

**Innominate**

# mGuard

## Die innovative Lösung für mehr Sicherheit im Industrieumfeld

Seit Fertigungsumgebung und Office-Umgebung immer stärker vernetzt werden müssen, um den gesamten Betriebsablauf im Unternehmen effizienter zu gestalten, sind Produktionsleiter und IT-Verantwortliche gleichermaßen in der Pflicht, die Sicherheit und Verfügbarkeit ihrer Anlagen zu gewährleisten. Industrierechner, die z. B. Fertigungsroboter steuern, vor Viren, Würmern und anderen Attacken aus dem Netzwerk zu schützen, ist deshalb ein hochbrisantes Thema.



Dabei wird häufig übersehen, dass die Gefahren von außen genauso groß sind, wie die von innen. Schon des Öfteren wurden bei der Wartung von Industrierobotern die Steuerrechner über die Notebooks der Servicetechniker unbemerkt mit einem „Malicious Code“ infiziert. Die Schäden, die dadurch entstehen können, sind immens.

### "Never touch a running system" –

verändere nie ein funktionierendes System. In kaum einem anderen Bereich wird diese alte IT-Weisheit so konsequent befolgt wie im Fertigungsumfeld der Industrie. Denn jedes Update, Upgrade oder Patch beeinflusst die Funktion eines Rechners und kann zu bösen Überraschungen führen. Deshalb müssen in der Regel umfassende Testreihen in Versuchsumgebungen erfolgen, bevor die Software in Robotern, Steuerrechnern oder gar Leitrechnern verändert werden kann. Ein aufwendiger, langwieriger und daher teurer Prozess, der deshalb weitestgehend vermieden wird. Bei zunehmender unternehmensweiter Vernetzung entstehen daraus aber sehr ernsthafte Sicherheitsprobleme.

Eine zusätzliche Problematik ergibt sich bei so genannten validierten Systemen, bei denen nur unter Beachtung strenger Auflagen Veränderungen an Hardware und Software vorgenommen werden können. In der pharmazeutischen Industrie sind solche Systeme beispielsweise sehr häufig anzutreffen. Hier ist es nahezu unmöglich, Sicherheitslücken durch Software- oder Hardware-Aktualisierungen zu schließen. Diese Systeme trotzdem zuverlässig und vor allem wirtschaftlich zu schützen, ist eine enorme Herausforderung.



### **Proprietär oder Standard:**

#### **Die Sicherheitsproblematik ist brisant**

Viele, besonders ältere Industrierechner arbeiten mit proprietären Betriebs- und Bussystemen. Sie werden als sicher eingestuft, weil man glaubt, dass es für Hacker uninteressant ist, für diese wenigen Systeme „Malicious Codes“ in die Welt zu setzen. Man kennt also die Sicherheitslücken oft gar nicht und hat sich kaum Gedanken über die Abwehr von Attacken gemacht. Niemand weiß, ob und wie die spezialisierten Betriebssysteme auf die in Massen vorhandenen Viren, Würmer und Trojaner reagieren. Deshalb sind gerade diese Systeme durch die zunehmende Vernetzung stark gefährdet.

Es gibt auch noch zahlreiche Industriesysteme mit älteren Prozessortechnologien (z. B. Intel 386 oder 486) oder Betriebssystemversionen. Das hat durchaus Vorteile wie die lüfterlose, kompakte Bauweise, die Robustheit und die hohe Zuverlässigkeit der Systeme. Die ältere Prozessortechnologie hat aber auch Nachteile wie die mangelnde Unterstützung für Upgrades oder softwarebasierte Sicherheitslösungen.

Neuere Fertigungsautomaten arbeiten zwar immer häufiger mit Standards wie Windows, Ethernet, TCP/IP und HTTP. Aber gerade dadurch sind diese Systeme zunehmend Sicherheitsrisiken aus dem Netzwerk ausgesetzt. Die Sicherheitslücken von Windows sind hinreichend bekannt. Die zahlreichen Patches von Microsoft, selbst für das neueste Betriebssystem Windows XP, belegen die Sicherheitslücken und hohen Risiken. Zudem gilt immer noch: „Never touch a running system“ und vermeintliche Vorteile durch Standards werden zu erheblichen Nachteilen, weil das Aufspielen der Patches im Industrieumfeld mit besonders hohem Aufwand verbunden ist. Die älteren Betriebssysteme wie Windows 95, Windows 98 oder Windows NT4 werden von Microsoft gar nicht mehr unterstützt.

### **Warum übliche Sicherheitstechnologien wenig nutzen**

Nun gibt es verschiedene Sicherheitstechnologien, die auch für Industrierechner genutzt werden könnten. Aber fast alle – egal ob hardware- oder softwarebasiert – haben den gleichen Nachteil: Bereits bei der Implementierung sind immer Veränderungen am System erforderlich. Und gerade das soll im Industrieumfeld vermieden werden.

