ISMS: Conclusiones del IV Foro de la Ciberseguridad

El IV Foro de la Ciberseguridad organizado por ISMS Forum Spain, y al que acudieron 200 asistentes, reunió en el Auditorium CaixaForum Madrid a grandes expertos del mundo de la Ciberseguridad, tanto nacionales como internacionales, para analizar, estudiar y debatir sobre el impacto que pueden llegar a tener las ciberamenazas en el ámbito empresarial, así como la necesidad de concienciar a empresas y usuarios del valor que tiene la protección de uno de sus activos más importantes: los datos.

La inauguración del foro corrió de la mano de Erka Koivunen, ex director del CERT finlandés, quien a través de su ponencia «El poder del Hacking empresarial» analizó la importancia de la Ciberseguridad en las grandes empresas. Koivunen inició la ponencia dando su visión particular sobre qué es el hacking y añadió los tipos de hackers tradicionales existentes, a los que añadió un nuevo tipo de hacker: «el ejecutivo empresarial». Para describir este último tipo de hacker se centró en uno de los casos más actuales del panorama internacional: «El caso Volkswagen» donde explicó el autohacking que esta empresa realizó para conseguir ahorrar en inversión. Tras la ponencia inaugural en la que Erka Koivunen explicó el papel que la Ciberseguridad tiene en las grandes empresas se dio paso a los talleres prácticos «Análisis y gestión de nuevas amenazas», donde se analizaron en detalle las últimas ciberamenazas y sus posibles soluciones. Para ello se contó con la colaboración de cuatro de los principales players del Sector como: Federico Dios, Service Line Manager, Akamai; Alberto Cita, SE Manager, Southern Europe, Blue Coat; Renaud Bidou, Seur Technical Director, Trend Micro; y Carlos Fernandez, Cybersecurity Technical Leader, Symantec.

Federico Dios, explicó la existencia de un nuevo tipo de amenaza de denegación de servicios que ha tenido una gran relevancia en el último año: el XOR DDos, un tipo de ataque que afecta a máquinas Linux, actúa a través de fuerza bruta y que es bastante complicado de eliminar. Alberto Cita centró su taller en explicar las técnicas que se utilizan en Malvertising. El Malvertising es una técnica de distribución de malware que combina de una forma única publicidad web con los Exploit Kits.

Renaud Bidou, por su parte, analizó algunos de los malware bancarios más importantes hasta el momento y destacó el «Pkybot», un malware bancario reciente que comenzó a operar a principios de octubre y que todavía se mantiene activo. Se trata de un conjunto de herramientas en evolución dirigidas a navegadores web que aprovechan vulnerabilidades recientes que se encuentran en plugins y que, además, es capaz de detectar los antivirus, para así, no ser descubierto.

Por otro lado, el IV Foro de la Ciberseguridad contó con la presencia de Carlos Fernández para poner fin a los talleres prácticos, quien se centró en explicar una amenaza ya popular: Cryptolocker, un ataque que cita ficheros de datos residentes en máquinas infectadas y exige el pago de una suma de dinero. Tras las cuatro intervenciones prácticas, tuvo lugar la tercera sesión del encuentro de la mano de Emmanuel Roeseler, Security Systems Sales Manager Spain, Israel y España de IBM Software, quien con su ponencia «La Seguridad es tan robusta como su eslabón más débil» analizó la importancia de concienciar a los usuarios de los peligros que se encuentran detrás de muchas aplicaciones de dispositivos móviles. Roeseler considera a los usuarios ese «eslabón débil» puesto que, muchas veces por falta de conocimiento o por no entendimiento, aceptan términos y condiciones que sobrepasan los límites de la Ciberseguridad. A continuación tuvo lugar la Mesa Redonda «¿Ciberseguridad sin Continuidad?» donde participaron: Alfonso Martínez, experto en Resiliencia, Intel Security; Manuel Sicilia, jefe de la Sección de Análisis del Servicio de Ciberseguridad y OCC, CNPIC; Enrique Ríos, jefe de Planificación del departamento de seguridad corporativa, Abertis; y Rodrigo Jiménez, Security advisor, Necsia; todo ello moderado por Javier Carmona, director de Seguridad de la Información y Comunicación, Iberdrola. Todos ellos