

Schutz des Teilnehmersystems

Zum Schutz des Teilnehmersystems im Online-Banking sind folgende Sicherheitsmaßnahmen zu ergreifen:

- Das für das Online-Banking vom Teilnehmer genutzte System ist durch technische Maßnahmen gegen das Ausspähen der Sicherheitsmerkmale (z. B. PIN oder TAN-Liste) zu sichern. Es ist ein Betriebssystem einzusetzen, das dessen Hersteller für den Zugang zum Internet vorgesehen hat und für das er bei Bedarf Programmänderungen (z. B. Sicherheitspatches) zur Verfügung stellt, die erkannte Sicherheitsrisiken beheben.
- Die Systemeinstellungen sind entsprechend den Herstellerempfehlungen vorzunehmen. Bietet der Hersteller mehrere Sicherheitsstufen an, ist eine hohe Sicherheitsstufe einzustellen.
- Zusätzlich ist das System – soweit technisch verfügbar – durch ein Antivirenprogramm zu schützen sowie der Datenverkehr durch ein Firewallprogramm zu kontrollieren.
- Betriebssystem, Programme, die den Zugang zum Internet vermitteln (z. B. Browser), sowie die installierten Schutzprogramme sind nach den Empfehlungen des jeweiligen Herstellers aktuell und sicher zu halten.

Weiterführende Hinweise zum Schutz des Teilnehmersystems können den Sicherheitshinweisen der Sparkasse entnommen werden, die auf den Internetseiten für das Online-Banking veröffentlicht und aktualisiert werden.