# Sagen Sie nichts!

## Sprachassistenten wie Siri und Alexa sind im Büro und vor allem im Homeoffice beliebt – stellen aber ein erhebliches Sicherheitsrisiko dar.

BERND SCHÖNE

Wer die Arbeit an einem IT-System unterbricht, tut gut daran, das Gerät gegen Missbrauch zu sperren. Sonst können unautorisierte Personen es missbrauchen. Etwa um politisch brisante Botschaften zu verschicken, Waren zu bestellen oder Dateien zu löschen. Früher wurde diese Schutzmaßnahme von den Nutzern oft vergessen. Dann kamen die ersten automatischen Tools. Nach einiger Zeit ohne Aktion, wird das Gerät automatisch gesperrt. Ganz gleich, ob PC, Workstation, Tablet oder Smartphone, heute ist „Locken" fast überall vorinstalliert. Wer von der Pause zurückkehrt, muss sich mit seinem Passwort erneut anmelden. Siri, Cortana, Bixby und Alexa können diesen Schutz aushebeln, darauf haben Experten jetzt hingewiesen.

**22**

**SCHWACHSTELLEN** haben Forscher bei Cortana, Siri, Alexa und Bixby gefunden. Die meisten sind nur provisorisch oder noch gar nicht behoben.

### Service auf Kosten der Sicherheit?

Nicht zum ersten Mal hebeln Servicefunktionen, die dem Nutzer das Leben mit der IT erleichtern sollen, zuvor erarbeitete Sicherheitskonzepte aus. Denn um den größtmöglichen Service zu bieten, müssen Sprachassistenten naturgemäß stets wach sein, und auf Befehle warten. Die Programmierer der Sprachassistenten sind sich des Problems offensichtlich durchaus bewusst gewesen, denn nur als „harmlos" geltende Befehle werden im gelockten Zustand befolgt. Wer mehr will, muss sein Passwort eingeben. Doch so harmlos sind die harmlosen Befehle nicht. Denn zusammen mit einigen Programmierfehlern ermöglichen sie es Angreifern, sehr schnell die Herrschaft über die Geräte zu übernehmen – ohne das Passwort des Besitzers zu kennen.


Sprachassistenten sind standardmäßig auch bei gesperrtem Bildschirm aktiv. Wünscht der Nutzer dies nicht, muss er es recht umständlich konfigurieren.

Foto: Pixabay

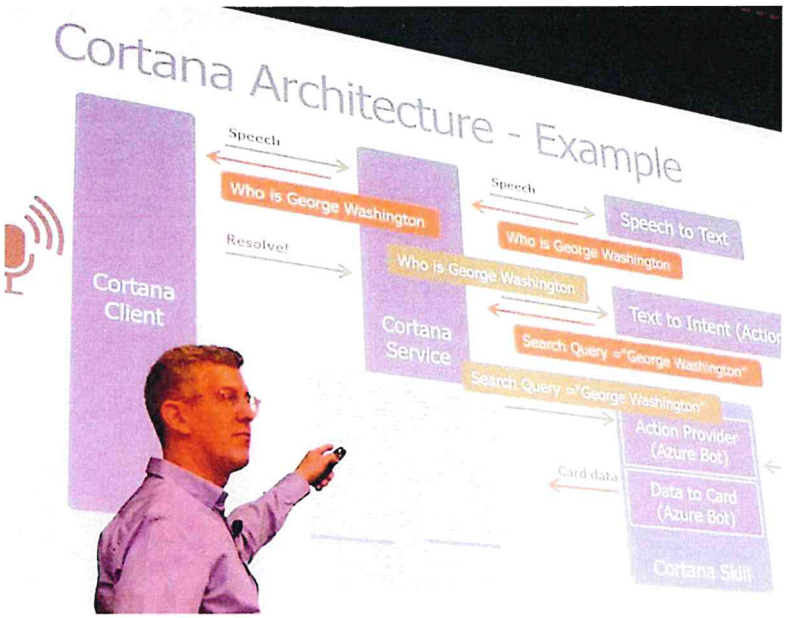


Foto: Bernd Schöne

Sprachassistenten weisen eine komplexe Architektur auf und enthalten etliche Schwachstellen. Die israelischen Forscher Amichai Shulman (Foto) und Yuval Ron untersuchen sie.

Sprachassistenten arbeiten alle ähnlich. Sie schicken Spracheingaben über das Internet an Server, wo KI-gestützte Tools die menschliche Sprache analysieren und in computerlesbare Informationen verwandeln. Das allein stellt bereits ein Sicherheitsrisiko dar. In vielen Betrieben ist ihr Einsatz untersagt oder klar geregelt. Gerade in Zeiten der Coronapandemie nimmt Homeoffice weltweit zu, und in der eigenen Wohnung sind Sprachassistenten gerade in der jungen Generation weit verbreitet. Das gilt erst recht für Smartphones. Für IT-Verantwortliche ist es kaum möglich, den Gerätepark der Angestellten im privaten Umfeld zu kontrollieren. In vielen Ländern, darunter Deutschland, wäre das rechtlich auch nicht zulässig.

