Ciclo de Desayunos Fundación ASTIC 2012
Securizando aplicaciones distribuidas en la nube

POR MAOLE CEREZO
REDACTORA JEFE DE BOLETIC
FOTOS AITOR DIAGO

Evento patrocinado por

IT agility. Your way.

La nube puede aportar ahorros, tan importantes en las circunstancias actuales, pero no se han de descuidar aspectos cruciales como el de la seguridad para evitar que las virtudes de la cloud se tornen en complicaciones. Por ello, tal y como indicó Francisco Antón en la inauguración del desayuno de trabajo "Securizando aplicaciones distribuidas en la nube" "hemos de gestionar procesos e información en la nube, pero bajo control y con todas las precauciones".

En el evento, F5 presentó su propuesta para ayudar a mejorar el rendimiento, la seguridad y disponibilidad de la gestión de la información. Para ponerla en contexto, Javier Fernández, Gerente de Cuentas de F5 comenzó su exposición explicando cómo la tecnología de F5 "permite optimizar las aplicaciones de forma que sean más accesibles y, por lo tanto, más disponibles". Al mismo tiempo, "proporciona soluciones de seguridad dirigidas a afrontar los retos del momento actual, en que los aspectos relacionados con la seguridad han cobrado una especial importancia. Esto ha ocurrido, principalmente,

porque las aplicaciones han experimentado un proceso progresivo de "weberización", incorporando muchos más contenidos, haciendo que las medidas clásicas de seguridad resulten insuficientes en muchos casos". Los ataques que sufren los sistemas "han evolucionado mucho con el paso del tiempo, destacando en este momento la presencia masiva del malware y la proliferación de hackers, que desde 2005 priorizan sus ataques sobre las aplicaciones".

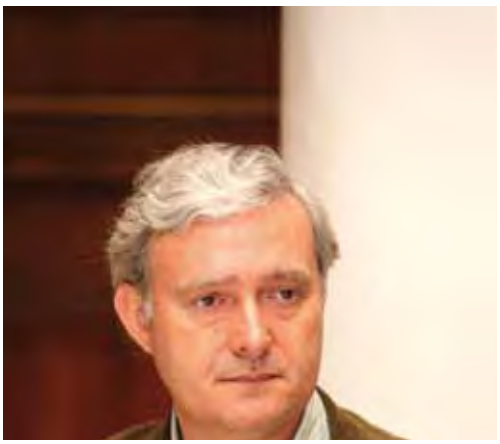
Estos fenómenos implican "un fuerte coste para las organizaciones, que tienen la alternativa de desarrollar sus propios sistemas de seguridad, pero sin duda, ello conllevará una inversión elevadísima" señaló el directivo de F5. Frente a ello, "nuestras soluciones, basadas en red y en protocolo SSL, son constantemente actualizadas y supervisadas de forma permanente por expertos, y priorizan tres campos de actuación: la infraestructura del cliente (servidores, servicios DNS, etc.), las aplicaciones y el acceso remoto a las aplicaciones".

La protección de las aplicaciones mediante firewall que ofrece la compañía "aplica tecnologías de seguridad positiva combinadas con tecnologías de seguridad negativa y, en el caso de las aplicaciones que permiten efectuar pagos a través de tarjetas bancarias, se puede eludir el desarrollo de una solución específica. Estas propuestas son compatibles con el uso de herramientas de auditoría y análisis de vulnerabilidad".

A su vez, el acceso remoto ve incrementada la problemática de la seguridad debido, como apuntó Javier Fernández, "al gran incremento experimentado por el teletrabajo y por la proliferación de dispositivos". Es necesario "ejercer un correcto control del usuario para garantizar que éste acceda de forma segura y correcta a las aplicaciones, lo que hace muy importante contemplar el contexto de la conexión: plataformas corporativas, IPad, etc. para poder determinar una adecuada política de seguridad. Un nivel de rendimiento elevado se basa en una buena gestión de las conexiones y en la compatibilidad entre fabricantes".

