ISMS Forum Spain

ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN

Resumen: conclusiones de la VI Jornada Internacional

Con la cabeza en las nubes y los pies en la tierra

Las capacidades del CISO deben evolucionar rápidamente, en este entorno de crisis económica mundial, para adecuarse a la transformación de modelos de servicio, internacionalización de amenazas y hábitos de consumo.

Los responsables de seguridad de la información deben ser capaces de asumir una gestión global del riesgo en entornos cambiantes.

El entorno del Parque Tecnológico de La Cartuja, en Sevilla congregó el pasado 24 de noviembre a más de 200 expertos en Seguridad de la Información en torno a la VI Jornada Internacional de ISMS Forum Spain. Titulado "Impactos de la Transformación Económica y Social en la Seguridad de la Información", este encuentro facilitó el debate en torno a los retos funcionales e internacionales del CISO, las implicaciones de seguridad en los modelos de outsourcing y cloud computing, los riesgos de la fuga de datos o las amenazas inherentes a las redes sociales. La célebre frase "renovarse o morir" podría constituirse en lema del congreso, como veremos por las conclusiones de los distintos ponentes.

30-11-2009 Por ISMS Forum Spain

La jornada estuvo poblada de comentarios y anécdotas que conformaron un adecuado análisis de la situación actual y de cómo la crisis mundial (todos los expertos internacionales admitieron que influía notablemente en el mercado de la seguridad) ha hecho evolucionar los riesgos tradicionales y a la vez plantea a la industria la necesidad de afrontar nuevos planteamientos.

La introducción de la jornada corrió a cargo de **Gianluca D'Antonio**, presidente de **ISMS Forum Spain** y CISO del **Grupo FCC**, quien recordó lo importante que es entender el pasado y el presente para comprender lo que

puede deparar el futuro. Apuntó asimismo que ISMS Forum lleva ya tres años organizando dos jornadas internacionales anuales para reflexionar sobre el futuro de la sociedad de la información, en las que expertos internacionales colaboran aportando su experiencia acerca de lo que ocurre más allá de nuestras fronteras. Ya en la introducción se avanzó la sensación generalizada de que 2010 se anuncia duro, pues la crisis seguirá con nosotros, introduciendo así el contexto de las siguientes conferencias sobre el impacto de la crisis en el sector y cómo ésta afecta a la seguridad. Sobre el *cloud computing*, **D'Antonio** mencionó que, aunque lleva ya dos años entre nosotros, requerirá aún tiempo y conocimiento para aprovechar estas nuevas formas de hacer negocio, sabiendo gestionar el riesgo que esto también entraña. A este respecto, se entregó a todos los asistentes una llave USB con la nueva versión 2 del documento denominado "Guía para la Seguridad en áreas críticas de atención en Cloud Computing", que ha sido traducido por cortesía del ISMS Forum Spain desde el original en inglés de Cloud Security Alliance.

Enrique Polanco, director de Seguridad Corporativa del Grupo PRISA, impartió la conferencia inaugural, que analizó los desafíos de seguridad a los que se enfrentan las corporaciones españolas que tienen intereses en el extranjero y el reto de los cambios económicos y sociales. Entre los factores que potencian el riesgo destacó la diversidad de legislaciones -sobre todo en lo concerniente a seguridad privada- además de la inestabilidad política y los diferentes grados de corrupción o de libertad de expresión en algunos países. Todo ello puede comprometer las operaciones de las compañías españolas con intereses en Latinoamérica. Recomendó la implantación de un Sistema Integral de la Seguridad, fruto de unificar la gestión de la Seguridad de la Información, Física, Laboral y Medioambiental. "El nuevo Director de Seguridad Corporativa es un *Risk Manager*", resumió Polanco, enfatizando las funciones del CISO como gestor del riesgo global que debe abordar los cambios desde un punto de vista internacional. "El primer paso para poder dar con las soluciones adecuadas es conocer bien los problemas a los que nos enfrentamos" aseveró.

Enrique Polanco

El caso del Grupo PRISA da una idea de este contexto. Presente en casi toda Iberoamérica, y por tanto sujeta a entornos legales y sociales muy diversos), debe afrontar notables desafíos que hace 20 años se consideraban riesgos emergentes y ahora han pasado a ser estratégicos y operativos. "Y no podemos olvidar – aseveró Polanco- que hoy la amenaza es global, difícil de prever, y puede tardar sólo unos segundos en propagarse".

