Schutz vor Phishing bei der Handy-Signatur

RTR-GmbH

Stand: 21.07.2016

1 Vorbemerkung

Die Sicherheit der Handy-Signatur wurde in manchen Medienberichten der letzten Monate in Frage gestellt. Dabei ging es aber weniger um die Sicherheit der Handy-Signatur selbst als um Phishing: Eine Nutzerin bzw. ein Nutzer kann, beispielsweise durch einen per E-Mail verbreiteten Link, dazu gebracht werden, die für die Erstellung einer Handy-Signatur erforderlichen Daten (Mobiltelefonnummer, Signaturpasswort und TAN) auf einer unter Kontrolle des Angreifers befindlichen Webseite einzugeben. Der Angreifer kann diese Daten missbrauchen, um ein beliebiges Dokument mit der qualifizierten elektronischen Signatur der Nutzerin bzw. des Nutzers zu versehen.

Bei entsprechender Sorgfalt sind solche Angriffe für Nutzerinnen und Nutzer erkennbar. Das vorliegende Dokument enthält Hinweise, wie man sich als Nutzerin bzw. Nutzer der Handy-Signatur vor Phishing und manchen anderen Gefährdungen schützt.

2 Sorgfaltspflicht

Wie bei der handschriftlichen Unterschrift auf Papier hat man auch bei der elektronischen Signatur darauf zu achten, was man signiert. Dabei muss man auf das „Kleingedruckte“ ebenso achten wie darauf, dass einem nicht von Dritten etwas Nachteiliges zur Signatur „untergeschoben“ wird. Wichtig ist in diesem Zusammenhang, dass man die vom Anbieter bereitgestellten Informationen über den richtigen Umgang mit der Handy-Signatur beachtet.

Dazu gehört vor allem,

- in Verbindung mit der Handy-Signatur eingesetzte Apps nur aus offiziellen App-Stores der jeweiligen Anbieter (iTunes App Store, Google Play Store, Windows App Store bzw. BlackBerry World) zu beziehen;
- die Sicherheitsmechanismen des Mobiltelefons nicht durch Rooten oder Jailbreak[1] zu umgehen;
- aktuelle Sicherheits-Software (Antivirus, Firewall) einzusetzen;
- im Webbrowser das automatische Speichern eingegebener Formulardaten und Passwörter zu deaktivieren;
- auf die Trennung der technischen Komponenten zu achten und das Signaturpasswort nicht auf demselben Gerät einzugeben, auf dem auch die TAN empfangen wird;
- das Signaturpasswort ausschließlich auf Webseiten einzugeben, auf denen in der Adresszeile des Browsers der URL (Internetadresse) https://www.a-trust.at/ oder https://www.handy-signatur.at/ aufscheint, und
- vor Eingabe der TAN in das Webformular zu prüfen, ob der auf dem Mobiltelefon (in der Handy-Signatur-App oder einer SMS-Nachricht) dargestellte Vergleichswert mit dem im Webformular dargestellten Wert übereinstimmt.

Der Anbieter der Handy-Signatur empfiehlt auch, zusätzliche Hinweise zu beachten. Diese Empfehlungen sind sinngemäß für sämtliche Applikationen und Dienste, besonders für sensible Anwendungen, relevant.

[1] Darunter versteht man, vereinfacht ausgedrückt, das Entsperren geschützter Systembereiche, auf die dann nicht nur berechtigte Nutzerinnen und Nutzer, sondern auch Schadprogramme zugreifen können.

3 Vorsicht bei Links in E-Mails

E-Mails mit Links zu Seiten, auf denen eine elektronische Signatur erstellt werden muss, sind grundsätzlich verdächtig – vor allem dann, wenn Link und angezeigter Text nicht übereinstimmen –, denn das Versenden solcher Links widerspricht den üblichen Praktiken. Grundsätzlich wird empfohlen, die gewünschte Internetadresse selbst in die Adresszeile des Browsers einzugeben oder die Seite ggf. über eine Suchmaschine abzurufen. Bei derartigen Vorgängen sollte man ganz besonders darauf achten, ob die Kommunikation vertrauenswürdig ist.

