Dos

Mitos del hacking

El hacking, ha sido injustamente relacionado con ilícitos y los hackers son confundidos con delincuentes, debido a diversos mitos que resultan equívocos, toda vez que ser hacker implica desarrollar un pensamiento diferente, y hacking, una actitud loable hacia la creación y el conocimiento compartido, en cualquier campo.

Federico Gacharná Gacharná, MSc.

El término "hack", se traduce como hachazo o golpe. Antes de los años 60 se llamaba hackers a los leñadores, pero luego del auge tecnológico y surgimiento de las redes de computadores, se dio un giro a este término, principalmente para designar a personas relacionadas con tecnología e informática. En la actualidad, no hay consenso en la definición formal, y el vocablo no está incluido en el diccionario de la Real Academia Española de la Lengua. En la red, se encuentran definiciones muy disímiles, no oficiales ni consensuadas, respecto al hacking o los hackers, esto compone el primer mito.

Probablemente, el término se usó por primera vez para designar un grupo de estudiantes del MIT[1] que en 1959 lograron operar una computadora IBM 407 mainframe, desde un mini ordenador, precursor del actual PC, dada la dificultad y demora que implicaba esperar los resultados del operador un par de días, para conocer el resultado de un programa escrito con tarjetas perforadas.

Hacker, hacking, hackear, se derivan del término pero se emplean con un sentido que, en opinión del autor, es equivocado o por lo menos no exacto. En los siguientes párrafos se argumentarán las razones de dicho equívoco, el cual es debido al uso inadecuado por parte de periodistas mal informados y medios de comunicación tendenciosos y parcializados, que apenas si investigan acerca del hacking y lo aplican como no es o en un contexto ambiguo, logrando desinformar a la opinión pública.

Evolución del hackerismo y lo ilícito

Es necesario aclarar que los conceptos de tecnología relacionados sobre todo con Internet, van evolucionando diariamente y son dinámicos, porque su entorno así se desarrolla. Con el tiempo, algunas de sus características pierden relevancia o cambian de contexto, por ello resulta lógico deducir que no es lo mismo un hacker de hace cinco décadas, a un hacker contemporáneo; ni son lo mismo las redes ni sus usuarios, los servicios y las costumbres, los cuales *cambian* con el discurrir de los años.

En los orígenes del hacking informático no había bandos de buenos y malos, sólo hacking y hackers, y todos eran buenos, como debe ser, como en realidad es. Pero entonces, ¿cómo se llegó a relacionar los hackers y el hacking con actividades de propósitos oscuros?

No es sencillo responder este planteamiento. Básicamente, se han construido mitos alrededor de las actividades y consecuencias del hacking, que han originado su relación con acciones contrarias a la ley. Por ejemplo, la búsqueda “hacker roba”, produce resultados como: “hacker roba banco”, induciendo a pensar que quien robó el banco lo hizo por ser hacker y no por ser un delincuente. Compárelo con el titular

[1] MIT, del ingles Massachusetts Institute of Technology / Instituto Técnico de Massasuchetts

“arquitecto roba banco”. Parece carecer de sentido, no se percibe mucha relación entre arquitecto y robo; la diferencia es que el término hacker se ha asociado en forma continua con diversos delitos, y arquitecto no. Esto le hace mucho daño al hacking y a los hackers, pero esta realidad no es muy fácil de corregir.

Otro ejemplo que ilustra muy bien este malentendido es la búsqueda “hackers famosos”, con resultados tan disparatados como: “Grace hooper” y “Kevin Mitnick”. De la misma forma, como es posible comparar: “…Una ingeniera contralmirante de la marina americana, precursora del compilador B.0, que hizo posible sentar las bases de los lenguajes de programación modernos, al traducir instrucciones del inglés a un lenguaje de programación, e inspiradora del conocido COBOL…”, con “…Un delincuente que ha estado recluido en varias cárceles, en más de seis ocasiones con cargos de fraude corporativo por computador, robo de software, terrorismo electrónico, intrusión indebida, posesión ilegal de códigos de acceso y uso ilegal de acceso telefónico, además de violar en repetidas ocasiones su régimen de libertad condicional, y que causó pérdidas millonarias con sus acciones a diferentes corporaciones…”.

