Una tarea complicada para los CISO dada la variedad de tecnología cruzada en torno a la seguridad

En busca del presupuesto perfecto

Uno de los grandes retos del CISO (o del CIO por extensión cuando no existe la figura de responsable de seguridad TI) es atinar con el presupuesto de seguridad, algo que resulta una ardua tarea dado el complejo ecosistema de tecnologías, proyectos y programas que se ven implicados. La firma analista Gartner aconseja que este capítulo debe oscilar en el rango del 3% al 6% del gasto total en Tecnologías de la Información; sin embargo, se observa que este axioma no funciona de la misma forma en cada compañía.

R. CONTRERAS

● El mundo de la seguridad es cada vez más difuso -o confuso- pues afecta a diversos aspectos que las compañías tienen que abordar de forma proactiva. Como si de generales estrategas se tratase, los responsables de seguridad TI tienen que atender diversos fuegos sabiendo que no pueden descuidar ningún frente; y es que los enemigos proliferan por doquier: spam, ataques de Internet, virus, agujeros de seguridad, continuidad de negocio, phishing, movilidad, redes sociales, infraestructuras críticas, ciberterrorismo, bots, fraude, robo de información, piratería, ciberterrorismo… todo ello requiere estar preparado con los suficientes recursos para poder ganar la batalla al malware. Lo más habitual es compararse con la competencia, con rivales de similar tamaño y cercanos geográficamente, como punto de referencia para saber si se está aplicando la debida diligencia en el capítulo de la seguridad. En este sentido, una encuesta reciente de Gartner señala que las compañías promediaron un 5,6% en seguridad TI y gestión de riesgos, lo que no supone una uniformidad en los resultados cosechados.

Normalmente, los gastos en seguridad se dividen en hardware, software, servicios (outsourcing y consultoría) y personal, sin embargo en la encuesta de Gartner un tercio de las empresas desconocía su auténtico presupuesto en seguridad. Esto sucede porque los sistemas de contabilidad contemplan la seguridad como un campo separado, mientras que muchos procesos de seguridad son llevados a cabo por personal que no dedica su tiempo completo a la seguridad, lo que hace imposible cuantificar ese gasto (que representa el 40% del total). En términos generales, los CISO no pueden determinar el gasto completo que su empresa dedica al capítulo de la seguridad.

Los CISO no puede fijar el gasto completo que su firma dedica a la seguridad

Aunque las cifras publicadas representan lo que Gartner llama 'stalking horse' (es decir, una posición derivada del análisis de los datos que representan las tendencias y los resultados), cada organización debe evaluar su propia situación con cuidado, y no debe cambiar arbitrariamente para ajustarse a los resultados publicados que no necesariamente representan las mejores prácticas.

Y es que las estadísticas sobre el gasto en seguridad no representan la verdadera magnitud de las inversiones empresariales en tecnologías de seguridad ya que las características de seguridad se están incorporando en hardware, software o iniciativas que no están específicamente dedicados a la seguridad. Por tanto la consultora aconseja que aunque el gasto esté fuera del presupuesto del CISO, el departamento de seguridad debe ser un factor de influencia o de asesor en el gasto en otros ámbitos, y por lo tanto a menudo deben tener visibilidad en dicho gasto.

Existe una amplia serie de ejemplos donde se produce esta circunstancia como son el caso de los equipos de red que han incorporado funciones de seguridad, tales como las redes privadas virtuales de apoyo o el cifrado de datos en movimiento, lo cual puede ser cargado al presupuesto de telecomunicaciones o comunicaciones de datos. O el de la protección del escritorio que son achacables al usuario final. Prácticamente todas las aplicaciones de la empresa tienen algunas funciones de seguridad, como ERP o SCM (Gestión de la Cadena de Suministro).

De la misma manera, proyectos tales como gestión de identidades y acceso (IAM) no deben ser gestionados por el equipo de seguridad, sino por el de gestión de clientes proporcionando autoservicio o apoyo a otras aplicaciones.

Seguridad estratégica

Las organizaciones tienen que proteger su infraestructura informática, respondiendo a las amenazas y mantener la vigilancia, pero el gasto en seguridad también está siendo vinculado a iniciativas estratégicas del negocio. Por ejemplo, un portal de colaboración segura para el cuadro directivo de comunicaciones incluye una cantidad significativa de la funcionalidad de seguridad, pero que rara vez se trata como parte del presupuesto de seguridad.

