DE LAS LECCIONES APRENDIDAS EN MESI 2.0 AL HORIZONTE DE LA ENSEÑANZA EN CIBERSEGURIDAD

Conferencia magistral Tercer Taller Iberoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información TIBETS 2015. Quito, 12 de noviembre de 2015

NECESIDAD DE UNA NUEVA FORMACIÓN EN SEGURIDAD: CIBERSEGURIDAD

Seminario Internacional de Ciberdefensa y Seguridad en las Comunicaciones. Quito, 10 de noviembre de 2015

Documento de apoyo a las diapositivas presentadas en sendas conferencias
Figuras, tablas y gráficas, las encontrará en la presentación pptx (ver bibliografía)

Ponente: Dr. Jorge Ramió Aguirre
Profesor Titular UPM, director Criptored, intypedia, Crypt4you, MESI, Thoth

Keywords*: seguridad informática, seguridad información, protección información, enseñanza universitaria seguridad, proyecto MESI, ciberseguridad.*

1. Introducción

La enseñanza, universitaria o no, de los conceptos relacionados con la seguridad y protección de los equipos y sistemas informáticos, así como de la protección de la información y los datos, sean estos corporativos o personales, ha pasado por diferentes etapas en las últimas cuatro décadas. Esto es debido al tipo de amenazas existentes en este entorno -el digital- que por definición es inseguro y que, por su naturaleza, es mutante, cada vez más sofisticado y con resultados más dañinos. Además, el importante impacto que estas amenazas tienen en la continuidad del sistema, nos plantea la necesidad de contar con ingenieros y técnicos cada vez más capaces de poder definir y seguir políticas de seguridad y, en su caso, ser capaces de afrontar serios incidentes de seguridad en el entorno digital a los que se enfrentan tanto las organizaciones como los particulares.

2. ¿Una nueva formación?

Las características de estas amenazas según la década en que nos ubiquemos, han influido en los perfiles de asignaturas que se han ofrecido en las titulaciones relacionadas con la ingeniería en informática, la ingeniería de telecomunicaciones y otras titulaciones afines en la universidad española. Es así como las primeras asignaturas desde los años 80 a los 90 apostaban fuertemente por un perfil mayoritario de la criptografía; ya en la década de los 90 comienzan a aparecer asignaturas de gestión de la seguridad y seguridad en redes, y en la primera década del siglo XXI se acrecienta la importancia de estas dos última líneas, disminuyendo la primera, irrumpiendo además la temática legislativa. Por último, en el ecuador de la década actual nos encontramos además con asignaturas de forensia computacional, hacking ético y delito informático, aunque eso sí sólo de manera anecdótica al tratarse de casos aislados.

En España hemos asistido en las últimas tres décadas a un incremento espectacular de la oferta de estas asignaturas de seguridad en las universidades españolas, pasando de las 37 asignaturas que se ofrecían en el año 1999 a las 230 asignaturas dedicadas totalmente a la seguridad en el 2015, más otras 120 cuya

dedicación es parcial. En sus perfiles se han abarcado desde los inicios de la seguridad informática, concebida como aquella centrada en aspectos de la seguridad que inciden directamente en los medios informáticos en los que la información se genera, se gestiona, se almacena o se destruye, siempre desde el punto de vista tecnológico de la informática y de la telemática, hasta la seguridad de la información, en donde se tienen en cuenta además aspectos sistémicos de la gestión de esa seguridad, como sería el caso de las políticas y planes de seguridad que toda organización debe plantearse, la orientación de esta seguridad hacia la continuidad del negocio, así como su adecuación al entorno legal y al cumplimiento de las normativas internacionales.

En las universidades españolas estos dos aspectos se han cumplido de manera exitosa en su oferta formativa de grado, con esas 230 asignaturas dedicadas exclusivamente a la seguridad, así como a los 26 másteres de seguridad informática, de la información y ciberseguridad que se ofrecen actualmente.

