SEGURIDAD DE LAS TIC EN EL AMBITO FINANCIERO

La Fundación Círculo de Tecnologías para la Defensa y la Seguridad llevó a cabo 26 de junio un seminario sobre la seguridad de las TIC en el ámbito financiero.
Con la bienvenida a todos los asistentes del representante y anfitrión de la Caixa Pedro Esteban Cobreros, director adjunto de seguridad de la entidad, comenzó el acto. En sus palabras introductorias citó que los ciberincidentes consumen el 1% del PIB mundial y que el 65% de las empresas solo tiene un experto en esta materia entre sus empleados. La escasez en materia de personal ha sido una constante durante toda la jornada. Las empresas deben invertir en biometría, conmutación cuántica, cifra e inteligencia artificial, para que todos los sistemas que tratan con las tecnologías de la información tengan la capacidad de poder autenticarse y evitar o minimizar las amenazas y eliminar los daños derivados hacia la reputación de las entidades financieras.

Nuestro presidente Vicente Ortega Castro subrayó la importancia de las TIC, su rápida y trepidante evolución y a la vez la de los delitos asociados a esta expansión de le tecnología. Quedó de esta forma abierta la jornada que fue creciendo en interés partiendo desde los aspectos básicos y conceptuales de la ciberdefensa hasta las últimas tendencias empresariales en materia de ciberincidentes financieros y su contra medidas.

El Departamento de Seguridad Nacional, representado por Mar López Gil, jefa de la oficina de ciberseguridad, explicó el sentido de la nueva estrategia nacional de ciberseguridad y la creciente importancia de la banca *on-line*. La Estrategia Nacional es fruto de la decisión del presidente de gobierno quien encargó al secretario de la Comisión de Seguridad Nacional, Félix Sanz Roldán su elaboración. En esta nueva estrategia han participado las comunidades autónomas y los representantes de las comisiones del Congreso y del Senado. Esta nueva estrategia es menos técnica, pero es más política y más social. Está adaptada a la norma NIS de la UE.

Básicamente se estructura en unas ideas de propósito general, unas líneas de acción y unas medidas a adoptar para mejorar la situación actual y establecer un futuro más claro en la seguridad de los procesos relacionados con las TIC. También se establece en este marco un Foro Nacional de ciberseguridad.

Cabe citar también la constitución de una Comisión Permanente que permitirá establecer medidas correctoras. Finalmente la estrategia tiene como reto en el próximo escenario, con más de 4.000 millones de usuarios y más de 20.000 millones de terminales, de adecuarse a la tecnología 5G para poder defenderse de los numerosos ataques que el sector está teniendo, permitiendo su resiliencia y eficacia a través de la unidad de acción de toda la Administración.

Posteriormente el cuerpo Nacional de Policía y la Guardia Civil representados por el inspector Antonio López y el Comandante Oscar de la Cruz, explicaron que el número de atracos clásicos pasaron del 204 en 1.998 a la cifra de 22 en 2018, aunque esto no quiere decir que el atraco a las entidades financieras está disminuyendo, simplemente está cambiando de método. Las dificultades legales son un hecho, subrayándose que la suplantación de identidad no es un delito a día de hoy, a no ser que haya ánimo de lucro en ella, con lo que se dificultan las medidas coercitivas contra esta nueva ola de suplantadores de identidades. Las nuevas tendencias deben ir hacia la mejora de la política de acreditaciones, autenticaciones, operaciones de inteligencia artificial y cooperación entre entidades bancarias.

Los fraudes informáticos han ascendido a 88.854 en el año 2018, han aumentado un 47 % respecto

a años anteriores y las cifras siguen en ascenso. Son delitos asimétricos separados en tiempo y en espacio, su ocultación es fácil y por regla general la cooperación internacional es necesaria para evitarlos, descubrirlos e imputarlos. Los informes de ciberdelincuencia están en la red, pero lo que las Fuerzas y Cuerpos de Seguridad del Estado recomiendan como medidas preventivas aumentar los procedimientos cifrados y la formación de la población con carácter general en estas materias.

Cierto es que el delincuente utiliza productos que se encuentran en la red, que se utilizan *mulas* para ocultar los orígenes de los beneficios, pero la cooperación internacional consigue éxitos evitando ataques organizados desde otros países y con intervalos de tiempo diferentes. La proliferación de criptomonedas, bitcoins y otros sistemas dificultan la labor de las Fuerzas y Cuerpos de Seguridad del Estado aunque la vigilancia es constante.

La Caixa por su parte, explicó como su equipo *red team* dirigido por Alba Barreiro experimenta las posibilidades de penetrar en sus sistemas de ordenadores. A través de estos experimentos organizados se proponen mejoras para la autoprotección creando un círculo de trabajo que se podría resumir como una mejora de la defensa de la entidad a través de descubrir como penetrar en sus sistemas TIC. El análisis de vulnerabilidades es constante y las medidas para mitigarlas también.

El director de la Escuela Técnica Superior de Ingenieros de Telecomunicación, Félix Pérez Martínez coordinó una mesa redonda con representantes de las empresas del sector GMV, IECISA y el grupo Oesia y Telefónica. El mercado de la seguridad financiera está en alza y la falta de personal especializado sigue siendo un problema. Las empresas trabajan para asegurar la cadena de valor financiera y la transformación digital supone un avance pero también un riesgo si no se acomete de forma racional.

GMV abogó por el factor sociológico de la información bancaria y el traslado de las transacciones al sector de los terminales móviles, lo que supone un nuevo reto para las entidades financieras.
El Corte Inglés, con una decidida defensa de sus clientes, recordó que la reputación de las empresas tiene un valor incalculable y por ello la defensa de los intereses pasa por la de su información y sus transacciones económicas.

Pedro Pablo Pérez de Telefónica, nos recordó que el miedo a las nuevas tecnologías no debe existir ya que la tecnología de 5G que viene ya se está experimentando en España y es más segura que los anteriores sistemas, ya que sus enlaces están cifrados en todo momento, pero el riesgo no es el transporte de la información, el riesgo verdadero está en el tratamiento de la información. Los operadores son meros transmisores de las señales y su trabajo es permitir el transporte de la señal, ya que los contenidos son responsabilidad de los usuarios, los propietarios de la información.

Concluía el acto el director del CCN, señalando que es el sector financiero el que más gasta en ciberseguridad. Está demostrado que el 95% de los incidentes está dirigido contra este sector, quedando muchos problemas a resolver, las técnicas de infección de malware están evolucionando y ya hay APT,s *Advanced Persistent Threat* (Amenaza Avanzada Persistente), que inyectan códigos dañinos en la memoria de los dispositivos, lo que los hace más difíciles de detectar.

Los pilares de la defensa del sector deben residir en varios factores:

- Disponer de técnicos apropiados. Mano de obra especializada.

- Intercambiar información en los foros específicos del sector. Compartir información sobre los tipos de ataques es esencial para evitar su repetición.

- Los reguladores del sector deben impulsar normativas reguladoras que eviten la proliferación de los ataques. El ENS (Esquema Nacional de Seguridad) puede ser un ejemplo de la política a seguir en el mundo empresarial.