Desayunos ASTIC

Protección y TIC: Retos en las Administraciones Públicas

POR MAOLE CEREZO
REDACTORA JEFE DE BOLETIC
FOTOS AITOR DIAGO

Evento patrocinado por

EMC² where information lives

Bajo el título "Protección y TIC: Retos en las Administraciones Públicas" EMC presentó las soluciones que ofrece su división de seguridad RSA, en un desayuno de trabajo en el que asistieron más de una veintena de directivos TIC de la Administración. Javier Bustillo, Director de AAPP de la compañía recordó de forma muy escueta la fortaleza de su propuesta, avalada por "una firma líder en la industria de verificación de identidad y control de acceso, encriptación y administración de claves, administración del cumplimiento de normas e información de seguridad, y protección contra fraudes como es RSA, la división de seguridad de EMC". Éstas "protegen la integridad y la confidencialidad de la información durante todo su ciclo de vida, sin importar dónde se transfiere, quién accede a ella o cómo se utiliza".

El tema objeto del encuentro se abordó desde una triple perspectiva que adelantó Bustillo: una fue la referida a "la gestión de logs de seguridad, capaces de registrar quien, cuando, donde y bajo que circunstancia se ha accedido a la información que, en numerosas ocasiones desconocemos donde se encuentra, aún siendo de gran valor". Otra, "la prevención de la pérdida de información" y, por último, una tercera perspectiva centrada en "la suplantación de identidades en las páginas web". Circunstancia de la que, tal y como apuntó Bustillo son susceptibles, fundamentalmente, aquellos organismos de la Administración que realizan transacciones económicas, como son los casos de "la Agencia Tributaria, pionera en el pago de tributos por Internet; la Dirección General de Tráfico o el Ayuntamiento de Madrid, estos últimos, organismos que permiten abonar sus multas a través de la red".

Manuel Lorenzo, Ingeniero Experto en Seguridad de RSA entró en materia asegurando que "jaquearnos una web completa es bastante complicado, la mayoría de los fraudes se producen mediante la suplantación de identidad, los "ladrones" utilizan nuestra imagen y nuestros procedimientos para engañar al ciudadano". Recordó como "esta situación se dió en la agencia tributaria, y por ello RSA empezó ayudar al organismo". Pero si bien hay que hacer desarrollos seguros, tenemos que implantar un modelo de seguridad que "sea proporcional al riesgo". Porque, insistió el directivo, "si por un exceso de celo la utilización de los servicios por vía telemática se hace muy complicada, con muchas trabas para el ciudadano, éste desistirá de interactuar por esta vía".

En RSA se trabaja "con un enfoque que hemos utilizado históricamente en la banca durante años y que, ahora, estamos transmitiendo a otros negocios no financieros, entidades públicas y privadas. Se basa en tres pilares, por un lado nos centramos en proteger el ecosistema del fraude, el *farming*, el *fishing*, usos que realizan los defraudadores de nuestra imagen pero que no tiene que ver con que nos

jaqueen nuestro entorno, se refiere a lo que queda fuera de él. Por otro, atacamos lo que queda dentro, nuestros sistemas, ello con la monitorización de los loggings, del acceso... Y un tercer flanco al que dirigimos nuestro esfuerzo es hacia aquellas páginas que, además, hacen cobros, monitorizando las transacciones en sí".

Cómo evitar la fuga de datos es algo que, en los últimos tiempos, preocupa a las organizaciones, y sobre todo en momentos en los que el teletrabajo se puede ver incrementado como consecuencia de situaciones similares a la generada por la gripe A. En muchos casos, tal y como asegura el Experto en Seguridad de RSA, "ésta no se produce intencionadamente, sino por descuido de los propios usuarios". Para evitarla, "hay que cubrir todas las opciones de pérdida de datos en distintos puntos del entorno tecnológico, teniendo en cuenta su localización, su flujo a través de la red y el destino final".

Tener el control de la evolución de los entornos tecnológicos sobre los que se trabaja, con proveedores de tecnología que presentan una gran dispersión y con servicios prestados en modelo outsourcing, es de vital importancia en materia de seguridad. En un contexto heterogéneo y distribuido como el citado, en el que no siempre todo se maneja por un administrador "nuestro control sobre la infraestructura decae y para cumplir la normativa, debemos dedicar un mayor esfuerzo. Ello requiere entender todos los elementos involucrados (servicios, aplicaciones, servidores, conexiones de red...), implementar los controles, monitorizar constantemente en tiempo real y corregir las desviaciones, algo en lo que ya desde hace tiempo estamos trabajando en RSA", afirma Manuel Lorenzo.

