Instituto Tecnológico Campus Monterrey

Integración de Seguridad Informática en Redes y Sistemas de Software

Actividad con Sentido Humano: Aspectos Éticos, Legales y Técnicos.

Por: Eduardo Antonio Maldonado Guzmán

La ciberseguridad es una preocupación mundial y un tema de investigación académica. Muchas naciones han tomado la iniciativa en la creación de agencias gubernamentales para coordinar la respuesta del país a los ataques cibernéticos. La guerra se ha convertido en ciberguerra; y ambos son una realidad para la que debemos prepararnos.

La ciberseguridad se ha convertido en una preocupación mundial y un campo de estudio académico. Más de 100 naciones han firmado convenios internacionales para mejorar la seguridad cibernética en los equipos y sistemas del Estado. Además, varios organismos regionales intentan generar una cultura de seguridad cibernética y negociar el cumplimiento de las normas en materia de ciberseguridad en las naciones que conforman la región. Las acciones gubernamentales por lo general se reflejan en las normas internacionales. Por ejemplo, la Unión Europea (UE) y la Organización Mundial de la Salud (OMS) han adoptado directrices para reducir los riesgos asociados con la ciberseguridad. Estas directrices no sólo animan a las naciones a hacer aviones para presentar lucha contra la ciberseguridad, sino que también ponen énfasis en formar comisiones nacionales responsables de implementar las medidas recomendadas para mitigar los daños cibernéticos.

Ahora comenzamos una nueva era en el área, llena de desafíos actuales. El nuevo RGPD (control general de seguridad de la información) está preparado para alterar significativamente la forma en que los proveedores de servicios y los comerciantes pueden crear, medir, usar y compartir información de los consumidores constantemente. Esta aceptación por parte del Parlamento Europeo de la aprobación de esta norma el 27 de abril de 2016 otorga a los proveedores de servicios solo 24 meses para cumplir con el RGPD. Y este término en su totalidad puede implementarse el 28 de mayo de 2018: el tiempo se acaba rápidamente. Esto plantea un problema potencialmente intimidante para los comerciantes y proveedores de servicios que deben tomar las medidas mejores, más rápidas y más seguras antes de la fecha límite. El incumplimiento puede dar lugar a actividades legales o multas de hasta el 4 % de la facturación mundial de la organización o 20 millones de euros.

Sin embargo, la declaración más alarmante de la reciente llegada a la imagen de los servicios judiciales fue el estudio del Barristerblogger Matthew Scott sobre cómo, debido al error de seguridad de datos en el sistema de aplicaciones en línea del portal de alumnos, se supo que la controvertida periodista de comunicación diaria Katie Hopkins estaba 'configurada para convertirse en el abogado

Al juntar todo eso, se dijo que GDPR creaba el nuevo y valiente mundo de privacidad y seguridad de la información para los ciudadanos de la UE. Más bien, su implementación no es solo revertir las protecciones anteriores que amaban sus ciudadanos, sino que está afianzando, bajo la seguridad legal, todos los componentes más invasivos de la privacidad de nuestra sociedad moderna de vigilancia digital.

En el caso de el reto de la materia de ciberseguridad, tuvimos que crear un sistema que involucra una aplicación móvil, una API, y una página de administración para la API, el sistema es vulnerable a ciberdelitos, como cualquier otro sistema, por lo que se tiene que

hacer todo lo posible para que el sistema tenga todas las capas de protección para no recibir ataques.

Referencias

Leetaru, K. (May. 2018). Will The EU's Data Protection Act Actually Lead To Less Online Privacy? Forbes. Retrieved from https://www.forbes.com/sites/kalevleetary/2018/05/08/will-the-eus-data-protection-act-actually-lead-to-less-online-privacy/