Cybersicherheit und Digitale Aufklärung

Gefährdungsfeld Smart Home

Zunächst verschafft sich der Hacker Zugriff auf den Smart-Fernseher und infiziert diesen mit Schadsoftware. Über eine Nachricht auf dem Bildschirm verlangt er Lösegeld in Bitcoins.

Oft reicht es, wenn sich der Hacker Zugriff auf ein einziges (ungeschütztes) Gerät verschafft. Darüber kann er über alle weiteren (vermeintlich sicheren) Geräte im Smart Home die Kontrolle übernehmen, die selbst nicht angreifbar wären.

Der digitale Assistent leitet das Kommando an die Smart Home-App weiter, welche den Alarm sowie die Eingangstüren steuert. Das Türschloss wird geöffnet, ohne physische Einbruchsspuren.

Diese Angriffsfläche gilt als besonders gefährlich: Wenn ein digitaler Assistent und ein Lautsprecher kombiniert Ziel eines Hacking-Angriffs werden, können diese alles, was über Sprachkommandos läuft, neu programmieren.

Wenige Sekunden später hat der Hacker bereits einen Textbefehl an einen vernetzten Lautsprecher gesendet. Der Lautsprecher wandelt den Text in Sprache um und trägt diesen einem digitalen Assistenten vor. „Alarm ausschalten. Türe öffnen" lautet der Befehl aus dem Lautsprecher.

Digitale Assistenten sind sprachgesteuerte, internetbasierte, intelligente Geräte. Sie übertragen die im Raum gesprochenen Worte digital zum Hersteller, wo die Befehle verarbeitet werden.

Zum Spaß entscheidet der Hacker, auch in die Nutzungsdaten der Smart-Toilette einzudringen.

Über Nutzungsprotokolle kann er auf sensible Gesundheitsdaten des Toilettenbesitzers zurückgreifen, die sich aus den von der Toilette gesammelten Daten ableiten.

Als nächsten Sprachbefehl programmiert der Hacker: „Kaufe mir die neueste Drohne". Auch hier leitet der digitale Assistent die Bestellung an einen Online-Lieferanten weiter, der wiederum mit dem Bankkonto des Opfers verbunden ist.

Ein Hacker dringt in die Überwachungskamera eines Smart Homes ein. Über die Kommunikation der Kamera kann er die Geräteadressen (IP-Adressen) anderer vernetzter Produkte im selben Netzwerk abfangen.

Überwachungskameras sind leichtes Ziel für Hacker-Attacken. Oft wird bei der Installation das Standardpasswort beibehalten. Hacker können mithilfe einer im Internet zugänglichen Software das Standardpasswort in den wenigen Sekunden finden.

Zuletzt sucht der Hacker nach privaten Sprachdateien, die der digitale Assistent aufgenommen und gespeichert hat. Anschließend hackt er sich in die Social-Media-Account des Opfers ein und veröffentlicht dort die gefundenen Sprachaufzeichnungen, um sein Opfer bloßzustellen.

VORLAGE