El estigma Hacker, entre lo bueno y lo malo

Federico Iván Gacharná G.

Recibido el 15 de marzode 20111. Aprobado el 26 de abril de 2011

Resumen
El presente artículo pretende aclarar el hecho que un grupo reducido de personas que ejercen una actividad, profesión u oficio, y el mismo decide actuar de forma reprochable o contraria a la ley, esto no puede ser pretexto para estigmatizar la profesión misma; La situación descrita, es la que ha tenido que afrontar el hackerismo por la mala publicidad que, por desconocimiento o desinformación, se ha dado de hechos aislados, creando en el imaginario público una imagen negativa del hacking, emitiendo comentarios lesivos ("Hacker roba banco"), frente a lo cual se recomienda llamar delincuente a la persona que comete un delito, independiente de la profesión que ejerza, y abstenerse de emitir juicios de valor sobre su profesión u oficio.

Palabras clave
delito informático, estigma, ética, hacker, hackerismo, hacking.

Abstract
The intention is preset clear that if a small group of persons engaged in an activity, occupation or profession decide to act in a blameworthy or contrary to law is no excuse to stigmatize the profession itself, a situation that has faced the hackers by the bad publicity, due to ignorance or misinformation has been given to isolated incidents in the public imagination by creating a negative image of hacking, emitting harmful comments ("Hacker steals bank"), against which there are delinquent should call the person who commits a crime, regardless of the profession to exercise, and refrain from making judgments about their profession or trade.

Keywords
computer crime, cyber crime, ethic, hacker, hacking, stigma

I. Introducción

Si una persona aplica a un cargo de analista de seguridad, y en el proceso de selección menciona que es Hacker, probablemente lo rechazarán. Pero, si el seleccionador es una persona que tiene conciencia de lo que realmente significa ser hacker, dejaría de buscar e inmediatamente, lo contrataría.

Asimismo, conociendo la opinión generalizada acerca de los Hackers, si un profesional en una reunión de colegas, hablando de actividades de cada uno, señala que es Hacker, probablemente sus compañeros cuestionarán su ética, procedencia, o se harían conjeturas prejuiciosas sobre sus actuaciones.

De lo anterior, es posible reconocer una actitud común entre quienes ejercen la actividad de hacking, y es que se ven forzados a asumirla de

manera silenciosa o anónima, como reacción frente al rechazo social.

Este rechazo, aunado al periodismo amarillista-tendencioso, con el paso del tiempo se volvió un estigma, y este señalamiento origino que muchos grupos de hackers pasaran a la clandestinidad, el anonimato y la negación de su actividad, ratificando en el público la idea que efectivamente había algo peligroso que esconder, y, en defensa de su actividad y viéndose vulnerados sus derechos, ***algunos*** pocos hackers violaron la ley y se convirtieron en delincuentes, dando origen al fenómeno del "Netwar[1]" y sus múltiples leyendas, unas publicadas, otras guardadas en celoso secreto, sobre los ataques de los hackers a sus persecutores (entiéndase: CIA, FBI, INTERPOL). *El resultado de las actividades de este reducido grupo, propició el estigma que hoy en día se asocia, de forma generalizada, al término HACKER.*

II. Entre lo bueno y lo malo

Refiriendo a las profesiones, y tomando como ejemplo la medicina, es incorrecto afirmar que existe una medicina buena y una mala, en realidad un juicio de valor solo es posible concebirlo desde la persona que ejerce la medicina, solo desde una valoración del ejercicio de la profesión es posible calificar sus actuaciones como correctas o equivocadas, así, un hacker brillante en la aplicación de técnicas de aseguramiento de la información es reconocido como un "buen hacker". Además, debe ser una persona que domina los conceptos con profundidad, con ***ÉTICA*** profesional intachable, que se apega a las normas y estándares internacionales, en su actuar profesional es responsable, respetuoso y posee altas calidades humanas. Por otra parte, un "mal hacker" sería una persona que se autodenomina hacker y hace comentarios como: "mira lo buen hacker que soy, descubrí la contraseña de tu casilla de correo"; Evidenciando con esta actitud que es una persona con principios éticos cuestionables, y que no posee los conocimientos fundamentales que implican la actividad hacking; Estas personas se aprovechan de la poca información que los usuarios tienen sobre el tema, para ofrecerles servicios como: "hackear el Internet inalámbrico del vecino", "hackear los discos duros para recuperar los archivos borrados", "hackear conversaciones privadas de mensajería instantánea de los empleados o sus mensajes de correo electrónico" y otras actividades similares, que hacen que se refuerce la idea que todos los hackers se dedican a este tipo de cosas. También resulta muy perjudicial para el hacking, que estos personajes publiciten en sus páginas Web, foros, listas de correo, blogs y buscadores sus dudosas actividades, confundiendo aún más la opinión pública sobre lo que REALMENTE significa ser Hacker.

