones básicas en seguridad: la autenticación.

Estas son algunas de las conclusiones extraídas del estudio independiente realizado a más de 1.490 responsables de TI de organizaciones con más de 250 empleados, en todo el mundo. El informe arroja las siguientes conclusiones:



- Casi la mitad de los responsables de TI españoles (42 %) considera que la pérdida de datos corporativos y/o confidenciales de clientes es el mayor riesgo de operar con una red inalámbrica no segura.
- El 69 % han adoptado una estrategia en la nube para la gestión de su infraestructura inalámbrica y el 88 % confía en la nube para un futuro despliegue inalámbrico.
- El 52 % de los ITDMs españoles facilitan el acceso en sus redes inalámbricas corporativas a personas invitadas, lo que nos sitúa por encima de la media mundial (43 % y la de EMEA, 41 %); el 15 % de estas organizaciones lo hacen sin ningún tipo de control sobre estos accesos.

Redes Inalámbricas en riesgo

De acuerdo con el estudio de Fortinet, las redes inalámbricas se sitúan como la infraestructura de TI más vulnerable, ocupando uno de los primeros puestos para el 47 % de los responsables de TI españoles. Estos, sitúan las redes inalámbricas como una de las más vulnerables dentro de la infraestructura de redes, siendo considerado alto por el 32 % de los ITDMs.

Las infraestructuras de bases de datos (19 %), aplicaciones (20 %) y almacenamiento (17 %) fueron consideradas las menos susceptibles desde el punto de vista de la seguridad por parte de los encuestados españoles. Además, el 35 % de los encuestados confesó no haber aplicado ni la más básica medida de seguridad para la autenticación en entornos inalámbricos. Un significativo 43 % y 46 % de las empresas, pasan por alto las funciones de seguridad de firewall y antivirus cuando se trata de establecer su estrategia inalámbrica.

Otras medidas de seguridad consideradas fundamentales para la protección de la infraestructura básica, tales como IPS (desplegado por el 30 %), control de aplicaciones (29 %) y filtrado de URL (17 %), tienen una menor presencia en los despliegues inalámbricos.

A la hora de considerar el futuro de sus estrategias de seguridad inalámbrica, 45 % de los encuestados españoles confirmó que mantendrían la atención en las funcionalidades de seguridad más comunes —firewall y autenticación— mientras que la demanda de más seguridad emerge, con un 28 % en la prioridad de tecnologías complementarias en España con IPS, antivirus, control de aplicaciones y filtrado de URL —para protegerse contra el nuevo panorama de amenazas—.

Crece la preocupación por una seguridad inalámbrica insuficiente

De los ITDMs encuestados a nivel global, el 83 % cree que la seguridad inalámbrica que aplica no es suficiente (75 % en España), siendo los CIOs, con un 92 %, los más preocupados por esta cuestión (89 % en España). De las regiones analizadas en el estudio, los responsables de TI de APAC (Asia Pacífico) son los más preocupados por la seguridad inalámbrica, siendo un 44 % los que se consideran muy preocupados. Son datos que contrastan con el 30 % en América y el 20 % en la región EMEA.

A nivel global, los niveles de confianza en la seguridad inalámbrica son variados; China encabeza la tabla con un 71 % "muy preocupado", frente al 13 % en Japón. Los resultados sugieren que una mayor concienciación sobre la seguridad conduce a mayores niveles de preocupación, y los dos países más concienciados— China e India— implementan más funciones de seguridad inalámbricas de media que los dos países menos afectados, Italia y Japón.

Para el 42 % de los responsables de TI españoles, la pérdida de datos sensibles corporativos o de clientes es el mayor riesgo de las redes inalámbricas

La pérdida de datos, lo que más preocupa

Ante la cuestión sobre los riesgos de operar en una red inalámbrica no segura, el 42 % de los responsables de TI españoles consideraron la pérdida de datos sensibles corporativos y/o de clientes como el mayor riesgo para su organización. El segundo riesgo considerado más preocupante es el espionaje industrial y fue citado por sólo el 23 % de ITDMs españoles, seguido por el incumplimiento de regulaciones de la industria (14 %), con la interrupción de servicios y/o aplicaciones (12 %).

La gestión de la nube se convierte en la norma

La infraestructura inalámbrica gestionada por un controlador in situ es cosa del pasado de acuerdo a los resultados, siendo los controladores inalámbricos in situ la forma menos habitual de gestión (31 %). Esta tendencia de gestión basada en la nube se prevé que vaya a seguir creciendo, tal y como lo indica que sólo el 12 % de los ITDMs españoles se niegue a confiar en la nube para la gestión futura.

De los que ya están preparados para la nube, el 64 % querría usar una infraestructura de nube privada para la gestión inalámbrica y el 36 % se decanta por subcontratar un proveedor de servicios gestionados. El 11 % de aquellos que están considerando la externalización, solo lo harían si la nube estuviera alojada en su mismo país, mientras que el 25 % adoptaría una gestión inalámbrica como un servicio en la nube pública, independientemente de su ubicación geográfica.