4 Vertrauenswürdigkeit der Kommunikation

A-Trust empfiehlt, das Signaturpasswort nur auf Seiten anzugeben, auf denen in der Adresszeile des Browsers der URL https://www.a-trust.at/ oder https://www.handy-signatur.at/ aufscheint. Oft ist aber das Formular, in das das Signaturpasswort einzugeben ist, in die Webseite eines Dritten eingebettet. Da man in diesem Fall in der Adresszeile des Browsers nur den URL dieser Webseite sieht, ist auf den ersten Blick nicht ersichtlich, ob die Kommunikation tatsächlich über einen vertrauenswürdigen Server von A-Trust erfolgt. Es besteht jedoch immer die Möglichkeit, das Formular zur Eingabe des Signaturpassworts in einem eigenen Browserfenster darzustellen und den in der Adresszeile dieses Browserfensters dargestellten URL zu vergleichen.

Zu diesem Zweck folgt man vor Eingabe von Signaturpasswort und TAN dem Link „Eigenes Fenster“ (in Abb. 1 rot markiert).

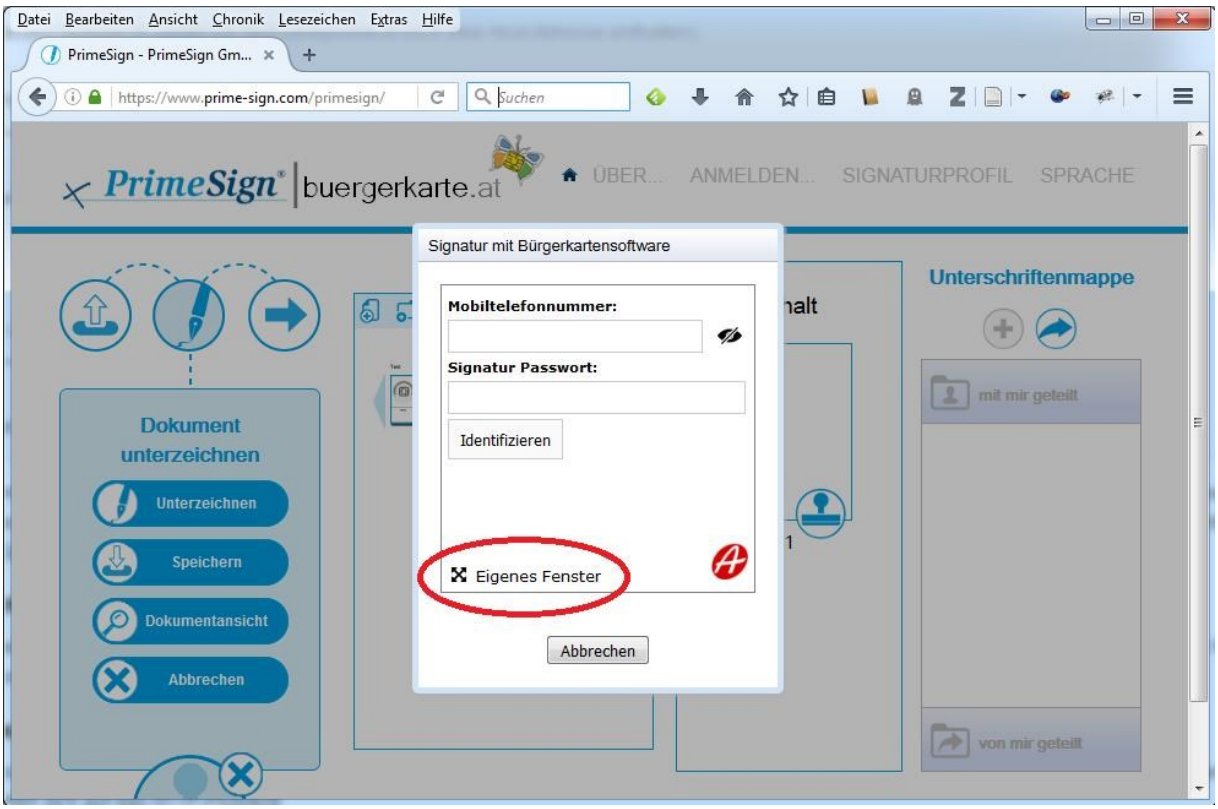

Abbildung 1

Daraufhin öffnet sich ein Browserfenster mit eigener Adresszeile. Nur dann, wenn in der Adresszeile dieses Browserfensters der URL https://www.a-trust.at/ oder https://www.handy-signatur.at/ aufscheint (in Abb. 2 rot markiert), sollte die Signaturerstellung fortgesetzt

werden. Jeder andere URL würde darauf hindeuten, dass ein Angreifer die eingegebenen Informationen abfängt.

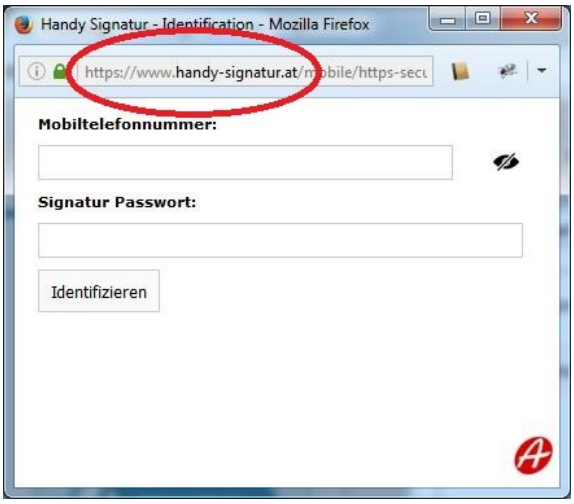

Abbildung 2

Abbildung 3

5 Prüfung der signierten Daten

