Bugcrowd-Studie:
Hacker halten es für unwahrscheinlich, dass generative KI menschliche Cybersecurity-Fähigkeiten ersetzen wird

Jährlicher Bugcrowd-Bericht "Inside the Mind of a Hacker" zeigt wachsende Zusammenarbeit: 89 Prozent der Befragten sagen, dass Unternehmen Hacker in einem positiveren Licht sehen

SAN FRANCISCO, 12. Juli 2023 – Bugcrowd, die einzige Multi-Solution-Crowdsourced-Cybersecurity-Plattform, hat seinen jährlichen „Inside the Mind of a Hacker"-Report für 2023 veröffentlicht. Die internationale Studie zeigt, dass 72 Prozent der Hacker glauben, dass künstliche Intelligenz (KI) die Kreativität von Menschen bei der Sicherheitsforschung und dem Schwachstellenmanagement nicht ersetzen wird.
Der Bericht befasst sich mit einer breiten Palette von Themen, darunter die Auswirkungen von KI auf die Sicherheit, wie professionelle Hacker heute sind und wie der aktuelle Stand des Hackens ist.

Auswirkungen von KI und generativem KI-Hacking
Generative KI ist ein wichtiges Thema im Bericht 2023. Mehr als die Hälfte der Befragten (55 Prozent) gab an, dass sie die Fähigkeiten der Hacker bereits übertreffen kann oder in den nächsten fünf Jahren dazu in der Lage sein wird. Fast drei von vier Befragten (72 Prozent) sind der Meinung, dass generative KI nicht in der Lage sein wird, die Kreativität von Hackern zu übertreffen.

Auf die Frage, wie generative KI eingesetzt wird, nannten die Hacker vor allem die Automatisierung von Aufgaben (50 Prozent), die Analyse von Daten (48 Prozent), die Identifizierung von Schwachstellen (36 Prozent), die Validierung von Ergebnissen (35 Prozent) und die Durchführung von Erkundungen (33 Prozent). Fast zwei von drei Befragten (64 Prozent) glauben, dass generative KI-Technologien den Wert von Ethical Hacking und Sicherheitsforschung erhöht haben.

Der Anstieg der KI-Nutzung unter Hackern deckt sich mit den Richtlinien des US-Verteidigungsministeriums aus dem Jahr 2022. Präsident Bidens stellte in der Cybersecurity Executive Order (EO 14028) fest: „Der Mehrwert aufgrund der Nutzung von KI in Cybersicherheitsanwendungen wird immer deutlicher... Die Methoden sind sehr vielversprechend, um Muster in Milliarden von Datenpunkten schnell zu analysieren und zu korrelieren, um eine Vielzahl von Cyberbedrohungen in Sekundenschnelle aufzuspüren."

Hacker-Stereotypen
Die meisten Hacker sind der Gen Z im Alter von 18-24 Jahren (57 Prozent) oder Millennials im Alter von 25-34 Jahren (28 Prozent) zuzuordnen. Dennoch erwies sich der Stereotyp des jugendlichen Hackers als zutreffender als sein Gegenstück, den Phreakern der Generation X: 5 Prozent waren unter 18 und nur 2 Prozent über 45 Jahre alt. Darüber hinaus erwies sich das Klischee, dass Hacker überproportional männlich sind, als zutreffend: 96 Prozent der Befragten bezeichneten sich als männlich und nur 4 Prozent als weiblich, weitere 0,2 Prozent bezeichneten sich als nicht-binär oder geschlechtsneutral.

Die meisten Hacker (82 Prozent) hacken nicht hauptberuflich, sondern betrachten es entweder als Teilzeitjob, Nebenjob oder als etwas, das sie gerade zu einer Vollzeitbeschäftigung machen wollen. Nur 29 Prozent bezeichneten das Hacken als ihren Vollzeitberuf. Die Beweggründe für ethisches Hacken waren vielfältig, aber die wichtigsten Anreize waren persönliche Entwicklung (28 Prozent), finanzieller Gewinn (24 Prozent), Aufregung (14 Prozent) und die Herausforderung (12 Prozent). Weitere 6 Prozent der Befragten gaben an, dass sie für das Allgemeinwohl hacken, und 87 Prozent sagten, dass das Melden einer Sicherheitslücke wichtiger ist als Geld damit zu verdienen.

