

Innominate

mGuard

Die innovative Lösung für mehr Sicherheit bei Bankautomaten



Wenn's um Geld geht, dann sind Sicherheit und Fehlerfreiheit oberstes Gebot. Doch bei vielen Bankautomaten ist es reine Glücksache, dass es bisher zu keinen größeren Problemen mit den integrierten IT-Systemen gekommen ist. Das kann sich aber sehr schnell ändern.

Sicherheitsrisiko Rechnersystem

Bankautomaten sind immer in das Netzwerk des Unternehmens integriert. Zum einen, um den erforderlichen Datenaustausch für den Geldverkehr zu regeln und durch Fernabfrage ständig aktuelle Informationen, z. B. über den verfügbaren Geldbestand, zu erhalten, zum anderen, um die Systeme zu überwachen, damit beispielsweise bei Störungen schnell reagiert und der Automat wieder in Betrieb genommen werden kann. In allen Bankautomaten sind deshalb Rechner integriert.

Da Bankautomaten in der Regel zehn Jahre und länger ihre Aufgabe erfüllen, arbeiten zahlreiche dieser Geräte oft noch mit älteren Prozessortechnologien (z. B. Intel 386 oder 486) sowie älteren Betriebssystemversionen. Das hat durchaus Vorteile wie die Robustheit und die hohe Zuverlässigkeit der Systeme und nicht zuletzt die geringen Kosten. Aber auch Nachteile wie die mangelnde Unterstützung für Upgrades oder softwarebasierte Sicherheitslösungen.

Ältere Systeme sind extrem gefährdet

Etliche dieser Standard-PC-Systeme laufen unter Windows. Nun sind die Sicherheitslücken von Windows hinreichend bekannt. Zahlreiche Patches, die von Microsoft selbst für das neueste Betriebssystem Windows XP ständig ausgegeben werden, belegen die Sicherheitslücken und die hohen Risiken. Noch verschärfter stellt sich die Situation der Sicherheitsrisiken bei den in Bankautomaten weit verbreiteten älteren Windows-Betriebssystemen 95, 98 oder NT4 dar. Microsoft unterstützt diese Versionen nicht mehr und deshalb gibt es dafür keine Sicherheits-Updates.



Doch auch bei der in der Bankenwelt weit verbreiteten OS/2-Umgebung sowie bei Betriebssystemen anderer Hersteller sind die Probleme ähnlich, wenn diese in Bankautomaten integriert sind. Ältere Versionen werden oft nicht mehr unterstützt, Sicherheitslücken können nicht mehr durch Patches geschlossen werden. Einer Attacke durch Hacker und Angriffen durch Viren und anderen so genannten „Malicious Codes“ steht bei diesen älteren Systemen Tür und Tor offen.

Warum übliche Sicherheitstechnologien wenig nutzen

Nun gibt es verschiedene Sicherheitstechnologien, die auch für Bankautomaten genutzt werden könnten, aber fast alle haben in diesem Anwendungsbereich erhebliche Nachteile. Egal welche Sicherheitstechnologie eingesetzt wird, ob hardware- oder softwarebasiert: Beide haben den prinzipiellen Nachteil, dass die Implementierung und Konfiguration immer sehr aufwendig ist, weil das Rechnersystem verändert werden muss. Das kann nur durch einen Techniker vor Ort erfolgen und kostet Zeit und sehr viel Geld.

Hardwarebasierte Systeme (Router, Bridges) haben den Nachteil, dass sie immer an ihrer IP im Netz erkennbar und deshalb angreifbar sind. Vor allem, weil in aller Regel bei vielen Systemen sämtliche Standard Ports offen stehen, um den problemlosen Datentransfer zu ermöglichen.

