Evento patrocinado por

Symantec

CICLO DE DESAYUNOS FUNDACIÓN ASTIC 2013

Claves para escapar del escándalo de robo y filtración de información, protegiendo derechos y libertades

POR MAOLE CEREZO
Fotos de Aitor Diago

En el Desayuno de trabajo con Symantec, celebrado el pasado mes de enero, se revisaron los incidentes de ciberseguridad actuales, cada vez más sofisticados, en entidades públicas y privadas.

Además de la identificación de las amenazas y sus fuentes, se aportaron posibles soluciones para contrarrestarlas en el ámbito de la seguridad perimetral y de las aplicaciones, tomando como ejemplo el caso implantado en el Ministerio de Empleo y Seguridad Social. Nuestro compañero, Joseba García Celada, nos compartió su caso en el que se han considerado elementos tecnológicos, organizativos, normativos y procedimentales, en una aproximación a la protección frente a ataques dirigidos, que está permitiendo identificar y remediar amenazas reales 24x7x365

Como indicó Emilio García, Presidente de ASTIC, al inaugurar el encuentro, algunos ataques recientes ponen de manifiesto que el CiberCrimen es una realidad que busca beneficios económicos mediante la compra-venta de información crítica o financiera, o bien se propone destruir infraestructuras

consideradas críticas para las organizaciones, con el consecuente impacto en términos de degradación de servicios, costes económicos y reputación.

El reto, como señaló el Responsable de desarrollo de negocio en soluciones de seguridad de Symantec, David Fernández, reside en identificar anomalías mediante el análisis del tráfico de usuarios realizando actividades autorizadas, con controles tales como la monitorización de anomalías de comportamiento, que permiten ir más allá en los niveles de detección y estar acordes con las nuevas técnicas de hacking.

Rocío Montalbán, Subdirectora General Adjunta de TIC del Ministerio de Industria y vocal de la Junta Directiva de ASTIC, responsable de contenidos de los desayunos organizados por la Fundación ASTIC, al tiempo que introdujo a los representantes de Symantec, resaltó la importancia de promover la confianza y la simplicidad en el uso de los entornos TIC asumiendo los menores riesgos posibles ante las crecientes amenazas.

SYMANTEC, con presencia en España desde hace catorce años, cuenta con una amplia experiencia al servicio de la Administración Pública, donde "se ha podido observar una importante evolución en materia de seguridad hasta llegar a la protección inteligente de la gestión de la información en el marco de una red global de inteligencia con monitorización del tráfico de Internet. La ciberseguridad, de hecho, se ha convertido en el quinto elemento en materia de defensa" señaló David Fernández.

El experto en seguridad de la compañía se refirió también a la proliferación de ataques a corporaciones y organizaciones estatales en estos últimos tiempos, con grave peligro para la seguridad nacional, basados en el empleo de malware y que persiguen, tanto conseguir información, como dañarla. Muchas de ellas "no están capacitadas para afrontar estas amenazas y asumir sus consecuencias". A la vez, planteó como tema de debate el grado de preparación de las administraciones públicas españolas para afrontar ataques de magnitud importante. Explicó que Symantec está intentando integrar distintas herramientas entre sí, al tiempo que busca el equilibrio ideal entre "defensa dinámica" y "seguridad adaptativa".

Actuar sobre las infraestructuras, establecer las mejores prácticas y mejorar la gobernanza de la seguridad puede resultar una tarea muy compleja, que se aborda determinando cinco ámbitos: seguridad de infraestructuras, monitorización y operación de seguridad, protección de información crítica, políticas y procedimientos de seguridad y protección y concienciación de los usuarios, concluyó el especialista de seguridad de Symantec.

El Caso de Empleo

Como explicó Joseba García, en el Ministerio de Empleo se cuenta con una infraestructura TIC mediana si "nos referimos a los servicios centrales del departamento, que registra un gran número de operadores en teletrabajo". De éstos, seis mil son usuarios físicos y siete mil virtuales, que acuden a la oficina una vez por semana y trabajan mediante dispositivos corporativos con distintas formas de conexión. También los hay que dependen de administradores locales.

