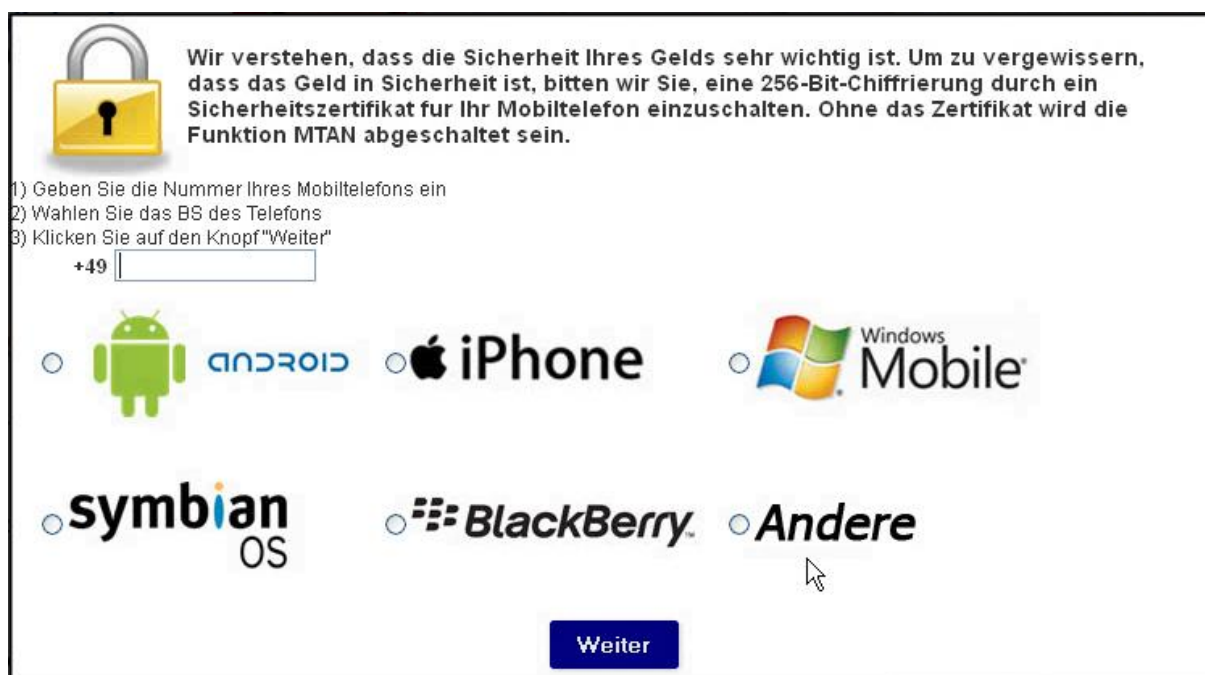


Trojaner versucht durch Social Engineering Methode Smartphones zu infizieren

Bei einem VR-Bank-Kunden wurde eine Social Engineering-Methode beobachtet, mittels derer Betrüger versuchten, das für das mobileTAN-Verfahren genutzte Smartphone zu infizieren. Beim Einloggen ins Online-Banking wurde die Aufforderung eingeblendet, ein "Sicherheitszertifikat" auf dem Smartphone zu aktivieren, ohne das mobileTAN nicht mehr möglich sei.



The screenshot shows a phishing interface for activating a security certificate. At the top left is a yellow padlock icon. The main text reads: "Wir verstehen, dass die Sicherheit Ihres Gelds sehr wichtig ist. Um zu vergewissern, dass das Geld in Sicherheit ist, bitten wir Sie, eine 256-Bit-Chiffrierung durch ein Sicherheitszertifikat für Ihr Mobiltelefon einzuschalten. Ohne das Zertifikat wird die Funktion MTAN abgeschaltet sein." Below this, three instructions are listed: "1) Geben Sie die Nummer Ihres Mobiltelefons ein", "2) Wählen Sie das BS des Telefons", and "3) Klicken Sie auf den Knopf 'Weiter'". A text input field contains "+49" followed by a cursor. Below the input field are six radio button options for mobile operating systems: Android, iPhone, Windows Mobile, Symbian OS, BlackBerry, and Andere. A blue "Weiter" button is at the bottom center.

Kommen die Nutzer des Online-Bankings dieser Aufforderung nach, wird auf das Smartphone im Erfolgsfall ein Trojaner installiert. Da der Angriff über den PC der Betroffenen erfolgt kann zudem davon ausgegangen werden, dass die Zugangsdaten zum Online-Banking den Betrügern hinter diesem Angriff bereits bekannt sind. Wird das Smartphone erfolgreich infiziert, können die Betrüger TANs für Überweisungen generieren und die SMS entsprechend umleiten, so dass der betroffene Kunde dies nicht sofort mitbekommt.

Quelle: [intern](#)