Praxisidee: Cyberangriff

Infomaterial für Lehrpersonen

Modul A: Black Hat und White Hat

Die Aktivität des Hackens ist zunächst wertfrei. Es gibt aber viele verschiedene Motive und Methoden von Hacker:innen, einige moralisch einwandfrei, andere verwerflich. Je nachdem, ob es sich um „gutes“ oder „böses“ Hacken handelt, werden die Hacker:innen oft als „Black Hats“ oder „White Hats“ bezeichnet.

Diese Bezeichnungen haben ihren Ursprung im Westernfilm. In frühen Schwarz-Weiß-Western trugen die guten Charaktere meist weiße Hüte, die bösen schwarze Hüte, um sie trotz der eher schlechten Filmqualität gut unterscheidbar zu machen.

Black Hat-Hacker

Diese Hacker:innen sind Kriminelle, die nur zum eigenen Vorteil handeln. Meist geht es ihnen um finanzielle Bereicherung, indem sie ihren Opfern Bankdaten entlocken oder sich direkt in Zahlungssysteme von Banken hacken - was jedoch wesentlich schwieriger ist. Eine weitere Methode ist Erpressung: Hier benutzen sie persönliche Geheimnisse oder sperren die Computer ihrer Opfer durch spezielle Verschlüsselungsprogramme (Ransomware) und geben sie erst nach Bezahlung eines Lösegelds wieder frei.
Auch Spionage im Auftrag eines Staates, Sabotage oder das Ausspionieren von Firmengeheimnissen fällt unter den Bereich Black Hat-Hacking.

White Hat-Hacker

White Hats werden von Firmen und Regierungen bezahlt, um Schwachstellen in ihren Computersystemen zu finden. Sie bedienen sich derselben Methoden wie Black Hats, ihr Handeln ist aber legal, und ihr Ziel ist es, die Netzwerke sicherer zu machen. Dennoch wissen die Mitarbeiter:innen in den geprüften Firmen oft nichts vom Einsatz von White Hat-Hacker:innen - denn es geht ja auch um Sicherheitsrisiken im Verhalten der Belegschaft.

Grey Hat-Hacker

Die Grey Hats dringen zwar ebenfalls unerlaubt in Computersysteme ein, ihre Motive sind aber andere als die der Black Hat-Hacker:innen. Sie handeln aus spielerischer Lust an der Herausforderung, im Wettbewerb gegen andere Hacker:innen oder aus wissenschaftlicher Neugier. Sie achten darauf, möglichst keine Spuren zu hinterlassen und keinen Schaden anzurichten. Wenn sie eine Schwachstelle finden, informieren sie die Netzwerkbetreiber:innen meist darüber und verlangen auch ein angemessenes Honorar, vergleichbar mit den White Hat-Hacker:innen.
Dennoch ist ihr Handeln letztlich illegal. Auch politische Aktivist:innen, die ihre Botschaften über gehackte Netzwerke verbreiten („hacktivists“), sind als Grey Hats einzustufen, da der Zugriff illegal erfolgt. Sie handeln aber oft moralisch, wenn sie etwa über soziale Netzwerke in autoritär regierten Staaten Informationen verbreiten, die ansonsten zensiert würden.

Hacking-Methoden

Alle Hackerinnen und Hacker bedienen sich im Grunde derselben Methoden. Nur Methoden, die das Netzwerk selbst beschädigen, sind den Black Hat-Hacker:innen vorbehalten. Einige der wichtigsten Methoden sind:

Social engineering

Die größte Schwachstelle eines Systems sind oft die Menschen. Social engineering macht sich die Psychologie zunutze, um Menschen zu manipulieren und z.B. zur Herausgabe eines Passworts zu veranlassen.

Trojanisches Pferd

Auf einem Computer im Ziel-Netzwerk wird ein Programm installiert, das den Zugriff von außen ermöglicht. Dieses Programm wird entweder über einen E-Mail-Anhang oder einen physischen Datenträger wie etwa einen USB-Stick eingeschleust.

Backdoor

In vielen Systemen haben die Programmierer:innen „Hintertüren“ eingebaut, um ohne aufwendige Anmeldeprozeduren schnell im System arbeiten zu können. Wenn Angreifer:innen diese Hintertür finden, können sie unbemerkt in das Netzwerk eindringen.

Denial of Service

Ein Online-Service wird durch Überlastung blockiert. Das kann durch Zufall geschehen oder durch einen Angriff, bei dem zur gleichen Zeit eine hohe Zahl an Anfragen an den Server geschickt werden. Bei großen Firmen führt eine solche Blockade zu enormen finanziellen Einbußen.

Virus

Viren werden über einen Computer eingeschleust und vermehren sich dann im ganzen Netzwerk. Die Schäden, die sie anrichten, sind unterschiedlich. Manche verlangsamen das System, andere führen zum kompletten Datenverlust. Virenschutzprogramme bieten Schutz, weil aber immer wieder neue Viren auftauchen, müssen die Schutzprogramme laufend aktuell gehalten werden.

Modul A : Antworten zu „Gutes vs. Böses Hacken“

Welche Motive hat Luis, sich in das Netzwerk der Schule zu hacken?

Die Motive von Luis sind Stolz auf die eigene Leistung (Selbstwirksamkeit), Anerkennung durch andere und der Wunsch, anderen zu helfen.

Hilft er seinen Mitschüler:innen wirklich mit dieser Aktion?

Nein. Anstatt die Aufgaben zu liefern, hätte Luis den Mitschüler:innen mehr geholfen, wenn er sein Mathematik-Wissen weitergegeben hätte.

Hat Luis mit dieser Aktion jemandem geschadet?

Ja. Er hat der Schule geschadet, indem er eine Schwachstelle im Netzwerk gefunden hat, die in Zukunft immer wieder ausgenutzt werden kann.

Modul 1: Antworten zur Wissensvermittlung

Wie ist Luis aufgrund dieser Aktion in der Hacker-Typologie einzustufen - als White Hat, Grey Hat oder Black Hat?

Luis ist am ehesten als Black Hat einzustufen. Er hat zwar nicht aus Gewinnstreben gehandelt, aber sehr wohl aus persönlichen Motiven wie dem Gewinn von Anerkennung. Sein Eindringen in das Netzwerk war unerlaubt, und er hat der Schule Schaden zugefügt.

Was hätte Luis tun bzw. unterlassen sollen, um in der Hacker-Typologie anders eingestuft zu werden?

Hätte Luis nach dem Eindringen in das Netzwerk die Schule über die Schwachstelle informiert, damit diese behoben werden kann, wäre er als Grey Hat-Hacker einzustufen. Das Eindringen war zwar unerlaubt, aber das Ergebnis letztlich positiv.