Softwarebasierte Lösungen (Personal Firewall, Anti-Viren-Software) haben andere, zusätzliche Nachteile: Auf manchen proprietären Betriebssystemen sind sie gar nicht lauffähig. Auf Systemen mit älterer Prozessortechnologie können sie oft nicht eingesetzt werden, weil die erforderliche Performance fehlt. Die Abwehr einer Virus-Attacke würde die Prozessorleistung dermaßen beanspruchen, dass das ganze System lahm gelegt wird. Und: Software erfordert stets regelmäßige Updates, sonst können Virus-Attacken aufgrund der immer wieder aufgedeckten Sicherheitslücken ganz einfach zum Betriebssystem durchdringen. Doch Updates sind aufwendig und erfordern entsprechend teure Ressourcen.

Sichern Sie Ihre Bankautomaten einfach, zuverlässig und wirtschaftlich

Der mGuard ist eine überragende, innovative Sicherheitslösung, die als „device attached security“ bezeichnet wird. Alle bekannten Nachteile herkömmlicher Sicherheitstechnologien werden mit der mGuard Technologie auf einzigartig einfache, zuverlässige und wirtschaftliche Art gelöst. Denn die mGuard Komponenten sind einfach und schnell zu installieren, erfordern weder Veränderungen an der Rechnerkonfiguration noch regelmäßige Software-Updates und arbeiten unabhängig von Prozessortechnologie und Betriebssystem.

Höchster Sicherheitslevel, unabhängig vom Gateway

Automaten in Bankfilialen sind üblicherweise in das Filial-Netzwerk eingebunden und durch herkömmliche Gateway Appliances mit dem gleichen, einheitlichen Sicherheitsstandard wie die Büro-PCs geschützt. Ein exponiertes, unternehmenskritisches System wie der Bankautomat erfordert aber einen Sicherheitslevel, der weit höher liegt. Bei Bankautomaten in Innenstädten, Einkaufszentren, Bahnhöfen usw. ist es noch schwieriger, den erforderlichen Sicherheitslevel zu gewährleisten.

Mit der mGuard Technologie können Sie jetzt jedem Bankautomaten seine eigene Sicherheitskomponente zuweisen und mit dem Innominat Security Configuration Manager zentral verwalten: mit individuellem Sicherheitslevel, mit speziell konfigurierter Zugriffsberechtigung und mit zahlreichen weiteren einzigartigen Vorteilen.



Einfach integriert, ruck, zuck installiert

Der mGuard ist ein eigenständiges System, das direkt am Bankautomaten zuerst an das Netzkabel angeschlossen und dann mit dem Rechner verbunden oder bei Bedarf als PCI-Karte integriert wird. Die mGuard Produkte können im Prinzip von jedem Mitarbeiter installiert werden. Es muss nichts am Rechner konfiguriert werden, es müssen keine Treiber oder andere Software geladen werden, und es muss das Betriebssystem nie mehr durch Sicherheitspatches aktualisiert werden. Das spart Kosten bei der Implementierung, der Verwaltung und der Überwachung und es bringt Sicherheit auf Dauer. Es ist auch belanglos, mit welchem Betriebssystem oder mit welcher Rechnerplattform der Bankautomat arbeitet. Die mGuard Technologie ist zu allen Systemen kompatibel.

Grundlegende Funktionen des mGuard

Die „device attached security“-Lösung mGuard von Innominat vereint alle Funktionen, um IP-Verbindungen zuverlässig abzusichern:

- VPN für sichere Datenübertragung über öffentliche Netze (hardwarebasierte DES-, 3DES- und AES-Verschlüsselung, IPsec-Protokoll).
 - Konfigurierbare Firewall schützt vor unberechtigten Zugriffen von „außen“. Der Paketfilter untersucht Datenpakete anhand der Ursprungs- und Zieladresse und blockiert unerwünschten Datenverkehr auch von „innen“.
 - Integrierter optionaler Kaspersky-Virenschutz mit Unterstützung für die Protokolle HTTP, SMTP und POP3 (ausschließlich empfohlen für die Versionen enterprise und enterprise XL). Die Virenprüfung erfolgt bereits außerhalb des Rechners.
- Also: mehr Sicherheit für den Rechner, mehr verfügbare Leistung auf dem Rechner.