Die Sprachassistenten sind per Default auch bei gesperrtem Bildschirm aktiv. Wünscht der Nutzer dies nicht, muss er es recht umständlich anders konfigurieren. Die Entwickler haben sich im Zustand „Locked Device" aber auf solche Befehle beschränkt, von denen ihrer Meinung nach kein Risiko ausgehen kann. Also etwa Fragen wie: „Cortana, wie spät ist es?", oder „Siri, welche Termine muss ich noch abarbeiten?". Wird mehr von den Sprachassistenten verlangt, sollten sie diese Wünsche eigentlich ablehnen, bis der Bildschirm durch Eingabe des Passwortes entsperrt wurde. Doch den Entwicklern sind Fehler unterlaufen. Einer davon schlummert in der „Photo Reminder"-Funktion. Eigentlich ist es ein Service, bei dem ein Foto geladen wird, um an den abgebildeten Gegenstand oder die abgebildete Person zu erinnern. Ein Bug ermöglicht es allerdings, nicht nur Fotos zu laden, sondern beliebige Dateien. Letztendlich kann ein fremder Nutzer so den kompletten Rechner übernehmen.

Dies ergaben die Analysen von Professor Eli Biham vom Technion Cyber Security Research Center in Israel. Seine Mitarbeiter Amichai Shulman und Yuval Ron trugen die Ergebnisse während der Konferenz „IT Defense 2020" der Cirosec AG vor. Die Experten informierten Microsoft bereits 2018 über die Sicherheitslücke. Der Konzern überwies ihnen 50.000 US-Dollar aus dem „Bug Bounty"-Programm und versuchte, den Bug zu beheben. Doch wie konnte es dazu kommen? „Cortana ist ein komplexer, fetter Client", so Amichai Shulman, „mit zahlreichen Unterdiensten". Eventuell übersahen die Microsoft Techniker aus diesem Grund einige Fehler in zugekauften Programmteilen. Weitere Sicherheitslücken fanden die Forscher im sprachgesteuerten Webbrowser. Er führt potenziell gefährliche Nicht-SSL-Links ohne Warnung aus. Webseiten mit Schadcode ließen sich so aufrufen. Die Vorgehensweise ist auch von Erpressungstrojanern bekannt. Sie surfen eine Seite im Darknet an, und installieren von dort die verhängnisvollen Programme. Überraschenderweise konnten die Forscher beide Schwachstellen auch beim Konkurrenzprodukt Siri nachweisen. Eventuell ein Hinweis auf eine gemeinsame Quelle.

„Nicht zum ersten Mal hebeln Servicefunktionen, die dem Nutzer das Leben mit der IT erleichtern sollen, zuvor erarbeitete Sicherheitskonzepte aus."

**Bernd Schöne,**
freier Mitarbeiter des PROTECTOR.

## Sicherheit der Nutzer hängt vom Zufall ab

Ein zusätzliches Risiko stellt die Verschachtelung von Assistenden dar. Zwar werden die wenigsten Nutzer mehre Sprachassistenten auf einem Gerät gleichzeitig nutzen. Doch es ist durchaus möglich, einem Sprachassistent den Befehl zu geben, einen weiteren aufzurufen und zu installieren. Das bewerten Shulman und Yuval Ron als zusätzliche Bedrohung, denn die Schwachstellen addieren sich naturgemäß. In ihren Experimenten konnten sie über den Assistenten Cortana den Assistenten Alexa von Amazon starten. Auch waren sie in der Lage, vom übernommenen Endgerät eine fingierte Spende auf ein falsches Amazon-Charity Konto zu überweisen.

Manchmal geht es noch einfacher. Etwa beim Sprachassistenten Cortana. Wer ihn 2018 aufweckte und die Leerzeichentaste drückte, konnte trotz „Locked Device" beliebige Befehle über die Tastatur eingeben. Inzwischen haben die Forscher 22 Schwachstellen bei Cortana, Siri, Alexa und Bixby gefunden. Die meisten sind nur provisorisch oder noch gar nicht behoben. Oft schalteten die Hersteller die Dienste nur auf den Cloud-Servern ab. Die Sicherheit des Nutzers hängt dann vom Zufall ab. Wird er mit einem aktualisierten Cloud-Server verbunden, hat er Glück, wenn nicht, eben Pech.

Die Verbreitung der Updates, das fanden die Sicherheitsforscher heraus, dauerte oft Wochen. Alternativ besteht die Möglichkeit, kritische Features der Sprachassistenten im Menü des eigenen Gerätes zu blockieren. Etliche der Teilnehmer der Bonner Konferenz wollten das noch vor Ort tun. Dies erwies sich allerdings als schwierig und zeitaufwendig, da zwischen den diversen Sprachassistenten erhebliche Unterschiede bestehen. ■

**BERND SCHÖNE,**
FREIER MITARBEITER DES PROTECTOR