Relatório sobre a diferença ética entre Hacking Ético e Hackerativismo

TAG de Ética

UFRJ

Thais Angelo Ferreira de Oliveira

Hacking Ético X Hackerativismo

Atualmente, empresas das mais variadas áreas como bancos, telecomunicações, agências governamentais entre outras organizações estão em uma busca constantemente por profissionais e empresas especializadas em Ethical Hacking para combater a crescente ameaça à segurança de TI. Com o constante crescimento da tecnologia é muito fácil se tornar alvo de uma falha de segurança que pode ser explorada por invasores e possivelmente causar prejuízos gigantescos, como roubo de informações e dinheiro, prejuízos à imagem da instituição, paralisação de seu serviços e diversos outros danos.

Um profissional ou uma empresa especializada em etical hacking, tem como função cuidar da cibersegurança da empresa, ou seja, o objetivo deles é a identificação e consequentemente a criação de métodos de proteção contra vulnerabilidades existentes no sistema. Assim, o trabalho dele é em parte realizar a invasão de computadores com a autorização do dono para explorá-lo de maneira profissional, com base na direção do cliente e, posteriormente, apresentam um relatório de maturidade destacando seus riscos e vulnerabilidades gerais e sugestões para melhorar.

No meu ponto de vista , não há desvantagem em contratar um serviço desse tipo pois, se o profissional ultrapassar as defesas atuais do sistema, será dado ao cliente a oportunidade de fechar os problemas achados antes mesmo que o invasor descubra as vulnerabilidades para começar a explorá-las. Se não for encontrado nada, o cliente ficará satisfeito, pois ele sabe que seus sistemas são “seguros o suficiente para usa-los” .

O principal beneficio do hacking etico é impedir que dados sejam roubados e mal utilizados por invasores e bem como:

- Descobrir vulnerabilidades do ponto de vista de um invasor para que pontos fracos possam ser corrigidos.

- Implementar uma rede segura que evita violações de segurança.

- Ganhar a confiança de clientes e investidores, garantindo a segurança de seus produtos e dados.

A prática do hackerativismo vai muito além de invadir e derrubar sites. O objetivo maior por trás de toda a operação é contestar uma causa e gerar impacto. Ele é usado para promover ideologia política.

Com o passar do tempo, o hacktivismo ganhou diversos perfis e diferentes grupos ficaram conhecidos por ações como interceptação de dados, desenvolvimento de aplicativos que permitissem furar bloqueios de censura de internet, paródias virtuais, DDos, desfiguração de sites, entre outros.Esta ação pode ser vista como uma forma de ciberativismo e a sua prática vai muito além de invadir e derrubar sites. O objetivo maior por trás de toda a operação é contestar uma causa e gerar impacto.

A sua eficiência é incontestável, qualquer profissional da área de tecnologia da informação, mais especificamente da área de segurança da informação, é capaz de realizar uma ação hackerativista. Ademais, realizar ações ativistas por meio desta pratica exige apenas uma pessoa ou um grupo pequeno, enquanto formas comuns de ativismo exige um número muito maior e notório de indivíduos para realizar ações que geram o mesmo impacto e a mesma pressão.

Um exemplo desta pratica é o caso da Caça às baleias. Em dezembro de 2015, websites do primeiro-ministro, dos ministérios do Interior e do Meio Ambiente da Islândia foram

derrubados por um grupo de ativistas em protesto à caça das baleias, prática polêmica que acontece amplamente no norte do Oceano Atlântico. O grupo convidava os internautas a utilizarem uma rede social para postar comentários sobre o assunto. O mesmo aconteceu com o site da montadora japonesa Nissan, que pagou pela prática do governo de seu país ao também incentivar esse tipo de pesca.

Agora, com os conceitos já explicados é possível ver que por mais que essas atividades tenham seus meios comuns a diferença ética entre os dois é grande. Por mais que no primeiro o profissional tem permissão para invadir o sistema em busca de vulnerabilidades que possam ser exploradas, ele precisa ter ética ao realizar este trabalho, pois ele tem acesso a todas as informações da empresa e pode fazer alguma ação maliciosa com elas. Já no segundo, a ação realizada pode até ser por uma causa considerada justa por muitos, mas ela não é ética pelo fato de realizar ataques, ou seja acessar o sistema alvo sem permissão, com objetivos de gerar algum impacto, seja considerado bom ou não.