Tecnológico de Monterrey

Evidencia de sentido humano: Amenazas, legislación, código de ética de Ingeniería de Software & Metodologías de mitigación y protección.

Integración de seguridad informática en redes y sistemas de software

Abraham Cepeda Oseguera

A00827666

Lunes 18 de octubre del 2021

ACTIVIDAD CON SENTIDO HUMANO: Amenazas, legislación, código de ética de Ingeniería de Software.

A medida que nuestra sociedad evoluciona, los cambios tecnológicos han ido interconectando al mundo de una manera que nunca en la historia de la humanidad se había logrado. De modo que, ahora lo que sucede en un almacén de servidores en Suecia puede tener un impacto en millones de personas alrededor del mundo. Esto además de proveernos con una inmensa cantidad de nuevas posibilidades, trae consigo diversos desafíos que pueden llegar a ser catastróficos tales como los ataques cibernéticos. Este tipo de ataques son bastante peligrosos, ya que pueden robar información confidencial, alterar la información, robar cuentas bancarias, entre muchas otras acciones que pueden perjudicar gravemente tanto a individuos como a empresas o instituciones gubernamentales. Además, cabe recalcar que el cibercrimen representa una pérdida enorme de recursos económicos, debido a que cuesta alrededor de 575 millones de dólares al año, lo cual representa el 0.5% del PIB mundial. Por otro lado, el cibercrimen también afecta gravemente a nuestro país, ya que somos el segundo país con más ciberataques de América Latina, teniendo al 57.4% de la población conectada a internet. Por lo tanto, resulta crucial entender los diferentes tipos de ataques que existen para así poder desarrollar e implementar las herramientas necesarias para proteger a los sistemas y redes de estos ataques. Dentro de los tipos de ataques más comunes se encuentran los delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, delitos relacionados con la informática y los delitos relacionados con el contenido.

Ese tipo de delitos tienen como objetivo ya sea robar información sensible al obtener las credenciales o accediendo directamente al sistema, atacar la infraestructura y sistema de red para dejarla inhabilitada y fuera de servicio o bien buscan alterar los datos a su conveniencia o buscando perjudicar a la empresa. Dentro de los ataques más comunes de este tipo se encuentran *hacking, malware* y *DDoS.* El primero se puede mostrar en diferentes formas tales como *SQL injection,* el cual puede alterar las tablas que se encuentren en una base de datos, *Phishing,* el cual generalmente viene en la forma de

un enlace en un mail que busca compartir información confidencial o, incluso, instalar *malware* en el dispositivo. Por otro lado, los ataques de *malware* mas comunes comprenden *worms, spyware, ramsomware, adware* y *trojans.* Los *worms* pueden tener distintos objetivos finales pero lo que buscan es infectar una red de computadores, ya que tienen la habilidad de replicarse por lo que pueden infectar un gran número de computadoras y así incrementar el trafico de la red. El ataque de *spyware,* es un programa capaz de observar y recopilar información sensible del dispositivo sin ser detectado. Al contrario, un ataque de *ramsomware* es más activo a diferencia del *spyware,* puesto que bloquea las funciones principales del sistema y evita que el usuario puede acceder a sus archivos personales, esto con el objetivo de que el usuario le pague al atacante cierta cantidad de dinero para que le devuelva el acceso. Por otro lado, el *adware* es un programa que le muestra anuncios al usuario al utilizar el navegador con el objetivo de recopilar información y posteriormente venderla. Existen diferentes tipos de troyanos, pero generalmente al lograr infiltrarse en el dispositivo al hacerse pasar por un programa legítimo pueden dañar al dispositivo mediante la eliminación, bloqueo, modificación y la copia de datos. Finalmente, el ataque de *DDoS* sucede comúnmente en las empresas debido a que busca saturar el tráfico de red de la infraestructura web de una empresa con el objetivo de dejarla fuera de línea, lo cual le genera tanto pérdidas económicas a la empresa como pérdida de credibilidad y confianza ante sus clientes.

Dentro de los delitos del cibercrimen se encuentran los relacionados con la informática, los cuales incluyen fraude o falsificación informática, delitos de identidad relacionados con la informática, enviar o controlar el envío de spam, infracciones de derechos de autor o marcas comerciales con la informática, actos informáticos que causen daños personales, solicitud o *grooming* de niños relacionada con la informática. Este tipo de ataques son extremadamente comunes, ya que algunos pueden resultar sencillos de realizar tales como el acoso, el cual se puede dar a través de las redes sociales donde una persona puede hacerse pasar por alguien que no es para interactuar con otra y así sacarle información, extorsionarla o, incluso, quedar de verse para realizar un secuestro, entre otras acciones peligrosas.

