

Innominate

mGuard

Die innovative Sicherheitslösung für alle Automatenysteme



Bargeldlos bezahlen ist sehr beliebt. Doch neben EC- und Kreditkartenterminals gibt es viele weitere Systeme, über die Zahlungsverkehr abgewickelt wird: die Computerkasse im Supermarkt, das Lotto- und Toto-Terminal im Schreibwarengeschäft, der Fahrkartensystem im Betriebsrestaurant. Dazu kommen immer mehr andere „Automaten“, die vernetzt sind: Spielautomaten, Zigarettenautomaten, Getränkeautomaten, Info-Terminals (so genannte Kiosksysteme), die neuen Paketautomaten der Post u. v. m.

Welche Vorteile bringt die Vernetzung?

Die Kunden bekommen einen besseren und schnelleren Service und mehr Komfort. Die Unternehmen gewinnen an Flexibilität, steigern die Planungssicherheit und sparen Kosten. Kreditkartenunternehmen können Zahlungen sofort bestätigen. Supermarktketten wissen jederzeit über ihren Warenfluss Bescheid und können Nachbestellungen und Lagerhaltung vollautomatisch steuern. Lotterieverwaltungen nehmen Spielscheine jetzt bis Samstagmittag an, weil die Scheine bereits in der Annahmestelle erfasst und per Internetleitung in die Lottozentrale übermittelt werden. Fahrkartensystemen können ähnlich wie Verkaufsautomaten fernüberwacht werden. Der Aufwand ständiger Überprüfungen vor Ort entfällt. Nur wenn wirklich nachgefüllt oder Störungen beseitigt werden müssen, wird gezielt ein Mitarbeiter eingesetzt. Zudem kann an immer mehr dieser Automaten mit EC-Karte bezahlt werden. Geldkartensysteme, beispielsweise in Betriebsrestaurants, ermöglichen bargeldloses Bezahlen im Vorbeigehen, Warteschlangen an der Kasse werden vermieden. Entertainment-Systeme schließlich können unabhängig vom Bargeldbestand deutlich höhere Gewinnsummen anbieten. Auch können mehrere Automaten an unterschiedlichen Orten einzeln oder im Team gegeneinander antreten. Das garantiert mehr Unterhaltung und Attraktivität für die Spieler, mehr Profit für den Betreiber.



Der Nachteil: hohe Sicherheitsrisiken

Alle diese vernetzten Automatenysteme haben zwei Dinge gemeinsam: einen integrierten Computer samt Betriebssystem und Anwendungssoftware sowie eine Netzwerk-Verbindung – in der Regel über das Internet. Und sie haben das gleiche Problem: Sie sind selten ausreichend gesichert, deshalb angreifbar und jeder einzelne ist eine gefährliche Sicherheitslücke im zentralen Firmennetzwerk. Ein zusätzlicher Aspekt: Häufig ist der Zugriff auf die Daten der Systeme im Prinzip für jeden Mitarbeiter möglich. Um unternehmensinterne Informationen zu schützen, sollten die Zugriffsrechte eingeschränkt sein.

Nicht nur ältere Systeme sind extrem gefährdet

Etlliche Computer in Automatenystemen arbeiten mit älteren Prozesstechnologien (z. B. Intel 386 oder 486) und deshalb mit älteren Betriebssystemversionen. Das hat durchaus Vorteile: kompakte, lüfterlose Rechnerbauweise mit hoher Robustheit und Zuverlässigkeit der Systeme bei gleichzeitig geringen Kosten. Aber auch Nachteile wie die mangelnde Performance und fehlende Unterstützung für Upgrades oder softwarebasierte Sicherheitslösungen.

Selbst Standard-PCs, die unter Windows laufen, haben ihre Probleme. Die Sicherheitslücken bei Microsoft – auch bei Windows XP – sind hinreichend bekannt. Noch verschärfter sind die Sicherheitsrisiken bei den älteren Windows-Betriebssystemen, da Microsoft diese Versionen nicht mehr mit Sicherheitsupdates unterstützt.

