

A close-up, slightly blurred photograph of a white computer keyboard. A silver metal padlock is placed over the spacebar and the 'Shift' key to its right, symbolizing security or access control.

SIX Terravis AG

Prüfung Treuhänderverwaltung

25. Oktober 2013

Quelldokument:	report_81872_terravis_partner_v1.1.docx
Version:	v1.1
Projektnummer:	81872
Autor(en):	Michael Fisler, Compass Security AG
Auslieferungsdatum:	25. Oktober 2013
Klassifikation:	PUBLIC



1 Management Summary

1.1 Gesamtbeurteilung

Aufgrund der Ergebnisse der im Oktober 2013 durchgeführten Sicherheitsüberprüfung, beurteilt Compass Security die Sicherheit der Terravis Nominee Web Applikation mit dem momentanen Funktionsumfang als gut. Die Analysten haben keine Bedrohungen festgestellt, welche die Integrität, Verfügbarkeit und Vertraulichkeit der Daten zur Folge haben. Es wurden lediglich leicht gewichtete Schwachstellen identifiziert, die zur Erreichung eines sehr guten Sicherheitsniveaus behoben werden sollten.

1.2 Einleitung

SIX Terravis AG wird im Jahr 2013 eine neue Funktion in die bestehende Plattform integrieren, welche es der SIX erlaubt, als Treuhänder für Register-Schuldbriefe zu fungieren. Im Rahmen einer Abnahmeprüfung wurde die Sicherheit der neuen Funktionalität und Systeme beurteilt. Compass Security hat diese Sicherheitsüberprüfung im Juni 2013 vorgenommen.

Die Sicherheitsüberprüfung sollte dazu dienen, einen Überblick über die Bedrohungslage von Seite Internet zu erhalten. Insbesondere sind folgende Erkenntnisse erarbeitet worden:

- ✦ Einschätzung des Bedrohungspotentials der implementierten Architektur und Internetanbindung aus der Sicht des Angreifers vom Internet
- ✦ Überprüfung der neuen SMS-Challenge-Authentisierung
- ✦ Detaillierte Empfehlungen zur Verbesserung der Sicherheit

Die im Juni 2013 gefundenen Schwachstellen wurden von den Entwicklern adressiert. Um sicherzustellen, dass die Sicherheitsprobleme behoben sind, hat Compass im Oktober 2013 die Applikation erneut überprüft.

1.3 Ergebnisse

Die "Cross-Site Scripting"-Schwachstelle, durch welche die Darstellung in der Webseite manipuliert werden und eine Umleitung des Benutzers auf eine Web-Seite mit Schadcode stattfinden konnte, wurde erfolgreich beseitigt.

Im Weiteren wurde die Autorisierungs-Schwachstelle behoben, durch welche ein Bankmitarbeiter oder Notar Funktionen eines SIX SIS Mitarbeiters aufrufen konnte.

Die Schuldbrief-Depots sind nun für alle Banken strikt getrennt.

Es verbleiben lediglich leicht gewichtete Schwachstellen.

1.4 Empfehlungen

Compass Security empfiehlt, dass die verbleibenden, leicht gewichteten Schwachstellen mittelfristig ebenfalls behoben werden.