Octubre, mes europeo de la Ciberseguridad

Madrid, 1 de Octubre de 2017

Bajo el lema **"Para, piensa, conéctate. La Ciberseguridad es una responsabilidad compartida",** ENISA (Agencia Europea de las Redes y de la Información) organiza por quinto año el mes de la ciberseguridad que se desarrolla del 1 al 31 de octubre.

Su principal objetivo es concienciar a los ciudadanos de la necesidad de preservar la información y abogar por un cambio en la percepción de las ciberamenazas mediante la promoción de la seguridad de los datos y la información, la educación, el intercambio de buenas prácticas y la competencia.

Para esta campaña de 2017 se han presentado más de 341 actividades que se realizarán en 28 países de la UE.

En el sitio web https://cybersecuritymonth.eu/ se detallan las actividades que se llevarán a cabo en cada país. Así mismo la campaña propone dedicar cada sema del mes a un tema importante relacionado con la ciberseguridad. Los temas propuestos son los siguientes:

Semana del 2 al 6 de octubre: Ciberseguridad en el sitio de trabajo

El objetivo es sensibilizar a los empleados de la empresa, los profesionales de TI y la alta dirección sobre amenazas tales como Ransomware, Phishing, Malware y proporcionar asesoramiento general sobre "Higiene" de seguridad.

Semana del 9 al 13 de octubre: Gobernanza, Privacidad y Protección de Datos

Cuenta atrás para el cumplimiento: Asegúrese de estar listo! El objetivo de este tema es descubrir cómo preparar a su organización para cumplir con las nuevas directivas y reglamentos de la UE, como la Directiva NIS y el RGPD.

Semana del 16 al 20 de octubre: Ciberseguridad en el hogar

El objetivo es sensibilizar a los usuarios en general sobre las amenazas de IoT, el fraude en línea y las estafas y proporcionar orientación sobre cómo proteger su red doméstica y proteger su privacidad en línea.

Semana del 23 al 27 de octubre: Habilidades en Ciberseguridad

El tema busca apoyar a los jóvenes con la adquisición de habilidades de ciberseguridad a través de formación práctica y educación con el fin de hacer crecer la próxima generación de profesionales capacitados en ciberseguridad.

En España este mes de octubre viene precedido de dos grandes eventos relacionados con la ciberseguridad que se han llevado a cabo en Madrid:

- **El 21 de septiembre se celebro el "IBM Security Summit 2017"**[1] durante el mismo Marc van Zadelhoff, director general de IBM Seguridad, destacó que el objetivo de IBM es ayudar a que los sistemas de seguridad funcionen como el sistema inmunitario humano. Del mismo modo que los órganos del cuerpo reaccionan conjuntamente para combatir una infección o enfermedad, las diferentes soluciones de seguridad de una organización deben trabajar de forma integrada para dotar a las organizaciones de una detección y respuesta rápida y eficaz. *"Cuando caemos enfermos, nuestros órganos entienden la amenaza y envían señales al sistema nervioso central para crear anticuerpos y frenar esa dolencia. Es lo que llamamos 'respuesta inmune'. De la misma manera, un sistema de seguridad inmune utiliza la tecnología cognitiva y la analítica para identificas las amenazas en tiempo real, orquestar la respuesta y bloquear dichas amenazas"*.
- **El 27 de septiembre se celebro el "VI Foro de la Ciberseguridad de ISMS Forum"**[2] durante el mismo Anthony Bucci, experto en inteligencia artificial comentó: que actualmente el coste de la ciberseguridad es de 400.000 millones de dólares al año.
    - "Lo preocupante es que el 75% de los ataques no son detectados a tiempo, el 72% de las empresas, que son pymes, son atacadas de forma consistente y no salen en el telediario a pesar de las pérdidas que le supone. Para el 2017 nos enfrentamos a 400 nuevas amenazas por minuto.
    - "El problema es que hay una gran asimetría entre el atacante y los defensores. Si es una vulnerabilidad conocida para hacerla frente cuesta poco, pero en las importantes se calcula que se invierte el trabajo de hasta seis meses para recuperar la normalidad. El problema es que actualmente todo es reactivo. Se hacen cosas tras detectar el ataque. Se diseña un antivirus… tras detectar el virus. Y para los que quieren anticiparse con heurística, con el estudio del comportamiento humano, también hay que haber conocido un patrón humano. Así que se trabaja con lo que ya ha sucedido".

