# Die Sprachassistentin schläft nie

**IT-SICHERHEIT:** Ob Siri, Cortana oder Alexa – Spracheingaben sind bequem – und gefährlich.

**Lauernd lauschen** Alexa, Siri, Cortana & Co. im Hintergrund und warten auf Befehle – manchmal auch von Fremden.

Foto: PantherMedia/Andriy Popov

VON UWE SIEVERS

Sprachassistenten sind beliebt. Einfach eine Nachricht ins Smartphone zu diktieren oder eine Suchanfrage ins Notebook zu sprechen, geht schneller und einfacher, als zu tippen. Siri, Cortana & Co. lauern lauschend im Hintergrund und warten auf Befehle. Gleichzeitig drohen im Hintergrund aber auch neue Gefahren und Risiken.

Unbehaglich erscheint die Vorstellung, dass ein Fremder im Vorbeigehen die Kontrolle über das Gerät übernehmen könnte und etwa mit dem Befehl „Hey Cortana, format my disk" die Festplatte löschen bzw. Siri anweisen könnte, Kontakte oder Fotos zu löschen. Doch allzu weit entfernt ist diese Vorstellung nicht.

**Zwei Sicherheitsspezialisten von der Technischen Universität Israels,** dem Technion in Haifa, präsentierten solche und ähnliche Ergebnisse im Februar auf dem Fachkongress für IT-Sicherheit „IT-Defense" in Bonn. Seit Jahren beschäftigen sich Amichai Shulman und Yuval Ron mit den Gefahren von digitalen Sprachassistenten sowie deren Auswirkungen, dabei finden sie immer neue Sicherheitslücken. „Wir haben bisher schon 20 Security-Probleme gefunden und rund 50 000 $ an Bug Bounties bekommen", resümiert Amichai Shulman. „Bug Bounties" zahlen die großen IT-Unternehmen als Belohnung, wenn ihnen gravierende Sicherheitslücken gemeldet werden.

Doch verwundert stellt Shulman fest: „Aber nur drei davon sind bisher als CVE erschienen." „Common Vulnerabilities and Exposures" (CVE) sind offiziell vom Hersteller anerkannte Sicherheitslücken. Die anderen sind zum Teil noch immer offen und können von Angreifern ausgenutzt werden.

Zudem scheine es, als ob Microsoft mit so manchem Fix eine neue Lücke aufmacht, kritisiert Shulman. Die Probleme entstehen, weil trotz gesperrtem Bildschirm gesprochene Befehle ausgeführt werden, was bei Windows 10 als Standard voreingestellt ist. „Deshalb hat Microsoft eingeführt, dass zuerst das Gerät entsperrt werden muss, bevor ein Befehl ausgeführt wird", erklärt Shulman. Angeblich sei das vielen Nutzern aber zu aufwendig gewesen, weshalb Microsoft dies nach Beschwerden zum Teil wieder rückgängig gemacht habe, berichtet er.

Die Forscher demonstrierten an Beispielen, wie man bei gesperrtem Notebook mit Cortana auf das Betriebssystem zugreifen kann: Bei einigen Sprachbefehlen lassen sich Dateien oder Webseiten öffnen und vereinzelt sogar Programme ausführen. „Ein aktiver Sprachassistent auf einem gesperrten Gerät ist keine gute Idee", kommentieren Shulman und Ron ihre Erkenntnisse. Cortana kann zwar auf dem Sperrbildschirm abgeschaltet werden, das erfordert jedoch Änderungen durch den Nutzer.

## Erkennung der Nutzerstimme wäre schon eine signifikante Verbesserung

Die Problematik lässt sich noch steigern: Die Wissenschaftler zeigten, wie kritische Angriffe dadurch entstehen, dass verschiedene Sprachassistenten zusammenwirken. Unlängst habe Microsoft Cortana für Drittanbieter geöffnet, erzählt Yuval Ron. Amazon hat daraufhin seine Alexa-Systeme mit Cortana gekoppelt. Windows-Nutzer, die ein Alexa-Gerät besitzen, können vom Laptop aus Sprachbefehle an Alexa senden.

**Es beginnt mit der Ansage:** „Hey Cortana, öffne Alexa." Was für Nutzer komfortabel erscheint, kann teuer werden. Denn Alexa-Besitzer können an Initiativen, die bei Amazon-Charity gelistet sind, Geld spenden. Sich dort als Spendenempfänger eintragen zu lassen, sei nicht aufwendig, so Ron. Anschließend können mit einem einfachen Sprachbefehl – auch bei einem gesperrten PC – sogar vierstellige Beträge ahnungsloser Nutzer dorthin transferiert werden.

Mehr und mehr Drittanbieter machen von der Cortana-Schnittstelle Gebrauch, auch Google. Aber diese Anbindungen seien häufig unsicher, bemängelt Ron. Gleichzeitig würden immer mehr Anwendungen auf dem Sperrbildschirm verfügbar. Außerdem lerne Cortana mittels Machine Learning ständig neue Befehle, berichtet der Forscher. Damit entstünden permanent neue Sicherheitsprobleme. Ron: „Wir können immer neue Sätze an Microsoft melden, weil sie Sicherheitslecks beinhalten." Aktuell nimmt Microsoft an Cortana signifikante Änderungen vor. Sicherheit und Datenschutz sollen erhöht werden, die Nutzung wird an ein Microsoft-Konto geknüpft. Details bleiben abzuwarten.

**Die Sicherheitsprobleme der smarten Assistenten** beschränken sich keineswegs auf Microsofts Cortana. Das Team um Shulman und Ron findet regelmäßig auch Lücken bei Googles Assistant oder bei Apples Siri. Apple hat mit dem jüngsten Catalina-Update etliche Siri-Lücken geschlossen und sich explizit bei den israelischen Forschern bedankt.

Doch die beiden suchen nicht nur Lücken, sie haben auch Ideen, wie die Sicherheit bei Sprachbefehlen erhöht werden könnte. „Die Erkennung der Nutzerstimme wäre schon eine signifikante Verbesserung, aber dieses Feature wurde von den Herstellern entfernt", sagt Shulman. Es lief nicht zuverlässig.

Die israelischen Wissenschaftler sind nicht die Einzigen, die sich mit Sicherheitsdefiziten bei Sprachassistenten beschäftigen. In einem gemeinsamen Forschungsprojekt entdeckten Wissenschaftler der Bostoner Northeastern University und des Londoner Imperial College, dass Sprachbefehle auch unbeabsichtigt ausgelöst werden können. „Jeder, der schon einmal Sprachassistenten eingesetzt hat, weiß, dass sie manchmal versehentlich aufwachen und mithören, auch wenn das ‚Weckwort' nicht gesprochen wurde", schreiben sie in ihrer Studie. Dabei würden ähnlich klingende Wörter und Phrasen als Weckbefehl missverstanden.

Ganz besonders oft geschehe dies bei im Hintergrund laufenden Fernsehern. Die Wissenschaftler ließen daher TV-Programme 24 Stunden durchlaufen und stellten fest, dass einige Systeme bis zu 19-mal am Tag reagierten und anschließend mitlauschten. Die Studie läuft noch, Risiken sind noch nicht endgültig abschätzbar. Eins ist jedoch jetzt schon klar: Datenschutzrechtlich bedenklich ist das allemal.