Las organizaciones deben cumplir con la normativa y requisitos legales. Los directores CISO han de justificar los gastos mediante la inclusión de las parámetros medibles de mejora de la seguridad o de mitigación de riesgos en todas las solicitudes de compra. El CISO tiene que ejercer presión para asegurarse de que las unidades de negocio incluyen el dinero para los gastos de seguridad que sea relevante para todos los proyectos de TI.

Las organizaciones más seguras probablemente gastan menos del promedio general del presupuesto TI. Sin embargo, el 20% de las organizaciones que invierten menos en seguridad está compuesto tanto por compañías inseguras como por aquellas seguras que han implementado las mejores prácticas en sus operaciones de TI y de seguridad (tales como mejores prácticas de gestión de configuración) que reducen el total de complejidad de la infraestructura de TI y rebajan el número de vulnerabilidades de seguridad.

El gasto en seguridad se utiliza a menudo para compensar las deficiencias en las operaciones de negocio y de TI. Al reducir estas deficiencias el gasto TI aumenta, al tiempo que el gasto en seguridad de la información se reduce en un porcentaje.

En entornos corporativos más maduros y seguros, los gastos y actividades explícitas de seguridad disminuyen a medida que se integran dentro de las operaciones globales, desarrollo de sistemas, implementación gestión de procesos, y así las funciones de seguridad se consolidan y se gestionan de manera más eficiente.

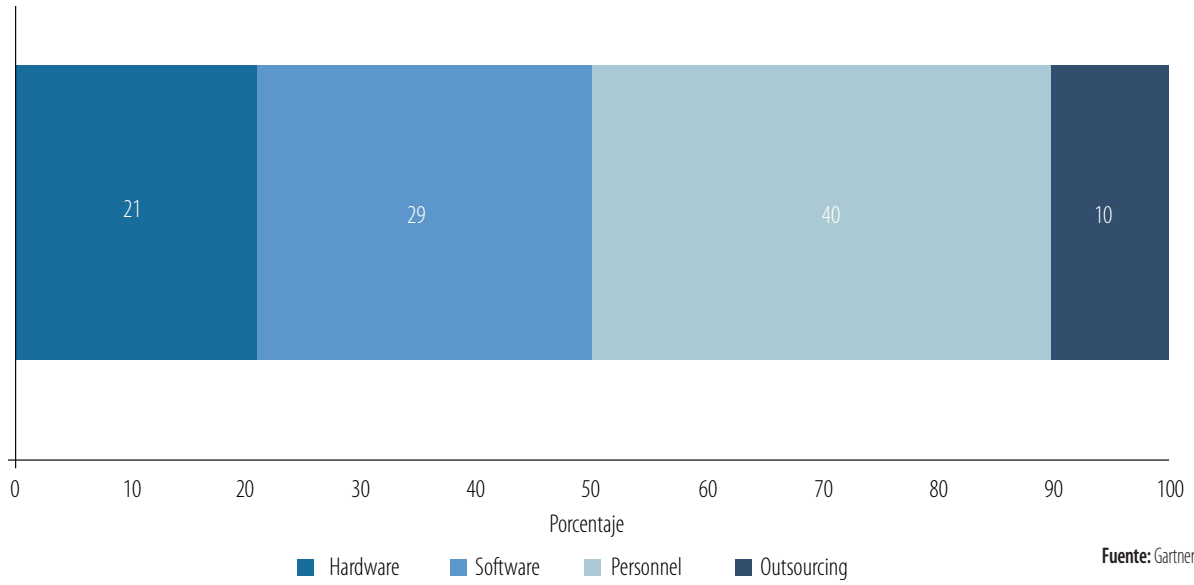
Las compañías no seguras, por el contrario, tienen que comprar más 'soluciones por pánico', debido a una ineficiente gestión de los recursos y una infraestructura descontrolada, en la que se produce más tiempo de inactividad.

Los gastos explícitos en seguridad también se verán reducidos al tiempo que las capacidades de seguridad cada vez se encuentran más integradas a la red, al mundo del desktop y a las funcionalidades basadas en la nube, como consecuencia directa de la progresión propia de las Tecnologías de la Información.