Esquema Nacional de Seguridad

Francisco Antón, Presidente de ASTIC reparó en el hecho de que "la seguridad es algo que también se ve afectada por recortes presupuestarios" apuntando que "aquellos organismos que gestionan impuestos pueden recibir mayores inversiones". Por su parte, Carlos Maza, de Industria, compartió su opinión sobre el nivel de seguridad de la Administración, que "es medio-alto". A la vez invitó a poner la mirada en el Esquema Nacional de Seguridad, regulado mediante un Real Decreto que, en fase de proyecto, está bastante avanzado y que impone "obligaciones de todo tipo a la Administración, que van a requerir recursos humanos y económicos". ¿Cómo RSA podrá ayudar para acompañar a los directivos TICs a cumplir sus exigencias?, concluyó el Vicepresidente de ASTIC. EMC propuso "ir por fases".

Como primer paso, señaló Lorenzo, se ha de "cubrir el correo corporativo, ya que es por donde se produce la mayor parte de fuga de datos" A su vez, aconseja "clasificar y proteger su información" y "estar alerta y prepararse ante futuras incidencias de fraude" ya que "en tiempos de reducciones y crisis hay más gente ociosa que se presta al crimen". Puesto que en la Administración "hay información extraordinariamente confidencial que hay que proteger". Algo, esto último, en lo que José Ramón García Amo, de la Biblioteca Nacional, manifestó su plena conformidad, insistiendo en que "a nosotros, los responsables de tecnologías, nos preocupa mucho la seguridad de esta información". Ello lo pone lo pone de manifiesto el hecho de que, tal y como comenta Alejandro Lazcano del Ministerio de Trabajo, "en todos los departamentos ministeriales hay un Plan Director de Seguridad. El nivel de de seguridad de la Administración es elevadísimo, nos lo demuestran los indicadores de contraste que, en los últimos tiempos, estamos empleando con frecuencia en el sector público". Nosotros "tenemos definido el nivel de seguridad que hemos de asegurar, otra cuestión es que contemos con el presupuesto para ello".

24 directivos TIC de la Administración participaron en el debate en el que EMC fue la empresa invitada

El Subdirector TIC del Ministerio de Trabajo puso sobre la mesa el hecho de que, "si bien en la actualidad la Administración no está sufriendo de manera importante el ataque de los hackers" la situación seguramente cambiará en el momento en que "con la aplicación de la Ley 11/07 se incremente el número de ciudadanos que hagan uso de los nuevos servicios web, que muy pronto estarán disponibles". A la vez, manifestó su preocupación por el hecho de que las exigencias de la Ley puedan llevar a poner a disposición del ciudadano servicios "con las suficientes garantías en materia de seguridad" e hizo una propuesta a sus compañeros de "colaboración entre los distintos »

El Presidente de ASTIC Francisco Antón, inauguró el Desayuno

Celia Tenés

Javier Bustillo, durante una de sus intervenciones

Belen Sánchez, Carlos Maza y Javier Bustillo

Manuel Lorenzo, presentó las fortalezas de la división de seguridad de EMC

organismos contra los defraudadores". Algo que, confirmó Manuel Lorenzo, "hacen los directores de seguridad de los bancos". Porque "ir en solitario, no da resultado". A su vez, Lazcano puso de manifiesto que "el pago de prestaciones y de subvenciones son dos de los apartados más susceptibles para el fraude" en su ministerio.

En el SAMUR, tal y como confirmó Borja Prieto, del Ayuntamiento de Madrid, se manejan muchos datos sensibles, confidenciales. Sin embargo, no están ajenos a que sus usuarios, aún de forma inconsciente y por descuido, los pierdan, "evitar las fugas, es algo que no tenemos resuelto". Fidel Pérez, Director Comercial División Seguridad de EMC le respondió asegurando que "para luchar contra el insider, el hacker que tenemos dentro de nuestra organización, hay que disponer de buenas políticas de seguridad y herramientas que nos obliguen a que se cumplan". EMC puede "cubrir la seguridad de los datos confidenciales mediante las tecnologías DLP, que protegen la red corporativa, el correo, los data centers, los repositorios documentales y el PC del usuario".

