



CORISECIO - Mobile Firewall

Mobile Suite - more than just Device Management

Die Mobile Firewall bietet Funktionen für den Schutz der gesetzten Einstellungen sowie zur Blockierung und Überwachung risikoreicher Schnittstellen. Benutzerrechte zur Veränderung von Einstellungen, Regeln zur Verwendung von Bluetooth- und WLAN-Adaptoren, IrDa- Schnittstellen und Digital-Kameras können bis auf Treiberebene umgesetzt werden. Geschützte Einstellungen für Internetverbindungen, Access Points, VPN-Tunnel und Proxy Server schützen die Infrastruktur ebenso wie die mobilen Geräte und unternehmenskritische Daten.

BENUTZERRECHTE

Das Fehlen von Benutzerrechten auf Windows Mobile basierten Geräten macht jeden Benutzer zum Administrator. Die Folge sind ungewollte Veränderungen der Konfiguration und damit ein steigendes Helpdesk-Aufkommen sowie Probleme und Risiken durch die Nutzung unerwünschter Applikationen. Die Mobile Firewall bietet die Möglichkeit, Benutzerrechte zur Veränderung von Einstellungen zu definieren. Netzwerkmanagement, Internet und Corporate Networks werden dabei unterstützt. Rechte zum Anlegen, Editieren und Manipulieren für Modems, Proxy Server, VPN-Verbindungen, E-Mail Konten, etc. müssen explizit vom Administrator erlaubt werden.

SICHERE VERBINDUNGEN

Durch ein Rechtekonzept kann zudem ein gesicherter Verbindungsaufbau automatisiert werden. Durch die Remote-Konfiguration kann bspw. die Nutzung firmeneigener Proxy Server und Internet-Access Points umgesetzt werden. Häufige Anwendungsfälle - wie ein verpflichtendes VPN für alle IP-Verbindungen - sind einfach umzusetzen.

CONNECTIVITY

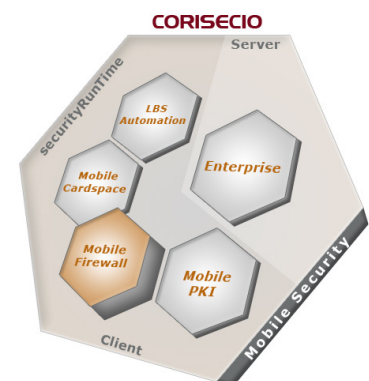
Den Risiken der Always-On-Geräte begegnet CORISECIO mit Firewall Funktionalität für drahtlose Schnittstellen. Für die Nutzung von WLAN-, Bluetooth- und Infrarot-Adaptoren bedarf es der expliziten Erlaubnis durch die Firewall Einstellungen. Im Negativfall werden diese Schnittstellen für den Benutzer zuverlässig gesperrt. Mit dieser Technologie können zudem dedizierte Regeln zur Nutzung der Geräte erstellt werden. Rechte zur vorgeschriebenen Nutzung definierter (firmeneigener) Access Points können ebenso erstellt werden, wie die Einschränkung der Bluetooth Nutzung auf bestimmte Gerätetypen (z.B. Headsets).

FACTS

- Durchsetzung der Security Policy
- Schließen von Sicherheitslücken
- Kontrolle von Applikationen
- Kontrolle von Features, Schnittstellen & USB Synchroniation
- Reduzierung von Fehlbedienungen
- Sichere Verwendung von Over-the-Air Technologien

BENEFITS

- Erhöhte Sicherheit
- Effiziente PDA Nutzung
- Deutlich verringerte Helpdesk-Kosten
- Höhere Verfügbarkeit
- Verbesserte Usability
- Plattformunabhängigkeit



USB ACTIVE SYNC

Neben den drahtlosen Schnittstellen kontrolliert Mobile Firewall auch Verbindungen zu Desktop PC via USB Active Sync. IT-Administratoren bestimmen, welche mobilen Geräte mit welchen Desktop PCs Daten (z.B. E-Mails, Kontakte) austauschen, aktualisieren oder kopieren dürfen. Die Berechtigungsvergabe ist flexibel, dass auch unternehmensintern Rechte auf Corporate-, Standort-, Abteilungs- oder Mitarbeitererebene vergeben werden können.

In Verbindung mit der optionalen Desktop Komponente werden firmeneigene PC, Notebooks und Netbooks vor unerwünschter Synchronisierung geschützt und der Datenaustausch ausschließlich mit unternehmenseigenen Geräte erlaubt. Bei der Initiierung einer ActiveSync Verbindung prüft CORISECIO die Berechtigung und baut nur im Erfolgsfall eine Datenverbindung auf. Ungewünschte Verbindungen, wie bspw. die unberechtigte Verwendung privater Pocket PCs mit unternehmenseigenen Notebooks oder die Synchronisation von Firmen Smartphones mit dem heimischen Desktop PC werden zuverlässig gesperrt.

MOBILE APPLIKATIONEN UND FEATURES

Mobile Geräte sind mit einer Vielzahl an Applikationen und Features ausgestattet. Da nicht jede Applikation im Unternehmenseinsatz erlaubt ist, unterbindet Mobile Firewall die Nutzung unerwünschter Applikationen. Über Positiv- oder Negativlisten definieren die Administratoren, welche Programme ausgeführt und welche Features genutzt werden dürfen. Auf diese Weise lassen sich Programmaufrufe, Netzwerkzugriffe sowie die Nutzung eingebauter Digital-Kameras oder SD-Karten einfach reglementieren. Neben Standardapplikationen unterstützt CORISECIO auch Eigenentwicklungen und 3rd Party Software. Der grafische Window-Scanner bietet Administratoren ein einfaches generisches Werkzeug zur Definition von Firewall Regeln für mobile Anwendungen. Zur Verbesserung der Usability für den Endanwender können nicht benötigte und gesperrte Applikationen und Settings einfach ausgeblendet werden.

SECURITYRUNTIME KONFIGURIERT – MOBILE FIREWALL SICHERT AB

Die Mobile Firewall ist eine leistungsstarke Ergänzung der securityRunTime. In Kombination können die Geräte automatisch konfiguriert und die getätigten Einstellungen wirkungsvoll gegen Veränderung geschützt werden. IT-Verantwortliche erhalten damit eine leistungsstarke Lösung, die die Sicherheit erhöht, Kosten senkt sowie Stabilität, Benutzerkomfort und die Produktivität deutlich steigert.

KEY FEATURES

- Geschützte Netzwerkeinstellungen
- Geschützte E-Mail Konten
- Geschützte Exchange Konfiguration
- Kontrolle der WLAN Schnittstelle
 - Deaktivieren des WLAN Adapters
 - Definierte Access Points (SSID-Positivliste)
 - Definierte Authentisierung/ Verschlüsselung
- Kontrolle der Bluetooth Schnittstelle
 - Deaktivieren des Bluetooth Adapters
 - Deaktivieren der Scan Option
 - nur definierte Profile (z.B. Headset)
 - nur definierte Geräte (optional)
- Kontrolle der IrDA Schnittstelle
 - Eingehende Verbindungen sperren
- Applikationssperre
 - Windows Mobile Standard Applikationen
 - Beliebige Applikationen
- Konfiguration des Startmenüs und Einstellungen
 - über Black & Whitelists
 - Konfiguration der TOP-Programme
- Featuresperre
 - Deaktivieren der Digital Kamera
 - Sperren des SD-Karten Zugriffs
- Kontrolle der Synchronisationsvorgänge
- Registry Überwachung
- Vorgeschriebenes Backup