Lamentablemente, para un espectador neófito ambos podrían ser hackers, pero lo cierto es que no hay punto de comparación, entre un hacker y un delincuente.

Durante la historia de la evolución de Internet, desde que se concibió como el proyecto militar Arpanet hasta ahora, el hacking se ha ido transformando, y sus propósitos como descubrir fallas en los sistemas operativos, protocolos y aplicaciones implicados en la transmisión de datos, se han mantenido, sólo que hace cinco décadas no había disponibilidad de dominios ni hosting gratuitos y, por ello, algunos hackers comenzaron a realizar pruebas en sitios disponibles que precisamente eran militares u oficiales en su mayoría (CIA, Pentágono, NASA).

Es pertinente aclarar que en aquel tiempo no existía una legislación particular sobre lo que era permitido o lícito en este terreno, pero para desgracia del hacking. Fue entonces cuando empezaron a publicar fallos que posteriormente explotaron, una de las razones por las que se le da al hacking una connotación delictiva. También esto marcó una constante lucha entre quienes descubrían los fallos y los reportaban sin ninguna pretensión distinta a informar sobre la existencia de la misma, y otros que se dedicaban a explotarlos, publicarlos u ofrecer servicios para su solución.

Clasificaciones de los hackers

Una vez que surgen intereses mezquinos, se inicia una puja entre académicos realmente motivados por el conocimiento y otros con intenciones de beneficio propio. Para marcar diferencia, se han hecho ingentes esfuerzos.

La primera clasificación conocida fue la de hackers y crackers, buenos y malos. Pero luego, hacia los años 80's, se conocieron White Hat, Gray Hat y Black Hat, según su actuación fuera buena, mala o combinada. Más adelante, con el progreso de Internet, se conoció toda una fauna de hackers por sus actividades: lammers, script kiddies, newbies, wannabe, defacer, copyhacker, bucaneros, coders, carders.

Con el paso de los años, y de acuerdo con las tendencias, los hackers fueron clasificados según su principal habilidad y reconocidos como hackers de web, bases de datos, voz sobre IP, servidores, aplicaciones, cajeros automáticos, y celulares. Más recientemente se han conocido puristas, a quienes llamaremos en este contexto verdaderos hackers, con un propósito netamente académico, que realizan pruebas en ambientes controlados y nunca sin permiso previo; crean herramientas para pruebas que liberan en la red, observan las buenas prácticas, reportan confidencialmente los fallos descubiertos al fabricante o dueño, y su intención es mantener una actitud de entusiasmo hacia el conocimiento y nunca causan daño en el desarrollo de sus actividades, toda vez que su objetivo es la seguridad.

Todas estas clasificaciones han existido, algunas se utilizan comúnmente y otras son menos conocidas, y gracias al dinamismo conceptual que las acompaña, se puede observar en muchos textos combinaciones de ellas, incluso si están en desuso, porque no hay un consenso o autoridad que regule al respecto. De ahí que muchas de ellas se mantendrán.

Lo anterior se considera un mito, porque las diversas clasificaciones de los hackers se mezclan con ciberdelincuentes y se usan para designarlos, creando así en una persona sin mucho conocimiento del tema, la idea errónea de que los hackers se dedican a delinquir.

Comportamiento y personalidad de los hackers

Mucho se ha dicho sobre la personalidad de los hackers y su comportamiento, pero, ¿qué hay de verdad?