Hardwarebasierte Systeme (Router, Bridges) haben den Nachteil, dass sie immer an ihrer IP im Netz erkennbar und deshalb angreifbar sind. Vor allem, weil bei vielen Systemen auch noch sämtliche Standard Ports offen stehen.

Softwarebasierte Lösungen (Personal Firewall, Anti-Viren-Software) haben andere, zusätzliche Nachteile: Auf manchen proprietären Betriebssystemen sind sie gar nicht lauffähig, weil die Kompatibilität fehlt. 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: Sicherheitssoftware erfordert immer regelmäßige Updates. Doch das bedeutet wieder Veränderungen mit hohem Aufwand und hohen Kosten.

## Die Innominate mGuard Technologie sichert Industrierechner ohne Eingriffe ins System

Die Nachteile anderer Sicherheitstechnologien, die Veränderungen am Industrierechner erfordern, werden mit den mGuard Produkten von Innominate auf einzigartig einfache, zuverlässige und wirtschaftliche Art gelöst. Denn die mGuard Komponenten sind immer kompatibel. Sie erfordern weder Veränderungen an der Rechnerkonfiguration noch irgendwelche Software-Updates auf dem Rechner und arbeiten unabhängig von Prozessortechnologie und Betriebssystem.



## Höchster Sicherheitslevel, unabhängig vom Netzwerk

Doch egal, mit welchen Komponenten ein Netzwerk vor Angriffen von außen geschützt wird, es bleiben immer noch genügend Gefahrenpotenziale innerhalb eines Unternehmens. Angefangen von unwissentlich eingeschleusten Viren bis hin zu vorsätzlichen Spionage- und Sabotageversuchen. Ist ein durch Viren verursachter Ausfall eines Mailservers in der Regel ziemlich fatal, ist der Angriff z. B. auf einen Leitrechner katastrophal, weil dadurch die Bandbreite in Richtung der darunterliegenden Steuerrechner und Produktionsroboter derart gedrosselt werden kann, dass die gesamte Produktion lahm gelegt wird.

Mit der mGuard Technologie können Sie jetzt jedem Industriesystem, ob Leitrechner, Steuerrechner oder Produktionsroboter, seine eigene Sicherheitskomponente zuweisen: mit individuellem Sicherheitslevel, mit speziell konfigurierter Zugriffsberechtigung, mit zahlreichen weiteren einzigartigen Vorteilen und einfach und zentral verwaltet mit dem Innominate Security Configuration Manager.

## Einfach integriert, ruck, zuck installiert

Die mGuard Plattform ist ein eigenständiges System, das direkt am Industrierechner zuerst an das Netzkabel angeschlossen und dann mit dem Rechner verbunden oder bei Bedarf als PCI-Karte integriert wird. Für Industrierechner, die in 19-Zoll-Racksystemen zusammengefasst sind, bietet Innominate das mGuard bladePack mit redundanter Stromversorgung. Damit können bis zu zwölf Rechner einzeln oder bis zu sechs Rechner im Hot-Standby-Modus gesichert werden. Darüber hinaus gibt es den mGuard industrial, der speziell für den Einsatz im industriellen Umfeld auf Hutschienen-Basis konzipiert ist. Die Implementierung beider Systeme ist genauso schnell und einfach, die Funktionen und Leistungen sind absolut identisch.

Egal, welches mGuard System zum Einsatz kommt: Am Rechnersystem muss absolut nichts konfiguriert werden, es müssen keine Treiber oder andere Software geladen werden und es muss das Betriebssystem nie mehr durch Sicherheitspatches aktualisiert werden. Das spart Zeit und Kosten und bringt Sicherheit auf Dauer.

## Grundlegende Funktionen

Die „device attached security“-Lösung mGuard von Innominate vereint alle Funktionen, um IP-Verbindungen, z. B. für die Remote-Wartung des Systems zuverlässig abzusichern:

- VPN für sichere Datenübertragung über öffentliche Netze (hardware-basierte DES-, 3DES- und AES-Verschlüsselung, IPsec-Protokoll).
- Konfigurierbare Firewall schützt vor unberechtigten Zugriffen. Der Paketfilter untersucht Datenpakete anhand der Ursprungs- und Zieladresse und blockiert als unerwünscht definierten Datenverkehr.
- 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 außerhalb des Rechners. Also: kein Eingriff in den Rechner und trotzdem Sicherheit für den Rechner und 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 erkennt und benutzt dieselbe IP wie der zu schützende Rechner, ist also für einen Angreifer nicht erkennbar und deshalb nicht angreifbar. Ein weiterer Vorteil: Die Implementierung des mGuard erfolgt durch die automatische Erkennung der Rechner-IP in Sekunden. Gerade im Industrieumfeld, wo die Produktion nicht eine Minute stillstehen darf, ein entscheidendes Argument.

### 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 Netzwerkimtegration 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 und 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 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.