Sin embargo, en los últimos 5 años, esto es prácticamente desde el inicio de esta última década, venimos asistiendo a un cambio radical en el escenario de las amenazas que se ciernen sobre nuestros equipos, sistemas industriales, en la red global, en los países y en las personas, incluso peligrando su integridad física, que recomiendan por tanto hacer un nuevo esfuerzo imaginativo docente y adaptar las futuras enseñanzas a este nuevo escenario de manera que permita tratar de forma adecuada un entorno que se ha venido a llamar ciberseguridad, si bien esta palabra tiene diferentes matices e interpretaciones.

Para poder entender por qué hemos llegado a la situación actual, en donde la línea que separa el ciberdelito o cibercrimen con la del ciberterrorismo es muy delgada, y por tanto de máxima preocupación para la protección de las infraestructuras críticas de nuestras ciudades, veremos a continuación cómo se han manifestado estas amenazas en las últimas cuatro décadas.

3. La seguridad según las décadas

El concepto y la importancia de la seguridad informática en el desarrollo y evolución de la sociedad han pasado por diversas fases en estos últimos 35 años. Podríamos dividir esos años de una manera simplista en 4 bloques, que forman a su vez cuatro décadas, en las que esta seguridad ha influido de una manera diferente y especial en cada una de ellas, acorde con el desarrollo de la informática, las redes y el mundo interconectado.

3.1. Década de los 80

En la década de 1981 a 1990, la percepción de la seguridad y nuestras preocupaciones como usuarios de ordenadores se centraban en estos aspectos:

a) Una seguridad asociada al equipo, normalmente del usuario final.
b) Aparecen programas malignos que inciden en la calidad de la producción, el software o el hardware dejan de funcionar.
c) La amenaza principal se centra en el equipo personal, que normalmente era caro y en muchos casos único, con el agravante de que hay pocos expertos que puedan reparar ese mal funcionamiento. Existía además escasa información y mucho menos de fácil acceso.
d) Podríamos definir nuestro estado emocional como de alarma personal; el afectado soy yo, mi ordenador, es mi dinero.
e) Con todo lo que esto podía significar para el usuario afectado, la criticidad de estas amenazas sólo puede considerarse como baja.

f) La imagen que podemos asociar a esta década es el mítico PC de IBM con monitor verde y con dos disqueteras, aunque ya a mediados de la década se podía contar con un disco duro de sólo unas decenas de Megabytes de capacidad.

3.2. Década de los 90

Esta década desde 1991 al año 2000, se caracteriza por:

a) Una seguridad asociada a redes locales que me entregan servicios y me facilitan el modo de trabajar, mucho más cómodo y productivo al existir una filosofía de cliente servidor.
b) Nos preocupaban en aquel entonces los gusanos y programas malignos, que inciden en la productividad y en la disponibilidad del software y/o del hardware de la red y que podían dejan de funcionar.
c) Comienza a hablarse de robo de datos, de espionaje industrial.
d) La amenaza principal es ahora mi red local; si se cae no puedo seguir trabajando con el PC de mi puesto de trabajo, pues los programas son más complejos y requieren de una mayor velocidad de proceso y capacidad de almacenamiento que la de mi PC.
e) El estado emocional pasa a un nivel de alarma corporativa; los afectados pueden ser muchas personas, todo un departamento, toda una empresa, etc., por lo que ahora la criticidad de la amenaza podríamos definirla como media.
f) Una imagen característica de esta década es la de una red corporativa, normalmente del tipo LAN y un gusano propagándose por la red.