¿Externalización completa?

Ante las voces que apuestan por externalizar todo lo relativo a seguridad, Francisco Antón se interesó por conocer la opinión de la compañía a este respecto. Como le explicó Javier Fernández, F5 "aporta su experiencia y capacidad para determinar qué datos deben permanecer en el data center y cuáles son susceptibles de ser migrados a la nube. Una vez allí, se recomiendas que los SLAs fijen la ubicación (o ubicaciones) del dato, los plazos de recupe- »

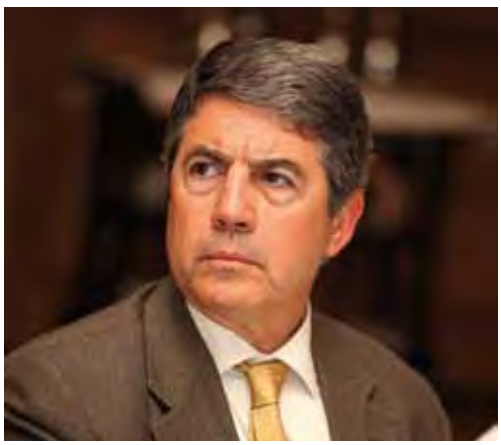


Adolfo Arquimbao

Ángel Luis Sánchez

Carmen Cabanillas

Fernando Morón



Francisco Antón

Ignacio Bellido

ración del mismo, etc. Nosotros estamos recomendando recurrir a modelos de nube híbrida que supongan una externalización parcial (datos antiguos, no críticos, etc.)"

El Presidente de ASTIC incidió en el hecho de que la gestión de la Administración no sigue los mismos mecanismos que la empresa privada, lo que "complica la toma de decisiones acerca de la migración de datos, así como de las tareas de seguimiento y control de los mismos". Y al respecto Sánchez sacó a colación iniciativas en debate que podrían paliar este problema, como "la creación de una empresa pública que actuase como proveedora de servicios en la nube para la Administración, a la vez que garantizase el mantenimiento y el control de los datos".

Y ¿Sería posible abordar de una forma más suave la transición hacia IP versión 6, obteniendo mayores niveles de seguridad con los equipos de F5? Preguntó Carmen Cabanillas, del Ministerio de Educación.

Raúl Flores Responsable Técnico de F5 le respondió que "la compañía ya ha asumido con éxito encargos de ese tipo en la Administración, concretamente en el Ministerio de Industria, pionero en un proceso que forma parte del "core" tecnológico de F5".

¿Afecta a los tiempos de respuesta el hecho de que las herramientas de seguridad analicen tanto los perfiles de los usuarios como el contexto de las conexiones? insistió la Subdirectora General Adjunta del Ministerio de Educación. Flores comentó que "son herramientas inteligentes, que no trabajan sobre todos los intentos de conexión, que son customizables, y disponen de elementos, como el geolocalizador, que facilitan la tarea de la herramienta contribuyendo a no perjudicar los tiempos de respuesta".

Ataques en movilidad

Y, con respecto a la movilidad ¿se está experimentando un incremento en la detección de ataques originados desde dispositivos móviles (Ipads, smartphones)? El Responsable Técnico de F5 respondió que, en España, y hasta ahora, no. Pero "dada la proliferación masiva de dispositivos de ese tipo y su rápida evolución tecnológica, lo normal sería que se comenzasen a registrar problemas con origen en tabletas y teléfonos".