Estas capacidades son contempladas en la próxima generación de firewalls, protocolos de seguridad web, que ahora incorporan funciones antispyware, antivirus, VPN y conductas proactivas de bloqueo de conductas. La competencia entre los productos multifuncionales y los servicios también favorecen la reducción de los precios. Finalmente, las organzaciones pueden externalizar muchas funciones de seguridad. Las medianas empresas incrementarán el uso de appliances UTM unificados de bajo coste, externalizarán la monitorización de la red de seguridad (como prevención de intrusos) así como servicios de gestión de fraude, vulnerabilidad de activos y gestión de vulnerabiidades.

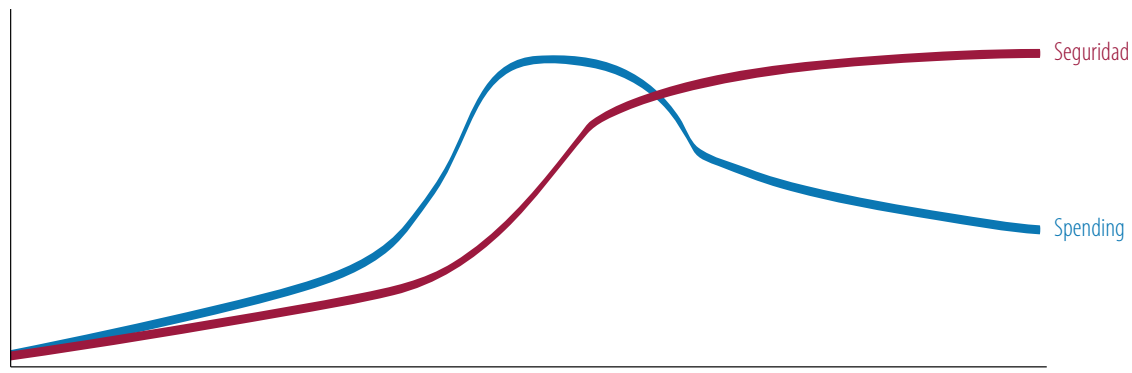
En suma, las compañías gastarán de acuerdo al lugar donde se sienten que están en su ciclo de actualización de la tecnología, y sobre la base de su vulnerabilidad percibida o real. Cuando las amenazas son estáticas, los costes de seguridad se pueden incluir dentro de las operaciones en general, dejando vías presupuestarias para la protección contra nuevas amenazas. La regla general de Gartner es que las empresas deben tener entre el 3% y el 6% de sus presupuestos, destinados a seguridad de TI, menor en el rango si tienen sistemas maduros, mayor si están abiertos y en situación de riesgo.

Distribución del gasto en seguridad de la información



Fuente: Gartner

Relación entre seguridad y gasto en seguridad



Fuente: Gartner

Gasto total en servicios de seguridad por segmentos de mercado 2010-2015 (millones de dólares)

Segmento	2010	2011	2012
Consultoría	8.598	9.644	10.274
Integración y desarrollo	10.257	11.316	11.943
Gestión TI	6.872	8.032	9.361
Soporte de Software	4.407	5.010	5.490
Mantenimiento de Hardware	996	1.115	1.201
Total	**31.129**	**35.117**	**38.269**

Fuente: Gartner

Gasto total en servicios de seguridad por región 2010-2015 (millones de dólares)

Region	2010	2011	2012
Norteamérica	12.321	13.563	14.628
Europa Occidental	9.593	11.020	11.915
Japón	4.425	4.770	5.071
Asia/Pacífico	3.295	3.985	4.661
Latinoamérica	718	867	1.012
Oriente Medio y África	469	553	596
Europa Oriental	309	360	385
Total	**31.129**	**35.117**	**38.269**

Fuente: Gartner)