3.3. Década de los 00

Del año 2001 al 2010 podemos indicar:

a) Una seguridad asociada casi por completo a Internet, que me entrega servicios y me facilita el trabajo. Los clientes también generan información, inicio del concepto nube.
b) Aparece el malware generalizado, en diferentes formas, se hace común el robo de datos, el espionaje industrial, el soborno, la exfiltración de información sensible, etc. Comienza a hablarse con propiedad de delito informático, aparece la deep web.
c) Internet facilita el envío masivo de malware y facilita las intrusiones a los sistemas.
d) La amenaza principal proviene y está en Internet, que somos todos, y si ésta se colapsa ya no podemos trabajar; mis aplicaciones y muchos de mis datos están ya en la nube.
e) Ahora el estado emocional es el propio de una alarma colectiva; la criticidad es alta.
f) La imagen que podemos asociar a esa década es la de las redes sociales como YouTube, LinkedIn, Twitter, Facebook, etc., buscadores como Google, clientes de correo como Gmail, espacios de almacenamiento, etc., un mundo interconectado.

3.4. Década de los 10

En los 5 años que llevamos de esta última década, las amenazas han cambiado nuevamente y podemos vislumbrar un futuro mucho más complejo y preocupante:

a) La seguridad está y estará asociada al Internet de las cosas IoT, que nos entregará todo tipo de servicios y que me permite (ya no sólo facilita) trabajar y vivir cómodamente. La filosofía cliente servidor emigra hacia una nube generalizada.
b) Se comienza escuchar de vulnerabilidades y ataques a través de IP a sistemas de control industrial controlados por sistemas operativos SCADA.

c) Los ataques además de generalizados se vuelven dirigidos, hechos a medida, hay un aumento del ciberdelito, secuestro de ordenadores, deep web, un cibercrimen cuya línea de separación con el ciberterrorismo es muy delgada, ciberejércitos declarados, hostilidades entre países en el ciberespacio, espionajes a gran escala reconocidos.
d) La amenaza principal son ahora las infraestructuras críticas de los países; si estas IICC dejan de operar, pueden causar graves perjuicios a la población, incluso costar vidas humanas.
e) El estado emocional en este caso, y en el que ya nos encontramos, es de alarma mundial; está en juego la seguridad de un país o de varios países, por lo que la criticidad es muy alta.
f) Imágenes habituales de esta situación las encontramos en el Internet de las Cosas IoT, con todo tipo de aparatos electrónicos y electrodomésticos controlados a distancia desde un teléfono móvil así como equipos industriales también controlados de forma remota mediante redes inalámbricas, con la inseguridad que todo ello conlleva, maniobras de simulacro de ataques y defensa realizadas de forma conjunta por fuerzas armadas y civiles, normativas para la protección de infraestructuras críticas, etc.

4. Ciberseguridad: un nuevo escenario para la formación

El panorama que se nos presenta ante este nuevo entorno de la ciberseguridad no deja de ser preocupante, no sólo por las consecuencias que algunos ataques dirigidos y amenazas persistentes avanzadas, conocidas como APTs Advanced Persistent Thread, pudiesen traer a las infraestructuras críticas de una ciudad o país, y a la propia población, sino por el déficit mundial de profesionales de la seguridad que tengan estas nuevas aptitudes. Aptitudes que tal vez se encuentren muy en la línea tradicional del entorno hacking, pero en el que de forma incomprensible la universidad no ha se interesado ni profundizado en ello, ni en materias de enseñanza ni en investigación. Como todo en la vida, existen casos aislados, pero no dejan de ser anecdóticos y a todas luces insuficientes para cubrir las necesidades del mercado laboral. Para confirmar esto, baste un par de párrafos de noticias publicadas en mayo y octubre de 2015 en sendos periódicos de España de tirada nacional:

El Mundo: 31/05/2015
"Telefónica no encuentra desarrolladores punteros; ni científicos de datos suficientes. Google no da con ingenieros informáticos con capacidad para el tratamiento de datos; GMV tiene dificultades para fichar expertos en ciberseguridad." "Según las previsiones de la UE, apuntan a la creación de casi 900.000 empleos tecnológicos de aquí a 2020."

La Vanguardia: 20/10/2015
Encuentro Internacional de Seguridad de la Información (9Enise), organizado por el Instituto Nacional de Ciberseguridad, León. Sobre la intervención de D. Orlando Ayala, vicepresidente de Microsoft.
"En su conferencia, se ha referido a los desafíos técnicos de la ciberseguridad a nivel mundial, pero también a las oportunidades de desarrollo económico que ofrece el sector, con 6 millones de puestos de trabajo pendientes de ser ocupados por profesionales expertos."