Unangreifbar durch den Innominate Stealth Mode

mGuard, das „device attached security“-System von Innominate, verfügt über den einzigartigen Innominate Stealth Mode. Das Device arbeitet absolut transparent und benötigt keine eigene IP-Adresse. Es benutzt dieselbe IP wie der zu schützende Rechner, ist also für einen Angreifer nicht erkennbar und deshalb nicht angreifbar. Durch die werksseitige Standardeinstellung des Stealth Mode muss am mGuard nichts konfiguriert oder geändert werden. Es ist jedoch möglich, jeden einzelnen mGuard auch im Stealth Mode an spezielle Sicherheitsanforderungen und die Security Policies im Unternehmen individuell anzupassen – etwa entsprechend der Netzwerkverbindung. Bei den in Zukunft zunehmenden kostensparenden X-DSL-Verbindungen können beispielsweise Zugriffe über die offenen Standard Ports gezielt eingeschränkt werden. Die Konfiguration, das Roll-out, die Verwaltung, aber auch die Wartung der mGuard Devices wird am besten und einfachsten durch den Innominate Security Configuration Manager unterstützt.

Maximaler Datendurchsatz für VPN und Firewall

Die Basis der integrierten Sicherheitslösung ist das von Innominate konfigurierte Embedded Linux, das auf einem speziellen Netzwerkprozessor mit XScale-Kern von Intel (IXP 42x) läuft: mit bis zu 533 MHz Prozessorleistung, bis zu 64 MByte SDRAM Arbeitsspeicher und 16 MByte Flash-Speicher. Im Intel Prozessor gibt es fest

verdrahtete Befehle für die Verschlüsselungsverfahren DES, 3DES und AES. Das garantiert den überragenden Durchsatz bei Firewall (bis zu 99 Mbit/s) und VPN (bis zu 70 Mbit/s). VPN-Verbindungen sind auch im Stealth Mode schnell und zuverlässig aufzubauen.

Auf einen Blick

- „device attached security“-System: unabhängig von Rechnerplattform und Betriebssystem.
- Einfachste Integration: keine Rechneranpassungen, keine Treiberinstallation, nie mehr Updates.
- Rückwirkungsfreie Netzwerkintegration durch transparenten Innominate Stealth Mode.
- Hoher Datendurchsatz durch hardwarebasierte Verschlüsselung für High Speed VPN/Firewall.
- Leistungsfähige Anti-Virus-Lösung basierend auf Kaspersky-Technologie (optional).
- Volle Interoperabilität mit anderen Standard-Security-Lösungen (IPsec) innerhalb des LAN/WAN.
- Integrierbar in zentrale Management-Umgebungen (SNMP).
- Komfortable, unternehmensweite Konfiguration aller Security Devices per drag and drop mit dem Innominate Security Configuration Manager (optional).

Einfach integrieren, bequem administrieren

Maßgeblich unterstützt wird die plattformübergreifende Sicherheit der mGuard Devices durch den Innominate Security Configuration Manager (ISCM), der auf der bewährten Technologie des Solsoft Policy Servers aufsetzt. ISCM ist eine gruppenbasierte Plattform. Anhand eines grafischen Netzwerkmodells werden die Sicherheitseinstellungen für mehrere mGuard Systeme gleichzeitig schnell und komfortabel konfiguriert. Es werden die gesetzten Regeln automatisch überprüft und die Vollständigkeit und Korrektheit bestätigt. Es werden die generierten Firewall-Regeln, VPN-Konfigurationen und NAT-Einstellungen direkt auf alle Devices einer Gruppe geladen und sofort aktiviert. Darüber hinaus werden VPN-Verbindungen zwischen mGuard Devices untereinander und mit Gateways anderer Hersteller eingerichtet und verwaltet. Alles komfortabel über die grafische Oberfläche. Alles einfach per Mausclick.

Was durch die Konfiguration einzelner Systeme bisher komplex, zeitraubend und fehleranfällig war, wird mit der Gruppenverwaltung des Innominate Security Configuration Managers plötzlich ganz einfach, in kurzer Zeit und fehlerlos konfiguriert. Der Aufwand und die Kosten werden deutlich reduziert.