Hackers

Hoy en día es un término que provoca temor entre aquellos que han sido víctimas de sus fechorías, los medios de comunicación lo satanizan y a la vez lo elogian, algunas organizaciones invierten decenas de miles de pesos para evitar su presencia y otras más gastan cantidades similares para contratarlos. Nos referimos a los *hackers* o piratas informáticos. Pero ¿por qué es un término tan disímbolo? ¿Por qué tan enigmático? Para comprenderlo mejor es necesario conocer algunos aspectos básicos que delinean el perfil de estos controvertidos personajes.

Los *hackers* y la cultura asociada con ellos se iniciaron en las décadas de los 60 y 70, en universidades como MIT, Carnegie Mellon, Berkeley, CalTech o Standford, que tenían la capacidad de mantener equipos de cómputo y una gran cantidad de alumnos sedientos de conocerlos, programarlos y experimentar con ellos, hasta llegar a las entrañas mismas de su arquitectura. Sin embargo, a lo largo de los años este término se ha enrarecido y hasta mitificado dentro del ámbito de lo ilegal, lo maligno y lo destructivo. Si nos detenemos a revisar la definición de *hacker*, encontraremos autores como Sweigart (2013), quien lo detalla como un individuo que estudia un sistema (informático) para comprenderlo tan profundamente que pueda ser capaz de modificarlo de distintas formas, en su mayoría creativas. Por su parte, Erickson (2008) señala que el *hacker* resuelve problemas en formas inimaginables comparado con aquellos que se circunscriben a resolverlos mediante metodologías convencionales. Incluso Palmer (2001) describe el término *hacker* como aquella persona que programa de manera entusiasta y aprende en detalle los sistemas de cómputo.

En efecto, un *hacker* es una persona que tiene profundos conocimientos de informática, es decir, maneja muy bien los sistemas operativos, la programación, la arquitectura de computadoras y los sistemas de comunicación de datos, entre otros. Su objetivo principal es conocer y demostrar que conoce. Sin embargo, ¿por qué se han ido creando la fama de ser individuos que están fuera de la ley? La respuesta más simple es por la falta de autorización. Muchos *hackers* penetran sistemas informáticos sin que sus propietarios o administradores tengan conocimiento de ello; eso justamente los hace caer en la ilegalidad, y además, una vez realizada su fechoría, la información obtenida puede ser empleada para cometer actos criminales.

A pesar de ello, no todos los *hackers* siguen esa línea de acción. Long (2010) asegura que la diferencia entre los buenos *hackers*, también llamados *hackers* de sombrero blanco (*white hat hacker*) o *hackers* éticos y los *hackers* malos (*black hat hackers*) o *crackers*, es que los primeros tienen autorización expresa de revisar, probar, desentrañar y modificar los sistemas informáticos con la finalidad de detectar vulnerabilidades y posteriormente desarrollar y aplicar medidas de seguridad, parches o mejoras; en cambio, los segundos irrumpen en dichos sistemas con la intención de robar o destruir información, sabotear, cometer fraudes y generar caos actuando de manera ilegal e irresponsable. La gran ventaja de los *hackers* de sombrero blanco es que, al tener habilidades y capacidades muy parecidas a las de sus contrapartes, ejercen acciones preventivas eficientes que les permiten proteger adecuadamente los sistemas para evitar posibles ataques que pudieran debilitar la seguridad de la infraestructura informática de una organización.

Pero, para complicar más las cosas, saltan al escenario los *hackers* de sombrero gris (*gray hat hackers*). Como su color lo indica, son una mezcla entre los sombreros blancos y los negros. Se dedican a identificar vulnerabilidades y, en ocasiones, a comprometer la seguridad de los sistemas; una vez que las encuentran, establecen contacto con los propietarios para informar al respecto, y solicitan eventualmente algún tipo de pago o recompensa económica por sus servicios. En principio, sus propósitos no son malignos, pero al hacerlo sin permiso caen en la ilegalidad. Adicionalmente, están los *script kiddies*, personajes que, con poca experiencia en el área del cómputo, hacen uso de herramientas empleadas o desarrolladas por los *hackers* y realizan ataques informáticos, en general únicamente para llamar la atención de sus "pares".

Alrededor de la comunidad *hacker* se han creado muchos mitos; los medios de comunicación en general y Hollywood en particular se han encargado de nutrirlos, haciéndolos parecer ante la sociedad como auténticos héroes o villanos, personajes del bajo mundo protegidos por mafias o individuos inadaptados que actúan solos y a la sombra del anonimato. Películas como The Net (1995), Hackers (1995), Pirates of Silicon Valley (1999), Takedown (2000), Swordfish (2001) o Duro de matar 4.0 (2007) dan cuenta de ello. Por esta razón, el *hacker* se ha convertido en un ser enigmático y profundamente atractivo para muchos jóvenes. Aunado a lo anterior, el acceso masivo y casi ilimitado a la tecnología móvil, al Internet y a las redes sociales, inherentes a las nuevas generaciones, pueden provocar que la información sobre el *hacker* y todo su entorno provenga de fuentes poco confiables, esté tergiversada o sea mal interpretada, afianzándolo aún más como un personaje mítico.

Así pues, los *hackers* no son necesariamente sinónimos de ilegalidad, delincuencia, crimen organizado o acciones fraudulentas. Al conocer un poco más de ellos no solo es posible comprender la importancia que tienen en la protección de los sistemas, sino además advertir que su lado oscuro obligará a diseñar e instrumentar más y mejores medidas de seguridad, mantener actualizadas las tecnologías de la información y hacer más eficiente el trabajo de los encargados de la seguridad informática.