arcserve®
Protect what's priceless.

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

Sicherheitsrisiken von ChatGPT: Wie Unternehmen ihre Daten schützen können

Von Florian Malecki, Executive Vice President Marketing bei Arcserve

ChatGPT, entwickelt vom US-amerikanischen Unternehmen OpenAI, ist ein Chatbot, der weltweit für Aufsehen sorgt. Bisher ist ChatGPD die am schnellsten wachsende App der Geschichte und hat in nur zwei Monaten 100 Millionen aktive Nutzer erreicht – der bisherige Rekordhalter TikTok benötigte dafür neun Monate.

Dieses leistungsstarke Open-Source-Tool ist zum Beispiel in der Lage, Schulaufsätze zu schreiben, rechtliche Vereinbarungen und Verträge aufsetzen oder komplexe mathematische Probleme zu lösen. Sogar medizinische Zulassungsprüfungen konnte das Tool bestehen. Es hat aber auch das Potenzial, die Art und Weise, wie Unternehmen arbeiten, zu revolutionieren. Mit ChatGPT lassen sich schnell Berichte erstellen und Kundendienstanfragen effizient bearbeiten. Das Tool kann sogar den Code für das nächste Produktangebot schreiben, Marktanalysen durchführen und bei der Erstellung von Unternehmenswebseiten helfen.

ChatGPT bietet zwar viele Vorteile für Unternehmen, wirft aber auch dringende Sicherheitsfragen auf. Eines der größten Risiken im Zusammenhang mit dieser Technologie besteht darin, dass auch Cyberkriminelle ohne Programmierkenntnisse die Möglichkeit haben, bösartige Software zu erstellen und einzusetzen. Mit ChatGPT kann jeder, der böse Absichten hegt, Schadsoftware entwickeln und einsetzen und so in Unternehmen verheerenden Schaden anrichten.

arcserve®
Protect what's priceless.

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

Das Sicherheitsunternehmen Check Point Research berichtet, dass innerhalb weniger Wochen nach der Veröffentlichung von ChatGPT Personen in Cybercrime-Foren, auch solche mit begrenzten Programmierkenntnissen, das Tool nutzten, um Software und E-Mails für Spionage, Ransomware-Angriffe und bösartiges Spamming zu erstellen. Zwar äußert sich Check Point dahingehend, dass es noch zu früh ist, um zu sagen, ob ChatGPT zum bevorzugten Tool der Dark-Web-Mitglieder wird. Dennoch hat die Cyberkriminellen-Community ein starkes Interesse an ChatGPT gezeigt und nutzt es bereits zur Entwicklung von bösartigem Code.

In einem von Check Point beschriebenen Beispiel offenbarte ein Malware-Entwickler in einem cyberkriminellen Forum, dass er ChatGPT verwendet, um bekannte Malware-Stämme und -Techniken zu replizieren. Als Beweis teilte die Person den Code für einen Python-basierten Informationsdiebstahl, den sie mit ChatGPT entwickelt hat. Der Cyberkriminelle sucht, kopiert und überträgt 12 gängige Dateitypen von einem kompromittierten System, darunter Office-Dokumente, PDFs und Bilder.

ChatGPT erhöht die Gefährdung durch Hackerangriffe

Cyberkriminelle können ChatGPT und andere KI-Tools nutzen, um Phishing-Betrügereien effektiver zu gestalten. Herkömmliche Phishing-Nachrichten sind oft leicht zu erkennen, weil sie in plumpem Englisch verfasst sind. Aber ChatGPT kann das ändern. Redakteure der Ziff-Davis-Publikation Mashable testeten beispielsweise die Fähigkeiten von ChatGPT, indem es eine Phishing-E-Mail bearbeiten sollte. Es verbesserte und verfeinerte nicht nur schnell die Sprache, sondern ging sogar noch einen Schritt weiter und erpresste den hypothetischen Empfänger, ohne dazu aufgefordert zu werden.

OpenAI behauptet zwar, über strenge Richtlinien und technische Maßnahmen zum Schutz der Nutzerdaten und der Privatsphäre zu verfügen, doch sind

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

diese möglicherweise nicht ausreichend. ChatGPT sammelt Daten aus dem Internet, was Sicherheitsrisiken mit sich bringt. Beispielsweise kann das Scraping von Daten dazu führen, dass sensible Informationen wie Geschäftsgeheimnisse und Finanzdaten an Konkurrenten weitergegeben werden. Auch der Ruf eines Unternehmens oder einer Person kann geschädigt werden, wenn die durch Data Scraping gewonnenen Informationen ungenau sind. Außerdem kann das Auslesen von Daten IT-Systeme für Schwachstellen öffnen und von böswilligen Akteuren ausgenutzt werden.

Da sich die Angriffsfläche durch das Aufkommen von ChatGPT dramatisch vergrößert hat, stellt sich die Frage, wie sich dies auf die Sicherheitslage von Unternehmen auswirkt. Früher fühlten sich kleine und mittelständische Unternehmen vielleicht sicher, weil sie dachten, dass es sich für Cyberkriminelle nicht lohnen würde, sie zu hacken. Da es mit ChatGPT jedoch einfacher geworden ist, bösartigen Code in großem Maßstab zu erstellen, hat sich die Anfälligkeit für Cyberkriminalität für alle Unternehmen deutlich erhöht.

ChatGPT zeigt, dass die Zahl der verfügbaren Sicherheitstools zwar zunimmt, diese Tools aber möglicherweise nicht mit den neuen KI-Technologien Schritt halten können. Angesichts der steigenden Bedrohung durch Cyberkriminalität muss sich jedes Unternehmen der potenziellen Risiken bewusst sein, die von ChatGPT und anderen fortschrittlichen KI-Systemen ausgehen. Deshalb muss es Maßnahmen ergreifen, um diese Risiken zu minimieren.

