Wenn Cyberkriminelle die Seiten wechseln: Der Einsatz von Ethical Hackers

Unternehmen stehen ständig vor der Herausforderung, mit der wachsenden Bedrohungslandschaft Schritt zu halten. Eine Möglichkeit, um Sicherheitslücken in Systemen frühzeitig zu identifizieren, ist der Einsatz sogenannter Ethical Hackers. Zu ihren Aufgabengebieten gehören etwa Penetrationstests von Netzwerken, Rechnern, webbasierten Anwendungen und anderen Systemen, um potenzielle Bedrohungen aufzudecken. Oft handelt es sich bei diesen Mitarbeitern um Hacker, die ihre Fähigkeiten in der Vergangenheit für illegale Aktivitäten wie etwa Einbruch in Unternehmenssysteme und -netzwerke genutzt haben. Geläuterte Cyberkriminelle bieten damit einen umfangreichen Erfahrungsschatz sowie neue Denkansätze und können Lösungen vorschlagen, die nicht gleich auf der Hand liegen.

Bug-Bounty-Programme: Kopfgeldjagd auf Softwarefehler

Ein gutes Beispiel für das Einsatzspektrum von ethischen Hackern sind sogenannte Bug-Bounty-Programme. Mit diesen setzen Unternehmen quasi ein Kopfgeld auf Schwachstellen aus. Damit bieten sie Hackern finanzielle Anreize, um Fehler in einem bereitgestellten Softwareprodukt zu identifizieren und zu melden. Unternehmen können dadurch zeitnah reagieren und Schwachstellen beheben, bevor sie öffentlich bekannt werden. Die Sicherheitslücken Meltdown und Spectre sind gute Beispiele für Schwachstellen, die in einer grossen Anzahl von Systemen gefunden und rechtzeitig gepatcht wurden, bevor sie umfangreich missbraucht werden konnten. Hätten böswillige Angreifer diese Lücken entdeckt, wären die Auswirkungen sehr weitreichend gewesen.

Mögliche Probleme beim Einsatz von Ethical Hackers

Wenn Unternehmen zulassen, dass Hacker versuchen, in ihre Systeme einzudringen, birgt das natürlich auch Risiken. Denn im Erfolgsfall muss darauf vertraut werden, dass der Hacker unternehmensloyal handelt. Ein probates Mittel dafür sind deshalb Bug-Bounty-Programme, da sie den Aufwand des Hackers von vornherein monetarisieren. Sobald eine Schwachstelle gefunden und bestätigt wurde, wird der Hacker für seinen Aufwand bezahlt. So gibt es nur einen begrenzten Anreiz, Daten zu stehlen oder den Exploit weiterzuverkaufen.

Wichtig ist: Die Geschäftsbeziehung zwischen Bug-Bounty-Plattform und Hacker basiert auf gegenseitigem Vertrauen und Respekt. Es gibt Fälle, bei denen sich Hacker nicht an die Regeln und Einschränkungen des Bug-Bounty-Programms gehalten haben. Dies kann rechtliche Konsequenzen durch das Unternehmen nach sich ziehen. Ebenso sind einige Unternehmen und Bug-Bounty-Plattformen bekannt dafür, Hacker nicht zu bezahlen, obwohl die gemeldete Schwachstelle bestätigt wurde. Solch ein Verhalten schädigt das Vertrauen der Ethical-Hacker-Community enorm und kann sogar dazu führen, dass das Unternehmen und die Plattform auf eine Liste mit Zielen für böswillige Angriffe gesetzt werden.

Bedenken beim Einsatz ehemalig krimineller Hacker

Es gibt potenziell immer Personen, die Hacking nur wegen des Nervenkitzels betreiben. Deren Fähigkeiten können jedoch durch legale, herausfordernde Aufgaben positiv umgeleitet werden. Natürlich mag die Frage aufkommen, wie man sich sicher sein kann, dass ein ehemaliger Krimineller nicht wieder straffällig wird, doch dies ist kein spezifisches Problem der Cyberbranche. Wichtig ist, ein Umfeld zu schaffen, bei dem technische Herausforderung, Lern- und Weiterbildungsmöglichkeiten sowie entsprechende Vergütung gut ausgelotet sind. Ãœberwiegen diese Vorteile, lohnt sich das Risiko einer Straftat nicht.

Auch ist es wichtig, dass die Gesetzeslage mit der Technologieentwicklung Schritt hält, damit strafrechtliche Konsequenzen gut bekannt sind und genügend Abschreckung bieten. Cyber-Straftaten werden oft immer noch nachgiebiger geahndet als andere Delikte mit vergleichbarem finanziellem Schaden. Ein Grund, weshalb organisierte Banden immer mehr in die Online-Welt abwandern.

Von Kontrolle zu Freiheit: Zusammenarbeit von Unternehmen und Hackern

Es sollten auf beiden Seiten sehr klare Vereinbarungen getroffen werden, die die Möglichkeit bieten, gegenseitiges Vertrauen aufzubauen. Beispielsweise können Unternehmen zu Beginn Zeit und Ort für die Nutzung internetfähiger Geräte begrenzen, um eine bestimmte Aufgabe zu erfüllen. Ethische Hacker sollten Vorgaben und Abmachungen klar einhalten. Gleiches gilt für das Unternehmen. Werden Vereinbarung durch das Unternehmen nicht erfüllt, ist dies genauso schädlich für die Beziehung. Hat sich das gegenseitige Vertrauen schliesslich bestätigt, sollten ehemalig straffällig gewordene Hacker wie jeder andere Mitarbeiter behandelt werden und die Verantwortung und Rolle erhalten, die ihnen gebührt. Dauerhafte Stigmatisierung erhöht erwiesenermassen die Wahrscheinlichkeit einer Rückfälligkeit. Der Glaube an eine Rehabilitation ist ein wichtiger Bestandteil für ihr Gelingen.