Baden-Württemberg

LANDESKRIMINALAMT
PRESSESTELLE

BEREIT FÜR SICHERHEIT

Medieninfo

Stuttgart, 4. März 2021

Warnung vor betrügerischen SMS

Es trifft in erster Linie Android-Nutzerinnen und Nutzer: Kriminelle verschicken massenhaft SMS. In dieser kündigen sie die Zustellung eines Pakets an und verlinken hierzu eine Paketverfolgung. Diese SMS beinhaltet einen Download-Link zu einer Schadsoftware mit erheblichen Gefahrenpotenzial.

Um diesen Service zu nutzen, sollen die Adressaten auf ihrem Smartphone die Installation von fremden Inhalten freigeben. Sobald die Nutzerinnen und Nutzer dies tun, erhalten sie mehrere Warnhinweise vom System. Sobald sie dennoch zustimmen, schnappt die Falle zu. Denn es geht hier nicht um die vermeintliche Paktzustellung. Die Kriminellen kapern das Smartphone und verschicken von diesem Smartphone zahlreiche SMS an andere Nutzerinnen und Nutzer weiter. In Baden-Württemberg sind mehrere hundert Smartphones betroffen.

In Einzelfällen verursachen diese SMS einen Schaden bis in den dreistelligen Euro-Bereich, wenn die Nutzerinnen und Nutzer keine Flatrate besitzen und für jede SMS bezahlen müssen. Doch darum geht es den Kriminellen nicht: Sie wollen an die gespeicherten Passwörter auf dem Smartphone. Die App lässt sich durch eine Neuaufsetzung des Smartphones entfernen. Anschließend sollten die Nutzerinnen und Nutzer für jeden Dienst, den Sie auf Ihrem Smartphone nutzen, ein neues Passwort vergeben.

Taubenheimstraße 85 · 70372 Stuttgart · Telefon 0711 5401-2044 · Telefax 0711 5401-1012
pressestelle-lka@polizei.bwl.de · www.lka-bw.de · www.polizei-bw.de

„Diese Nachricht ist nur das Einfallstor, um die Schadsoftware zu verbreiten. Erst im zweiten Schritt geht es darum, an die Passwörter der Nutzerinnen und Nutzer zu kommen. Damit könnten die Täter beispielsweise Gutscheine in den App-Stores kaufen und diese wie Bargeld verwenden“, sagt Ralf Michelfelder, Präsident des LKA BW.

Derzeit nehmen sich Sicherheitsbehörden mehrerer Bundesländer diesem Phänomen an. Die Polizeipräsidien in Baden-Württemberg ermitteln, das LKA BW fungiert als Info-Sammelstelle und gewährleistet den reibungslosen Austausch mit dem Bundekriminalamt und Bundesamt für Sicherheit in der Informationstechnik. Trotz aller Ermittlungen in enger Abstimmung mit den Kooperationspartnern liege der Schlüssel zur Schadensabwehr primär beim Nutzer. „Seien Sie achtsam und klicken Sie nicht unbedacht auf einen Link. Überlegtes Handeln schützt auch am Handy vor großen Schäden“, so Michelfelder.

Das können Sie tun, um sich vor diesem Angriff zu schützen:

- Klicken Sie auf keinen Fall auf Links von unbekannten Absenderinnen und Absendern. Sollten Ihnen diese bekannt sein, fragen Sie auf alternativem Weg nach, was sich hinter dem Link verbirgt und ob der Versand beabsichtigt war.
- Bestätigen Sie keine Installation von fremden Apps auf Ihrem Smartphone. Android-Geräte sind besonders gefährdet, da bei diesen Geräten prinzipiell eine Fremdinstallationen schädlichen Apps möglich ist.
- Deaktivieren Sie bei Android die Möglichkeit, unbekannte Apps zu installieren. Gegebenenfalls ist in Ihrer Android-Version diese Funktion nicht im Sicherheitsbereich sondern im App-Menü zu finden. Geben Sie unter Einstellungen in der Suche beispielsweise „unbek“ oder „ext.“ an. Möglicherweise werden Sie nun in den Bereich „Unbekannte Apps installieren“ geführt, bei denen Sie einzelnen Apps diese Erlaubnis erteilen oder entziehen können. Ohne diese Erlaubnis ist die Installation von Apps aus fremden Quellen nicht möglich. Bitte beachten Sie: Je nach Android-Version und Smartphone kann diese Einstellung variieren.
- Richten Sie unbedingt bei Ihrem Mobilfunkprovider die Drittanbietersperre ein, um weitere Kosten zu vermeiden. Dieser Service ist kostenlos.

- Wenn Sie eine Smishing-SMS erhalten, heißt das nicht zwangsläufig, dass die Schadsoftware auf Ihrem Smartphone installiert ist. Solange Sie den Link nicht angeklickt und die App nicht installiert haben, kann noch nichts passiert sein.

Wenn Sie die App bereits auf ihrem Smartphone installiert haben, sollten Sie Folgendes tun:

- Schalten Sie Ihr Smartphone in den Flugmodus.
- Informieren Sie Ihren Provider.
- Richten Sie die Drittanbietersperre ein.
- Prüfen Sie, ob durch die SMS bereits Kosten entstanden sind. Fragen Sie bei Ihrem Provider nach und bitten um einen Kostennachweis.
- Erstatten Sie Anzeige bei Ihrer örtlichen Polizeidienststelle. Bringen Sie dazu das Smartphone, gegebenenfalls Fotos vom Bildschirm, Kostennachweise und weitere relevante Informationen mit.
- Nachdem Sie eine Anzeige erstattet haben, sollten Sie das Smartphone auf die Werkeinstellungen zurücksetzen und für jeden Dienst, den Sie auf Ihrem Smartphone nutzen, ein neues Passwort vergeben.

Landeskriminalamt Baden-Württemberg
Pressestelle
E-Mail: pressestelle-lka@polizei.bwl.de
Telefon: 0711 5401-2044