Es importante dejar claro que un hacker es un experto en el tema en el que se desempeña. En otras palabras, no es posible ser hacker informático de redes, si no es primero un experto en redes. De esta afirmación se deriva que el hacker es especialmente "juicioso", o dedicado. Además de ello, es curioso, lo caracteriza una fuerte pasión por descubrir, conocer, crear y compartir conocimiento. Tal vez las características más deseables en un hacker son la rectitud, su responsabilidad con sus acciones y el apego a las normas, lo que significa respeto por los bienes ajenos (información), sin llegar nunca a causar un daño o perjuicio, como consecuencia de sus actos.

Por otra parte, no corresponde a una profesión, actividad u oficio, porque el hacking es una actitud hacia el conocimiento; una forma de pensar que se acerca al pensamiento lateral y que ejemplifica muy bien Pete Herzog en su escrito "Jack of All Trades", donde explica que un hacker debe pensar de manera diferente al común de la gente. Es decir, que en lugar de detenerse en cómo funciona y falla una cosa, debe razonar en cómo no funciona y cómo hacer que falle.

Esta visión permite al hacker informático explorar y descubrir nuevos usos para los que no fue concebida la tecnología, además de fallas en la programación, diseño u operación de sistemas operativos, protocolos y aplicaciones.

Sobre los rasgos de personalidad de un hacker se ha escrito mucho, basta citar la "Biblia del Hacker", "El Manifiesto Hacker", "El Libro Negro de los Hackers". Uno de los textos más aceptados globalmente ha sido el "Hagakure, código Samurái", conocido mejor como "Bushido", escrito por Tsunetomo Yamamoto, a finales del siglo XIX, que se puede resumir en siete principios básicos, a saber: Rectitud y Justicia (GI), Valor (YU), Benevolencia (JIN), Cortesía (REI), Veracidad (MAKOTO), Honor (MEYO) y, El deber de la Lealtad (CHUGO).

Los principios del Código Samurái reflejan muy bien las características deseables en un hacker y, por ello, algunos se asignan un NICK de Samurái, para dar a entender que conoce, entiende, acepta y respeta este código.

El hacking ético

Se conocen diferentes modalidades de hacking ético como análisis de vulnerabilidades, hacking ético y pruebas de penetración. En el primero, se hace un análisis superficial para conocer los peligros a los que está expuesta una infraestructura de red o sus servicios y usuarios. En hacking ético se realizan pruebas de estrés, de inseguridad, de intrusión, además de pruebas de concepto para determinar la eficacia y eficiencia de un esquema. En pruebas de penetración son adelantados análisis de fondo, considerando la mayor cantidad de variables posibles y sólo para sistemas a los cuales ya se les han aplicado técnicas de seguridad, con el fin de conocer si aún es posible ejecutar vectores de ataque exitosos. Para esta labor normalmente se requiere todo un equipo de expertos. Comercialmente, se establecen condiciones como el permiso previo por escrito, el conocimiento pleno de las pruebas a ejecutar, la presencia del encargado del sistema a evaluar, y la consideración de contingencias en caso de fallos. Este mito es uno de los más publicitados y conocidos.

En otras palabras, el hacking ético no existe, es una figura comercial, se acuñó el término con el propósito de introducir el tema empresarialmente, para ofertar pruebas de seguridad y penetración a sistemas de información, orientados a conocer sus debilidades e informarlas para corregirlas; así se reducía el efecto nocivo que hasta el momento se asocia al ejercicio del hacking. Cuando este tipo de consultoría surgió era muy complicado que una persona no familiarizada con tecnología, lograra entender que un hacker no es un delincuente y, por ello, se hacía referencia a que la ética acompañaba al hacking.

Significado e implicaciones de un verdadero hacker

Hacker no es una persona, "ser hacker" implica trabajar muy fuerte en adquirir la habilidad del pensamiento lateral, desarrollando una actitud correcta en la creación, aplicación y compartición del conocimiento, en el que el hacker es experto. Así mismo, significa que las actividades del hacking y sus consecuencias, nunca deben ocasionar daño o perjuicio a ninguna persona o bien material.

