Rahmen eines Feldversuchs der genossenschaftlichen FinanzGruppe damit aus.

Werden die nur 48 x 28 Millimeter großen G&D-Aufkleber als MasterCard-Kreditkarten eingesetzt, können Benutzer damit an über 350.000 kontaktlosen PayPass-Bezahlterminals in weltweit 37 Ländern bezahlen. Jede Transaktion wird dabei auf der Kreditkartenabrechung ausgewiesen. Bei Beträgen bis 25 Euro entfallen PIN-Eingabe oder Unterschrift, wodurch sich die Transaktionszeit gegenüber einer gewöhnlichen Kartenzahlung um etwa ein Viertel verkürzt, gegenüber Barzahlungen sogar um die Hälfte. Bei Beiträgen über 25 Euro bestimmt die ausgebende Bank, ob eine Authentisierung durch PIN oder Unterschrift erforderlich ist. In Deutschland können Bankkunden bereits an verschiedenen PayPass-Akzeptanzstellen bezahlen. Dazu gehören Aral, Vapiano, McDonalds, Thalia, Douglas sowie Edeka. MasterCard stellt auf seiner Webseite *http://www.mastercard.com/interactivelocator/paypass-de.html* über seinen PayPass Locator eine Übersicht der kontaktlosen Bezahlterminals in der eigenen Umgebung bereit.

Deutsche Post startet die Digitalisierung der Arbeitslosengeld I-Akten

Die Deutsche Post startet am 27.07.2012 planmäßig mit der Aktendigitalisierung für die Bundesagentur für Arbeit (BA). Unter dem Projektnamen „e-Akte" (elektronische Akte) wird der Logistikkonzern mehrere Millionen BA-Kundenakten und täglich rund 260.000 eingehende Dokumente in speziellen Verarbeitungszentren einscannen und für eine elektronische Weiterbearbeitung bereitstellen. Bis Ende 2012 soll die e-Akte bei der BA bundesweit eingeführt sein.

Die Deutsche Post besitzt langjährige Erfahrung bei der Abwicklung von datensensiblen Großprojekten: Die Digitalisierungszentren der Post unterliegen höchsten sicherheitstechnischen und datenschutzrechtlichen Anforderungen und sind vom Bundesamt für Sicherheit in der Informationstechnik (ISO 27001) und dem TÜV (ISO 9001) zertifiziert. Alle Mitarbeiter der Deutschen Post sind zudem auf die Geheimhaltung der Daten verpflichtet.

In der Vergangenheit hat die Deutsche Post bereits andere Scanprojekte für Behörden und Verwaltungen erfolgreich durchgeführt, beispielsweise die Altaktendigitalisierung für die Deutsche Rentenversicherung oder die Erfassung der Anträge auf Abwrackprämie für das Bundesamt für Wirtschaft und Ausfuhrkontrolle im Jahr 2009.

Die Bundesagentur für Arbeit hatte die e-Akte Mitte 2011 als Pilotprojekt in ihrer Regionaldirektion Sachsen-Anhalt/Thüringen mit rund 4.000 Mitarbeitern eingeführt. Da sich das Projekt aus Sicht der Bundesagentur sowohl in betrieblicher als auch datenschutzrechtlicher Hinsicht bewährt hat, soll das Verfahren nun bis Ende 2012 bundesweit ausgedehnt werden.

Dabei digitalisiert die Deutsche Post die Vorgänge zum Arbeitslosengeld I durch Hochleistungsscanner mit einem Durchsatz von bis zu 10.000 Seiten pro Stunde. Anschließend werden die Daten über die Dokumenten-Management-Lösung von IBM auf die Computer der Mitarbeiter der Bundesagentur übertragen. Die rund 40.000 Beschäftigten der Arbeitsagenturen können so schneller und standortunabhängig auf die Kundeninformationen zugreifen.

Die Bundesagentur für Arbeit, verspricht sich von der e-Akte eine effizientere Vorgangsbearbeitung, Kosten- und Papiereinsparungen und einen besseren Kundenservice.

Wave Sicherheitstechnologie für Lenovo-Computer

Am 25. Juli 2012 wurde die Unterzeichnung einer weltweiten Vertriebsvereinbarung zwischen Wave Systems Corp. (NASDAQ:WAVX) und Lenovo bekannt gegeben. Im Rahmen dieser Vereinbarung wird Lenovo die Sicherheitslösungen von Wave auf Resale-Basis und über seine Channel-Partner vertreiben.

Der zunehmende Fokus auf Trusted Computing veranlasst die Sicherheitsindustrie, verstärkt Hardware-basierte Sicherheitstechnologien einzusetzen, die eine bessere Zugriffskontrolle, Verschlüsselung sowie die frühzeitige Erkennung von Malware ermöglichen. Insbesondere selbstverschlüsselnde Laufwerke (SEDs) und Trusted Platform Module (TPM) bieten mehr Sicherheit für die Endnutzer und zuverlässigeren Schutz für ihre kritischen Daten. Mit den Lösungen von Wave können die Lenovo-Kunden Daten auf ihren Endgeräten absichern, Daten bei der Übertragung (Data-in-Motion) schützen und gewährleisten, dass nur vertrauenswürdige Geräte Zugriff auf das Unternehmensnetz erhalten.

„Mit der Vereinbarung erhalten die Lenovo-Kunden direkten Zugriff auf die Endpunkt-Sicherheitslösungen von Wave und können PCs und die robusten Sicherheits- und Managementlösungen von Wave jetzt aus einer Hand erwerben", so Wes Williams von Lenovo. „Diese Vereinbarung vereinfacht den Kaufprozess für unsere Kunden, die Wave-Lösungen nutzen, um SEDs und TPMs zu aktivieren und zu verwalten, erheblich. Mit diesen können sie permanente, eindeutige Identitäten schaffen und Advanced Persistent Threats frühzeitig erkennen."

Wave verwaltet derzeit mehr SEDs als jeder andere unabhängige Software-Hersteller der Welt. Mit dem erweiterten Portfolio von Wave, zu dem mittlerweile auch die Data Loss Prevention (DLP) Suite von Safend gehört, können Unternehmen:

- Daten schützen. Das Portfolio von Wave bietet den Kunden optimale Möglichkeiten, Daten bei der Übertragung zu schützen, Daten auf Endgeräten abzusichern und Full Disk Encryption im gesamten Unternehmen zu verwalten.
- Unautorisierte Nutzer, Geräte und Malware abwehren. Der Löwenanteil aller Unternehmensdaten ist auf Endgeräten im Netzwerk gespeichert. Safend Protector und Inspector können eine ungewollte Datenpreisgabe über physische Ports, Wireless-Schnittstellen oder Wechseldatenträger verhindern und Beschränkungen für Geräte nach Typ, Modell oder Seriennummer auferlegen. Außerdem können sie die Datenpreisgabe via E-Mail prüfen, klassifizieren und blockieren sowie die Übertragung von Dateien überwachen.
- Neue Bedrohungen erkennen. Mit ERAS können Unternehmen die Trusted Platform Module (TPM) in ihren PCs aktivieren und verwalten. So gewährleisten sie, dass nur vertrauenswürdige Geräte Zugriff auf die Netzwerke und Dienste erhalten. Wave Endpoint Monitor versetzt Unternehmen in die Lage, Advanced Persistent Threats zu erkennen, da beim Einschalten der Systeme unautorisierte Veränderungen in der Pre-Boot-Umgebung bemerkt werden.