

# Wegfahrsperrre verteidigt Maschinen und Anlagen vor Produktpiraten

Oliver Winzenried

Das Bundesministerium für Bildung und Forschung und der VDMA nehmen Produktpiraterie als Bedrohung für deutsche Unternehmen wahr und unterstützen die Entwicklung von Abwehrmaßnahmen. Die aktuelle Umfrage des VDMA über Produkt- und Markenpiraterie verdeutlicht die stetig wachsende Schattenwirtschaft mit Plagiaten und Nachbauten im Maschinen- und Anlagenbau. Der jährliche Schaden dieser Branche beträgt 6,4 Milliarden Euro; der größte Schaden entsteht durch den Nachbau ganzer Maschinen und Komponenten. Um die Angriffe von allen Seiten abzuwehren, bedarf es einer durchgängigen Schutzstrategie, die alle beteiligten Unternehmen berücksichtigt. Das Ziel ist eine wirkungsvolle Wegfahrsperrre, an der sich die Piraten die Zähne ausbeißen. Ein Beispiel aus der Textilindustrie verdeutlicht mögliche Angriffspunkte innerhalb eines Prozesses:

**Klassische Softwarepiraterie** – Mit Hilfe der Designsoftware werden Bildmotive mit optimierten Stickmusterdaten erstellt. Die PC-Software könnte als Raubkopie oder als gecrackte Version, die im Internet zu einem niedrigeren Preis verkauft wird, den Softwarehersteller schädigen.

**Designpiraterie** – Eine Textilie zeichnet sich durch ein herstellertypisches Stickmotiv (Logo) aus. Werden die Produktionsdaten des Logos weitergegeben, können Piraten Plagiate, markiert als hochwertige Qualität, herstellen. Den Schaden haben die Auftraggeber der Textilien.

**Produktpiraterie** – Schaden entsteht, wenn Plagiate von ganzen Maschinen hergestellt werden, indem die mechanischen Teile nachgebaut und die eingebaute Embedded-Software kopiert werden. Auch das Knowhow muss vor Reverse-Engineering geschützt werden, um die Analyse und den unerlaubten Einsatz von Verfahren und Prozessen zu verhindern. Mit geschützten Produktionsdaten wird gleichzeitig die unbemerkte Produktion von Graumarktprodukten in der Fabrik verhindert.

Beim Forschungsprojekt Pro-Protect geht es seit 2008 darum, eine einheitliche Lösung zum Schutz der unterschiedlichen Angriffspunkte von Produktpiraten zu schaffen. Neben WIBU-SYSTEMS sind das Forschungszentrum Informatik FZI und die Firmen GIS, HOMAG und ZSK Stickmaschinen als Konsortialpartner gemein-



Angriffspunkte der Produktpiraten am Beispiel von Stickmaschinen. Rechts unten: Neue Hardware der CodeMeter-Technologie schützt Industrie-PCs. Grafik und Foto: WIBU.

sam aktiv. Das Pro-Protect-Konsortium hat eine Schutzstrategie entwickelt, deren Basis die CodeMeter-Technologie von WIBU-SYSTEMS ist, die bisher zum Schutz klassischer PC-Software eingesetzt wurde. Pro-Protect erweiterte CodeMeter als Wegfahrsperrre für Maschinen und Anlagen, wobei die besonderen Spezifikationen der Industrie und die verschiedenen Angriffstaktiken berücksichtigt wurden.

**Schutz der PC-Software** – Eine Stickmaschine benötigt Software und Produktionsdaten. Beides muss zusammen mit digitalen Rechten vieler Unternehmen in einem System funktionieren, und zwar geschützt und eindeutig zugeordnet.

**Schutz der Daten** – Beliebige Dateiformate werden verschlüsselt, sodass diese nur entschlüsselt werden, wenn die passenden

Rechte vorhanden sind. **Schutz der Embedded-Software** – Um die industriellen Standards zu erfüllen und das Schutzkonzept nachträglich auf bestehende Embedded-Systeme einzusetzen, entwickelte WIBU-SYSTEMS spezielle Schutzhardware, das heißt Karten für die MikroSD-, SD- und CompactFlash-Schnittstelle, die die in der Industrie gebräuchlichen Schnittstellen unterstützen und unter harten Umgebungsbedingungen laufen. Vorteilhaft ist der Flash-Speicher auf jeder Karte, um darauf Programme und Produktionsdaten zu speichern. Damit diese Karten auch mit

Betriebssystemen wie Windows Embedded, Windows CE oder OSADL Real-Time Linux funktionieren, wurden sowohl die notwendige Laufzeitsoftware als auch die Tools entwickelt, die die Embedded-Software auf hohem Level schützen.

Der Prozessor im Embedded-System oder im IPC muss den Code lesen, verstehen und ihn ausführen. Keinesfalls liegen der gesamte Code und die Ressourcen zu irgendeinem Zeitpunkt unverschlüsselt im Arbeitsspeicher. Gleichfalls ist die Codeanalyse durch Obfuskation erschwert und Anti-Debugging- und Crack-Detection-Techniken greifen, sobald ein Angriff durch Produktpiraten erkannt wird. Dann wird die Lizenz gesperrt und der Angreifer kann nicht beliebig oft versuchen, den Schutz auszuhebeln. Dabei dürfen die Betriebssicherheit, die Integrität, das Echtzeitverhalten und die gesamte Zuverlässigkeit nicht leiden. Die Produktionsdaten werden so geschützt, dass im Schutzsystem der Maschine die Stickanzahl mitgezählt wird. Ähnlich wie beim Software-schutz wird die digitale Maschinenakte – Servicedokumente, Zeichnungen, Teilleisten oder auch die Dokumentation von Serviceeinsätzen – geschützt und die verschiedenen Serviceeinsätze durch eine elektronische Signatur manipulationssicher dokumentiert. CodeMeter passt die aufgezeigten Schutzstrategien am Beispiel der Stickmaschinen flexibel für andere Branchen an. Um weiterhin den hohen Schutzgrad zu gewährleisten und zusätzliche Funktionen zu realisieren, wird CodeMeter demnächst mit weiteren in Embedded-Systemen verbreiteten Betriebssystemen, beispielsweise VxWorks oder SoftSPS, funktionieren.



**Autor:**  
Dipl.-Ing.  
Oliver Winzenried  
Vorstand  
WIBU-SYSTEMS AG  
76137 Karlsruhe  
Kontakt:  
www.wibu.de,  
www.codemeter.de