Celia Tenés del Ministerio de Presidencia, se interesó por las soluciones de EMC para evitar la fuga de datos y luchar contra el *phishing*, que "se incrementará notablemente con la aplicación de la Ley 11/07, porque el *hacker* se va a dar cuenta del gran nicho que tiene para suplantar identidades en la Administración". La compañía, tal y como expusieron sus directivos, lleva muchos años trabajando en esta línea en la banca. "Tenemos un centro anti malware en Israel, especializado en monitorizar las actividades de la red global para detectar el phishing, incluso antes de que los usuarios reciban los correos. Contamos con un ecosistema de servicios y relaciones con proveedores de correos como Yahoo, Hotmail o Amazon; con todas las policías locales del mundo y con proveedores de páginas web, que nos permite parar un ataque con una media de dos horas. Estamos identificados por todos ellos y, cuando les hacemos una solicitud para frenar una página, la respuesta es inmediata. Ello se debe a años de colaboración. Es nuestro aval como compañía", le respondió el experto de seguridad de EMC.

En nuestra organización la seguridad es esencial, intervino José Antonio Pera del INE, "trabajamos con muchos datos sensibles como los del padrón municipal o el censo electoral, y hemos de tener muy en cuenta pérdidas y fugas y cumplir la normativa de protección de datos". Personalmente creo que "tenemos que continuar innovando, empleando todas las herramientas a nuestro alcance para mejorar la seguridad de nuestra información, probando »

nuevas tecnologías..., independientemente de que tengamos un Plan de Seguridad".

Más servicios, mayor vulnerabilidad

Santiago Domínguez, de la Dirección General de Tráfico, coincidió con alguno de sus compañeros en que la puesta de disposición de más servicios implicará que "tengamos que abrir más los CPDs para ofrecer más servicios, exponiéndonos a ser más vulnerables, más inseguros". Si bien lo que impera es "ofrecer más funcionalidad sobre la seguridad, hay que ir con pies de plomo para hacerlo correctamente". La seguridad requiere "inversión económica y aporta poca funcionalidad, es poco visible. Iremos avanzando en este apartado, a medida que se vayan implantando los servicios y el número de incidencias crezca exponencialmente".

Su compañero en Tráfico, Luis de Eusebio, recordó que el papel de los directivos TICs tiene que ser, en parte, de prescriptor, "concienciando sobre las soluciones en las que se tienen que apoyar los servicios y transmitiendo confianza". En tráfico, "la figura del insider la tenemos controlada", concluyó. En el Ministerio del Interior, como comentó Manuel Martínez, "hace años introdujimos un sistema de prevención de fuga de información de víctimas de terrorismo que nos supuso un gran esfuerzo. Por ello, me planteo ¿qué súper estructura y esfuerzo conllevaría, aún cuando todo el servicio se externalizase, implantar seguridad a todos los niveles?".

Manuel Lorenzo respondió al directivo señalando que, en la actualidad, "los sistemas se centran en disponer de un sistema más abierto, que monitorizan los contenidos y estudian que se está haciendo, que te permiten colocar piezas en los lugares más estratégicos". Son "sistemas menos intrusivos, capaces de cubrir mucho más sin llegar al punto de cifrar el objeto final". Fidel Pérez, a la vez, apuntó que, además "la organización tiene que saber que es confidencial, porque éstas soluciones rastrean la información sensible, la buscan para detectar donde se encuentra". Y, si bien, "la confidencialidad evoluciona con el tiempo, tenemos que saber donde está para protegerla". El primer paso a dar, es "saber que es confidencial —algo que, con los Planes Directores de Seguridad, en la Administración se tiene fácil— y posteriormente, implantar las políticas adecuadas", insiste.