En el punto de mira... de los hackers

Ciberterrorismo

Infraestructuras críticas, el objetivo de mira más sensible y olvidado

Este año, nos hemos encontrado con varias noticias relacionadas con ataques a infraestructuras críticas o sistemas SCADA (centrales nucleares, transporte, red eléctrica, suministro de agua, etc.). Diversos fabricantes de soluciones de seguridad han alertado del peligro de los ataques a estas infraestructuras debido a su exposición a Internet y a que éstas no hayan sido diseñadas con la seguridad como premisa básica, pudiéndose producir una amenaza real a la seguridad nacional. Un ejemplo lo encontramos en una noticia publicada recientemente sobre la denuncia de un hacker ante la vulnerabilidad de los sistemas que controlan el suministro y el tratamiento del agua. PrOf, que así se dio a conocer el hacker, publicó datos de una planta de Polonia de tratamiento de aguas residuales, los datos de un programa de gestión de un generador, y lo que se atribuye a archivos de medición de agua de España y Portugal. El hacker solo quería criticar la pobre configuración de los sistemas, el bajo nivel de las contraseñas y la inexistencia de restricciones al acceso del interfaz.

La protección de las infraestructuras críticas sigue siendo la asignatura pendiente para empresas y para administraciones públicas. Los fabricantes de servicios y productos de seguridad recomiendan potenciar la colaboración y el intercambio de información entre todos los participantes en este ámbito; la colaboración público-privada; garantizar la adaptabilidad de la protección a nuevas situaciones; y abordar la protección desde el punto de vista físico y lógico.

Nuevas amenazas 'as a Service'

Cloud, la desconfianza de una información en manos de terceros

Las empresas se enfrentan al reto de gestionar los programas maliciosos e infecciones, pero también, han de mantener vigilados los nuevos métodos de acceso a aplicaciones y datos, como los que se ofrecen a través del cloud computing. La seguridad y la disponibilidad de la información se han convertido en uno de los grandes hándicaps de los servicios en la nube, ante la desconfianza de que los datos corporativos estén en manos de terceros. Y es que el modelo aún se basa en componentes de hardware por lo que no es inmune a la pérdida de datos. En este sentido, el CPD que aloje estos servicios debe de disponer de sistemas que garanticen la disponibilidad de la información, una red tolerante a fallos, que garantice el acceso en tiempo real desde cualquier ubicación, políticas de backup, control de acceso a través de procesos de autenticación, administración de identidades, y soluciones de disaster recovery. Por su parte, los clientes que hayan contratado o vayan a contratar servicios en la nube deben conocer dónde están sus datos y qué medidas aplicará su proveedor para la protección de la información. También, es necesario controlar quién accede a la información y asegurarse de que las comunicaciones sean seguras.

En este nuevo paradigma, la carga recaerá en los administradores de TI, que tendrán que garantizar la seguridad de los datos críticos de su empresa a medida que se suban datos y aplicaciones corporativas a las nubes públicas.

Ingeniería social

Las redes sociales redefinen la privacidad

El gran abanico de posibilidades de comunicación y de interacción que ofrecen las redes sociales está dando lugar también a una nueva problemática, especialmente en las empresas, fruto de los problemas en la seguridad y la privacidad de la información, y cada vez más, de los intentos de ataques por parte de ciberdelincuentes.

Los ataques a través de la ingeniería social está siendo utilizado para llegar a más víctimas potenciales en las redes sociales. Los llamados spammers y scammers han sabido aprovechar los 'trending topics' de los medios sociales para mejorar sus tácticas y métodos de piratería e ingeniería social, robando datos de millones de usuarios de redes sociales en todo el mundo. Como consecuencia, los legisladores han comenzado a exigir que los sitios de redes sociales implementen políticas y mecanismos para proteger la privacidad de sus usuarios.

En el último año, Facebook, Twitter y Youtube han sido las redes preferidas por los ciberdelincuentes, que han aprovechado su gran popularidad para conseguir nuevas víctimas que les reportaran beneficios económicos.

Malware móvil

El reto de la movilidad y de la tendencia 'Bring your on device'

La proliferación de los dispositivos móviles, como los smartphones y los tablets, está dando lugar a una tendencia a nivel global que se ha denominado como 'Bring your on device' (traiga su propio dispositivo), en la que los trabajadores cada vez más tienden a utilizar su dispositivo móvil personal, además, como herramienta de trabajo. Esto estimulará la adopción de soluciones VDI (Virtual Desktop Infraestructure), y la conectividad inalámbrica, entre otras cosas, pero también, el acceso a información confidencial, que generará una nueva problemática para los responsables de TI en el ámbito de la seguridad y del cumplimiento de las políticas corporativas. Por este motivo, se prevé que las organizaciones inviertan mucho tiempo, dinero y esfuerzo en este aspecto. Y es que, será necesario concentrarse en contar con la protección básica para los nuevos modelos y dispositivos utilizados, sin olvidar las herramientas de seguridad dentro también de la empresa.

