

## IT-SECURITY

# Compilierter Code unter der Lupe

Jede Woche beantworten Sicherheitsexperten Leserfragen und geben Ratschläge, wie sich die Sicherheit in einem Unternehmen erhöhen lässt.

## Frage: Wann sollte ich eine Applikation einem Reverse Engineering unterziehen?

Als Reverse Engineering («verkehrt herum entwickeln» oder besser «rekonstruieren») wird das Erstellen eines Bauplans auf Basis des fertigen Produktes bezeichnet. Es handelt sich dabei um eine gängige Analyse-methode, welche in den unterschiedlichsten Gebieten der Wissenschaft genutzt wird: Sowohl der Teilchenphysiker als auch der Genetiker betreiben dies täglich, um die Funktion des Ganzen zu verstehen.

In der Informatik bezeichnet Reverse Engineering die Analyse des kompilierten Codes einer Software. Dies kann etwa eine ausführbare Datei oder eine Bibliothek (DLL) sein. Hierbei wird aus dem ausführbaren Code ein quasi-Quellcode erstellt. Der Maschinencode – die Instruktionen an den Prozessor – werden analysiert und grafisch dargestellt. So erhält der Reverse Engineer einen ersten Überblick zur Programmlogik und den verwendeten Routinen. Variablen und Sprungadressen werden anschliessend mit Namen versehen und durch die Analyse externer Funktio-

nen wird bald ersichtlich, welcher Programmcode für welche Aufgabe zuständig ist.

Reverse Engineering von Software ist in Verruf geraten, weil viele Hersteller dies in ihren Lizenzbedingungen ausdrücklich verbieten. Die Klausel soll aber eher als Abschreckung dienen und würde vor Gericht nicht standhalten. Reverse Engineering zu verbieten wäre mit ei-

## «Aus Security-Sicht sollte eine Software grundsätzlich keine Geheimnisse bergen.»

nem Verbot der Autohersteller, unter die Motorhaube zu schauen vergleichbar. Wer hingegen Reverse Engineering nutzt, um einen Kopierschutz zu umgehen – was mit dieser Technik bestens klappt – macht sich allerdings nach wie vor strafbar.

Aus Security-Sicht sollte eine Software grundsätzlich keine Geheimnisse bergen. Problematisch sind oft Client-Applikationen, welche eine Benutzer/Passwort-Kombination beherrschen, um sich bei einem Serverdienst anzumelden. Der Programmierer kann hier noch so stark verschlüsseln: Solange sich das «geheime» Element in der Software befindet, muss es

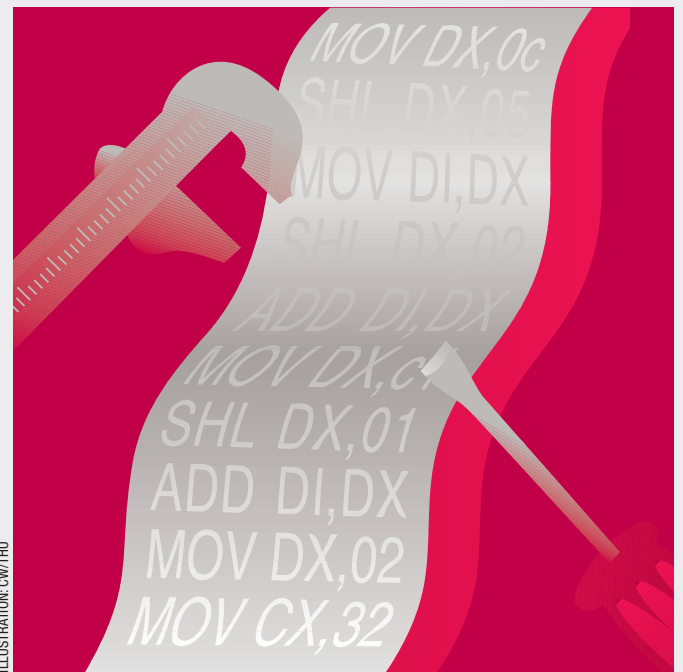


ILLUSTRATION: GW/THÜ

als öffentlich betrachtet werden. Aus diesem Grund müssen sämtliche sicherheitsrelevanten Entscheidungen serverseitig getroffen werden und die Passwörter in den Köpfen der Benutzer, beziehungsweise Zertifikate auf Smartcards bleiben. Alles andere deutet auf unsicheres Design hin.

Gibt es also eine Berechtigung für ein Reverse Engineering im Zusammenhang mit einer applikatorischen Sicherheitsüberprüfung? Ein Security Tester wird zunächst aus seiner Erfahrung heraus «blind» versuchen, typische Programmierfehler zu identifizieren und Laufzeitfehler zu provozieren. Diese Tests können relativ schnell zum Erfolg führen, sind aber eher als Stichproben zu betrachten.

Um weitere Schwachstellen zu finden, benötigt der Tester entweder Zugriff auf den Source Code, den er einem «Code Review» unterzieht, oder eben die binäre Datei, welche er mittels Reverse Engineering analysieren kann. Schwachstellen können auf beide Arten gefunden werden, weshalb oft die Firmenpolitik entscheidet, ob der Source Code oder das Kompilat abgegeben wird.

Sowohl bei der Analyse von Binär- als auch von Quellcode lassen sich Automatismen nutzen, um typische Anfälligkeiten wie unterminierte Puffer zu entdecken. Ein seriöser Tester wird sich aber speziell auf bestimmte Eintrittspunkte wie den Netzwerkdienst oder die Authentisierung fokussieren, um Fehler aufzudecken, die seine Tools evtl. übersehen haben. Aus Kostengründen macht es aus Kundensicht selten Sinn, die komplette Applikation auf diese Weise zu prüfen.

Ein bössartiger Angreifer, der eine Schwachstelle nutzen will, um in ein System einzudringen, wird sich übrigens über den Quellcode zwar freuen, da er jedoch die Schwachstelle auch ausnutzen will, mehr Verwendung für das binäre Kompilat haben. ■



**Der Autor**  
Simon Wepfer ist CTO bei der Sicherheitsberatung Oneconsult, Thalwil. [www.oneconsult.com](http://www.oneconsult.com)

**Unsere Experten beantworten Ihre Fragen.** Schreiben Sie uns: [it-security@computerworld.ch](mailto:it-security@computerworld.ch)

Ein Archiv der Helpdeskartikel finden Sie im Internet: [www.computerworld.ch](http://www.computerworld.ch)