Sin embargo, el responsable de seguridad de PRISA añadió que algunos países latinoamericanos, como Argentina y Chile, destacan en asuntos como la protección de datos; de hecho, explicó que Argentina incorpora el concepto de *habeas data* en su Constitución, aunque por lo general existe poca regulación al respecto. Por último, habló acerca de los esfuerzos que se están realizando en el ámbito internacional en pro de un ambiente global más seguro y de una adecuada gestión de riesgos global, principalmente desde la OTAN. Allí se estudia en profundidad lo que se conoce como el Futuro Ambiente de Seguridad (o FSE por sus siglas en inglés), que valora el riesgo desde varios niveles, estratégico, regional y transnacional. La vulnerabilidad -acentuada por la crisis económica- y la amenaza creciente son los dos vectores a contemplar en esta gestión del riesgo.

La siguiente ponencia fue impartida por **Andrew Jaquith**, analista Senior de Forrester Research en Estados Unidos. Comenzó insistiendo en que la economía actual está realmente mal, y las amenazas se incrementan a ritmos vertiginosos. Una de las consecuencias será que el *outsourcing* forzará a las empresas a centrarse en proteger los datos, en vez de proteger los dispositivos, como venía siendo común hasta ahora; este cambio será debido a la tendencia hacia el *outsourcing*, la consultoría estratégica, y el incremento de relaciones con terceros. Adelantó algunos datos, como que la externalización mediante *offshoring* crecerá a un 25% en el 2010 en Europa, respecto al 20% actual; siendo un 23% la previsión para los Estados Unidos en este año próximo.

Andrew Jaquith

Por ello recomendó la realización de estrategias de protección de datos que no dependan de los dispositivos, mediante diversas fórmulas; en unos casos accediendo de forma remota a la información, mediante clientes ligeros; en otros casos con datos replicados y la posibilidad de eliminar los datos en caso de pérdida o robo; o bien utilizando procesos de información en "burbujas" de seguridad (con virtualización por ejemplo); bien protegiendo los datos con plantillas de confidencialidad de la información dentro del propio documento o, por último, realizando una monitorización de la red, permitiendo o bloqueando el intercambio de datos con marcas de agua de tipo *hash* y *fingerprint* y tecnología DLP. "Focalizarse en la protección de los datos, no en la de los dispositivos permite a los CISOs decir sí a las nuevas oportunidades emergentes, como el uso del *cloud computing*, que se está incrementando exponencialmente", indicó.

Jaquith presentó la clasificación de Forrester sobre *cloud computing*, en una torre de cuatro capas, desde de la infraestructura física **IaaS** hasta la prestación de servicios basados en web y el **SaaS** *(Software as a Service)*. Indicó, sin embargo, que los CISOS son aún cautelosos respecto a la nube, pues les preocupan las cuestiones de seguridad, privacidad y adecuación legal y normativa. Para resolver los miedos relativos a cada uno de los riesgos, sugería una posible solución. Además, los análisis muestran la tendencia de los responsables ejecutivos de las empresas (directores financieros, gerentes, servicios jurídicos…) a influir cada vez más en las decisiones de tecnología, que necesitan que esté perfectamente alineada con la estrategia empresarial. Además, problemas intrínsecamente tecnológicos se han convertido en problemas de negocio, como es el caso del fraude, la propiedad intelectual, el espionaje industrial, el gobierno corporativo, la retención de empleados, la integridad del negocio, e incluso la ética corporativa. Algunos de los consejos que dio a los presentes: "El Plan del año pasado conviene revisarlo y actualizarlo en aras de alinearlo con el negocio"; "Ser proactivo en la gestión de riesgos, y aplicar métricas y Gobierno Corporativo". **El analista** concluyó que las competencias clave del nuevo CISO incluyen ser capaz de darle la vuelta al concepto tradicional de seguridad, mirando al futuro respecto a las funciones que serán necesarias para este replanteamiento de la seguridad. "*La nube será lo mejor que le habrá podido ocurrir a la industria de seguridad*", llegó a pronosticar **Andrew Jaquith** adelantando el motor de dichos cambios evolutivos.

