La práctica de “hackear” se ha convertido en un problema mundial. Los hackers (mal llamados piratas informáticos) de hoy día pueden ser desde curiosos estudiantes de escuela, universitarios, hasta criminales profesionales. Entre las razones para “hackear” se encuentran: el que estos individuos puedan probar sus destrezas y habilidades técnicas así como también sus capacidades para cometer actos fraudulentos y dañinos. Así que, no es sorpresa que la defensa contra este tipo de personajes se haya convertido en un componente vital.

Asimismo, durante los últimos años el término “hacking ético” ha despertado innumerables puntos de vista a favor y en contra. Por definición el hacking ético es conocido como una prueba de intrusión o “pentest”, que se define esencialmente como el “arte” de comprobar la existencia de vulnerabilidades de seguridad en una organización, para posteriormente a través de un informe se señalen los errores de seguridad encontrados, mitigarlos a la brevedad posible y evitar fugas de información y ataques informáticos.

Muchas empresas han propuesto el tema de hacking ético mediante la capacitación de sus empleados a través de cursos cortos y certificaciones en el área de seguridad informática. También han invertido en capacitar a sus empleados para que piensen y actúen como los hackers maliciosos y sean capaces de proteger los activos más importantes de la empresa: la información digital.

Pero este fenómeno trae como consecuencia, una pregunta incómoda para muchos y relevante para el tema: ¿cuál es la ética detrás del hacker ético?, ¿Acaso no, cuando capacitamos a un empleado para que actué y piense como un hacker malicioso no estamos arriesgando mucha de nuestra información y recursos? ¿Realmente estas capacitaciones nos están protegiendo o nos estamos arriesgando más? ¿Estamos durmiendo con el enemigo? ¿Cuál es el rol de las instituciones educativas mundiales en la enseñanza de hacking?

¿Cuál es la ética detrás del hacker ético?

De acuerdo a la Real Academia Española, la palabra ética proviene de la palabra “Ethos” que significa: “Conjunto de rasgos y modos de comportamiento que conforman el carácter o la identidad de una persona o una comunidad.” Lo que nosotros llamamos ética es la predisposición para hacer el bien.

Ahora bien, cuando se habla de la ética en IT se refiere a: “el comportamiento en el uso de la tecnología informática”. Por lo tanto, existe un código de ética para todos los usuarios de la informática. Ese código se basa en principios éticos fundamentales y es aplicable a situaciones que caracterizan las actividades de esta tecnología. De acuerdo a Doug Johnson (Teaching Students Right from

Wrong in the Digital Age) la ética en la informática se sustenta en varios principios filosóficos:

“Si una acción al menos contiene cualquiera de estas características es considerada una acción ética por ejemplo: promover la salud general de la sociedad, mantener o incrementar los derechos de los individuos, proteger las libertades, preservar a los individuos de daño, tratar a todos los humanos con valor dignidad y respeto, así como mantener el valor social, cultural y respetar las leyes.”

Desde este punto de vista, en el Hacking Ético se puede definir que la ética consistiría en la práctica de “hackear” sin tener de por medio alguna intensión maliciosa. Ahora bien, los hackers éticos emplean las mismas herramientas y técnicas que los cibercriminales o black hackers, pero no lo hacen con la meta de dañar el sistema o robar información. En su lugar su función principal es la de evaluar la seguridad de los sistemas y reportar sus hallazgos para que las vulnerabilidades puedan ser corregidas. La ética en este caso sería guardar de forma confidencial y privada toda la información que obtengo de la prueba realizada.

El objetivo fundamental del hacking ético consiste en:

Explotar las vulnerabilidades existentes en el sistema de interés, valiéndose de una prueba de intrusión, verifican y evalúan la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, etcétera.

Con la intención de ganar acceso y “demostrar” las vulnerabilidades en el sistema. Esta información es de gran ayuda a las organizaciones al momento de tomar las medidas preventivas en contra de posibles ataques malintencionados

Bien dice que para atrapar a un intruso primero debes pensar como uno, sin embargo, en términos de los aspectos legales y éticos que involucra esta práctica el mantener la confidencialidad y privacidad de los datos de mi cliente es un aspecto crítico a considerar.