Accesos "totalmente abiertos" para invitados

Más de la mitad de los responsables de TI españoles (52 %), facilitan el acceso a invitados en sus redes inalámbricas corporativas, el 15 % de ellos sin realizar ningún tipo de control. La forma más común para dar acceso seguro a un invitado en redes inalámbricas corporativas es a través de un nombre de usuario y contraseña única y temporal (46 %), por delante de un portal cautivo con los datos personales (35 %).

"Los resultados del estudio indican que a pesar del crecimiento en las estrategias de movilidad, la seguridad inalámbrica no ha sido una prioridad para las empresas hasta la fecha. A medida que los ataques persistentes avanzados entran por múltiples puntos de entrada y se populariza el uso de la nube, las organizaciones deberían de ser más precavidas. Resulta positivo ver como los líderes de TI comienzan a reconocer el papel que juega la seguridad inalámbrica a la hora de proteger sus activos críticos de negocio, aunque aún queda mucho por hacer. Para ofrecer una seguridad de red con conectividad ubicua, la red inalámbrica debe considerarse como parte de la estrategia integral de seguridad para garantizar una protección completa y consistente para usuarios y dispositivos a través del acceso por cable e inalámbrico", explica Acacio Martín, director general de Fortinet Iberia.

El informe muestra que 9 de cada 10 CIOs considera deficiente la protección de las redes inalámbricas

Fortinet
Tel.: 91 790 11 16

Muestra

Este estudio sobre seguridad inalámbrica ha sido realizado durante el mes de mayo de 2015 por la compañía de investigación de mercado Lightspeed GMI. La encuesta fue realizada online entre 1490 responsables de TI o decisores de TI cualificados —predominantemente CIOs, CTOs, Directores de TI y Jefes de TI— en empresas de más de 250 empleados en todo el mundo. En total 12 países participaron en la encuesta: España, Australia, Canadá, China, Francia, Alemania, India, Italia, Japón, Hong Kong, Reino Unido y EE.UU.

CENSECOM

Centro de Negocios y Servicios Complementarios

Tel.: 91 308 85 63
comercial@censecom.es

Zona Alcobendas

NUEVAS SOLUCIONES PARA TODAS LAS ECONOMÍAS

ALQUILER DE PUESTOS DE TRABAJO, DESPACHOS, ZONAS, SALAS, ESTUDIOS TV...

Son muchas las pequeñas empresas o profesionales que buscan una solución económica y práctica para ubicar su empresa.

La alternativa de compartir un espacio de trabajo crece cada día con el fin de rebajar los gastos y sin renunciar a las ventajas que ofrece un lugar que de buena imagen a su empresa.

COWORKING TEMATICO:

Aunque cualquier tipo de empresa puede instalarse en este centro de negocios, nos interesa ofrecer un valor añadido, por lo que damos preferencia a aquellas que tengan relación con el marketing, la comunicación, la multimedia o Internet, facilitando con la proximidad, interacciones, que ayudarán a su desarrollo.

SERVICIOS QUE PODEMOS OFRECER:

- **Despachos o zonas para una sola empresa** con o sin mobiliario.
- **Puesto de trabajo amueblado** en zona compartida con otras empresas o profesionales (incluye: mesa, sillón, teléfono de sobremesa, conexión ADSL y equipo informático opcional).
- **Domiciliación social, fiscal y comercial** (derecho a uso de nuestra dirección en su papelería corporativa, publicidad, tarjetas de visita, facturas, así como, del nº de teléfono y nº de fax).
- **Recepción, distribución y envío de correo**, en cualquier forma o cantidad según tarifa.
- **Utilización de las salas de reuniones, Terraza, y otras zonas comunes,** previa consulta y reserva, según condiciones del contrato, o según tarifas.
- **Utilización de platos para Internet TV** (Diferidos o directos) previa consulta y reservas según tarifas.

iiR España
Know-how. People. Results

UNIVERSIDAD PONTIFICIA ICAI ICADE COMILLAS MADRID

ICADE Business School

Itinerario Formativo

EXECUTIVE EDUCATION

Gestión Comercial Competitiva e Innovadora
Madrid • 29 y 30 de Septiembre, 23, 29 y 30 de Octubre de 2015

Directivos Recién Nombrados
Madrid • 1, 2, 22 y 23 de Octubre de 2015

Personal Assistant para la Alta Dirección
Madrid • 8, 9, 29 y 30 de Octubre de 2015

Comunicación Interna
Madrid • 27, 28 y 29 de Octubre de 2015

Habilidades Directivas para la Innovación y el Liderazgo II - ADVANCED
Madrid • 29 y 30 de Octubre, 18 y 19 de Noviembre de 2015

Autogestión y Productividad Directiva
Madrid • 18 y 19 de Noviembre de 2015

MEDIA PARTNER
directorTIC

Solicite más información en
www.iir.es o llámenos al 91 700 48 70