BHT Berliner Hochschule für Technik

Ethisches Hacking

vorgelegt von
Daniel Riel
Matrikel .Nr.: 842 072

Modulprüfung - Hausarbeit: Ethik in der IT-Sicherheit

Fachbereich VI
Informatik und Medien
Medieninformatik Online Bachelor
Berliner Hochschule für Technik, Berlin

Prüfungsdatum: 05. Juli 2022

Modulverantwortlicher
Prof. Dr. Matthias Schmidt Berliner Hochschule für Technik

Inhaltsverzeichnis

I Ethisches Hacking

1.1 Was ist ethisches Hacking?

Ein ethischer Hacker, der unter einer anderen Bezeichnung auch *White Hat Hacker* genannt wird, bezeichnet in der Cybersecurity einen Sicherheitsexperten, der von vielen Unternehmen angeheuert wird, um ihre IT-Systeme systematisch auf Schwachstellen in Unternehmensnetzwerken und Anwendungen aufzudecken. Im Gegensatz zu den *Black Hat Hackern*, die man heutzutage als unethische Hacker üblicherweise kennt, stehlen diese keinerlei unerlaubten Informationen, da die erfolgen Hackingangriffe mit der Genehmigung und der Kenntnisnahme der Unternehmen erfolgen. [Pol D]

Unabhängig vom Typ des Hackers stellt sich gleichzeitig auch die Frage, kann Hacken ethisch sein? Grundsätzlich kann diese Fragestellung mit einem Ja beantwortet werden. Dies knüpft jedoch an gewisse Bedingungen an. Zunächst einmal ist ein Hacker grundsätzlich nur eine Person, die nach Schwachstellen in einem System und das Eindringen in die IT-Infrastruktur sucht. Ob nun die Frage ist Hacken ethisch oder unethisch ist, müsste über die Hackerethik und die Absicht, die ein Hacker hat, geklärt werden.

1.2 Hackerethik

Sei es aus reiner Neugier oder aus Aktivismus, Hackingangriffe unabhängig des Ausmaßes und des Zwecks, muss es gewisse Grenzen geben, die besagen, wie weit eine Person gehen darf und was im Bereich des Guten liegt und was nicht mehr als OK angesehen werden kann und ggf. in den Bereich einer Straftat hinein manövriert. [Rie18] Aus diesem Anlass folgt ethisches Hacken einiger Leitlinien.

Der Chaos Computer Club e. V. definiert die Hackerethik (Auszug), die als eine Sammlung von Grundsätzen gilt, folgendermaßen:

- „Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
- Alle Informationen müssen frei sein.
- Mülle nicht in den Daten anderer Leute.
- Öffentliche Daten nützen, private Daten schützen.“

[Clu D]

Doch ist es notwendig, dass es gewisse Leitlinien gibt? Welcher Sinn steckt hinter einer Hackerethik? Ist es nicht interessanter, etwas zu tun, ohne groß über die Konsequenzen nachzudenken? „Der Impuls dazu: *Macht schafft Verantwortung*.“ [Rie18] Blickt man auf die Hackercommunity, wird schnell erkennbar, es gibt Menschen, die einen Höheren drang zum Wissen, der Neugier oder dem forschen besitzen als der durchschnitt. Dies birgt aber auch die Gefahr, etwas zu tun, das andere Menschen gewissermaßen ins schlechte Licht rücken könnte. Ihnen Schaden zuzufügen, sodass diese Menschen ein schlechteres Leben haben können. Aus diesem Grund sollten die Leitlinien der Hackerethik dem einen gewissen Riegel vorschieben. [Rie18]

1.2.1 Zugang von Informationen

Mit der Idee „*Macht schafft Verantwortung*“ [Rie18] ist bezugnehmend auf die heutige Gesellschaft nicht mehr so populär. Schaut man sich die Gesellschaft an, distanziert sich diese von den Werten Freiheit, Gleichheit und Brüderlichkeit hin zur Spaltung der Menschheit und weg von der Aufklärung. Nach dem Moto: *„Ich kann mich selber durchsetzten, der Rest der Menschheit ist mir egal.“* Aber genau die Werte der Aufklärung sind es, die Menschheit in eine bessere Zukunft zu führen. Doch was ist dazu nötig? Einfach gesagt: Wissen oder Aufklärung! Dies führt uns auch zu dem ersten Punkt in der Hackerethik.

„Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.“ [Clu D] Wenn man heutzutage an Informationen kommen möchte, gibt man seine Suchbegriffe bei Google oder einer anderen Suchmaschine ein. Die gesuchten Informationen werden mit sehr vielen Daten bezahlt oder im Hinblick auf Wissenschaftsverlage werden diese Information mit Geld bezahlt. [Rie18] Dies ist auch eng verbunden mit dem zweiten Punkt. Denn „Alle Informationen müssen frei sein.“ [Clu D]

1.2.2 Die Offenlegung und der Schutz von Daten

Abgeleitet aus dem allgemeinen Persönlichkeitsrecht, hat ein jeder das Recht und die Freiheit, genau so viele Daten freizugeben, wie ein jeder möchte. [jb-JB D]

Das Problem hinter der Offenlegung zu vieler privater Daten, das „Mülle nicht in den Daten anderer Leute“ [Clu D] macht den Menschen angreifbar. Als Beispiel kann die Webseite Facebook genannt werden. Nutzer, die auf dieser Seite ein Profil anlegen, geben sehr viele Daten über sich preis. Angefangen über seinen Vor- und Nachnamen, über seine Wohnorte, Bildungsgänge, seinen Hobbys bis hin zu seinem Arbeitgeber und noch vieles mehr kann angegeben werden. Hier werden schon sehr tiefe Einblicke in seine Privatsphäre mit der ganzen Welt geteilt. Wird ein Datenleck durch Sicherheitslücken anderer IT-Systeme aufgedeckt und gleichermaßen sensible Daten kommen zum Vorschein, kann einer Person sehr viel Schaden zugefügt werden.

II Fazit

Ethische Hackergruppen helfen Firmen zu Verstehen, welche Sicherheitsrisiken sie zu befürchten haben und welches Ausmaß auf ihre vertraulichen Daten diesbezüglich hat, wenn ein böswilliger Hacker z. B. Zugriff auf ihr System bekommt. Dabei wird *ethisches Hacking* eher als Tool angewandt, mit dessen potenzielle Sicherheitslücken aufgedeckt werden. Hacken trifft zwangsläufig mit beiden Welten der Guten sowie der bösartigen Seite zusammen. Wobei ethisches Hacken diesbezüglich eine grundlegende Rolle spielt im Hinblick der Sicherheit der sensiblen Daten und unethisches Hacken eher mit der Zerstörung und der Offenlegung sensibler Daten zu tun haben, mit dem Hintergrund Personen zu schaden. Demzufolge muss immer beachtet werden, welche Intentionen ein Hacker mit seinen Angriffen hat. Doch einen 100%-tigen Schutz gegen böswillige Angriffe wird es leider auch in naher Zukunft nicht geben.

Unabhängig des Sicherheitsstands der IT-Systeme sollte man sich auch weitergehend fragen, was wäre, wenn? Hier ein weiterführendes Beispiel: Person A dringt in ein IT-System ein und diese wird von einer Person B gehackt. Wie verhält sich dann Person A? Ist das, was sie tut, weiterhin legitim oder das eigene Handeln, was man zu Beginn mal vor hatte, noch gerechtfertigt? Die Antwort kann Ja sein, sie kann aber auch dahingehen, dass man vielleicht vorher hätte mal Nachdenken müssen, was man tut.

Literatur

[Clu D] Chaos Computer Club. Hackerethik. Website, o. D. Online erhältlich unter https://www.ccc.de/de/hackerethik; abgerufen am 30. Juni 2022.

[jbJB D] jura-basic Juristisches Basiswissen. Datenschutz (allgemeines). Website, o. D. Online erhältlich unter http://www.jura-basic.de/aufruf.php?file=3&art=6&find=Datenschutz_Pers%F6nlichkeitsrecht; abgerufen am 02. Juli 2022.

[Pol D] Uwe Poltoranin. Ethischer hacker. Website, o. D. Online erhältlich unter http://www.heise.de/tp/deutsch/inhalt/te/2860/1.html; abgerufen am 29. Juni 2022.

[Rie18] Frank Rieger. Hackerethik - eine einführung. NPR, 2018. Online erhältlich unter https://media.ccc.de/v/35c3-10011-hackerethik_-_eine_einfuhrung; abgerufen am 02. Juli 2022.