Ahora, para muchos quizá parezca una obviedad, pero dado el crecimiento y constante cambio en la industria IT y en el panorama de las ciberamenazas propongo los siguientes postulados éticos:

La información que los Pentesters encuentren no se le debe dar un mal manejo o uso más allá de los fines previstos por las pruebas.

Se deben indicar claramente en el contrato con la empresa cuáles son los objetivos específicos de las pruebas de penetración para evitar futuros malos entendidos

Existen una serie de buenas prácticas o normas generales en relación con la seguridad de la información y de forma particular para pruebas de penetración y almacenamiento de ciertos tipos de datos. Cualquier individuo que se dedique a realizar estas pruebas de penetración, debe tener al menos un conocimiento práctico de estas normas

Un marco o modelo a seguir que detalla los aspectos éticos de la industria de Pentesters es el modelo propuesto en Alemania llamado el Código de ética del (BDU)- Federal Association of German Corporate Consultants este modelo establece 10 principios éticos.

Código de Ética Profesional de Pen Testers: 10 Principios Éticos

Independencia: Cuando se trabaja de forma independiente se mantiene la objetividad del trabajo. Independencia es que el hacker ético no esté comprometido con algún vendedor comercial o proveedor de servicios profesionales que posea alguna solución de informática relacionada a la seguridad. Ejemplo, una compañía dueña de un producto que asegura detecta vulnerabilidades e intenta vender el producto como parte de las soluciones para proteger a la empresa que le contrató para hacer las pruebas de vulnerabilidad.

Prohibición de aceptar dinero por compañías de la competencia para realizar pruebas en otras compañías: La compañía X me contrata para hacer un análisis de vulnerabilidad de la compañía competidora.

Cuidado del cliente: Se le debe informar sobre los posibles riesgos de realizar algunas pruebas de vulnerabilidad

Profesionalismo y calidad en la operación

Responsabilidad corporativa- establecer bien claro las responsabilidades de las consecuencias de las pruebas

Imparcialidad, neutralidad y transparencia de procesos

Evitar el conflicto de intereses

Obediencia estricta a las leyes

Respeto por los humanos: Ingeniería social

Dar los créditos correctos en el informe final

Ahora, aún queda pendiente buscar posibles respuestas a los cuestionamientos planteados al principio del artículo. Así que comencemos.

Cuándo capacitamos a un empleado para que actué y piense como un hacker malicioso, pero le pedimos que opere bajo los lineamientos de la ética y la moral, ¿no estamos arriesgando mucha de nuestra información y recursos?

Este punto podría generar cierta controversia, principalmente si se analiza bajo el punto de vista de la mayoría de las investigaciones y reportes de fuga o roba de datos, que colocan a los empleados internos como unos de los principales vectores de riesgo, en alguna veces incluso por encima de los atacantes externos.

Ni que decir de aquellos empleados, que resentidos por su despido o terminación deciden hacer uso de sus antiguos privilegios y tomar venganza. Estos incidentes dejan en claro que cuando una empresa invierte en entrenar y capacitar a su personal técnico en seguridad IT debe establecer claramente políticas de seguridad para protegerse y evitar brechas o ataques.

Desde mi punto de vista, cuando el empleado tiene claras sus funciones y se capacita en aspectos éticos de su profesión muchas de estas situaciones se pueden prevenir o evitar. Tampoco está de más implementar una política de chequeo de credenciales antes de adiestrar o entregar a alguien los secretos más vitales de la empresa.

¿Realmente estas capacitaciones nos están protegiendo o nos estamos arriesgando más? o ¿Estamos durmiendo con el enemigo?