El siguiente ponente, **Carlos Alberto Saiz,** Vicepresidente del **ISMS Forum Spain**, adelantó los próximos proyectos y actividades de ISMS Forum Spain, que cuenta ya con 90 empresas asociadas y 600 profesionales dados de alta. Anunció la fecha de la siguiente edición, VII Jornada Internacional, para el **25 de mayo de 2010 en el Palacio de Congresos de Madrid**. En ella, entre otros temas, se hablará de cómo vincular competitividad, innovación y tendencias en el mundo de la seguridad y cómo la tecnología, CIOs y CISOS pueden aportar al negocio. También anunció que se realizaría una segunda edición del curso de Análisis de Riesgos para la primavera de 2010. Comentó otra de las recientes actividades de ISMS Forum, la creación del **Data Privacy Institute**, foro de referencia en la materia y abierto tanto a personas como a empresas, que ha puesto en marcha la primera **Certificación Española en Privacidad** (CDPP) que celebrará en junio de 2010 su primer examen de certificación, si bien existirá un esquema de "Grandfathering" para profesionales. Esta certificación, denominada "**Certified Data Privacy Professional**" está orientada a profesionales abogados, consultores, CISOs, responsables de LOPD en las Administraciones Públicas, etcétera. Además, el DPI prepara su **I Foro sobre Privacidad de Datos**, que se centrará en el **sector sanitario**, y que se celebrará con la colaboración del Consejo General de Colegios de Médicos de España el **21 de enero de 2010**, en Madrid.

Otra de las iniciativas que se lanzará en breve es el DLP Forum, un sitio web satélite de ISMS Forum para la promoción e intercambio de experiencias relacionada con la tecnología Data Leak Prevention. ISMS Forum trabaja también en otro portal, esta vez divulgativo, que servirá para fomentar buenas prácticas de seguridad entre todo tipo de usuarios que quieran conocer las medidas básicas que pueden tomar para proteger sus datos y sus equipos. Este proyecto, denominado "Protege tu información" cuenta con la ayuda del Ministerio de Industria, Turismo y Comercio, a través del Plan Avanza 2. Su presentación en sociedad está prevista para finales de 2010.

Nils Puhlmann

A continuación, el experto en Cloud Computing **Nils Puhlman**, Cofundador de ***Cloud Security Alliance,*** impartió una conferencia titulada *"A New Landscape to Protect: What's Coming Up on Information Security Challenges?* En ella, Puhlmann repasó los profundos cambios en hábitos de consumo y formas de trabajo que están cambiando por completo el enfoque que deben abordar los responsables de seguridad de la información de las organizaciones, que deben centrarse ahora en la protección de los datos (mientras que hasta ahora lo hacían en la de los dispositivos). El consumo de productos y tecnologías pensadas inicialmente para el usuario doméstico -como las redes sociales, los portales para compartir y publicar contenidos o los juegos en línea- se ha trasladado a las empresas (y al mismo tiempo se están sofisticando para cubrir sus necesidades y expectativas), lo que conlleva nuevas amenazas para la seguridad. Los nuevos profesionales que se incorporan a las compañías son los principales implantadores de esta migración, puesto que han crecido usando esta tecnología y los *gadgets* que la acompañan (y que se han convertido en herramientas para incentivar la creatividad y la productividad). Así, Puhlmann citó a numerosas grandes compañías que están usando sitios como YouTube o Second Life

para invertir, vender o promocionar sus productos con cifras de resultados muy llamativas. Pero este fenómeno -unido a un número cada vez mayor de dispositivos móviles que escapan al control de las compañías- trae consigo también la sofisticación de ataques con troyanos y otros tipos de malware, así como de perfeccionadas técnicas de ingeniería social que se apoyan en redes sociales como Facebook o Twitter para su difusión. **Puhlmann** enumeró alguna cifras sobre los millones de usuarios de ebay (85,7 millones en 2008), Zynga (60 millones), Google Voice (1.419 millones de usuarios, un 40% de uso diario), Skype (521 millones de usuarios registrados) además del dato de crecimiento del 700% anual de minutos invertidos en FaceBook. Por supuesto, el uso de estas redes trae consigo riesgos como la pérdida de privacidad, el robo o suplantación de identidades o la distribución masiva de malware. Innovación, agilidad, rapidez y colaboración son los pilares sobre los que deben trabajan los responsables de la seguridad de la información y la privacidad de datos, dijo Puhlmann. "Lo malo –apuntó- es que todas estas características están ya muy presentes en el lado de "los malos", mientras que la cultura empresarial a menudo rema en dirección contraria, puesto que las empresas no han asimilado aún esa cultura de la cooperación y de hacer frente común a las amenazas".

