



**GW-TEL<sup>®</sup> Secure APS schützt automatisierte Arbeitsplatz-Rechner, z.B. in der Messtechnik, im E2E-Monitoring oder für bedienerlose Präsentationen vor unberechtigtem Zugriff und Missbrauch bei Entwendung.**

## GW-TEL<sup>®</sup> Secure APS

Heute werden häufig Personal Computer autonom, d.h. ohne einen Anwender vor der Tastatur, z.B. zur Simulation von geschäftskritischen Business Cases im Service Level Management eingesetzt.

Diese Systeme unterliegen erhöhten Anforderungen unter Sicherheitsaspekten, insbesondere wenn Sie Daten oder Workflows verarbeiten, die aus echten Anwendungsumgebungen stammen.

Konkretes Beispiel sind hier u.a. Messagenten (z.B. für Client-Simulation, Lasttests), die ohne Benutzerbedienung aktiv in vorhandene Produktionsumgebungen hinein messen und über entsprechend autorisierte Zugangsdaten verfügen.

Hier setzt GW-TEL<sup>®</sup> Secure APS ein, indem es diese Systeme durch ein mehrstufiges Sicherheitskonzept schützt.

Automatisierte Systeme führen in der Regel selbstständig den Windows-Bootprozess aus, melden sich anschließend per Auto-Login am System an und starten dann den entsprechenden selbstablaufenden Prozess.

Bereits in der Bootphase greift nunmehr GW-TEL<sup>®</sup> Secure APS ein und installiert entsprechende Systemtreiber, die den externen Zugriff auf Tastatur und Maus unterbinden.

In einem zweiten Schritt werden entsprechende Treiber zur Bildschirm-Verdunkelung installiert, die ein Mitlesen der Prozessabläufe auf einem evtl. extern angeschlossenen Monitor verhindern. Wesentliches Merkmal hierbei ist, dass diese Bildschirmverdunkelung über die Hardware des Grafik-Controllers gesteuert wird, so dass im Gegensatz zu „normalen“ Bildschirmschonern, Applikationen weiterhin z.B. durch ein Anwendungsscript bedient und gesteuert werden kann.

Um die Anwendungen selbst, aber auch die Zugangs-Accounts und die systeminternen Informationen auch bei einem evtl. Diebstahl vor Missbrauch zu schützen (z.B. durch den Ausbau der Festplatte und Einbau in ein anderes System), wird als dritte Maßnahme ein Teil der Festplatte oder die gesamte Festplatte verschlüsselt. Dies erfolgt mit entsprechend starker Kryptographie bei laufendem Betrieb. Die Performance des Arbeitsplatzsystems wird hierdurch nicht beeinflusst.

Zur Konfiguration des Systems kann eine entsprechende Remote-Konsole verwendet werden, so dass auch eine zentrale Steuerung, z.B. bei verteilten Mess-Systemen weiterhin möglich ist.



### **Leistungsmerkmale:**

- Mehrstufiges Sicherheitskonzept für automatisierte Arbeitsplatz-Systeme
- Abschaltung der Tastatur- und Mausunterstützung beim Bootvorgang
- Deaktivierung der Bildschirmausgabe auf einen direkt angeschlossenen Monitor. Durch die Virtualisierung des Bildschirm ist es weiterhin möglich, Anwendungen über entsprechende Treiber zu bedienen (Scripting, programmgetrieben etc.)
- „On-the-fly“ Verschlüsselung- und Entschlüsselung bestimmter Festplatten-Partitionen oder der gesamten Festplatte
- Remote-Zugang via TCP/IP

### **Systemanforderung GW-TEL<sup>®</sup> Secure APS**

#### **Plattform:**

- Microsoft<sup>®</sup> Win32 Standard-Plattform

#### **Betriebssysteme:**

- Microsoft<sup>®</sup> Windows<sup>®</sup> 7
- Microsoft<sup>®</sup> Windows<sup>®</sup> XP SP3
- empfohlene Betriebssystemplattform Microsoft<sup>®</sup> Windows<sup>®</sup> XP SP3

#### **Prozessoren:**

- aktuelle Intel<sup>®</sup> oder AMD<sup>®</sup> Prozessoren

#### **Hauptspeicher:**

- empfohlen 2048 Mbyte oder mehr

#### **Festplattenspeicher:**

- 250 GByte Ultra ATA, ATA133, SATA oder SATA Revision 2

Sämtliche verwendeten Firmennamen, Produktnamen und Warenzeichen sind in der Regel Warenzeichen bzw. eingetragene Warenzeichen der entsprechenden Firmen. Copyright Geyer & Weinig EDV-Unternehmensberatung GmbH. Irrtum und Abbildungsfehler vorbehalten. Einschränkungen durch Weiterentwicklung vorbehalten.