

Das Bundeskriminalamt und das Bundesamt für Sicherheit in der Informationstechnik teilen mit:

Bundeskriminalamt und Bundesamt für Sicherheit in der Informationstechnik raten Nutzern zur Vorsicht: Neue Schadsoftware spioniert Kreditkarten- und Online-Banking-Daten aus

Wiesbaden/Bonn – Bundeskriminalamt (BKA) und Bundesamt für Sicherheit in der Informationstechnik (BSI) raten Nutzern zur Vorsicht: Derzeit verbreitet sich eine neue Variante von Schadsoftware, die Online-Banking- und Kreditkartendaten ausspioniert. Das Trojanische Pferd ist bereits seit mehreren Jahren aktiv. Die neue Variante hat es zurzeit gezielt auf TANs von Online-Banking-Nutzern und Kreditkartendaten abgesehen. Die Infektion des PCs erfolgt meist durch ein so genanntes Drive-by-Exploit, also den Besuch einer mit Schadcode infizierten Webseite.

Wenn der Computer eines Nutzers mit dieser neuen Variante der Schadsoftware infiziert ist und dieser die Anmelde-Webseite seines Kreditkarten- oder Bankportals öffnet, sorgt die Schadsoftware dafür, dass zwar die korrekte Webseite aufgerufen, dort aber manipulierte Inhalte angezeigt werden.

Unter Vorspielung falscher Tatsachen wird der Nutzer so dazu gebracht, bestimmte Daten preiszugeben. Die angebliche Begründung sieht zum Beispiel im Fall der Kreditkartendaten wie folgt aus:

„Die XY Portal passt sich den hohen Kundenansprüchen an. Wir bleiben immer auf dem neusten Stand mit Sicherheitsvorschriften um unseren Kunden mehr Sicherheiten zu bieten. Unser Sicherheitsabteilung erfand ein neues Sicherheitssystem, die Angriffe von Dritten verhindert um Betrugsfälle. Diese Sicherheitssystem muss von allen Online-Banking-Kunden genutzt werden. Wir empfehlen Ihre Daten zu Angleichung anzugeben. Sollte die Anmeldung in 48 Stunden nicht erfolgen, so wird Ihre Karte vorübergehend gesperrt, bis zu Ende der Anmeldevorgang.“

Dadurch sollen die Nutzer dazu gebracht werden, insbesondere Daten

- zur Kreditkartennummer,
- zum Inhaber der Kreditkarte,
- zum Gültigkeitsdatum,
- zur Prüfnummer (CVV2 / CVC2 auf der Rückseite
- zum Geburtsdatum des Karteninhabers

auf der entsprechend erscheinenden Maske einzugeben. In anderen Fällen manipuliert die Schadsoftware Online-Banking-Seiten und fordert dort unter anderem zur Eingabe von 20 TANs auf. Die auf dem Computer installierte Schadsoftware leitet diese Informationen an die Täter weiter, welche die Daten entweder persönlich gewinnbringend einsetzen oder damit handeln können.

Das Bundeskriminalamt und das Bundesamt für Sicherheit in der Informationstechnik raten daher zur Vorsicht:

Sollten Sie beim Aufrufen Ihres Kreditkarten- oder Bank-Portals die oben dargestellte oder eine ähnliche Aufforderung zur Eingabe ihrer Daten erhalten, geben Sie diese keinesfalls ein. Ihr Rechner ist dann mit hoher Wahrscheinlichkeit mit einer Schadsoftware infiziert. Nehmen Sie im Zweifelsfall zur Klärung Kontakt zu Ihrem Bank- bzw. Kreditkarteninstitut auf.

Um einer Infektion mit der Schadsoftware vorzubeugen bzw. eine bereits erfolgte Infektion des Rechners zu beseitigen, sollten Nutzer ein aktuelles Virenschutzprogramm einsetzen. Sie sollten darüber hinaus darauf achten, dass Sie regelmäßig die Sicherheitsupdates für Ihr Betriebssystem und für weitere verwendete Software installieren sowie eine Personal Firewall einsetzen. Vorsichtig sollten Nutzer auch bei Links oder Dateianhängen in E-Mails sein: Dahinter können sich Schadprogramme oder infizierte oder gefälschte Webseiten verbergen.