Por otro lado, existe otro tipo cibercrimen totalmente diferentes a los dos anteriores, ya que este se relaciona con el contenido que se publica en el internet. Este contenido conlleva explotación sexual comercial de niños, publicación de información falsa e instigación de actos terroristas o de delitos de la convención. El primer caso es un sumamente triste, ya que hay personas que se dedican a secuestrar menores de edad con el objetivo de generar pornografía infantil, lo cual esta totalmente penado en nuestro país. El segundo caso, puede crear manipulación en la sociedad para generar una tendencia de pensamiento o de actitud. En el caso de la política esto puede ocasionar que parte de la población se incline mas hacia un partido en lugar de otro, lo cual es inmoral debido a que significa mentir para influencias las decisiones de las personas sobre asuntos de relevancia para la sociedad. Finalmente, el último caso es bastante peligroso porque a través de foros de internet o medios de comunicación similares un grupo de personas pueden planear ataques terroristas contra el estado. Todas estas situaciones representan un grave peligro contra la sociedad.

Tras haber analizado las diferentes clases en las que se puede presentar un cibercrimen, resulta empírico estudiar las diferentes prácticas, convenciones y reglas que deben seguir los programadores al desarrollar un proyecto, al ser estas las que ayudan a prevenir este tipo de ataques y situaciones. Además, cabe mencionar que es nuestro deber como programadores conocer todos estos elementos de ciberseguridad para siempre dejar los proyectos los más protegidos posible.

Al hablar sobre las responsabilidades éticas de los desarrolladores de *software,* es vital mencionar los 8 principios que estipula el "*Software Engineering Code of Ethics and Professional Practice,"* el cuál lo recomienda la fuerza unidad de la *ACM/IEEE-CS.* En este código de ética se estipulan 8 principios a los cuales todo ingeniero de *software* debe apegarse y comprometerse a cumplirlos a lo largo de su vida profesional, los cuales son el público, cliente y empleador, producto, juicio, mantenimiento, profesión, compañeros de trabajo y si mismo. Estos principios deben de ser cumplidos y respetados en todo proyecto. Por lo tanto, a continuación, se analizarán cada uno de ellos al igual que sus implicaciones en el desarrollo de la aplicación móvil para el Museo Marco.

El primero se basa en que el programador debe actuar consistentemente con el interés público. Este primero resulta sencillo para el proyecto, ya que el mismo busca impulsar al público a tener experiencias culturalmente enriquecedoras al asistir al museo y aprender sobre nuevos temas. Sin embargo, el no cumplir con este principio ocasionaría desinterés por parte del público, lo cual terminaría perjudicando al museo, al ocasionar que menos gente asista a ver sus distintas exposiciones.

El igual que el primero, el segundo busca que los ingenieros deben actuar consistentemente en el interés de su cliente o empleador al igual que el del público. En este caso, estamos cumpliendo con el principio, ya que el proyecto fue totalmente desarrollado con base a los intereses tanto del público como del cliente. Sin embargo, en caso de no haber cumplido con esto ocasionaríamos que el cliente se disguste con nuestro trabajo y por ende podría haber desperdiciado su dinero y buscaría a otro grupo de programadores para llevar a cabo su proyecto.

Por otro lado, el tercero comprende que el desarrollador debe crear los productos que cumplan con los estándares profesionales más altos posibles. En cuanto a la calidad del producto se puede decir que se utilizaron herramientas de la más alta calidad como lo es *Xcode.* Sin embargo, al ser una aplicación sencilla y por ende no necesitar funciones nativas, la aplicación se pudo haber desarrollado una tecnología multiplataforma como los es *React Native,* evitando así tener que hacer el desarrollo de Android. De modo que, al haberlo realizado de esta forma, el cliente estaría perdiendo dinero y tiempo al tener que pagar y esperar el desarrollo de aplicación móvil para Android.

El cuarto, impulsa al programador a mantener su integridad e independencia respecto a su juicio profesional. En este caso, se puede decir que en todo momento mantuvimos nuestra integridad. Posiblemente, la independencia no al no haber podido elegir las herramientas y tecnologías de nuestra consideración para realizar el proyecto, pero se puede decir que nos ajustamos a los requerimientos del cliente. Sin embargo, en dado caso de no haber mantenido la integridad e independencia el cliente hubiera sido quien

se vería perjudicado, ya que la calidad y objetividad de nuestras entregas se verían comprometidas.

Similarmente, el quinto busca que los ingenieros de *software* mantengan una práctica ética en cuanto al mantenimiento del sistema de *software* desarrollado. A pesar de que el mantenimiento no ha sido discutido todavía, se puede inferir que se debe llegar a un acuerdo con el Museo Marco para estipular las políticas del mantenimiento. Por ejemplo, se puede establecer que cada cambio a la aplicación se cotizará por separado tomando en cuenta la complejidad y el tiempo requerido. O bien, se puede definir una mensualidad, la cual incluiría cambios ilimitados mientras se mantengan bajo cierto nivel de dificultad. Es importante que el acuerdo sea justo y benéfico tanto para los desarrolladores como el cliente, ya que se busca que los primeros tengan una recompensa económica atractiva, mientras que el segundo reciba los resultados esperados.