El juego online, los mundos virtuales y las redes sociales tienden a converger, con los nuevos riesgos que ello acarrea. Puhlmann recordó que el mundo virtual SecondLife tiene 16 millones de residentes registrados, y que en un solo día del pasado mes de agosto cambiaron de manos, en este mundo virtual, 120 millones de dólares "virtuales". Estas transacciones virtuales tienen su impacto en el mundo real, pues allí empresas como Nike y Adidas venden calzado real; Pontiac y Toyota venden coches reales, se alquilan servicios de seguridad y servicios de escort, y los perfiles se compran y venden en eBay con dólares reales. Este fenómeno de venta de perfiles, denominado *Gold Farming*, tiene como consecuencia un llamativo fenómeno de explotación, al más puro estilo esclavista, principalmente en el sudeste asiático.

Puhlmann planteó la problemática que plantea la velocidad de infección respecto a la velocidad de defensa de estas amenazas. "Cada 4-5 segundos se descubre un nuevo sitio propagador de *malware*", comentó. De las páginas afectadas, un 85% se encuentra en sitios web legítimos que han sido hackeados. Los ataques se incrementan de forma transversal por las redes sociales, llegando a los puestos de usuario. Ofreció datos sobre los 14 millones de PCs que se comprometieron por "*botnets*" en el segundo trimestre de 2009, un incremento del 16% sobre el trimestre anterior. Sobre los 150.000 nuevos ordenadores vendidos, fueron infectados un 20% de cada uno de ellos. Según el número de *bots* continúa creciendo, se empieza a ofrecer *Malware as a Service* para controlar a todos estos equipos. Aparte de que la protección antivirus no es suficiente, al requerirse entre 2 y 5 días para cada nueva firma, y más de 14 días para analizar y contrarrestar nuevos algoritmos de infección. El crimen libera nuevo *malware* más rápido que las actualizaciones de sistema antivirus, y cada vez hay más mutaciones.

¿Cómo afecta esto a los nuevos planteamientos de Seguridad TIC? En el viejo mundo, la gente utilizaba lo que le ofrecían, la infraestructura IT era estática, las webs se enlazaban unas a otras... Sin embargo, en el nuevo mundo, las tecnologías funcionan casi en el "Just-in-time", crecen los servicios SOA, la computación en la nube, los modelos de pago por uso), todo ello produce un adelgazamiento en las infraestructuras y potencia los entornos ágiles y las infraestructuras flexibles. El nuevo Internet trata sobre la gente, acerca de cómo ésta hace uso de Internet y cómo se interconectan entre sí. De esta forma, la seguridad es un paraguas común para todo ello adaptándose a las tendencias de agilidad y velocidad.

¿Cuál es la parte mala en todo esto? **Nils** realizó un juicio crítico con el inmovilismo en la visión tradicional de la seguridad. Para los profesionales de la seguridad, la adecuación normativa y legal es el nuevo estándar, la nueva línea base. Solemos ser reacios al cambio y adversos a estructuras flexibles. Los fabricantes, por su parte, ofrecen soluciones para problemas antiguos, cada vez son menos

y menos innovadores y comprenden la seguridad principalmente desde el punto de vista técnico. Nils sentenció que “los malos tiene todas las ventajas sobre los buenos; y además que son más participativos y colaborativos", finalizando su intervención con la idea de que "el mayor error que ha cometido la industria es que hasta ahora ha trabajado en solitario".

