Bild iStockphoto/shapecharge

Das romantisierte Bild des ethischen Hackers

Sicherheitsrisiken realistisch einschätzen zu können und lösungsbasierte Ansätze für eine höhere Sicherheit aufzustellen ist für Unternehmen heutzutage wichtiger denn je. Daher spielt Hacking in unserer schnellwachsenden digitalen Gesellschaft eine immer grössere Rolle und entwickelt sich immer mehr zur Gefahr für viele Firmen.

Die Bedrohung durch Cyberattacken ist in den letzten Jahren deutlich angestiegen und gehört mittlerweile zum Alltag vieler Unternehmen. Nicht nur in der IT-Branche ist das Thema relevant. In das Augenmerk von Hacker:innen fallen immer mehr auch Klein- und Mittelständige Unternehmen in allen möglichen Bereichen und sogar Endverbraucher:innen werden anvisiert. Besonders der Begriff des «ethischen Hackers» gewinnt in diesem Kontext immer mehr an Popularität, da diese von vielen Unternehmen hinzugezogen werden, um Schwachstellen in Systemen zu entdecken und Gegenmassnahmen für diese zu finden.

Was sind ethische Hacker:innen?

Ethische Hacker:innen sind dafür zuständig, die Systemsicherheit zu umgehen und nach Schwachstellen zu suchen, die von Kriminellen ausgenutzt werden können, um Unternehmen zu schaden. Sobald diese Schwachstellen oder Sicherheitslücken gefunden sind, werden die Informationen dann vom Konzern genutzt, um die Sicherheit im System zu verbessern und dadurch gleichzeitig mögliche Angriffsflächen zu minimieren. «Zudem bieten vor allem grössere Firmen sogenannte Bug-Bounty-Programme an, bei denen nicht nur eine bestimmte Firma beauftragt wird, sondern die gesamte Öffentlichkeit zum Hacking animiert wird. Dabei erhalten die Finder von Sicherheitslücken Geld für die Preisgabe der Schwachstellen. Dies bietet den Firmen die Möglichkeit, die Lücken beheben zu können, bevor ein böswilliger Angreifer die Gelegenheit hat, sie auszunutzen», so Security Consultant Yves Kraft.

Romantisierung der Hackerkultur

Vor allem in Filmen und Serien werden Hacker:innen als Personen dargestellt, die schnellstmöglich unlösbare Codes knacken und sich innerhalb kürzester Zeit Informationen von millionenschweren Unternehmen verschaffen können, ohne sich dabei von ihrem Stuhl zu bewegen. Diese Vorstellungen entsprechen aber nicht der Wahrheit und werden von Regisseur:innen meist aufgrund von fehlendem Wissen falsch dargestellt. Normalerweise sind Angriffe auf Unternehmen und vorallem Nachrichtendienste wesentlich schwerer, als in Filmen gezeigt wird. «Im Schnitt dauert es etwa elf Tage, bis ein Cyberangriff erkannt wird. Es kann allerdings gut sein, dass ein Angriff über mehrere Wochen oder Monate abläuft und ein initialer Zugang zu einem Unternehmen zum Teil sogar im Darknet weiterverkauft wird», erklärt Kraft.

Häufigste Hackermethoden

Grundsätzlich sind die Angriffsmöglichkeiten von Hacker:innen so vielfältig wie das Vorgehen selbst. Hackerangriffe sind normalerweise von technischer Natur. Dennoch gibt es zwei Verfahrensweisen, wie Hacker:innen vorgehen, um sich Informationen zu beschaffen. Die bekannte Variante ist das Beschaffen von Auskünften durch Benutzerinteraktionen, wie die altbekannten Phishing-Mails, durch die heutzutage noch die meisten Angriffe ablaufen. Kraft betont, dass daneben auch fehlende Updates, unsichere Konfigurationen oder Lücken in der Webapplikation und Mobile Apps ausgenutzt werden, um an Informationen zu gelangen. Auch cloudbasierte Dienste sind besonders attraktiv für Hacker:innen, da Unternehmen immer mehr von selbstbetriebenen Lösungen in die Cloud wechseln, weil diese einfacher und meistens kostengünstiger sind. Der Nachteil dieser Dienste ist, dass der Anbieter die Sicherheit im Griff hat und nicht das Unternehmen selbst. Je nach Cloud-Modell kann dies nur bedingt oder gar nicht beeinflusst werden und man ist dem Anbieter möglicherweise komplett ausgeliefert. Zusätzlich ist es durch Cloud-Modelle einfacher, sich an mehreren Orten und von unterschiedlichen Geräten anzumelden.

Hier bietet die fehlende Zwei-Faktor-Authentisierung eine grosse Angriffsfläche, da diese mit dem Passwortschutz nicht gewährleistet ist. Neben Systemen können zudem Menschen angegriffen werden. Dabei nutzen Cyberkriminelle verschiedene psychologische Tricks, um Arbeitnehmende dazu zu verleiten, bösartige Anhänge zu öffnen oder persönliche Daten preiszugeben. Ebenso kann es dazu kommen, dass Kriminelle sich direkt mit den Opfern auseinandersetzen und diese zufällig ansprechen, um sie so in Fallen zu locken.

Schutzmassnahmen gegen Hacking

Rein technische Massnahmen genügen heutzutage nicht immer, um sich vor Cyberangriffen ausreichend zu schützen. Virenschutz, Sicherheitsupdates und regelmässige Datensicherungen zählen zu den Mindestanforderungen, die ein Unternehmen zu erfüllen hat, um eine gewisse Grundsicherheit aufzubauen. Um die Sicherheit in Unternehmen zu gewährleisten, trägt ethisches Hacken heutzutage zu einem grossen Teil der Cybersicherheit bei und bietet Lösungsansätze für Unternehmen, sich gegen solche Angriffe zu wehren. Das führt dazu, dass viele Unternehmen heutzutage ethische Hacker:innen damit beauftragen, Sicherheitslücken zu finden oder Infrastrukturen zu überprüfen. Dies erfolgt mit Angriffssimulationen, bei dem ein konkretes Szenario simuliert wird. Besonders in Verbindung mit Schulungen für Mitarbeitenden werden diese Simulationen oft demonstriert, damit alle Angestellten verstehen, wie so ein Angriff abläuft und was jede:r für sein Arbeitsumfeld zu beachten hat. Die grösste Bedrohung für Unternehmen stellen nämlich die eigenen Mitarbeitenden dar. Fehlende Awareness oder Sensibilisierung sind daher immer noch eine grosse Schwachstelle für Unternehmen.

Durch ethische Hacker:innen kann demonstriert werden, wie das Hacking abläuft und worauf sie besonders achten. Am Ende des Tages machen ethische Hacker:innen nämlich nichts anderes als kriminelle Hacker:innen – nur dass diese für die Unternehmen arbeiten statt gegen diese.

Text **Jessica Petz**