



Optimaler Schutz für dynamische Unternehmens-Netzwerke

Kaspersky Open Space Security schützt Firmen-Netzwerke jeder Größe inklusive externer Mitarbeiter und mobiler User zuverlässig – und wächst mit allen zukünftigen Anforderungen an die Unternehmens-IT.

Ihre Vorteile:

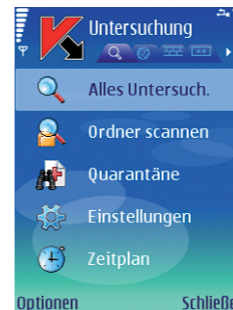
- Optimaler Schutz vor Viren, Spyware und Hackern auf allen Netzwerk-Ebenen
- Proaktiver Schutz der Workstations vor bisher unbekanntem Viren
- Echtzeit-Scan von Mails und Internet-Traffic
- Automatische Isolierung infizierter Rechner
- Zentrale Administration mit umfangreichem Berichts-System

Überzeugen Sie sich von der optimalen Skalierbarkeit und dem flexiblen Lizenzmodell unserer Produkte.



Kaspersky Open Space Security hat als erste Antiviren-Software weltweit das Zertifikat „Citrix Ready“ erhalten.

KASPERSKY Lab



Sicher unterwegs

Kaspersky Mobile Security Enterprise Edition 7.0 – Neben Notebooks brauchen auch Smartphones einen wirksamen Schutz gegen Viren, Spam und Diebstahl.

Moderne Smartphones offerieren neben Telefonie auch Internet- und Applikationsdienste. Systeme wie Symbian oder Windows-Mobile sorgen für die nötige Applikationsplattform. Doch die neuen mobilen Plattformen sind alles andere als sicher. Ein klassisches Handy funktioniert nicht ohne SIM-Karte. Ein Windows-Smartphone arbeitet sehr wohl ohne SIM und PIN.

Geschäftlich genutzte Smartphones brauchen daher einen zusätzlichen Schutz. Kaspersky offeriert für Nokia-Geräte mit Symbian S60v3 und Windows-Smartphones die Software Mobile-Security 7.0. Network Computing testete in den Real-World Labs Poing für das Network-Computing-Zertifikat die vom Hersteller angegebenen Funktionen – Remote-Management und Diebstahlschutz.

Für den Test nutzte Network Computing eine virtuelle Windows-XP-Maschine unter VMware 6.5. Diese VM hatte über USB Zugriff auf ein SMS-Modem. Als Smartphone kam ein T-Mobile-MDA mit Windows-Mobile-Software zum Einsatz.

Die Basis für die Fernwartung ist Kasperskys-Administration-Kit. Die frei herunterladbare Software nimmt die verschiedenen Softwaremodule von Kaspersky auf und verwaltet diese. Der Rechner mit dem Administration-Kit muss über Port 13292 aus dem Internet erreichbar sein. Via SSL nehmen die verwalteten Smartphones später regelmäßig Kontakt zum Administrationsserver auf und gleichen die Policies ab.

Network Computing installiert das Mobile-Security-Modul in das Admin-Kit und erstellt ein Installations-Paket mit der Software für das Smartphone. Diese CAB-Datei legt das Testteam auf einen Web-Ser-

ver. Über den Admin-Server und das SMS-Modem schickt die Kaspersky-Software dem Smartphone dann eine SMS. Die enthält die Quellangabe für den Download des CAB-Archivs. Verschlüsselt hängt Kaspersky der SMS die Informationen zum Zertifikat des Admin-Servers und dessen Zugangsdaten an.

Nach der Installation startet das Smartphone mit der Security-Suite im System. Diese fordert den Anwender zur Festlegung einer Sicherheitscode auf.

Über das Administrations-Kit erstellt der Verwalter nun ein Policy-Regelwerk für das Telefon oder eine Gruppe von Telefonen. Hier legt er fest, welche Features das Telefon nutzt und welche Einstellungen der Anwender am Telefon selbst ändern darf. Bei der nächsten Synchronisation übernimmt das Smartphone die Policy.

Neben Viren- und Spamschutz gibt es drei Funktionen für den Diebstahlschutz. Der SMS-Block verriegelt das Telefon, so dass es ohne die Eingabe des Sicherheitscodes weder mit noch ohne SIM-Karte funktioniert. Den Block aktiviert eine SMS. Merkt der Anwender, dass ihm sein Telefon entwendet wurde oder dass er es irgendwo vergessen hat, braucht er nur von einem beliebigen anderen Mobiltelefon eine SMS mit dem Inhalt »Block:« gefolgt von dem Sicherheitscode versenden. Das Smartphone setzt den Schutz sofort nach Eintreffen der SMS in Kraft.