Un debate posterior (en la imagen), en el que participaron **Vicente Aceituno**, Presidente de **ISSA Spain**; **Manuel Cortés Márquez**, de **Accenture**; **Peter Stremus**, de **IBM ISS Bélgica** y **Bart Vansevenant**, Director de estrategia de **Verizon Business Bélgica,** moderado por Nils Puhlmann, sacó a la luz algunos temas polémicos. Se cuestionó, por ejemplo, si el mercado está realmente evolucionando y si la industria se adapta o no a las nuevas realidades. Así, aunque las tecnologías de la información cambian, los medios, los canales de comunicación, los problemas y las soluciones parecen ser las mismas. Se planteó que el negocio actual de las redes sociales y de consumo reside en la publicidad, no en los millones de usuarios registrados. Se apostó por un proceso gradual de concienciación en seguridad de la información, como un método más eficaz, en lugar de “endurecer” la legislación con sanciones ejemplares.
Se cerró el debate comentando que el sector de la Pequeña y Mediana empresa constituye una gran oportunidad para hacer grandes cosas en seguridad con un pequeño esfuerzo.

La última intervención de la mañana fue la de **Oleg Mikhalsky**, director de Desarrollo de Negocio de Infowatch (Rusia) y se centró en la identificación de problemas y retos de la protección de la información sensible y la prevención de fugas de datos externas e internas mediante la tecnología DLP. Una de las anécdotas del día fue la pregunta al auditorio sobre aquellas empresas que están realizando actualmente implantaciones relacionadas con tecnología Data Loss Prevention. A pesar de que gran parte del sector coincide es que es uno de los nuevos puntales de generación de negocio, con tendencia actual en inversiones de seguridad con gran crecimiento, solamente un puñado de asistentes alzó la mano, lo que introdujo una paradoja entre las expectativas del mercado y los proyectos actuales que en realidad se están acometiendo en la materia.

Oleg Mikhalsky

Después del almuerzo, la conferencia de **Marcos Gómez Hidalgo**, Subdirector e-Confianza del **INTECO**, abordó su experiencia sobre los servicios y oportunidades para la Pyme española en Seguridad de la Información. Comenzó enumerando las actividades del **INTECO** respecto a Gestión de Incidentes de Seguridad, Centro Demostrador, Observatorio de la Seguridad, etc; y las perspectivas de extender el proyecto para darle continuidad a largo plazo. Resumió el objetivo de **INTECO** en el hecho de formar y concienciar a la PYME en materia de seguridad informática, especialmente en Sistemas de Gestión de Seguridad de la Información y en la implantación de los estándares ISO 27001. En resumen, dar un impulso al SGSI en el tejido industrial español, ejerciendo de tercero de confianza en la industria.

Marcos comentó, respecto al comportamiento medio de las micropymes en materia de seguridad, que su perfil de comportamiento es similar a cómo funcionaría un internauta individual; teniendo en cuenta el dato de que existen en España 3 millones de PYMES y 24 millones de internautas. El 30% de los encuestados dice tener una deuda pendiente con el hecho de ponerse al día en seguridad; aparte, un 50% de los encuestados está familiarizado con términos como "*phishing*"; aunque desconocen otros como *malware*, *troyano* o *keylogger*. **Marcos Hidalgo** finalizó su intervención con otros datos interesantes; como que **INTECO** atiende unas 20.000 incidencias de seguridad anuales, de las que un 30% se refieren al fraude por internet.

Francisco Hernández y Manuel Vázquez

Pedro Pablo Pérez

A continuación se inició el debate de la tarde, que fue uno de los más interesantes y entretenidos del día, salpicado de anécdotas, chascarrillos y algo también de polémica; además de llegar a consensos, y conclusiones muy productivas. En este debate intervinieron **Francisco Hernández Guerrero**, Fiscal del Servicio de Criminalidad Informática del Ministerio Fiscal, **Rafael San Miguel Carrasco**, de la red social Yumei, **Pedro Pablo Pérez**, Gerente de Marketing de Seguridad de Telefónica España y **Manuel Vázquez López**, Jefe de la Brigada de Investigación Tecnológica de la Comisaría General de Policía Judicial; moderado por **Antoni Bosch,** Director del Data Privacy Institute de ISMS Forum.