Bei PCs mit Betriebssystemen anderer Hersteller sind die Probleme ähnlich. Ältere Versionen werden oft nicht mehr unterstützt und Sicherheitslücken können nicht mehr durch Patches geschlossen werden.

Warum übliche Sicherheitstechnologien wenig nutzen

Es gibt verschiedene Sicherheitstechnologien, die auch für Automatenysteme 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 Implementierung und Konfiguration immer sehr aufwendig sind, 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 per Internetleitung 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 Prozesstechnologie können sie oft nicht eingesetzt werden, weil die erforderliche Performance fehlt. Die Abwehr einer Virus-Attacke würde die Prozessorleistung derart beanspruchen, dass das ganze System lahm gelegt würde. 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.

Die mGuard Technologie sichert alle Automaten-systeme: einfach, zuverlässig, wirtschaftlich

Die Nachteile anderer Sicherheitstechnologien werden mit der mGuard Technologie auf einzigartig einfache, zuverlässige und wirtschaftliche Art gelöst. Denn die mGuard Komponente ist einfach und schnell zu installieren, erfordert weder Veränderungen an der Rechnerkonfiguration noch irgendwelche Software-Updates auf dem Rechner und sie arbeitet unabhängig von Prozessortechnologie und Betriebssystem.

Höchster Sicherheitslevel, unabhängig vom Gateway

Mit dem mGuard System können Sie jetzt jedes computerbasierte Automaten-system – vom Bankautomaten bis zum Spielautomaten – als Gefahrenquelle für das Netzwerk hundertprozentig ausschließen. Denn mit den mGuard Devices weisen Sie jedem System bereits vor Ort seine eigene Sicherheitskomponente zu: mit individuellem Sicherheitslevel, mit speziell konfigurierter Zugriffsberechtigung, mit zahlreichen weiteren einzigartigen Vorteilen. Größere Installationen, wie sie beispielsweise bei zahlreichen Kreditkarten-Terminals, Fahrkartenautomaten oder Entertainment-Systemen erforderlich sind, können mit dem Innominate Security Configuration Manager einfach und zentral konfiguriert und verwaltet werden.



Einfach integriert, ruck, zuck installiert

Die mGuard Produkte sind eigenständige Systeme, die direkt am jeweiligen Automaten vor das Netzwerkkabel gesetzt oder bei Bedarf als PCI-Karte integriert werden. Es muss nichts konfiguriert werden, es müssen keine Treiber oder andere Software installiert werden, und es muss das Betriebssystem nie mehr durch Sicherheitspatches aktualisiert werden. Durch den Innominate Stealth Mode muss nicht einmal das Netzwerk geändert werden. Es ist auch unerheblich, mit welchem Betriebssystem oder mit welcher Rechnerplattform der Automat arbeitet. Die mGuard Technologie ist zu allen Systemen kompatibel und kann von jedem Systembetreiber einfach und schnell installiert werden.

Für Hersteller, die spezielle Lösungen entwickeln, gibt es den mGuard Core, eine Platine, die individuell an besondere Anforderungen angepasst und direkt in das Automaten-system integriert werden kann.

Grundlegende Funktionen

Die „device attached security“-Lösung mGuard von Innominate 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 Kaspersky-Virenschutz (optional) 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

Das „device attached security“-System mGuard 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, jedes einzelne mGuard Device auch im Stealth Mode an spezielle Sicherheitsanforderungen 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.

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

Konfiguration, Roll-out und Verwaltung der mGuard Devices werden zentral durch den Innominate Security Configuration Manager unterstützt. Er setzt auf der bewährten regelbasierten Technologie des Solsoft Policy Servers auf. Anhand eines grafischen Netzwerkmodells werden die Sicherheitseinstellungen für mehrere mGuard Systeme gleichzeitig schnell und komfortabel konfiguriert. Die gesetzten Regeln werden automatisch überprüft. 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 verwaltet. Alles einfach per Mausklick.

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 deutlich kürzerer Zeit und fehlerlos konfiguriert. Aufwand und Kosten werden entscheidend reduziert.