Por cómo priorizar el tráfico y resolver el problema derivado de una plena libertad para conectarse por parte de los usuarios, se interesó Sergio López, de la Comunidad de Madrid. Raúl Flores explicó que "las soluciones de priorización del tráfico y de optimización del acceso a las aplicaciones son siempre muy complejas, y pasan por utilizar una herramienta de firewall de aplicaciones

> “La gestión de la Administración no sigue los mismos mecanismos que la empresa privada, lo que complica la toma de decisiones acerca de la migración de datos, así como de las tareas de seguimiento y control de los mismos”

José Ramón García

Leonor Torres

Pablo Burgos

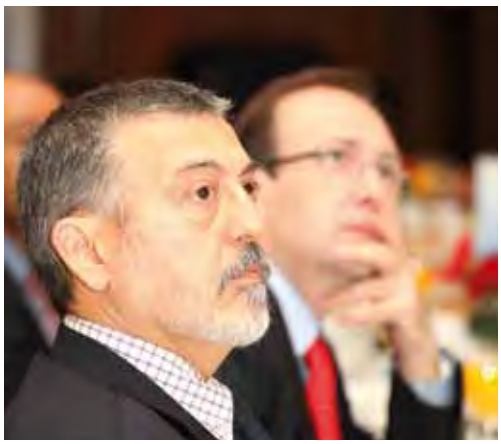
determinando el origen de los ataques con el fin de poner en cuarentena las IPs implicadas, modificando los anchos de banda y asignándoles un tamaño que desmotive al hacker, etc.”

Por su parte, Angel Luis Sánchez, del Servicio Madrileño de Salud, comentó que lleva seis años trabajando con F5 y que su departamento colabora “con entidades privadas cuyos usuarios acceden a los sistemas de la Administración a través de herramientas que gestionan los accesos seguros de los mismos”.

Explicó que “F5 no ayuda a sus clientes a implantar sus soluciones. Esa tarea corresponde a los integradores, que son los expertos en ello, y que en la práctica realizan una labor de consultoría muy importante en la posterior consecución de un rendimiento óptimo”.

¿Hay algún estándar definido para firewall 7 que permita a los desarrolladores entregar productos adaptables a cualquier entorno?, preguntó Sánchez. El Responsable Técnico de F5 le contestó que “nuestro producto es particularmente flexible, los desarrolladores no tienen que atenerse a normas para utilizarlo y adaptarlo a cualquier plataforma”.

Al interesarse Francisco Antón por un caso de éxito reseñable de F5, Raúl Flores se refirió a un ataque que “recientemente sufrió un gran banco por parte de »



Román Díez

Sergio López

Tomás de Lucas

“Anonymous consiguió tumbar el firewall, pero no afectó a los servidores debido a la acción de un balanceador de F5 con protección de denegación de servicios”

Anonymous que consiguió “tumbar” el firewall, pero que no llegó a afectar a los servidores debido a la acción de un balanceador de F5 con protección de denegación de servicios”. El directivo puntualizó que “el riesgo depende mucho del tipo de negocio, siendo mayor el riesgo de fuga de información en universidades y hospitales”. En el primer caso, “se llega a controlar de forma separada el acceso del profesorado y personal de administración del acceso del alumnado”.

El desarrollo factorial ¿exige requisitos especiales de seguridad? preguntó el Presidente de ASTIC. Javier Fernández le respondió que “existen herramientas de análisis de vulnerabilidad que se pueden combinar con herramientas de F5 y que permiten determinar una adecuada política de seguridad a ese respecto”.

Sobre la evolución y la disponibilidad de DNS Sec en los productos de F5 se interesó Fernando Morón, de la Casa de su Majestad el Rey. Raúl Flores explicó que “los clientes de F5 que ya tienen implantada una solución de seguridad disponen, con la misma tecnología, de la posibilidad de beneficiarse del DNs Sec en los próximos meses”.

Por su parte, Tomás de Lucas, del Ministerio de Educación preguntó si “los principales proveedores de servicios en la nube disponen de equipos de F5, puesto que suelen mostrarse reticentes a dar explicaciones sobre su infraestructura”. Muchos de esos proveedores disponen de equipos F5, más desde que la tecnología de F5 se puede virtualizar, contestó Javier Sánchez.