1&1 SERVIDORES DE ÚLTIMA GENERACIÓN

LANZAMIENTO EXCLUSIVO DE 1&1:

2 x 16 CORES

PROCESADOR AMD OPTERON™ 6272

- **Disponibilidad:** Avanzados centros de datos y disponibilidad de más del 99,9%
- **Comodidad:** Incluye Parallels® Plesk Panel 10.4 con dominios ilimitados
- **Flexibilidad:** Sistema operativo y funciones a elegir
- **Velocidad:** Tráfico ilimitado y más de 275 Gbps de ancho de banda
- **Soporte:** Asistencia telefónica 24 horas

Descubre todos los servidores de 1&1 en nuestra web.

LA NUEVA GAMA DE SERVIDORES DEDICADOS DE 1&1:

NUEVO: ¡1&1 SERVIDORES CON PROCESADORES INTEL!

SERVIDOR 4i

- **Intel® Xeon® E3-1220**
- 4 Cores de hasta 3,4 GHz
- 12 GB ECC RAM
- 1.000 GB RAID 1 con 2 X 1.000 SATA HDD

69,99 €/mes*

¡SOLO HASTA EL 29/2/12!

SERVIDOR XL 6

- **AMD Hexa Core**
- 6 Cores de hasta 3,3 GHz
- 16 GB ECC RAM
- 1.000 GB RAID 1 con 2 X 1.000 SATA HDD

¡3 MESES GRATIS!*

~~99,99~~ €/mes*

SOLO EN 1&1: ¡EL SERVIDOR MÁS RÁPIDO DEL MERCADO!

SERVIDOR XXL 32 CORE

- **2 x AMD Opteron™ 6272 (Interlagos)**
- 2 x 16 Cores de hasta 3,0 GHz
- 64 GB ECC RAM
- 2.400 GB RAID 6 con 6 x 600 SAS HDD

