it-production.com
Das Online-Magazin für erfolgreiche Produktion

Hard- und Software schützen mit Dongles

Bereits 1991 erkannte Copa-Data die Notwendigkeit, die eigenen Software-Produkte schützen zu müssen, ohne die Offenheit und Flexibilität der Lösungen mehr als nötig einzuschränken. Zu den Anforderungen an eine Lösung zählten die Kompatibilität mit Windows und der problemlose Einsatz für die Nutzer. Anwender sollten im Falle eines Rechnertauschs den Schlüssel auf neue oder modifizierte Geräte übertragen können. Außerdem muss die Produktion auch bei Schwierigkeiten wie dem Ausfall der Netzwerkverbindung weiterlaufen. Erfüllen konnten diese Anforderungen Hardware-Dongles von Wibu-Systems.

Zum Schutz des Software-Portfolios kam bei Copa-Data ein Hardware-basierter Softwareschutz zum Einsatz. Ein Dongle kann bei Embedded-Geräten genutzt, mit neuen Rechnern oder neuen Systemen verbunden werden und bietet in der Regel eine lange Lebensdauer. Beide Technologien Wibukey und Codemeter kommen vom Hersteller Wibu-Systems, mit dem das Unternehmen schon seit Anfang 1990 zusammenarbeitet.

Was Hardware-Dongles leisten

Teil der Anforderung an die Schutz-Technologien war die langjährige Abwärtskompatibilität, vor allem was die Gültigkeit der Lizenzierung betrifft. Auch die Besonderheiten industrieller Umgebungen mussten berücksichtigt werden, etwa wenn keine Internetverbindungen existieren. Software-basierte Lösungen sind an einen Rechner und dessen Bestandteile gebunden. Des Weiteren benötigen Software-basierte Schlüssel oft eine Internetverbindung, was bei einem Dongle nicht der Fall ist. Alles in allem bedeutete der Einsatz eines Dongles einen sehr geringen Verwaltungsaufwand. Als Lösung wurden schließlich die Dongles Wibubox und Cmdongle angeschafft. Werden nun Rechner ausgetauscht, wird der Dongle als Schutzkomponente und Lizenzträger einfach umgesteckt.

Wie funktioniert ein Dongle?

Bei der Codemeter-Technologie ist das Herz eines Cmdongles ein nicht klonbarer Smartcard-Chip, der einen Mikroprozessor mit einem sicheren Speicherbereich für kryptographische Schlüssel und für die Firmware enthält. Erst wenn Anwender die verschlüsselte Software und den passenden Dongle aufstecken, werden die gerade benötigten Programmteile entschlüsselt und nutzbar. Fehlt der richtige Dongle, wird die geschützte Software nicht gestartet.

Verschlüsselt wird der Code symmetrisch über Advanced Encryption Standard (AES) mit 128-Bit-Schlüsseln, die asymmetrische Verschlüsselung Elliptic Curve Cryptography (ECC) erfolgt mit 224-Bit-Schlüsseln. Die Schutz-Lösung arbeitet nach dem Plug-and-play-Prinzip.

Service und Lieferung

Die Technologie lässt sich in verschiedenen Lizenzmodelle beziehen. Dazu gehören zum Beispiel Netzwerk-Dongles mit einer bestimmten Anzahl Lizenzen oder Lizenzen mit Ablaufdatum, etwa für Test-Lizenzen.

(Quelle:Wibu Systems AG/Bild:Wibu Systems AG / Copa Data)

Internet: www.wibu.com

Marburg, den 02.02.2016