Medieninformation

TECHNISCHE UNIVERSITÄT DARMSTADT

Ferngesteuerte Neugierde in der Wohnung

Informatiker der TU Darmstadt decken kritische Software-Schwachstelle in Saugrobotern auf

Kommunikation und Medien
Corporate Communications

Karolinenplatz 5
64289 Darmstadt

Ihre Ansprechpartnerin:
Claudia Staub
Tel. +49 6151 16 - 20061
staub.cl@pvw.tu-darmstadt.de
www.tu-darmstadt.de/presse
presse@tu-darmstadt.de

Darmstadt, 31. Mai 2019. Ein Forscherteam vom Fachbereich Informatik der TU Darmstadt hat eine Schwachstelle in der Software von Staubsauger-Robotern gefunden, durch die eine Fernsteuerung erfolgen kann.

Staubsauger-Roboter sind mittlerweile in vielen Haushalten intelligente Helfer, die ihre Arbeit verrichten, sobald die Wohnung verlassen wird. Dabei sammeln diese Geräte etwa mit ihrer Kamera und anderen Sensoren Daten über die Wohnung und erstellen beispielsweise einen Grundriss, um sich autonom durch die Wohnung zu bewegen. Sensoren und Konnektivität, gepaart mit schlechten oder oft sogar fehlenden Sicherheitsvorkehrungen, verleihen diesen Geräten eine große Angriffsfläche. In der Vergangenheit fanden Sicherheitsforscher der TU Darmstadt bereits Schwachstellen bei einem Modell von Mi Robot, durch die ein schädliches Update eingespielt werden konnte. Auch bezüglich anderer Saugroboter wurden Sicherheitslücken veröffentlicht – bei den Modellen konnten Angreifer die Kontrolle übernehmen oder Kamera und Mikrofon ausgelesen werden.

Nunmehr hat das System Security Lab an der TU Darmstadt, das sich mit der Sicherheitsanalyse sogenannter IoT-Geräte (Internet of Things) beschäftigt, weitere Geräte getestet und dabei erhebliche Sicherheitsprobleme im Saugroboter Tesvor X500 gefunden. Dieses recht verbreitete Modell im unteren Preissegment wird über den Online-Handel vertrieben.

Fernsteuerung möglich

Die von den Forschern aufgedeckte Sicherheitslücke erlaubt einem Angreifer, aus der Ferne und überall auf der Welt alle Tesvor Saug- und Wischroboter anzusteuern und deren Status und den Grundriss der Wohnung abzurufen. Dazu muss vom Staubsauger-Roboter nichts weiter bekannt sein als die sogenannte MAC-Adresse, eine lange Zahlenfolge, über die man ein elektronisches Gerät eindeutig identifizieren kann. Die MAC-Adresse ist kein Sicherheitsmerkmal und kann vom Angreifer mithilfe bestimmter Techniken leicht herausgefunden werden.

Die Tesvor Saug- und Wischroboter nutzen als Back-End „Amazon Web Services (AWS) Internet of Things (IoT)“. Die App, mit der der

Staubsauger gesteuert wird, benutzt als Authentifikation für die Steuerungsberechtigung nur dessen MAC-Adresse. Der Angriff nutzt aus, dass MAC-Adressen in Folge vergeben werden und der Hersteller sonst keine weiteren Sicherheitsmaßnahmen (Zugriffsbeschränkung oder Ähnliches) verwendet. Der potentielle Angreifer muss nur MAC-Adressen aus dem Adressbereich des Herstellers der Reihe nach bis zum Treffer „durchprobieren“.

Auslieferung ohne Sicherheitszertifikat

Ein weiteres Sicherheitsproblem entsteht durch die Handhabung der Zertifikate durch den Hersteller. Normalerweise benutzt AWS IoT für Authentizität und Vertraulichkeit in der Kommunikation zwischen Gerät und Cloud Zertifikate, die bei der Produktion vom Hersteller auf das Gerät geladen werden sollen, damit das Gerät sofort bei Einrichtung eine geschützte Verbindung aufbauen kann. Die Geräte von Tesvor werden aber ohne Zertifikat ausgeliefert und fragen bei erstmaliger Aktivierung den Herstellerserver nach dem Zertifikat an, um sich danach mit AWS IoT zu verbinden. Dieser Zertifikatsaustausch ist dadurch nicht authentifiziert. Somit wird eine sogenannte Man-in-the-Middle-Attacke möglich, wodurch das Zertifikat quasi von einem Mithörer zwischen Roboter und Server „in der Mitte“ abgefangen werden kann. Der Angreifer kann dann die geschützte Verbindung zwischen Gerät und Cloud mitlesen, verändern oder sich als Gerät ausgeben. Des Weiteren könnte er selber Zertifikate vom Hersteller abfragen und sich damit als neues Gerät ausgeben.

Die TU-Forscher haben den Gerätehersteller mehrfach schriftlich auf die gravierenden Sicherheitsprobleme hingewiesen – eine Antwort steht noch aus.

Kontakt:
TU Darmstadt
Fachbereich Informatik
Professor Dr.-Ing. Ahmad-Reza Sadeghi
Telefon: 06151/16-25328
ahmad.sadeghi@trust.tu-darmstadt.de

TECHNISCHE UNIVERSITÄT DARMSTADT

Digitalisierung, Kernphysik, Energiesysteme, Strömungsdynamik und Wärme- und Stofftransport, Neue Materialien für Produktinnovationen. Wir entwickeln unser Portfolio in Forschung und Lehre, Innovation und Transfer dynamisch, um der Gesellschaft kontinuierlich wichtige Zukunftschancen zu eröffnen. Daran arbeiten unsere 312 Professorinnen und Professoren, 4.450 wissenschaftlichen und administrativ-technischen Mitarbeiterinnen und Mitarbeiter sowie knapp 26.000 Studierenden. Mit der Goethe-Universität Frankfurt und der Johannes Gutenberg-Universität Mainz bildet die TU Darmstadt die strategische Allianz der Rhein-Main-Universitäten.

MI-Nr. 40/2019, cst