Nach Eingabe des Signaturpassworts erscheint im Browserfenster entweder ein Formular zur Eingabe der TAN oder ein mit dem Mobiltelefon einzuscannender QR-Code. Jedenfalls enthält die Webseite auch einen Link „Signaturdaten anzeigen“ (in Abb. 3 rot markiert). Indem man diesem Link folgt, werden jene Daten dargestellt oder heruntergeladen, die bei regulärem Abschluss des Vorgangs signiert würden. Durch Prüfung dieser Daten kann man sich davon überzeugen, was man tatsächlich signiert. Eine Abweichung dieser Daten von den hochgeladenen Daten würde auf Manipulation hindeuten. In diesem Fall erscheint es ratsam, den Signaturvorgang abzubrechen.

6 Vergleichswert

Überdies enthält das oben (in Abb. 3) dargestellte Formular einen Vergleichswert, der auch auf dem Mobiltelefon (in der Handy-Signatur-App oder einer SMS-Nachricht) dargestellt wird. Normalerweise stimmen diese Werte überein. Eine Abweichung dieser Werte würde ebenfalls auf eine Manipulation hindeuten. Auch in diesem Fall erscheint es ratsam, den Signaturvorgang abzubrechen.

7 Was tun nach einem Phishing-Angriff?

Falls man trotzdem durch einen Phishing-Angriff überlistet worden ist und dabei die für eine Signaturerstellung erforderlichen Daten (Mobiltelefonnummer, Signaturpasswort und TAN) preisgegeben hat, empfiehlt es sich,

- den Vorfall der beim Bundeskriminalamt eingerichteten Meldestelle Cybercrime zu melden,
- die Umstände des Vorfalls zu Beweiszwecken genauestens zu dokumentieren und
- das der Handy-Signatur zugrundeliegende Zertifikat zu widerrufen oder zumindest das Signaturpasswort zu ändern.

Besser ist freilich, schon rechtzeitig Vorsicht walten zu lassen und jedes Mal genau zu prüfen, wofür man die Handy-Signatur einsetzt.