En la misma línea que ya habían apuntado alguno de sus compañeros, José Manuel Pacho, del Ministerio de Economía, alertó de que "no hay que caer en la tentación de pretender dotar de mayor seguridad al procedimiento electrónico, que sea más seguro de lo que es el actual, ya »

Carmen Cabanillas, José Ramón García, Fidel García, Director Comercial de la División de Seguridad de EMC y Pablo Burgos

Javier Sánchez Escribano, Senior Account Manager de EMC

José Antonio Perea, Borja Prieto, Leonor Torres y Javier de Andrés

Manuel Alonso, José Manuel Pacho y Alejandro Lazcano

Fernando Martín

que supondría levantar una barrera a la implantación de la Administración electrónica". En este sentido, el Director Comercial de RSA recordó que hay que pensar en una seguridad que "solo moleste a los posibles criminales, el 2% de nuestros usuarios". Si bien Francisco Antón se interesó por las estadísticas de evolución del fraude, los directivos de EMC le informaron sobre el hecho de que éste no se ha incrementa cada año más que lo que se tiene previsto por parte de las entidades bancarias, que son las que, a día de hoy, se ven más afectadas por ello. Porque "el único objetivo del criminal es el económico. Si en la Administración disponéis de información que se pueda convertir en dinero, entonces los hackers atacarán".

Javier Bustillo, concluyó apuntando a su compañero que en la Administración "además de por intereses económicos, se puede querer atacar un sistema por intereses políticos". Por su parte, Manuel Lorenzo recordó que "el papel del insider es crítico en el sistema de fraude, y que EMC, dispone de soluciones para informar a sus clientes de su existencia. Las redes de defraudadores son cada vez mayores, el 90% del correo de Internet es basura y su crecimiento es de un 80% anual, porcentaje que bloqueamos a nuestros clientes en un 100%. El fraude ya no solo afecta a los bancos, sino también a los foros sociales, los portales de compra... " Y parece que, en un futuro no muy lejano, también a la Administración.

Última hora

Bilbomática y FUNDASTIC firman un acuerdo de colaboración

Walter Mattheus, Director General de Bilbomática y Francisco Antón, Presidente de ASTIC

La Consultora e Ingeniería de software Bilbomática y la Fundación ASTIC (FUNDASTIC) han suscrito un convenio de colaboración en virtud de sus intereses y objetivos sociales, con el fin de aprovechar y potenciar sus recursos para desarrollar actividades en el ámbito de las Tecnologías de la Información y las Comunicaciones.
Las iniciativas perseguirán, el impulso de la Administración-e, con el fin de cumplir los requerimientos de la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, y que de ésta forma, los ciudadanos, las empresas y el sector público se beneficien de las ventajas y posibilidades que la Sociedad de la Información tiene. Bilbomática es una empresa de capital 100% español, orientada desde hace más de 20 años a la generación de soluciones en el ámbito de Tecnologías de la Información y las Comunicaciones. Cuenta con más de 350 profesionales y cerrará este año con una facturación de casi 20 millones de euros.

Bilbomática trabaja intensamente con la administración pública europea y española a nivel nacional, autonómica y local. En los últimos dos años, su presencia se ha incrementado de forma importante en la Administración General del Estado, debido a su sólida experiencia en materia de Administración-e y que dispone de herramientas que resultan de gran utilidad en el sector público, entre ellas eSentia, plataforma de soluciones Open Source que permite implantar estrategias de gobierno electrónico de forma más eficiente, rápida y escalable. Bilbomática, cuenta con la máxima clasificación administrativa para contratar, está incluida en el Catálogo de Adquisición Centralizada de la Dirección General de Patrimonio del Estado y dispone de varias certificaciones: ISO 9001, CMMI v2, ITIL, entre otras.

FUNDASTIC, fue aprobada en Asamblea de ASTIC del pasado 18 de junio y el 30 de septiembre se firmaron las escrituras públicas de constitución. Su misión fundamental es la de impulsar el cumplimiento de los fines de ASTIC, incidiendo en el desarrollo, promoción y utilización de las TIC en el ámbito principalmente de las Administraciones Públicas y, en general, en referencia a la Sociedad de la Información. La Fundación tendrá, como fin último, la contribución al éxito de un modelo de crecimiento sostenible basado en el incremento de la competitividad y la productividad, la promoción de la igualdad social y regional, y la mejora del bienestar y calidad de vida de los ciudadanos y las empresas. Todo ello, alineado con los objetivos de la Agenda de Lisboa, que persiguen la convergencia con los países europeos más avanzados de nuestro entorno en materia de Sociedad de la Información.