> *Estas actividades generan la idea errónea, promovida por los medios de comunicación, que cada vez que una persona se dedica al hacking, delinque; los periodistas aplican censura a la noticia dejando una duda razonable y reforzando la idea que la persona que cometió el delito lo hizo por el simple hecho de ser hacker.*

Se debe entonces aclarar que si un Hacker comete un delito debe ser visto como un delincuente por la acción cometida y no por el hecho de ser hacker; ***el hacking es una actividad licita y ética por ser un oficio respetable y necesario para impulsar el progreso de la sociedad, como cualquier otra profesión u oficio reconocida y aceptada socialmente***, por tanto, es importante revalorar la profesión como una actividad con el mismo estatus que tienen las demás, para otorgarle el reconocimiento que se merece por ser una de las profesiones que caracterizan el nuevo siglo y baluarte de la sociedad del conocimiento.

III.Buscando conocimiento gano mala fama

El origen de la actividad hacking puede ser cuando en 1959, los miembros del club TRM del MIT, desarrollaron el código para ingresar datos directamente sobre la IBM 407, para agilizar el procesamiento de datos, se vio como una actividad no autorizada, sin embargo, lo que el grupo pretendiera generar nuevas formas de explotar el potencial de las máquinas, para difundir los resultados de forma libre e irrestricta, posteriormente esta actividad fue reconocida como *copyleft*. Como este grupo pertenecía a una institución de muy alto nivel y el club de matemáticas era solo para algunos intelectuales muy selectos, sus actividades adquirieron la connotación de ser excluyentes: sólo para un grupo élite muy especifico, no así el conocimiento que se generó. Teniendo en cuenta lo anterior, es claro que desde su nacimiento, las circunstancias en que surgió esta actividad contribuyó en gran medida, a la creación del estigma que el hacking es una actividad oculta, secreta, excluyente y con visos de ilegalidad.

Con el paso del tiempo y el desarrollo de las tecnologías de las redes de comunicación sobre Internet,

1. Como Net-War o Network-Combat se conoció el enfrentamiento entre grupos de atacantes y sus contrapartes en el gobierno, sector militar e inteligencia de los estados, que se suscitó como reacción a las persecuciones hechas por unos y otros

se crearon nuevos recursos cómo los BBS[2], los cuales se convirtieron en los espacios para intercambiar información sobre vulnerabilidades y contramedidas de sistemas operativos, aplicaciones y protocolos de comunicación. Esto generó que se formaran tres corrientes: aquellos que se dedicaron a encontrar las debilidades de seguridad en los sistemas de comunicación e información (Bugs), aquellos que vieron una oportunidad de sacar provecho de estos Bugs creando programas maliciosos (xploits) y los sufridos fabricantes de hardware para redes y las casa de software que se desgastan programando soluciones (patches) para unos otros.

Cuando se hace público el resultado de cualquiera de las anteriores actividades se dice que fue producto de un Hacker, lo cual resulta ser bastante irrespetuoso para aquellas personas que dedican su esfuerzo para el desarrollo del conocimiento, al equipararlos con delincuentes. Se debe tener cuidado en la forma en que se usa el término, un Hacker construye conocimiento, cumpliendo con el compromiso ético que tiene como profesional, un delincuente informático destruye este conocimiento corrompiéndolo con sus actividades mezquinas de propósitos distantes al desarrollo tecnológico y social.