Existen entonces el hackerismo y el hacktivismo. Como hackerista se designa a cualquier persona dedicada al hacking; y, como hacktivista a quien persigue un fin político. Pero, no se

pueden calificar de hacktivismo o hackerismo, acciones relacionadas con delitos, esto no es hackear, sino delinquir.

Conclusiones

El término hacker no debe ser utilizado para referirse a un delincuente, porque afecta el buen nombre del hacking y de los hackers.

No es correcto acompañar el término hacking con el adjetivo "ético", toda vez que las actividades de hacking con fines ilegales son delictivas y, en otro caso, siempre se actúa con diligencia y en pro de mejorar la seguridad. Para la mayoría de personas, esta asociación resulta confusa.

En materia tecnológica, los conceptos no suelen ser absolutos, son dinámicos, y es fácil caer en errores que se difunden con rapidez y se asumen como correctos.

Antes de publicar una información de índole tecnológica en medios de circulación masiva, es muy recomendable (¿obligatorio?) realizar una investigación rigurosa, para no incurrir en la propagación de mitos que afecten la veracidad y causen confusión.

Cualquier persona puede ser hacker en su campo de conocimiento, si aplica a su oficio, la actitud y la forma de pensamiento del hacking.

Un mismo vector de ataque utilizado en forma académica, con fines de aprendizaje, realizado en un ambiente controlado y permiso previo, puede convertirse fácilmente en un delito, cuando se replica en ausencia de alguna de estas condiciones y, sobre todo, si se presenta daño o perjuicio en contra de un bien o persona.

Al movimiento del hacking se atribuyen muchos de los avances tecnológicos disponibles hoy en día, los cuales fueron aportes de hackers que han sido motores de desarrollo y progreso constante y veloz en la historia.

Finalmente, un hacker es una persona apasionada y dedicada con juicio a un campo de conocimiento, en el cual permanentemente explora, descubre, crea y comparte su labor; además, es poseedor de cualidades éticas elevadas, por lo cual debe ser respetado.

Referencias

[1] Ríos, Rubén H, La Conspiración Hacker: Los Robinhoods de la cibercultura, Longseller, 2003.

[2] Vieites, Gómez Álvaro, Enciclopedia de la Seguridad Informática, Alfaomega, 2007

[3] Sallis, Caracciolo Rodríguez, Ethical Hacking, Alfaomega, 2010

[4] Winkler Ira, El Zen y el arte de la seguridad de la información, Grupo Editorial Patria, 2008

[5] Jimeno García María Teresa, Miguez Pérez Carlos, Matas García Abel Mariano, Pérez Agudín Justo, La Biblia del Hacker Edición 2009, Anaya

[6] Himanen Pekka, La Ética del Hacker y el espíritu de la era de la información, Ediciones Destino, 2001

[7] Flor, Monsiriu Mar, Técnicas del Hacker para papas, Alfaomega, 2008

[8] Watson Jr., Thomas J, Petre, Peter, Padre Hijo & Cía.: Mi Vida En La IBM y Mas Allá, Editorial Norma, 1990

Federico Gacharná Gacharná. *Ingeniero de Sistemas, Consultor Sénior en Inteligencia Informática; Hacking Ético e Informática Forense para entidades de seguridad del Estado en Colombia, Guatemala, Panamá, Perú, y Salvador. Instructor Internacional en Hacking Ético, Computación Forense y Seguridad en Redes. Maestría en Seguridad Informática, universidad Oberta de Catalunya; Diplomado en Docencia Universitaria, universidad Minuto de Dios; Diplomado en Investigación, universidad Cooperativa; Director del Área de Seguridad de la Información del Programa de Tecnología en Redes y Seguridad Informática y, Director del Diplomado en Seguridad Informática, universidad Minuto de Dios; organizador del Congreso Nacional de Hacking Ético y Computación Forense. Presidente de Elite Hackers.*