Etwas radikaler arbeitet SMS-Clean. Erhält das Telefon hier die kodierte SMS mit dem gültigen Sicherheitscode, löscht die Kaspersky-Software Daten vom Telefon. Die Policy legt dabei fest, was entfernt wird. Zur Auswahl stehen: Nachrichten, Adressbuch, Dokumente, SD-Karten und die Netzwerk-Einstellungen sowie Zugangsdaten.

SIM-Watch überwacht, ob die richtige SIM-Karte im Telefon steckt. Tauscht jemand die SIM aus, übermittelt Kaspersky zwei in der Policy festgelegten Nummern eine SMS mit der neuen Nummer des Telefons und verriegelt es anschließend. So ist dem Benutzer die Telefonnummer des Diebes oder Finders bekannt.

Im Test arbeiten die Anti-Theft-Funktionen wie vom Hersteller versprochen. Der SMS-Block-Schutz ließ sich auch ohne SIM im MDA nicht umgehen. Die im Administration-Kit festgelegte Policy übernimmt das Smartphone zuverlässig.

Fazit: Die Kaspersky-Mobile-Security-Enterprise Edition 7 offeriert einen wirksamen Daten- und Diebstahlschutz für Smartphones. Der IT-Verwalter kann die Regelwerke hierbei bequem auf einer zentralen Management-Plattform verwalten.

ZERTIFIZIERTE FUNKTIONEN



Mobile Security Enterprise Edition 7.0
Hersteller:
Kaspersky

Preis: bei 1-14: 28 Euro (pro Lizenz)
bei 100-149: 16,35 Euro (pro L.)

Web: www.kaspersky.de

- ◆ Zentrale Policy-Verwaltung über Administration-Kit
- ◆ Diebstahlschutz durch SMS-Block
- ◆ Diebstahlschutz durch SIM-Watch
- ◆ Datenschutz durch SMS-Clean

Poing, 3/2009
Andreas Stolzenberger



Das sichere Büro in der Westentasche

Sicherheitssoftware – Bedrohungen durch Malware und Netzwerk-Attacken machen auch vor mobilen Geräten nicht halt. Gerade für Unternehmen hat daher der Schutz der Mitarbeiter-Smartphones höchste Priorität.

Auch vor Ort beim Kunden oder auf Geschäftsreise müssen Mitarbeiter heute rund um die Uhr auf Firmendaten zugreifen können und für Rückfragen erreichbar sein. Moderne Smartphones sind die idealen Geräte dafür, sie übernehmen neben der eigentlichen Telefonie immer mehr Funktionen, die früher dem Notebook vorbehalten waren: Terminkalender, E-Mail-Client, Internet-Browser und Online-Chat gehören mittlerweile zur Standardausstattung der kleinen Alleskönner.

Doch mit der Anzahl an Funktionen und Schnittstellen steigt auch die Verwundbarkeit durch mobile Malware und Hacker-Angriffe. Cyberkriminelle sind nicht nur an Ihren persönlichen Zugangsdaten fürs Online-Banking und anderen Web-Diensten interessiert, sondern auch an Ihrer persönlichen Kontakt-Liste sowie sensiblen Geschäftsdaten. Dabei werden diese Informationen entweder ausgespäht oder aber verschlüsselt, um so für die Wiederherstellung vom Opfer ein Lösegeld pressen zu können. Eine weitere

Einnahmequelle für Online-Betrüger sind trojanische Programme, die teure Premium-SMS-Nachrichten versenden.

Mindestens genauso gefährlich ist das Risiko des physikalischen Verlusts: Alleine in der Londoner U-Bahn werden jedes Jahr rund 100 000 Handys gefunden. Hinzu kommen noch die gestohlenen Geräte – und oft sind die Daten darauf wertvoller als die eigentliche Hardware.

Sicherheitsfunktionen heutiger Handys beschränken sich in der Regel auf die Abfrage des PIN-Codes beim Einschalten –

dies hilft aber nur gegen den Missbrauch der SIM-Karte, und auch nur dann, wenn das Gerät im ausgeschalteten Zustand verloren ging oder gestohlen wurde.