Zwar haben mehr als die Hälfte der Befragten einen Hochschulabschluss (54 Prozent) und 14 Prozent ein Studium absolviert, aber nur 24 Prozent haben das Hacken durch akademische oder berufliche Kurse gelernt. Die Mehrheit der Hacker (71 Prozent) hat sich das Hacken selbst beigebracht, die meisten durch Online-Ressourcen (84 Prozent), andere durch Ausprobieren (40 Prozent) oder Freunde und Mentoren (34 Prozent).

Status von Hacking und Schwachstellenmanagement
Die Meinungen darüber, wie viele Unternehmen ihr wahres Risiko eines Einbruchs kennen, gehen auseinander: 27 Prozent der Befragten gaben an, dass weniger als 10 Prozent der Unternehmen das Risiko wirklich bekannt ist. Ein weiteres Drittel der Befragten (33 Prozent) gab an, dass 10 bis 25 Prozent der Unternehmen ihr Risiko kennen, aber nur 16 Prozent sagten, dass mehr als die Hälfte der Unternehmen ihr wahres Risiko eines Einbruchs kennen.

Die Befragten zeichneten ein gemischtes Bild der globalen Bedrohungslandschaft. 84 Prozent gaben an, dass es seit dem Beginn der COVID-19-Pandemie mehr Schwachstellen gibt, und 88 Prozent sagten, dass punktuelle Sicherheitstests nicht ausreichen, um die Sicherheit der Unternehmen zu gewährleisten. Dennoch bestätigten 78 Prozent der Befragten, dass die Angriffsflächen der meisten Unternehmen immer schwieriger zu kompromittieren sind. Weitere 89 Prozent sagten, dass Unternehmen ethische Hacker zunehmend positiv sehen.

Fast zwei Drittel der Befragten (63 Prozent) attestierten, in den letzten 12 Monaten eine neue Schwachstelle gefunden zu haben, die sie zuvor noch nicht kannten. Darüber hinaus gab mehr als die Hälfte der Befragten (54 Prozent) an, dass sie eine Schwachstelle nicht gemeldet haben, weil es im Unternehmen keine klare Möglichkeit gab, sie zu melden, ohne rechtliche Konsequenzen zu riskieren.

Das Hacken wird zunehmend für die Karriereentwicklung genutzt, denn 42 Prozent der Befragten gaben an, dass der Aufbau langfristiger Beziehungen zu Entscheidungsträgern und Marken im Bereich Sicherheit eines ihrer wichtigsten Ziele beim Hacken auf Bugcrowd ist. Darüber hinaus gab mehr als die Hälfte der Befragten (53 Prozent) an, dass das Hacken ihnen geholfen hat, einen Job zu bekommen, bei dem sie Remote arbeiten.

„Mit diesem Bericht treten mehr Hacker aus dem Schatten ihrer Stereotypen heraus, um echte Geschichten zu erzählen und neu zu definieren, wie Hacking als Karriereweg aussieht", sagte Dave Gerry, CEO von Bugcrowd. „Da die weltweite Verbreitung von KI in Unternehmen eine kritische Masse erreicht, ist Bugcrowd stolz darauf, an der Spitze der Sicherheitsforschung zu stehen. Wir sind begeistert, dass immer mehr Unternehmen die vielfältigen Fähigkeiten und das Fachwissen von Hackern - genau zur richtigen Zeit - über unsere Plattform nutzen."

Die komplette Studie „Inside the Mind of a Hacker-2023“ steht hier zum Download bereit:

Über Bugcrowd
Bugcrowd, die einzige Multi-Solution-Crowdsourced-Cybersecurity-Plattform, kombiniert daten- und ML-gesteuertes Crowd-Matching mit jahrzehntelanger Anwendungserfahrung, um die richtige menschliche Kreativität zum richtigen Zeitpunkt auf das richtige Problem zu konzentrieren. Die Bugcrowd Security Knowledge Platform™, der Unternehmen auf der ganzen Welt vertrauen, ermöglicht es, verborgene Schwachstellen in ihrer gesamten Angriffsfläche zu finden, bevor sie ausgenutzt werden können, indem sie das Wissen von ethischen Hackern von Weltrang nutzen. Bugcrowd hat seinen Sitz in San Francisco und wird von Blackbird Ventures, Costanoa Ventures, Industry Ventures, Paladin Capital Group, Rally Ventures, Salesforce Ventures und Triangle Peak Partners unterstützt.

Schützen Sie Ihr Unternehmen mit Bugcrowd, Right Platform, Right Crowd, Right Time und besuchen Sie www.bugcrowd.com. Lesen Sie unseren Blog hier.

EMEA Pressekontakt:
Rose Ross (Omarketing)
Rose@omarketing.com
+44 (0)7976 154 597