En cuanto al sexto principio, se pretende que los ingenieros avancen su integridad y reputación de la profesión de manera consistente con los intereses públicos. Dado que este principio consiste principalmente en el desarrollo profesional de cada ingeniero de *software,* todavía no es algo que veríamos reflejado directamente en el proyecto desarrollado para el Museo Marco. Sin embargo, cabe recalcar que gracias a que programadores con mayor experiencia han cumplido con este principio, nuestra industria sigue prosperando. Por lo tanto, resulta empírico seguir su ejemplo e impulsar la integridad en nuestra área de trabajo para que se puedan seguir llevando a cabo proyectos que mejoren la vida de las personas de alguna forma. De modo que, el no cumplir con este principio resulta bastante catastrófico para nuestra industria, ya que provoca desconfianza de los programadores en la sociedad, lo cual limita el alcance de ingenieros que buscan tener un impacto positivo en la misma, así como la generación de nuevos proyectos.

El séptimo principio señala que los profesionistas de esta industria sean justos e impulsen a sus colegas a prosperar. Este principio se puede observar bastante en el desarrollo de este proyecto, ya que el equipo esta conformado por personas que tienen un poco más de experiencia desarrollando aplicaciones móviles utilizando *Xcode* y *Swift,* las cuales tomaron la iniciativa para ensañarles algunos conceptos a los que tenían menos experiencia con el objetivo de que expandan sus conocimientos y habilidades. En caso de no haber cumplido con esto los principiantes perderían la oportunidad de aprende de alguien con mas experiencia, los más experimentados tendrían mayor carga de trabajo y por ende el cliente podría recibir un proyecto de menor calidad a la esperada.

Finalmente, el último principio indica que los desarrolladores de *software* siempre se mantengan a la vanguardia en su área y siempre promuevan que los proyectos desarrollados mantengan una ética impecable. Este último principio nos toca aplicarlo en el futuro, ya que tendremos que seguir aprendiendo y adaptándonos a las emergentes tecnologías. Además, en cada proyecto que nos encontremos debemos de siempre tomar en cuenta estos ochos principios con el fin de asegurar una buena ética de trabajo. Sin embargo, en caso de no cumplir con este objetivo nosotros mismos nos veríamos afectados, ya que tendríamos una desventaja competitiva al no saber manejar las más recientes tecnologías.

Después de analizar tanto los retos que supone la informática y los principios que siguen los programadores para evitar la misma, resulta empírico discutir las legislaciones que impone el gobierno ante estos temas tan importantes. Puesto que, son estas legislaciones las que protegen no solo al gobierno, sino a cualquier empresa privada o persona que esté conectada a la red de ser víctimas de ataques cibernéticos de cualquier tipo. Especialmente en México es necesario impulsar la mejora de estas legislaciones debido a que no ha habido mejoras en los últimos cuatro años y nuestro lugar en términos de ciberseguridad se encuentra bastante lejos de nuestro lugar en cuanto al tamaño de nuestra economía. A pesar de durante el sexenio del expresidente se propuso e implementó la Estrategia Nacional de Ciberseguridad, según expertos se deben de hacer

modificaciones que protejan en mayor medida a los sistemas de red del país tanto gubernamentales como no gubernamentales.

ACTIVIDAD CON SENTIDO HUMANO: Metodologías de mitigación y protección

Dada la gran diversidad de ataques cibernéticos y la creciente demanda de infraestructura de red, cada vez resulta más relevante la implementación de metodologías de mitigación y protección contra este tipo de ataques. Es por esto por lo que organizaciones como la *"International Organization for Standardization"* y la "*International Electrotechnical Commission"* han publicado estándares como el ISO 27000 con el objetivo de que los mismos se implementen en todos los proyectos que utilicen algún tipo de infraestructura en la red y así estos se puedan proteger contra ataques cibernéticos.

Para el caso del desarrollo de este proyecto se tomaron en cuenta diferentes aspectos de seguridad que nos permiten brindarle mayor protección a la integridad de la aplicación. Algunas de las medidas que tomamos fueron el proteger la base de datos de un ataque de tipo *MySQL injection* al validar y limpiar las peticiones, utilizar un método seguro de autenticaciones de usuario con contraseñas fuertes, establecer conexiones seguras entre la API, la base de datos y la aplicación móvil, así como conexiones seguras con los servidores. De modo que, la aplicación se encuentra con un cierto nivel de seguridad que le permite tanto al cliente como al usuario final interactuar con la misma sin correr el riesgo de ser víctimas de un ataque cibernético, el cual podría ocasionar el robo de información sensible de los usuarios tal como contraseñas y datos bancarios o incluso la modificación de la información de la base de datos. Ambas situaciones serían extremadamente graves, ya que podrían perjudicar directamente al usuario y dañar la reputación del Museo Marco, lo cual podría conllevar a la disminución de visitas. Es por todas estas razones y más, que resulta crucial proteger toda la infraestructura de la aplicación lo más posible, lo cual se puede lograr estudiando los métodos más efectivos y recientes para contrarrestar los ataques cibernéticos. Además, es nuestra

responsabilidad como programadores estar al día con esta información y aplicarla en los proyectos.