Pedro Pablo Pérez habló de las dificultades de detección y respuesta al crimen electrónico en redes sociales, derivadas de la captación, la acción a distancia y la internacionalización. **Manuel Vázquez**, basándose en su experiencia en la Brigada, contó que la lucha contra el cibercrimen se juega hoy en un ámbito global. "La acción preventiva suele corresponder a las empresas y organizaciones, pero cuando los controles fallan, es cuando entra en escena la acción policial", comentó. Añadió que las redes sociales han servido para iniciar movilizaciones, incluso a veces causas nobles; pero muchas otras veces se ha utilizado para la comisión de delitos. Los menores, por ejemplo, no tienen la personalidad formada, por lo que son objeto de delitos a través de estas redes sociales, como es el caso del *Cyberbulling*. Las redes sociales son un elemento de nuestro tiempo; pero la tecnología va más rápido que las consideraciones morales y legales. El debate cobró especial interés a raíz de comentar el éxito de inscripciones de menores en el portal

de gestión de talentos del espectáculo **Yumei**, tras participar en el casting de un conocido programa de televisión, según comentó **Rafael Sanmigue**l. En este punto se abrió un interesante debate sobre legalidad, moralidad y responsabilidad de los padres, con aportaciones de todos los componentes de la mesa, y sentando cátedra en los temas por la autoridad y calidad de los ponentes. Por ejemplo, **Francisco Hernández** realizó una interesante reflexión sobre el hecho de que "si se otorga capacidad a los menores, hay que ser coherentes en las formas de persecución en las redes sociales", y también con respecto a la responsabilidad de los padres. **Manuel Vázquez** comentó el hecho de que se dan demasiadas pistas para facilitar la ingeniería social; es posible por ejemplo mediante fotografías en diferentes situaciones, generar el perfil psicológico y anímico de una persona. Aunque fue ecuánime en la utilización de estas redes: "prefiero que mis hijos estén en una red social que viendo determinados programas de la televisión que transmiten valores incorrectos" concluyó, como resumen de su planteamiento.

Rafael Sanmiguel

Pedro Pablo Pérez recordó, respecto a la responsabilidad de los padres y la capacidad de filtrado de acceso a Internet, que los padres pueden contratan para sus hijos un control parental de la líneas ADSL. **Antoni Bosch** aprovechó el debate del filtrado de acceso para introducir el tema del paquete europeo de telecomunicaciones, lo que hacía cada vez más intenso el debate. A pesar de los puestos de responsabilidad y los cargos que ocupaban representando a sus respectivas organizaciones, los ponentes no dudaron en "mojarse" y entrar al trapo en la cuestión. **Francisco Hernández** sugirió que, tal vez, si las empresas de comunicaciones estaban inflando las necesidades de consumo de ancho de banda con grandes velocidades y orientadas a la descarga masiva; tal vez no debieran pretender cortar el acceso por descargar determinados contenidos. Todos los ponentes coincidieron en que existe un nuevo pacto social; en el que ni las empresas deben pretender extralimitarse en las restricciones, ni la sociedad debe por su parte parapetarse en posiciones radicales de desprecio a toda regulación. **Manuel Vázquez**, matizó que desde la Policía nunca se han realizado investigaciones de forma directa contra usuarios de redes P2P, aunque sí sobre enlaces y propietarios de páginas. A lo largo del debate fueron varias las ocasiones en las que surgió la polémica, sin miedo a expresar opiniones. Se comentó que "cualquier incidente informático se magnifica, porque es un asunto que vende. El problema es que los políticos hacen más caso a la prensa que a sus asesores, porque representa la opinión de los ciudadanos." En general, el debate de la tarde fue muy ameno, pero a la vez muy profundo y uno de los platos fuertes del día.

El resumen y cierre de la jornada fue responsabilidad de **Gianluca D'Antonio**, que intervino esta vez en su doble vertiente como presidente de **ISMS Forum** y como CISO del Grupo FCC. Comentó la herramienta que utiliza su empresa, un informe de vigilancia que reúne todas las publicaciones donde se hace referencia a la empresa, su imagen y reputación corporativa, tanto para bien como para mal; resaltó su utilidad para poder gestionar los riesgos que esto conlleva. Al respecto, comentó que la reputación en las redes sociales puede afectar a las distintas economías, pues orienta el consumo de los clientes como ha ocurrido con alguna empresa o producto. Insistió en que la seguridad de la información se compone hoy de muy diversas funciones transversales que van mucho más allá de la tecnología. El CISO tiene ante sí, por todo ello, enormes retos.