Por otra parte, según explicó el responsable TIC de Empleo, se está »

Ana Bajo

Andrés Pastor

Ángel L. Sánchez

Antonio Arozarena

Antonio Cortés de Symantec

Arturo Ribagorda

Carlos Fernández, de Symantec

Carlos Ferro, de Symantec

Carlos Turmo

César Cid, de Symantec

Emilio García

Ester Arizmendi

Fernando Martín

Gerardo Silván

Javier Morales

José Antonio Perea

incrementando el número de dispositivos propiedad de los usuarios con uso corporativo. De esta forma, "toda la infraestructura de seguridad perimetral y protección del puesto de trabajo empleada por el departamento resulta insuficiente a la hora de evitar incidentes". Por ello, y "ante el ofrecimiento de Symantec, se trabajó en la integración de todas las herramientas disponibles".

De tal manera, "se recibe información de cada incidente con cualificación del mismo, descartando los falsos positivos y con conocimiento del lugar del ataque, de los dispositivos implicados y de la ruta que permite determinar el puesto final origen del problema. Los incidentes se etiquetan de forma precisa, y los de mayor gravedad, cuentan con un soporte técnico telefónico de Symantec, que abordan el problema de inmediato". El administrador "recibe un e-mail o un SMS en el caso de incidentes críticos, con la descripción y el origen del problema. También se pueden generar informes según cada caso concreto. Es importante disponer de bases de datos de nivel internacional que favorezcan la obtención de respuestas a través de un servicio 24x7".

García concluyó su intervención afirmando que "es la organización, en todo caso, quien determina sus propias políticas y establece su estructura de seguridad".

Incremento de la seguridad

La Directora General de Modernización, que quiso compartir con ASTIC el primer desayuno del año, tras mostrar su apoyo a las iniciativas de la Asociación, incidió en la importancia de la seguridad y manifestó su interés por conseguir un incremento de sus actuales niveles, que considera siguen siendo bajos, a pesar de los esfuerzos que se vienen realizando. A su juicio, "la minoración presupuestaria no puede ser óbice para abordarlos y es necesaria una mayor toma de conciencia por parte de las personas implicadas".

A su vez, el Director General de Inteco, planteó una reflexión más allá de la tecnología, "puesto que, si bien ésta resulta imprescindible, los usuarios siguen constituyendo el elemento clave". De hecho, "las nuevas formas y entornos de trabajo aportan nuevos problemas en materia de seguridad, haciendo más necesario un adecuado análisis de riesgos, el establecimiento de políticas y la concienciación de los usuarios".

En la necesidad de afrontar un cambio de paradigma recayó García Celada, ante "la proliferación de accesos a servicios corporativos mediante nuevos y distintos dispositivos, en ocasiones propiedad del usuario". Reseñó que las restricciones de uso de estos dispositivos "no pueden ser una solución", poniendo el ejemplo de las fugas de información que tienen lugar en soporte papel, sin que por ello, se limite su uso".

Miguel Ángel Rodríguez, del Ministerio de Turismo, intervino para resaltar los que, en su opinión, son "los tres pilares en materia de seguridad: las personas, los procedimientos y la tecnología". Incidió a su vez en que "la concienciación del usuario es una cuestión clave".

El responsable de Tecnología para España de Symantec, Cesar Cid, intervino para precisar que "habitualmente, en cada acceso se identifica la dirección IP, la cual está asociada a un usuario concreto, determinándose el destino de los accesos". Respecto a la intimidad en el tráfico de

comunicaciones, se "monitoriza con carácter general, con conocimiento del usuario y bajo especiales restricciones respecto a los accesos que permiten identificar las contraseñas del usuario, los destinos de navegación o el acceso al correo. Se establece una habilitación para el acceso a cada tipo de dato, como primera puerta de vigilancia".

Muy positivamente fue valorada la experiencia desarrollada por el Ministerio de Empleo por parte de José Antonio Perea, del I.N.E. Respecto a lo que se refiere a los usuarios, resaltó el hecho de que "muchos organismos de la Administración están haciendo un gran esfuerzo por incrementar el uso de la tecnología". En el caso de los dispositivos privados, "el usuario en ocasiones aporta mayor nivel de tecnología mediante su propio dispositivo, pero esto supone estar expuesto a un mayor riesgo". En su opinión, éste se paliaría en parte "si se proporcionasen herramientas corporativas por parte de la Administración, al menos a usuarios con necesidades de movilidad, que podrían limitarse técnicamente (acceso a Dropbox, conexión WIFI...) y mediante políticas de seguridad".

