

## Erweiterte Sicherheitseinstellungen

Angriffe im Onlinebanking zielen derzeit vor allem auf das Internetbanking und den beim Kunden hierfür genutzten Browser. Electronic Banking Software-Produkte standen bisher nicht im Fokus solcher Angriffe. Zukünftig ist aber damit zu rechnen, dass auch Kundenprodukte ins Visier von Angreifern geraten könnten.

Um das hohe Sicherheitsniveau der VR-NetWorld Software weiter zu halten, wurden bereits jetzt zusätzliche Hürden für zwei der wahrscheinlichsten Methoden integriert.

### Identität der VR-NetWorld Software

Beim Identitätsschutz wird von einem Szenario ausgegangen, bei dem eine Schadsoftware Teile der VR-NetWorld Software nachbaut. Der Anwender soll so dazu verleitet werden, im Glauben, dass er sich in der vertrauten VR-NetWorld Software befindet, sicherheitsrelevante Informationen wie z. B. PIN und TAN in den Nachbau der entsprechenden Masken einzugeben.

- **Persönliches grafisches Siegel**

Um einen Nachbau der VR-NetWorld Software oder Teile der VR-NetWorld Software für einen Angreifer zu erschweren, werden standardmäßig alle relevanten Eingabedialoge mit einem grafischen Siegel versehen. Das grafische Siegel enthält neben dem aktuellen Datum auch diverse Textinformationen zum geöffneten Dialog und der Art der einzugebenden Daten. Zusätzlich kann der Anwender einen persönlichen Text hinterlegen, der als persönlicher Sicherheitsanker ebenfalls im Siegel mit angezeigt wird.

Um einen Nachbau der Masken weiter zu erschweren, werden die Textinformationen als Rolltext in der Grafik eingeblendet.



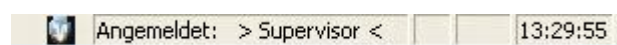
- **Signierter Mauszeiger**

Neben dem persönlichen grafischen Siegel können die Eingabemasken zusätzlich durch einen speziellen Mauszeiger abgesichert werden, der in einer Art Fahne ebenfalls die Informationen aus dem Siegel anzeigt.

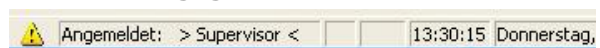
- **Signalisierung, ob ein Eingabefenster im Vordergrund ist**

Zusätzlich zu den beiden Mechanismen, die den Nachbau einzelner Masken der VR-NetWorld Software erschweren sollen, überwacht die VR-NetWorld Software, ob eine geöffnete Erfassungsmaske auch im Vordergrund steht und nicht von einer anderen Anwendung überdeckt wird. Der entsprechende Status wird unten in der Statuszeile angezeigt, sobald eine Erfassungsmaske geöffnet ist.

Hierbei signalisiert ein kleines Siegel, dass die Erfassungsmaske im Vordergrund ist.



Das Ausrufezeichen in einem gelben Dreieck warnt hingegen davor, dass eine andere Anwendung im Vordergrund ist.





## **Schutz vor dem Auslesen von sensiblen Informationen während der Eingabe**

Der Schutz vor dem Auslesen von Eingaben soll verhindern, dass potentielle Schadsoftware die Eingaben eines Anwenders mitliest oder manipuliert.

- **Verschleierung der Bedeutung von Eingabefeldern**

Bei der Entwicklung von Windows-Anwendungen ist es vorgesehen und üblich, dass alle Eingabefelder mit sprechenden Bezeichnungen versehen werden, die auch auslesbar sind. Diese Bezeichnungen nutzen z. B. spezielle Programme, die Sehbehinderten die Nutzung von Standardsoftware erleichtern sollen. Diese Informationen könnten aber auch Schadprogramme nutzen, um z. B. gezielt die Eingabe von Passwörtern auszulesen. Mit der Verschleierung der Bedeutung der Eingabefelder ist das nicht mehr möglich. Um sehbehinderten Menschen weiterhin die Nutzung der VR-NetWorld Software zu ermöglichen, wird der Anwender darauf hingewiesen, dass er in diesem Fall den Kompatibilitätsmodus für Sehbehinderte aktivieren muss.

- **Auslesen von Beschriftungstexten verhindern**

Zusätzlich zur Verschleierung der eigentlichen Eingabefelder kann auch ein Auslesen der Beschriftung der einzelnen Eingabefelder unterbunden werden.