399,99 €/mes*

MIEMBRO DE united internet

Llámanos al **902 585 111** o visita nuestra web

1&1

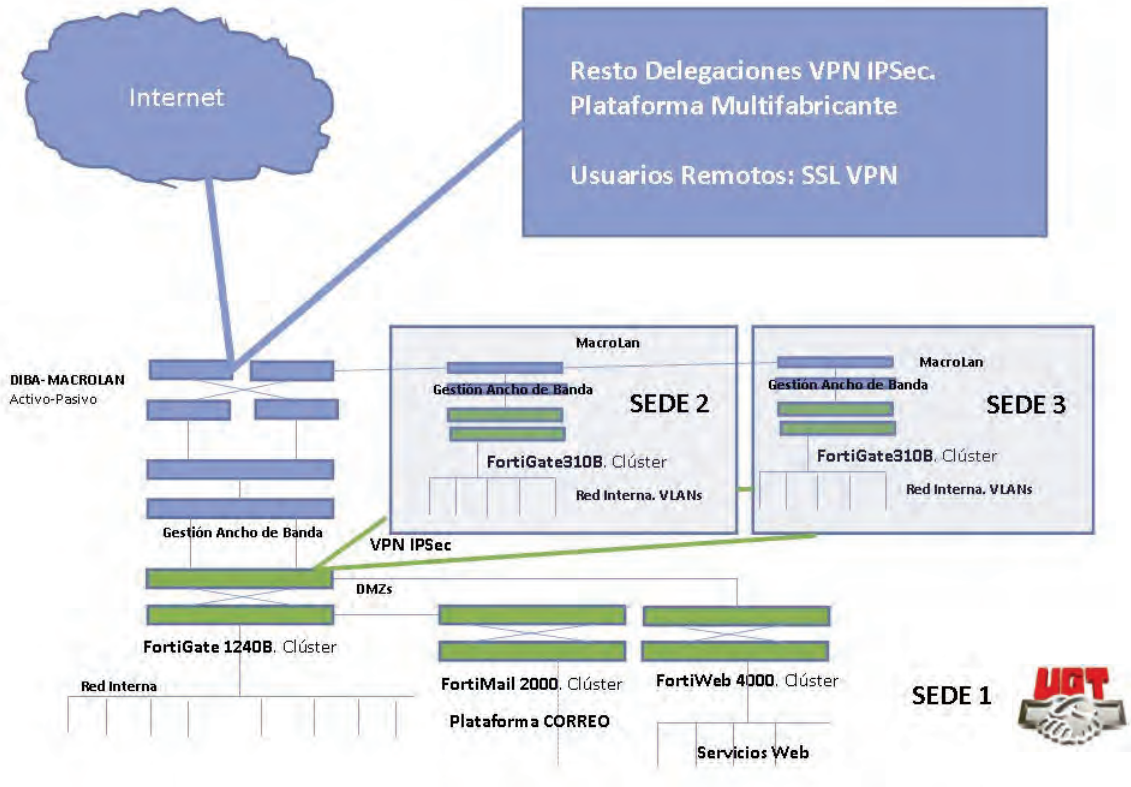
www.1and1.es

* Servidor Dedicado XL 6 gratis durante los 3 primeros meses. Después, 99,99 € al mes. Todos nuestros servidores están sujetos a un compromiso mínimo de permanencia de 12 meses y conllevan un coste por alta de servicio. Todos los precios mostrados no incluyen IVA. Para más información, consulta nuestras Condiciones Particulares en www.1and1.es.

La confederación apuesta por Fortinet para garantizar la seguridad de su perimetro, e-mail y servicios web

La confederación UGT blinda su territorio

La confederación del sindicato Unión General de Trabajadores (UGT) ha apostado por la tecnología de Fortinet para llevar a cabo, en colaboración con Telefónica, una modernización de su infraestructura de seguridad TIC. La solución desplegada combina los productos FortiGate, FortiMail y FortiWeb del fabricante para dar respuesta a los requerimientos de seguridad de la organización en tres grandes ámbitos: la seguridad perimetral, la seguridad del correo electrónico y la de sus aplicaciones web.



LOLA SÁNCHEZ

Nacida en 1888 y legalizada en 1977, la Unión General de Trabajadores (UGT) configura una confederación sindical que en la actualidad suma alrededor de 1,2 millones de afiliados. Organizada en órganos y departamentos confederales, 10 federaciones y 19 uniones territoriales, las comunicaciones resultan fundamentales en el desarrollo de las actividades de la UGT, específicamente a la hora de difundir información e interactuar sin descuidar un aspecto crucial: la protección de la información y la salvaguarda de los datos de afiliación, dando cumplimiento a la Ley Orgánica de Protección de Datos (LOPD).

"Las comunicaciones resultan cruciales en UGT, el uso de Internet se ha incrementado de forma notable, sobre todo con las redes sociales, y el correo electrónico se ha convertido en una herramienta indispensable", comenta el responsable de Sistemas y Comunicaciones de UGT, Luis de la Osa.

En ese escenario y con Telefónica como proveedor desde hace años, la confederación de UGT ha procurado contar con unos servicios que, además de satisfacer la demanda de los usuarios, ofrecieran plenas garantías de seguridad. "Empezamos haciendo uso de los servicios FrameRelay de Telefónica y ante el crecimiento de las necesidades dimos el salto al servicio Macro-LAN - DIBA (Datos Internet de Banda Ancha)", apunta.

A partir de ese momento y como añade de la Osa, "los niveles de seguridad que nos proporcionaba el propio operador no eran suficientes".

Correo y servicios web, críticos

Esa situación se hizo aún más patente cuando la organización decidió hace un par de años internalizar el servidor de correo, hasta el momento externalizado con Telefónica. "Asumimos el servicio de correo electrónico inicialmente para unos pocos usuarios, pero con el tiempo y especialmente a raíz de nuestra conversión en ISP alcanzamos una cifra de 8.000 buzones registrando la recepción de unos 400.000 correos diarios, lo que exigía niveles adicionales de seguridad".

