



MEDIENMITTEILUNG

Technische Sicherheitsanalyse der Mobile App «Temu»

Ungewöhnliche technische Auffälligkeiten bei der Temu-App – Vorsicht ist geboten

Zug, 5. Dezember 2024 –Die Temu-App weist technische Auffälligkeiten wie dynamisches Nachladen von Code und zusätzliche Verschlüsselungen auf, die eine abschliessende Bewertung erschweren. Kritische Sicherheitsrisiken oder belastbare Beweise für unerlaubte Überwachung liegen jedoch nicht vor.

Temu, eine beliebte E-Commerce-App aus China, erfreut sich in der Schweiz wachsender Beliebtheit. Gleichzeitig stehen Cybersicherheitsrisiken solcher Apps zunehmend im Fokus. Das Nationale Testinstitut für Cybersicherheit NTC hat eine unabhängige Sicherheitsanalyse der Temu-App durchgeführt, um die tatsächlichen Risiken für Nutzende zu bewerten.

Ungewöhnliche technische Auffälligkeiten

Die Analyse identifizierte einige «Red Flags»:

- **Dynamisches Nachladen von Code in proprietäre Laufzeitumgebung:** Dadurch kann die App ihr Verhalten eigenständig ändern. Entwickler können Funktionen und Inhalte flexibel anpassen – ohne App-Store-Updates, also ohne, dass Benutzende dies initiieren oder genehmigen müssten.
- **Zusätzliche Verschlüsselungsschichten:** Diese könnten zwar den Schutz von Daten erhöhen, aber auch potenziell zur Verschleierung unerwünschter Datenübertragungen genutzt werden.

Diese Eigenschaften sind zwar nicht zwingend bösartig, stellen jedoch Herausforderungen für eine vollständige Bewertung dar.

Andere Sicherheitsrisiken überwiegend unbedenklich

Die Untersuchung zeigt weiter, dass sich in der Temu-App sonst keine eindeutig kritischen Sicherheitsrisiken oder Beweise für unerlaubte Überwachung finden. Berechtigungen und Verhalten der App entsprechen weitgehend den Standards von E-Commerce-Anwendungen. Im Vergleich zu ähnlichen Apps setzt Temu weniger und unproblematischere Berechtigungen voraus.

Empfehlungen des NTC

Während die Analyse keine konkreten Beweise für bösartige Aktivitäten gefunden hat, empfiehlt das NTC, den Einsatz der Temu-App – wie auch bei Apps mit weitreichenden Berechtigungen – kritisch zu hinterfragen, insbesondere im geschäftlichen und behördlichen Kontext. Nutzerinnen und Nutzer sollten folgende Vorsichtsmassnahmen treffen:

- Minimierung der Berechtigungen, die der App gewährt werden.
- Regelmässige Updates des Betriebssystems sicherstellen.
- Alternative Nutzung über einen mobilen Browser erwägen, um die Angriffsfläche zu reduzieren.

Über Temu und Cybersicherheitsbedenken

Die App wird von der chinesischen PDD Holdings Inc. betrieben und unterliegt chinesischem Recht, das aus europäischer Perspektive als unzureichend für den Datenschutz gilt. Unternehmen und Behörden sollten dies bei der Nutzung der App berücksichtigen.

Unabhängigkeit der Untersuchung

Die Untersuchung wurde eigenständig vom NTC durchgeführt, ohne externe Einflussnahme. Die Ergebnisse konzentrieren sich ausschliesslich auf Cybersicherheitsaspekte und verzichten bewusst auf die Bewertung anderer kontroverser Themen wie Geschäftspraktiken oder Produktqualität.

[Zur Sicherheitsanalyse](#)

Medienkontakt:

Andreas W. Kaelin, Geschäftsführer

+41 41 210 11 03, andreas.kaelin@ntc.swiss

Über das Nationale Testinstitut für Cybersicherheit NTC

Das Nationale Testinstitut für Cybersicherheit NTC trägt zur Sicherheit und zur digitalen Souveränität der Schweiz bei, indem es kritische Schwachstellen vorausschauend erkennt und deren Behebung fördert. Als nicht gewinnorientierter Verein mit Sitz in Zug folgt das NTC den Prinzipien der Unabhängigkeit und Objektivität. Es führt Cybersicherheitsprüfungen von vernetzten Infrastrukturen, Geräten und Anwendungen durch, die für Gesellschaft und Wirtschaft von grosser Bedeutung sind. <https://www.ntc.swiss>