BSI warnt erneut vor vorinstallierter Schadsoftware auf Smartphones

Bonn, 6. Juni 2019. Erneut hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf mehreren Smartphones vorinstallierte Schadsoftware nachgewiesen.

Die Geräte wurden auf unterschiedlichen Online-Marktplätzen gekauft und auf eine bereits im Februar nachgewiesene Schadsoftware-Variante überprüft. Das BSI warnt daher auf Grundlage von §7 des BSI-Gesetzes vor dem Einsatz der Geräte Doogee BL7000

(https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/Produkte/190606_Doogee_BL7000.html)

und M Horse Pure 1

(https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/Produkte/190606_M_Horse_Pure_1.html)

und rät allen Anwenderinnen und Anwendern zu besonderer Vorsicht.

Auch auf dem Gerät Keecoo P11 wurde die Schadsoftware in der Firmware-Version

V3.02 (V362HH.SHWY.HB.HJ.P3.1130.V3.02) nachgewiesen. Für dieses Gerät steht eine Firmware V3.04 (V362HH.SHWY.HB.HJ.P3.0315.V3.04) ohne diese Schadsoftware über die Updatefunktion „Wireless Update“ des Herstellers zur Verfügung. Daneben hat das BSI auf dem Gerät VKworld Mix Plus die gleiche Schadsoftware nachweisen können, diese wurde allerdings nicht aktiv. Auch in diesen Fällen ist für Verbraucherinnen und Verbraucher besondere Vorsicht geboten.

„Unsere Untersuchungen zeigen ganz deutlich, dass IT-Geräte mit vorinstallierter Schadsoftware offensichtlich keine Einzelfälle sind. Sie gefährden die Verbraucherinnen und Verbraucher, die diese günstigen Smartphones kaufen und letztlich womöglich mit ihren Daten draufzahlen. Eine besondere Gefährdung entsteht zudem, wenn das infizierte Smartphone genutzt wird, um das smarte Zuhause inklusive Fenstersicherung oder Alarmanlage zu steuern. Um solche Angriffsszenarien zu verhindern, brauchen wir eine gemeinsame Anstrengung insbesondere seitens der Hersteller und der Händler, damit künftig derartig unsichere Geräte gar nicht erst verkauft werden können“, so BSI-Präsident Arne Schönbohm.

Einzelne Handelsplattformen haben die von der BSI-Warnung betroffenen Geräte bereits bis auf Weiteres aus dem Sortiment genommen. Was Verbraucherinnen und Verbraucher jetzt tun können haben wir hier zusammengefasst:

https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/produktwarnung-it-geraete.html

Hintergründe zur Schadsoftware

Dem BSI liegen sogenannte Sinkhole-Daten vor, die pro Tag Verbindungsversuche zu über 20.000 unterschiedlichen deutschen IP-Adressen mit einem maliziösen C&C-Server nachweisen. Es muss daher von einer größeren Verbreitung von Geräten mit dieser Schadsoftware-Variante in Deutschland ausgegangen werden.

Das BSI hat deutsche Netzbetreiber bereits mittels CERT-Bund Reports über infizierte Geräte in deren jeweiligen Netzen informiert. Die Provider wurden gebeten, ihre betroffenen Kunden entsprechend zu benachrichtigen.

Die von der IT-Sicherheitsfirma Sophos als „Andr/Xgen2-CY“ bezeichnete Schadsoftware übermittelt ad hoc verschiedene kennzeichnende Daten des Geräts an einen C&C-Server und verfügt daneben auch über eine Nachladefunktion.

Darüber könnten weitere Schadprogramme wie etwa Banking-Trojaner auf den jeweiligen Geräten platziert und ausgeführt werden. Eine manuelle Entfernung der Schadsoftware ist aufgrund der Verankerung im internen Bereich der Firmware nicht möglich. Nutzerinnen und Nutzer haben daher keine Möglichkeit, die Geräte zuverlässig zu bereinigen und ohne Schadfunktionalität zu betreiben, solange kein entsprechendes Firmwareupdate zur Verfügung steht.

Bundesamt für Sicherheit in der Informationstechnik


LichtBlick
Generation reine Energie