Mobile Malware aber infiziert Ihr Handy im laufenden Betrieb, zum Beispiel im Café oder im Bus. Der gefährliche Schadcode kommt dabei per SMS, Bluetooth oder E-Mail auf das Smartphone – oder bei der Synchronisation mit dem PC, bei der auch umgekehrt Ihr Handy den PC und somit das gesamte Firmennetz infizieren kann.

Sicher unterwegs

Schon deswegen ist eine Sicherheitssoftware auf jedem Mobiltelefon wichtig, die dafür sorgt, dass solche Programme gar nicht erst zum Zug kommen. Programme wie Kaspersky Mobile Security Enterprise Edition überprüfen in Echtzeit die Daten, die das Handy über Bluetooth, GPRS oder UMTS erreichen, und wehren verdächtige Aktivitäten sofort ab. Auch SMS-Nachrichten und Mails mit Spam sowie unerwünschte Telefonanrufe werden automatisch blockiert. Eine IP-Firewall mit verschiedenen Schutzstufen wehrt zudem Angriffe von außen ab.

Firmendaten gut geschützt

Doch was, wenn der Super-GAU eintritt? Geht Ihr Handy verloren oder wird es gestohlen, liegen die gespeicherten Geschäftsdaten, persönliche Bilder und Nachrichten normalerweise offen vor dem neuen – unberechtigten – Eigentümer. Nicht jedoch mit Kaspersky Mobile Security Enterprise Edition: Hier kann der Anwender oder Systemadministrator das Gerät nach Diebstahl oder Verlust blockieren sowie Dateien, Nachrichten und die Adressliste per Fernzugriff löschen. Zudem lässt sich leicht herausfinden, wer der »neue Eigentümer« des verloren gegangenen Gerätes ist:

♦ **SMS Block:** Bei Verlust kann der Smartphone-User eine spezielle für den Empfänger unsichtbare Kurzmitteilung an das verlorene Gerät verschicken, die den Zugriff auf das Gerät so lange vollständig blockiert, bis ein vorher festgelegtes Passwort eingegeben wird.

♦ **SMS Clean:** Statt wie bei SMS Block den Zugriff zu blockieren, löscht diese Funktion den Speicher vollständig.

KONTAKTDATEN

Kaspersky Labs GmbH
Steinheilstraße 13
85053 Ingolstadt
Deutschland

Tel. +0841 981 89-0
Fax +0841 981 89-100
vertrieb@kaspersky.de
www.kaspersky.de

Beispiel sicherstellen, dass nur Geräte mit aktuellstem Schutzstatus auf das Firmennetz zugreifen.

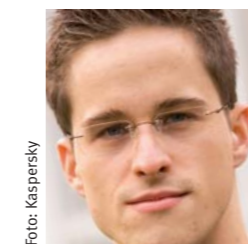
Die Antiviren-Datenbanken werden automatisch in vom Systemadministrator definierten Intervallen aktualisiert. Aktualisierungen sind über WAP/HTTP (GPRS, EDGE, WLAN etc.) verfügbar oder können über einen PC geladen werden.

Fazit

Kaspersky Mobile Security Enterprise Edition läuft unter Symbian sowie Windows Mobile und schützt Smartphones sowie die darauf gespeicherten Daten vor fremdem Zugriff. Für Unternehmen ist diese Schutzsoftware somit ein unverzichtbarer Baustein ihrer Sicherheitsstrategie. Die zentrale Administration erleichtert die Verwaltung der mobilen Clients und stellt die Durchsetzung von Unternehmensrichtlinien sicher.

Kaspersky Mobile Security Enterprise Edition ist erhältlich als Bestandteil von Kaspersky Open Space Security, dem zuverlässigen und plattformübergreifenden Schutz für alle Netzwerkknoten von Workstations über Datei- und Mail-Server bis hin zu Gateways und Smartphones.

Rüdiger Pein



Christian Funk,
Virus Analyst bei
Kaspersky Lab

»Insbesondere Unternehmen müssen beim Thema 'Mobile Gefahren' auf der Hut sein. Dem mobilen Minicomputer wird eine Vielzahl sensibler Daten wie Unternehmens-E-Mails, Kontaktdaten und Geschäfts-Notizen anvertraut, außerdem bietet er durch die vielfältigen Networking- und Synchronisierungsfunktionalitäten eine große Angriffsfläche für Malware, so dass man hier unbedingt Sicherheitsvorkehrungen treffen sollte.«