NACHRICHTEN AG

07. Juni 2025

Warnung für Sparkassen-Kunden: Gefährliche Trojaner bei Überweisungen!

Sparkasse warnt vor aktuellen Cyberangriffen: Trojaner manipuliert Überweisungsdaten. Kunden müssen besonders aufpassen!

Deutschland - Die Sparkasse warnt derzeit vor einer neuen Betrugsmasche, bei der Cyberkriminelle gezielt Überweisungsdaten von Kunden manipulieren. Diese Angriffe treffen insbesondere die Nutzer von Online-Banking, wobei vor allem Firmenkunden stark betroffen sind. Laut **Ruhr24** sind die Angriffe durch sogenannte Banking-Trojaner, die sich häufig auf Windows-PCs aktivieren, stark angestiegen.

Die Malware kann unbemerkt wirken, indem sie beim Online-Banking über gängige Browser wie Chrome, Edge oder Firefox die im Überweisungsformular eingegebene Empfänger-IBAN durch eine gefälschte IBAN ersetzt. Dies kann zu falschen und eventuell kostspieligen Überweisungen führen, die schwer zu

erkennen sind. Laut **watson** agiert der Trojaner besonders auffällig, wenn Kunden eine Überweisung mit einem höheren Betrag tätigen.

Risiken und notwendige Vorsichtsmaßnahmen

Das Computer-Notfallteam der Sparkasse empfiehlt, vor jeder Überweisung den Betrag sowie die Empfänger-IBAN in der TAN-Generator- oder pushTAN-App zu überprüfen. Falsche Daten sind in diesen Anwendungen ersichtlich, während sie im Online-Banking selbst oft nicht zu erkennen sind. Bei Feststellung von manipulierten Überweisungsdaten wird geraten, umgehend den Online-Banking-Zugang zu sperren.

Zusätzlich zu Trojaner-Angriffen gibt es eine Zunahme von Phishing-Angriffen. Falsche E-Mails und SMS, die angeblich von der Sparkasse stammen, fordern die Nutzer auf, ihre pushTAN-App zu aktualisieren und leiten sie auf betrügerische Webseiten weiter. Nutzer sind angehalten, darauf zu achten, keine persönlichen Daten auf verdächtigen Seiten einzugeben und solche Nachrichten im Spam-Ordner zu entfernen, so **BSI**.

Generelle Gefahren im Online-Banking

Phishing ist inzwischen ein weit verbreitetes Problem, das alle Online-Nutzer betrifft. Cyberkriminelle setzen hier auf täuschend echte E-Mails und Websites, um persönliche Daten wie PINs und TANs zu stehlen. Nutzer sollten niemals ihre Zugangsdaten in digitalen Nachrichten preisgeben und bei verdächtigen Aktivitäten direkt die eigene Bank kontaktieren.

Das Online-Banking bietet zwar Komfort, birgt jedoch auch erhebliche Sicherheitsrisiken. Regelmäßige Wachsamkeit und das Ergreifen der notwendigen Vorsichtsmaßnahmen sind entscheidend, um sich vor diesen kriminellen Angriffen zu schützen.

Details	
Vorfall	Cyberkriminalität
Ursache	Phishing, Trojaner
Ort	Deutschland
Quellen	• **www.ruhr24.de** • **www.watson.de** • **www.bsi.bund.de**