La educación de los usuarios en materia de seguridad fue el tema que sobre la mesa puso Victoria Figueroa, del Ministerio de Hacienda. Según ésta, "no se educa suficientemente, de forma que se fomente la correcta utilización de herramientas de almacenamiento o el uso del escritorio virtual, y se haga una diferenciación clara de los usos privado y corporativo". A su juicio, "la inversión en seguridad debe estar condicionada por una política común a todos los departamentos".

A todo ello, David Fernández respondió que "servicios como el escritorio virtual dan lugar a sistemas expuestos. Las entidades bancarias, por ejemplo, siguen buscando de forma permanente, soluciones tecnológicas para proteger este tipo de infraestructura, asumiendo, monitorizando y previendo los riesgos". Este es un problema que "Symantec aborda mediante soluciones de sandboxing, que funcionan a la perfección". »

La Directora General de Modernización, que quiso compartir con ASTIC el primer desayuno del año, tras mostrar su apoyo a las iniciativas de la Asociación, incidió en la importancia de la seguridad y manifestó su interés por conseguir un incremento de sus actuales niveles, que considera "siguen siendo bajos, a pesar de los esfuerzos que se vienen realizando".

José Luis Goberna

José Ramón García

Joseba García

Juan Aguiló de Symantec

Manuel Alonso

Manuel Escalante

María Jesús Casado

Miguel A. Rodríguez

Pedro L. Alonso

Rocío Montalbán

Román Díez

Victoria Figueroa

David Fernández de Symantec

Modelo adecuado

Que cada organismo tenga su propia visión en materia de seguridad, es algo que para Fernando Martín, del Tribunal de Cuentas, "resulta problemático y sería necesario que se impusiese un criterio más horizontal".

Rocío Montalbán comentó que ningún sistema de seguridad resulta perfecto, e incidió en la necesidad de seguir avanzando. En este sentido, puso como ejemplo la posibilidad de mejorar el tiempo de reacción frente a las incidencias, más allá de las habituales medidas de protección perimetral y de seguridad interna.

A su vez, Emilio García, reconoció la necesidad de seguir mejorando la protección e invirtiendo en seguridad, pero "siempre que se eviten repercusiones negativas sobre la productividad".

En cuanto a la concienciación del usuario sobre la importancia de la seguridad, Andrés Pastor, de la Gerencia Informática de la Seguridad Social afirmó que debe comenzar por la cúpula directiva, y que resulta imprescindible mentalizar a las administraciones en este aspecto, desde abajo hacia arriba. En su opinión, la limitación de los servicios dejaría insatisfechas las necesidades de los organismos, al tiempo que alejaría a las administraciones públicas de los beneficios de la tecnología.

El posible dilema entre seguridad y productividad, en opinión de Carlos Plaza, del Ministerio de Empleo, debe resolverse primando ésta última, al igual que se hace en las organizaciones privadas, y a través de mecanismos que incrementen la cooperación. Esto significa aprovechar todas las oportunidades que ofrece el mercado en cuanto a dispositivos y tecnología.

Para Manuel Alonso, de la IGAE, "la administración pública española constituye una referencia en cuanto a seguridad se refiere". Destacó "el alto nivel de concienciación de sus responsables TIC", y se refirió al Esquema Nacional de Seguridad para sustentar su afirmación. No obstante, "la velocidad con que evoluciona la sociedad de la información complica, en gran medida, el análisis de riesgos, por el ritmo con el que los usuarios incorporan a su vida las nuevas tecnologías". Por el mismo motivo, "cabe esperar en los próximos años grandes avances en materia de seguridad, que beneficiarán a usuarios mucho mejor formados".

Pero, por ello, según María Jesús Casado, de la Intervención General del Estado, "resta un gran camino por recorrer". A su juicio, "el punto de partida en este campo no lo constituye la tecnología, sino la actitud de los gestores responsables de la información y de los servicios". Deben "existir comités de seguridad que fijen políticas y procedimientos, teniendo en cuenta a los gestores, de forma que esas medidas sean susceptibles de llevarlas a la práctica de forma efectiva, e involucrando a todos los usuarios".

Como colofón, David Fernández, Especialista de Seguridad de Symantec concluyó que "los usuarios deben ser conscientes de la importancia del uso correcto de sus dispositivos particulares. El factor común a todos los problemas de seguridad es la información, y conviene centrarse en ella como núcleo del servicio y del negocio". ✱