El mensaje común de ambos eventos pone de manifiesto, al menos, estos aspectos:

1º) Que nos enfrentamos a un problema de enormes dimensiones, solo a nivel económico supone inmensas pérdidas (entorno a 400.000 millones de dólares al año) y que además, en vez de mejorar está empeorando como puso de manifiesto Daniel Largacha, director del centro de estudios en ciberseguridad de ISMS Forum: *"La seguridad ha empeorado en las*

[1] IBM: "Para ser eficaz, la ciberseguridad ha de funcionar como el sistema inmune humano"
http://www.muycomputerpro.com/2017/09/21/ibm-ciberseguridad-sistema-inmune-humano

[2] El VI Forum de la Ciberseguridad de ISMS Forum alerta: en cada minuto se viven ya 400 nuevos ciberataques
http://www.onemagazine.es/vi-foro-ciberseguridad-isms-forum-spain-que-se-ha-dicho-inteligencia-artificial

últimas décadas por la digitalización de la sociedad -sin tener un plan B, en caso de crisis-, por la hiperconectividad derivada de la reorganización. Ello supone que un pequeño problema que ocurre en una región de Asia, como fue el WannaCry, amenazó en 24 horas a todo el mundo. Y por último la interdependencia. No vale salvarse uno, sino que lo que le afectaba al de enfrente te afectaba a ti. Porque ya no se puede prestar un servicio sin contar con el otro".

2º) Que los productos y tecnologías que actualmente estamos utilizando para hacer frente a este problema son insuficientes, pues la ciberseguridad no ha mejorado. Aunque produce esperanza de mejora de la misma tanto la aplicación, a gran escala, de tecnologías de "inteligencia artificial" en los productos y servicios de seguridad que utilizamos, como la "necesaria integración" de dichos productos.

3º) El factor humano, la cooperación y delimitación de responsabilidades en los incidentes de seguridad. Es en este aspecto en el que más inciden las 341 actividades que se llevarán a cabo en 28 países de la UE durante este mes de la ciberseguridad. También es un aspecto clave tomar conciencia colectiva de la ciberseguridad y no bajar la guardia, pues cuando decimos que estos incidentes nos afectan a todos hemos de pensar con humildad que directa o indirectamente "yo podría ser el siguiente afectado, si es que no lo he sido ya".

Este mes de la ciberseguridad europea, también viene precedido de uno de los mayores incidentes de ciberseguridad. Acaecido durante el pasado septiembre en Equifax[3], el hecho de que en mayor medida haya afectado a ciudadanos de EE.UU., no debería ser óbice para que sus gravísimas consecuencias se comenten con mayor amplitud en España.

Informe del incidente de seguridad de Equifax hecho público en septiembre de 2017
Equifax dice que la brecha de seguridad ha expuesto a: • 143 millones de datos personales de los consumidores estadounidenses, incluyendo nombres, fechas de nacimiento, direcciones, números de Seguro Social y en algunos casos números de licencia de conducir; • 209.000 tarjetas de pago de los consumidores estadounidenses; • 182.000 documentos de controversias de crédito de consumidores estadounidenses, que contienen información personal; • 400.000 datos personales de los consumidores británicos, que la compañía almacenaba accidentalmente en sus servidores estadounidenses; • 100.000 datos personales de los consumidores canadienses.

[3] After Mega-Breach at Equifax, CEO Richard Smith Is Out
https://www.databreachtoday.com/after-mega-breach-at-equifax-ceo-richard-smith-out-a-10335

Si tenemos en cuenta que la población de EE.UU. es de 341 millones, incluidos los niños, el incidente afectaría[4] a casi el 50% de su población. De aquí que el pasado 8 de septiembre, Ellen Chang titulara su artículo referente al mismo con la frase *¿Por qué el incidente de seguridad acaecido en Equifax que ha afectado a 143 millones de consumidores debería enloquecer?*

La ciberseguridad nos afecta a todos, pero por nuestra responsabilidad como Ingenieros en Informática nos afecta bastante más. Aunque estamos viendo como desde altas instancias, incluidas las de Estado, se cuenta poco con nuestra ingeniería y preguntarnos en España si:

¿De verdad podemos permitirnos como país que nuestros Ingenieros en Informática, especialistas en seguridad, emigren?

[4] Why Equifax Breach of 143 Million Consumers Should Freak You Out
https://www.thestreet.com/story/14298348/1/equifax-breach-of-143-million-consumers-increases-identity-theft-odds.html