¿Qué es mejor, escoger un consultor interno o uno externo en el área de ciberseguridad? , ¿Qué es mejor, una compañía de seguridad externa o alguien de casa que conozca los manejos de la organización? Ambas preguntas tienen sus pros y contras. Por ejemplo: un consultor interno es aquel empleado que la empresa envió a certificarse en hacking ético y que trabaja en el área de sistemas y, ocasionalmente, se le requiere que corra ciertas pruebas de seguridad. El potencial problema de este recurso se llama “confianza”, porque estos consultores pueden crear un exceso de confianza en que los sistemas están tan seguros y pasar por alto ciertos problemas o detalles, que pueden convertirse en riesgos o vulnerabilidades. Mientras que un consultor externo es aquél al que la compañía contrata para que verifique la seguridad de sus sistemas externamente. Este consultor tiene la ventaja de que trae consigo una visión nueva y fresca de la organización y tiene el poder de visualizar posibles brechas de información y detectar deficiencias en el sistema que tal vez los profesionales de casa no

desean aceptar, pero debemos aceptar que fuera de sus credenciales, su tarjeta de presentación y la empresa que lo respalda no sabemos absolutamente nada de él. La pregunta persiste: ¿con cuál de los arriesgamos menos?

¿Cuál es el rol de las instituciones educativas en la enseñanza del hacking?

No es sorpresa que, en los escenarios actuales de robos masivos de datos, hacktivistas y "ciberterrorismo", las instituciones educativas mundiales hayan tomado un participación activa en las capacitaciones formales de individuos con destrezas de hacking en el área informática. Hoy, ya son cientos las universidades que ofrecen cursos de formación profesional enfocados al "hacking ético". Sin embargo, aún tenemos pendiente la discusión e incorporación (en algunos casos) de materias sobre aspectos de ética, de responsabilidad social y corporativa y de comportamiento ético en sistemas computadorizados de información.

La realidad es que muchos programas profesionales de certificación en hacking ético no tratan el tema de la ética con la seriedad y profundidad que debieran. Para muchos de estos estudiantes hackear se ha convertido en una norma, nada fuera de lo común. Microsoft, por ejemplo, solicitó a varias universidades alrededor del orbe a que enseñaran a sus alumnos a hackear, con el propósito de que detectaran problemas en el diseño de software y alertaran sobre la existencia de posibles "bugs" o vulnerabilidades.

De igual modo, la agencia Homeland Security del gobierno estadounidense recientemente lanzó una competencia llamada US Cyber Challenge, en la que estudiantes de escuela primaria y superior podrán competir en diversas categorías de hacking, el objetivo detrás de la contienda es permitir al gobierno detectar a nuevos jóvenes talentosos para adiestrarlos en seguridad IT. El problema es que muchas de estas iniciativas carecen de bases y fundamentos alrededor de la ética por lo que existe la posibilidad de que muchos de estos futuros profesionales no entiendan las implicaciones de sus acciones o, en el peor de los casos, se terminan formando parte del problema más que de la solución.

Es claro que, en términos de enseñanza las universidades mundiales tienen ante si la responsabilidad de capacitar individuos en el área de ciberseguridad con principios éticos y de buen comportamiento. Individuos que se mantengan en las esferas del "mundo bueno" y no se vean tentados por las "fuerzas del mal" y grupos extremistas cuyo fin es el cibercrimen.

Como profesional en el área de seguridad IT y profesora, me he encontrado en situaciones en donde es necesario traer a discusión casos reales de ética en informática para educar, capacitar y empoderar a los estudiantes sobre la responsabilidad que conlleva el manejo de ataques de vulnerabilidad y su

responsabilidad como usuarios y administradores de tecnologías. Es imperativo dialogar sobre las implicaciones éticas del hacking, así como establecer modelos y marcos de referencia para ser exitosos y proteger a las empresas que, eventualmente requerirán del servicio y talento de estos jóvenes.

Curbelo, A. M. 2012. Hacking Ético: sus claroscuros, implicaciones y beneficios. Recuperado de http://www.expresionbinaria.com/hacking-etico-sus-claroscuros-implicaciones-y-beneficios/