



Sicherer Bankautomat: Verschlüsselung für Geldausgabeautomaten (ATM)

Die Begriffe für eine technische Einrichtung zum Bargeldhandling sind in Europa sehr unterschiedlich. Sie sind unter den Namen Bankomat, Bankautomat, Automated teller machine (ATM), Geldausgabeautomat (GAA) usw. bekannt und haben alle gemeinsam, dass sie in den letzten Jahren verstärkt gestohlen werden. Mit spektakulären und filmreifen Aktionen werden die GAAs aus ihren Verankerungen gerissen und mit gestohlenen Fahrzeugen abtransportiert. Bis dato waren die Diebe nur an dem Bargeld der integrierten Geldkassette interessiert. Doch wie sieht es mit dem Schutz der Kundendaten und installierter Software aus, die ein Geldautomat speichert? Hinter dem Gehäuse eines GAA verbirgt sich ein ganz normaler PC, der sehr häufig mit einem Windows Betriebssystem ausgestattet ist. Somit verbergen sich in temporären-Dateien, der Auslagerungsdatei und Protokolldateien Informationen, die geschützt - „verschlüsselt“ - werden müssen. Die ideale Lösung hierfür ist eine sektorbasierte Vollverschlüsselung (FDE) der gesamten Festplatte.

Da der Betrieb eines Geldausgabeautomaten i.d.R. völlig automatisiert und ohne Benutzer-Authentisierung geschieht, stellen sich besondere Anforderungen an die Verschlüsselung und das Key-Management um einen reibungslosen und wartungsarmen Betrieb zu gewährleisten. Aus Sicherheitsgründen darf die Verschlüsselung nicht ohne eine PreBoot-Authentisierung (PBA) erfolgen, da sonst das Schlüsselmaterial auf der Festplatte vorhanden sein müsste und ein Angriff auf die Festplatte möglich wäre.

Was aber tun, wenn eine PBA notwendig ist, aber kein Benutzer vorhanden ist der die Authentisierung übernimmt? Genau an dieser Stelle bietet die CryptWare IT Security eine maßgeschneiderte Lösung an. Mit seiner netzwerkfähigen PBA-Technologie ist das Produkt CryptoPro Secure Disk in der Lage das notwendige Schlüsselmaterial automatisch und ohne Benutzerinteraktion von einem sicheren Backend-Server der Bank zu laden und das Betriebssystem zu starten. Gleichzeitig wird ein „interner“ User mittels Single SignOn am Betriebssystem angemeldet. Zusätzlich können in die Authentisierungsphase hardware-spezifische Eigenschaften des GAA integriert werden, um sicherzustellen, dass eine gestohlene Festplatte in einem anderen Rechner nicht gebootet werden kann.

Unterstützte Plattform:

- Windows 7
(32 und 64 Bit)
- Windows Vista (32 und 64 Bit)
- Windows XP
(32 und 64 Bit, SP3)

CryptWare IT Security GmbH
Frankfurter Str. 2
65549 Limburg

Phone: +49 (0) 6431 977790 - 0
Fax: +49 (0) 6431 977790 - 22
info@cryptware.eu