En la actualidad, han cerrado, perseguido –injustamente- comunidades hackers por percepciones equivocadas del sistema de justicia, de organismos de seguridad e inteligencia oficiales, que afirman que: "se combate el delito delinquiendo", aportando un elemento más para que el estigma gane fuerza, sin embargo, estos mismos organismos, aplicando una doble moral, han usado servicios de hacking para perseguir delincuentes y judicializarlos, así como en otras oportunidades han negociado las penas de los delincuentes informáticos a cambio de que trabajen para ellos, dejando al delincuente sin su debido castigo, propiciando la confusión de que un Hacker es necesariamente un delincuente.

IV. Conclusiones

· Han existido en el tiempo diversos estigmas que afectan negativamente la imagen del ejercicio del hacking, fundados en las circunstancias especiales que rodearon el inicio de esta actividad hacia la dècada de los años 60's, la persecución rabiosa y con poco fundamento legal y de procedimiento e incluso aún sin entendimiento de las implicaciones y consecuencias de la actividad misma y más impulsadas por tendenciosos titulares de prensa y la desinformación implicita en ellos.

· El hacking ha ayudado a desarrollar las tecnologías emergentes en las últimas cuatro decadas y sobre todo la Internet, gracias a los aportes hechos por los hackers, hoy en día existen avances como el IRC y los foros, y utilidades como detectores de intrusos, software antimalware e innumerables avances técnicos que deben su aparición y constante evolución a lso hackers y sus actividades.

· Las diversas actividades que es posible desarrollar en Internet, conllevan responsabilidades de orden social y legal que los usuarios rara vez entineden o ignoran concientemente. Es necesario desarrollar conciencia en los usuarios y directivos de las organizaciones y particulares ademas de usuarios en general y desarolladores de contenidos así como administradores de infraestructura tecnológica para evolucionar a modelos de comunicación más seguros, estables y cómodos para la comunidad usuaria, siempre en crecimiento

A manera de reflexión, tres importantes invitaciones:

Al público general, para que rechacen las malas prácticas sobre el uso de tecnologías y se informen muy bien sobre el verdadero propósito del hacking. Se recomienda leer sobre ética y filosofía hacker.

A los medios de comunicación, para que se reflexione sobre el uso del término Hacker cuando se haga referencia a un delincuente informático.

A los organismos de seguridad, inteligencia y al sistema judicial, para que no estimulen las actividades delincuenciales relativas a la informática.

V. Referencias

[1] Anónimo, (2000), *Linux Máxima Seguridad*, Madrid, Prentice Hall.
[2] Coleman, M. (1997), *Conspiración en la Red*,Ediciones Grupo Zeta.
[3] Coleman, M. (1997), *Tecla de Escape*, Ediciones Grupo Zeta.
[4] Goncalves, M. *et al*. (1997) Internet Privacy Kit, Indianápolis, Que.
[5] Himanen, P. (2001), *La Ética del Hacker y el espíritu de la era de la información*, Barcelona, Ediciones Destino.
[6] Mc Clure, S; Scambray, J & Kurtz, G. (2002), HACKERS 3, Mc Graw-Hill.
[7] Parker, D. (1998), *Fighting computer crime*. A new framework for protecting information, New York, John Wiley & Sons Inc.

2. Bulletin Board Systems: Los BBS se componían de una computadora y un módem que alcanzaba una red de computadoras personales con el fin de centralizar e intercambiar mensajes entre los usuarios

[8] Ríos, R. (2003), *La Conspiración Hacker*, 1ª.Ed. Buenos Aires. Longseller
[9] Verton, D. (2004), *BLACK ICE, La Amenaza Invisible del Ciberterrorismo*, Mc Graw -Hill.

Federico Iván Gacharná Gacharná. *Ingeniero de Sistemas, Diplomado en Docencia Universitaria, Master en Seguridad Informática, U. Ouberta de Catalunya, Director del Área de Seguridad de la Información, Corporación Universitaria Minuto de Dios (UNIMINUTO), Organizador del Congreso Nacional de Hacking Ético, CEO Comunidad Hackers Colombianos, Docente, Investigador. Experto en Inteligencia Informática, Cómputo Forense y Hacking Ético. Federico.gacharna@hackingetico.info.*