5. Conclusiones

Está claro que la temática relacionada con la seguridad informática, seguridad de la información y últimamente ciberseguridad, como se le quiera llamar, es un ámbito de grandes cambios y en constante evolución. Ello marca de manera notoria el interés de las universidades y empresas para estar al día ante las necesidades de formación a sus técnicos y expertos que la sociedad nos demanda. Ante un escenario de amenazas mutantes conocidas y las que estaban aún por descubrirse, a comienzos de esta década la universidad española reacciona adecuadamente mostrando un crecimiento espectacular de la oferta

docente en seguridad, multiplicando por más de 5 la oferta existente tan sólo quince años atrás. No obstante, nos enfrentemos ahora a un nuevo reto por amenazas de ataques cada vez más sofisticados, con perfiles de objetivos muy delimitados, con un crecimiento espectacular del cibercrimen y hay quien dice que estamos incluso a las puertas de una ciberguerra. Ante todo esto, no estamos respondiendo como nos pide la sociedad con una formación avanzada y adecuada para nuestros futuros ingenieros.

Si a todo ello unimos el hecho de que en este nuevo escenario resulta imprescindible la colaboración entre civiles y fuerzas armadas, núcleos de la sociedad que por lo general tenían objetivos diferentes, ciertamente nos enfrentamos a un importante reto en la formación de nuestros ingenieros en seguridad. ¿No va siendo hora ya de plantearnos de forma seria una nueva ingeniería en ciberseguridad? Nadie dice que esto sea fácil y seguro habrá muchos obstáculos que salvar, pero el mercado y la sociedad nos lo están demandando. Además, existe también un amplio abanico de líneas de investigación, de desarrollo y de innovación tecnológica y educativa a desarrollar. Más pistas es imposible dar.

6. Referencias

1. Introducción de las Enseñanzas de Seguridad Informática en los Planes de Estudio de las Ingenierías del Siglo XXI. JENUI 2001 Palma de Mallorca, J. Ramió
   http://bioinfo.uib.es/~joemiro/aenui/procJenui/ProcWeb/actas2001/raint73.pdf

2. Tesis Doctoral La enseñanza universitaria en seguridad TIC como elemento dinamizador de la cultura y la aportación de confianza en la sociedad de la información en España, Universidad de León, diciembre 2013, actualización abril 2014, J. Ramió.
   http://www.criptored.upm.es/guiateoria/gt_m001j1.htm

3. Reflexiones sobre la enseñanza de la seguridad en España – Razones que justifican el lanzamiento del proyecto MESI, Revista SIC, febrero 2104, J. Ramió
   http://www.criptored.upm.es/descarga/SIC108_MESI-JORGE%20RAMIO.pdf

4. MESI 2.0, un paso más en la generación del mapa definitivo de la enseñanza universitaria de seguridad de la información en España, Revista SIC, abril 2015, J. Ramió
   http://www.criptored.upm.es/descarga/SIC114_MESI20-JORGE-RAMIO.pdf

5. Ciberseguridad: un nuevo paradigma de la seguridad y nuevos retos en la formación especializada, UCEN Chile julio 2015, J. Ramió.
   http://www.criptored.upm.es/guiateoria/gt_m001o1.htm

6. El Mundo: 31/05/2015
   http://www.elmundo.es/economia/2015/05/31/5568a4a1268e3e9e518b4592.html

7. La Vanguardia: 20/10/2015
   http://www.lavanguardia.com/vida/20151020/54438244527/microsoft-espana-tiene- capacidad-para-ser-lider-mundial-en-ciberseguridad.html

   Presentación usada en la conferencia
   http://www.criptored.upm.es/descarga/PresentacionConferenciaMagistralTIBETS2015_JRA.pdf