Schutzmaßnahmen ergreifen

Als erste Schutzmaßnahme sollten Unternehmen herausfinden, wie verwundbar sie sind. Penetrationstests, auch als Pen-Tests bekannt, können zum Schutz der Daten beitragen, indem sie einen realen Angriff auf die

arcserve®
Protect what's priceless.

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

Systeme, Netzwerke oder Anwendungen im Unternehmen simulieren. So lassen sich Sicherheitsschwachstellen, die von böswilligen Akteuren ausgenutzt werden könnten, frühzeitig identifizieren. Indem Unternehmen ihre Schwachstellen in einer kontrollierten Umgebung aufdecken, können sie diese mit Hilfe von Pen-Tests beheben, die Sicherheitslage verbessern und das Risiko einer erfolgreichen Datenverletzung oder anderer Cyberangriffe verringern. In der neuen Welt von ChatGPT können Penetrationstests eine entscheidende Rolle dabei spielen, Daten zu schützen und ihre Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.

Unternehmen müssen außerdem ihre Strategie für die Datensicherheit ausbauen und einen soliden Datenschutzplan aufstellen. Ein Plan zur Datensicherheit beschreibt die Schritte, die ein Unternehmen durchführen sollte, um seine kritischen Daten und Systeme zu schützen und - im Falle einer Datenpanne - den normalen Betrieb so schnell und effizient wie möglich wiederherzustellen. Er bietet auch einen Fahrplan für die Reaktion auf Cyber-Bedrohungen, einschließlich detaillierter Anweisungen zur Sicherung von Systemen und Daten sowie zur Kommunikation mit den Beteiligten während und nach einem Vorfall. Durch die Einführung eines Data-Resilience-Plans können Unternehmen die Auswirkungen von Cyber-Bedrohungen und das Risiko von Datenverlusten minimieren und so den Erfolg und Fortbestand des Unternehmens sichern.

Eine weitere Möglichkeit, Cyberkriminelle, die ChatGPT nutzen, zu stoppen, ist die unveränderbare Datenspeicherung. Unveränderbarkeit bedeutet, dass Daten in ein Format konvertiert werden, in dem sie nur einmal geschrieben, viele Male gelesen, nicht gelöscht und nicht verändert werden können. Es gibt keine Möglichkeit, die Unveränderlichkeit rückgängig zu machen. Dadurch wird gewährleistet, dass Backups sicher, zugänglich und wiederherstellbar sind. Selbst wenn Angreifer vollen Zugriff auf ein Unternehmensnetzwerk

arcserve®
Protect what's priceless.

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

erhalten, können sie die unveränderlichen Kopien der Daten nicht löschen oder deren Zustand verändern.

ChatGPT bietet zwar Vorteile für Unternehmen, birgt aber auch erhebliche Sicherheitsrisiken. Unternehmen müssen sich dieser Risiken bewusst sein und Präventionsmaßnahmen ergreifen, um sie zu minimieren. Sie sollten in solide Cybersicherheitsmaßnahmen investieren und sich über die neuesten Sicherheitstrends informieren. Mit dem richtigen Schutz können Unternehmen die vielen Vorteile von ChatGPT nutzen und sich gleichzeitig gegen diejenigen verteidigen, die das Tool für böswillige Zwecke missbrauchen.

Folgen Sie Arcserve auf LinkedIn oder Twitter und lesen Sie unsere neuesten Artikel zum Thema Datenschutz und -management im Arcserve Blog.

###

arcserve®
Protect what's priceless.

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

Über Arcserve

Arcserve gehört weltweit zu den Top-5-Herstellern von Datensicherungslösungen und bietet als Anbieter von Unified Data Resilience Lösungen eine einheitliche Plattform für die Ausfallsicherheit von Daten an. Das Unternehmen stellt das breiteste Spektrum an Best-in-Class-Lösungen für die Verwaltung, den Schutz und die Wiederherstellung aller Datenumgebungen zur Verfügung. Die Lösungen von Arcserve eignen sich für KMUs und Großunternehmen, unabhängig von deren Standort und der Komplexität der Infrastruktur. Sie beseitigen die Komplexität und bieten gleichzeitig erstklassigen, kosteneffizienten, flexiblen und massiv skalierbaren Datenschutz und Sicherheit für alle Datenumgebungen. Dazu gehören On-Prem-, Off-Prem- (einschließlich DRaaS, BaaS und Cloud-to-Cloud), hyperkonvergente und Edge-Infrastrukturen. Dank der fast drei Jahrzehnte langen Erfahrung des Unternehmens mit preisgekrönten IP-Lösungen und der kontinuierlichen Konzentration auf Innovation können Partner und Kunden, darunter MSPs, VARs, LARs und Endbenutzer, sicher sein, dass sie den schnellsten Weg zu Daten-Workloads und -Infrastrukturen der nächsten Generation finden. Arcserve ist ein zu 100 Prozent channelorientiertes Unternehmen, das in über 150 Ländern vertreten ist und mit 19.000 Vertriebspartnern die kritischen Datenbestände von 235.000 Kunden schützt.
Erfahren Sie mehr unter arcserve.com und folgen Sie Arcserve auf Twitter oder LinkedIn.

Unternehmenskontakt
Jock Breitwieser
Arcserve
+1 408.800.5625
jock.breitwieser@arcserve.com

Agenturkontakt
TC Communications
Arno Lücht
+49 8081 9546-19
Thilo Christ
+49 8081 9546-17
arcserve@tc-communications.de