El desarrollo en paralelo de nuevas aplicaciones centralizadas como la Aplicación de Afiliaciones y otras aplicaciones web confederales, así como la intranet emergía como un acicate más para abordar una modernización de la infraestructura de seguridad TIC. Y es que, si bien UGT disponía de una infraestructura de seguridad TIC, esta protección se basaba en plataformas tecnológicas antiguas con un rendimiento que no estaban a la altura de los nuevos requerimientos.

"Los niveles de seguridad que nos proporcionaba el propio operador no eran suficientes"

En esa tesitura, la confederación UGT decidió a finales de 2010 llevar a cabo una evolución de su arquitectura de seguridad con el objetivo de ampliar su alcance tanto en lo relativo a funcionalidades como en cobertura de nuevos entornos, específicamente el de servicios web. Se trataba, por tanto, de dar respuesta a los requerimientos de seguridad en tres grandes ámbitos: seguridad perimetral, seguridad del correo electrónico y seguridad de las aplicaciones web. Eso, sí, con una plataforma que ofreciera una gestión unificada.

En el primer ámbito, un entorno que suma más de 2.500 usuarios, era necesario sustituir los antiguos firewalls perimetrales por una nueva generación de soluciones UTM que permitieran consolidar diversas funciones: políticas de firewall, control de aplicaciones, filtrado de URL, IPS, antivirus, etc. Esta solución UTM debía, además, integrarse con los repositorios LDAP y de Directorio Activo para posibilitar la aplicación de políticas basadas en perfiles de usuario.

Protección en alta disponibilidad

Tras analizar las soluciones de distintos fabricantes con productos implantados en otros órganos del sindicato - Cisco, SonicWall, WatchGuard, Zyxel y Astaro (adquirida por Sophos), entre otros-, la confederación de UGT determinó que "algunos no cumplían los estándares o eran demasiado caros, otros no ofrecían una solución total o resultaban muy complejos o simplemente no disponían de una solución integral". Finalmente y tras una fase intensiva de pruebas, la balanza se inclinó hacia Fortinet. "Empezamos probando los FortiGate-60 y los FortiGate-100, luego pasamos a los FortiGate-400 y 800 y al final decidimos dar el salto a los FortiGate-1240".

Ante los buenos resultados obtenidos durante las pruebas, la confederación de UGT abordó el proyecto con Telefónica como integrador y Altimate como mayorista. En concreto y como detalla de la Osa, "hemos instalado un cluster de dos FortiGate-1240B en alta disponibilidad en la sede de Azcona, donde se encuentra nuestro CPD principal, y sendos clusters de FortiGate-310B en las otras dos sedes -Avenida de América y Hortaleza". Asimismo y para proteger específicamente la plataforma de correo basada en Microsoft Exchange y los servicios web, la confederación de UGT ha levantado sendos clusters de FortiMail 2000 y FortiWeb 4000.

"Los tres productos generan una serie de informes y logs que se recogen en FortiAnalyzer permitiendo la visualización de toda esa información en una única plataforma", subraya el responsable de Sistemas y Comunicaciones de UGT, que ha descubierto, entre otros registros, que "entre el 70 y el 80% de los correos electrónicos que recibimos diariamente son spam o ataques".

El avance también ha resultado fundamental para la confederación de UGT a la hora de tener capacidad para la creación de túneles IPsec STS (Site-to-Site) y túneles SSL para facilitar el teletrabajo y posibilitar unas comunicaciones seguras entre las unidades territoriales. "Hoy por hoy", apunta de la Osa, "tenemos alrededor de 200 túneles IPsec y entre 700 y 800 túneles SSL".

Puntos claves

- Con Telefónica como integrador, la confederación de UGT ha abordado la modernización de su infraestructura de seguridad desplegando una solución de FortiNet que garantiza protección de su perímetro, e-mail y servicios web.
- El proyecto ha supuesto la instalación de un cluster de dos FortiGate-1240B en la sede de UGT en Azcona y de sendos clusters de FortiGate-310B en sus otras dos sedes de -Avenida de América y Hortaleza.
- Para proteger su plataforma de correo y sus servicios web, la confederación de UGT ha levantado dos clusters de FortiMail 2000 y FortiWeb 4000, utilizando FortiAnalyzer para unificar los informes relativos a los distintos entornos.