Oktober 2024
Kantonsschule Im Lee

Kantonsschule Im Lee

Maturitätsarbeit

Hacking und Cybersicherheit

Corsin Streit[1] unter Aufsicht von Thomas Graf[2]

[1]Student, Kantonsschule Im Lee, Winterthur

[2]Fachschaft Informatik, Kantonsschule Im Lee, Winterthur

Abstrakt

Das Ziel dieser Arbeit besteht darin, durch Literaturrecherche und selbstständiger Nachforschung einen für die Allgemeinheit verständlichen Überblick über das Thema Hacking und Cybersicherheit zu schaffen. Dazu werden technische Grundlagen und Hacking-Methoden erläutert und anhand von konkreten Beispielen anschaulich dargestellt. Ferner wird auf die Themen Dark Web, Künstliche Intelligenz im Bereich des Hackings und rechtliche Aspekte eingegangen.

Stichworte: Hacking, Cybersicherheit, Hacking-Methoden, Dark Web, Künstliche Intelligenz

Inhaltsverzeichnis

1 Einführung

Der Stereotyp ist schlecht wegzudenken. Schwarzer Kapuzenpulli, abgedunkelter Raum und ein Bildschirm mit kryptografischen Zeichen. Auf dem Computer laufen bösartige Programme, die Schwachstellen von anderen ausnutzen und dabei Unheil anrichten. Die Handlung ist kriminell und bestrafbar. Auch wenn diese stereotypische Beschreibung wohl auf eine sehr kleine Gruppe von Personen zutreffen mag, sieht die Realität bedeutend anders aus und die Welt der Cybersicherheit ist, zumindest konzeptuell, viel weniger abstrakt als die meisten Leute denken.

1.1 Bedeutung und Urpsrung des Begriffes

Im Grunde genommen ist ein «Hack» nichts mehr als eine «von Innovation, Stil und technischem Können durchdrungene» Lösung zu einem Problem, das nicht einmal einen Bezug zu Computern aufweisen muss. Den Ursprung nahm der Begriff im Modelleisenbahnclub des Massachusetts Institute of Technology, kurz MIT. Aus geschenkten Elektronikbauteilen bauten die Clubmitglieder die Steuerung ihrer Modellzüge. Durch verschiedene Optimierung, Hacks, versuchten sie, diese so elegant wie möglich zu gestalten. Ihr Ziel war nicht das simple Funktionieren. Es war nicht einmal wichtig, dass die Lösung einen grossen Nutzen zeigte. Was zählte, war die technische Eleganz, die hinter der Lösung steckte.
Mit dem Erscheinen erster Computer und der Gründung eines Computerclubs im MIT wurde die Bedeutung auf die technische Welt ausgeweitet. Als Steven Levy 1984 die Leiterprinzipen des Hackings zu einer «Hackerethik» zusammenfasste, formulierte er folgenden Satz: «Du kannst mit Computern Kunst und Schönheit schaffen.» [5]

Das Negative, das viele Personen heute mit dem Hacking assoziieren, wurde erst nach und nach dem Bedeutungskonzept hinzugefügt. Nach weiteren Grundsätzen der Hackerethik sollten sich Hacker*innen für freie Informationszugänglichkeit, Dezentralisierung und unlimitierten Zugriff auf alles, was einen etwas über die Welt lehren kann, einsetzen. Mit den gesetzlichen Richtlinien nahmen sie es nicht genau. Die Neugier, Wissensbegierde und allgemein das technische Interesse führte zur Entdeckung und Erkundung neuer «Spielwiesen», was in den 1960er-Jahre zum ersten «modernen» Hack führten. Findige Hacker fanden heraus, dass sich durch das Abspielen einer ganz bestimmten Frequenz das Telefonnetz so manipulieren liess, dass Anrufe nicht verrechnet wurden. Sogar Tech-Legenden wie die späteren Apple-Gründer Steve Jobs und Steve Wozniak beteiligten sich an dem sogenannten Blue-Boxing und verdienten Geld durch das Verkaufen von Frequenzgeneratoren, den Blue-Boxes.
Zeitungsartikel und Filme, insbesondere der 1983 veröffentlichte Titel War Games, trugen in grossem Masse zur heutigen Auffassung des Hackers bei. Ein Hacker*in ist

«jemand, der*die ohne Erlaubnis in die Computersysteme anderer Leute eindringt, um Informationen herauszufinden oder etwas Illegales zu tun.» (übersetzt von Cambridge Dictionary) [5, 3]

1.2 Motivation, Ethik und Begriffserklärung

Die Motivationen und Ethiken, die Hacker*innen verfolgen, fallen sehr unterschiedlich aus. Grob kann man sie in zwei Kategorien einteilen: die «Black Hats» (auch «Cracker» genannt) und die «White Hats» (auch «Penetration Tester» genannt).
Black Hat Hacker*innen verfolgen kriminelle Ziele, die (umwelt-)politisch, monetär oder egoistisch motiviert sein können. Oftmals verbreiten sie Malware (siehe Kapitel 3.3). Dabei ignorieren sie legale und ethische Grundsätze.
Ihre Gegenspieler sind die White Hat Hacker*innen. Diese benutzen dieselben Methoden, arbeiten aber im Rahmen der Gesetze und halten sich an ethische Grundsätze. Ihre Aufgabe ist es, Privatpersonen, Firmen oder ganz allgemein gefährdete Computer vor den Black Hats zu schützen. Um dies zu bewerkstelligen, hacken sie sich nach vorheriger Absprache mit den Besitzer*innen in Computersysteme ein, um mögliche Sicherheitslücken zu finden und zu beheben.
Dazwischen liegt die dritte Kategorie der Grey Hat Hacker*innen, die zwar oftmals illegal vorgehen, dabei aber keine negativen Absichten verfolgen. Beispielsweise hacken sie sich unberechtigt in ein Firmensystem ein, kommunizieren aber danach die gefunden Schwachstellen. [1, 2]

Ein weiterer oft verwendeter Begriff ist «Script Kiddies». Dies sind ungeschulte (meist junge) Person ohne tiefgründige Hacking-Kenntnisse, die «von anderen entwickelten Skripts oder Programme für hauptsächlich böswillige Zwecke verwenden» (übersetzt von Wikipedia). Nichtsdestotrotz können sie grosse Schäden anrichten. [4]

Sprach-Disclaimer

Es finden sich englische Begriffe in dieser Arbeit. Da Computerwissenschaften normalerweise nur in englischer Sprache praktiziert werden, existieren für einige Begriffe keine passende deutsche Übersetzungen. In diesem Falle wird auf den englischen Begriff zurückgegriffen.

Literatur

[1] Jean Abeoussi. „White Hat and Black Hat - The thin line of ethics.edited“. In: (Okt. 2019).

[2] *Black Hat-, White Hat- & Grey Hat-Hacker*. https://www.kaspersky.de/resource-center/definitions/hacker-hat-types.

[3] *HACKER | English meaning - Cambridge Dictionary*. https://dictionary.cambridge.org/dictionary/english/hacker.

[4] *Script kiddie - Wikipedia*. https://en.wikipedia.org/wiki/Script_kiddie.

[5] Christian Stöcker. *Kleine Geschichte der Hackerkultur | Cybersicherheit | bpb.de*. https://www.bpb.de/shop/zeitschriften/apuz/cybersicherheit-2023/521304/kleine-geschichte-der-hackerkultur. Mai 2025.

Abbildungsverzeichnis

Tabellenverzeichnis