

Kaspersky
Open Space
Security

KASPERSKY lab



Kaspersky Open Space Security

Kaspersky Open Space Security geht weit über den traditionellen Schutz des Arbeitsplatz-Computers hinaus und bietet eine völlig neue Flexibilität der Netzwerk-Sicherheit – zum Schutz einer immer mobileren und dynamischer vernetzten Arbeitsumgebung.

Die moderne IT bietet zahllose Möglichkeiten der Kommunikation und Zusammenarbeit, wodurch eine neue globale Arbeitsumgebung geschaffen wird, die physikalische Grenzen und Entfernungen außer Kraft setzt.

Wir können heute von praktisch jedem Punkt der Erde aus online mit unseren Kollegen, Partnern und Kunden in Kontakt treten und haben Zugang zum Firmen-Netzwerk, zu Online-Shops, Banken sowie einer Vielzahl von Informationen. Die Kehrseite dieser wachsenden Freiheit sind die steigenden Möglichkeiten für Cyber-Kriminelle, die ihre Methoden und Technologien zum Diebstahl vertraulicher Informationen ständig weiterentwickeln.

Unternehmens-Netzwerke haben sich im Laufe der letzten Jahre komplett verändert, sind offener und dynamischer geworden. Die Kaspersky-Lösungen passen sich diesen Veränderungen an. Früher waren Netzwerke klar definierte Strukturen, um die eine Schutzbarriere errichtet werden konnte. Heute kann ein Netzwerk zahlreiche Sub-Netzwerke mit Laptop-, Smartphone- oder PDA-Usern enthalten - eine dynamische Einheit, deren Parameter sich laufend ändern. Die Folge sind zahlreiche neue Sicherheitsanforderungen. Vor diesem Hintergrund wurde **Kaspersky Open Space Security** entwickelt.

Kaspersky Open Space Security ist eine moderne Lösung, die auch externe und mobile User erreicht. Wir sind überzeugt, dass Freiheit und Flexibilität in der Unternehmenskommunikation und ein zuverlässiger Schutz vor aktuellen Bedrohungen, wie Viren, anderen Schadprogrammen, Hacker-Attacken, Spyware und Spam absolut miteinander vereinbar sind.

Um einen wirklich umfassenden Schutz für Unternehmens-Netzwerke gewährleisten zu können, muss eine integrierte Lösung die folgenden Anforderungen erfüllen:

- ✓ **Eine umfassende Lösung für alle Knoten und Plattformen des Netzwerks.** In dynamischen Netzwerken ist es unmöglich, genau zu bestimmen, wo die Grenzen des Netzwerks liegen. Gegenwärtige Bedrohungen sind in der Lage, in das Netzwerk einzudringen, ohne über einen Server zu gehen (etwa wenn ein Anwender seinen Web-Mail-Account abrufen). Die einzige Möglichkeit, ein Netzwerk vollständig zu sichern, ist die Installation von Schutz-Software an jedem einzelnen Netzwerk-Knoten und auf jedem dazugehörigen Gerät.

Bei Kaspersky Open Space Security handelt es sich um verschiedene miteinander kombinierbare Lösungen – für Mobiltelefone, Smartphones, Laptops und Workstations bis hin zu File-Servern, Mail-Servern und Internet-Gateways. Natürlich auch unter allen gängigen Plattformen. Jedes Unternehmen kann genau die Lösung auswählen, die am besten zu Umfang und Komplexität seines Netzwerks passt.

- ✓ **Schutz vor allen Bedrohungen.** Immer häufiger trifft man bei Internet-Schädlingen auch auf Mischformen, wobei verschiedene Malware-Elemente in einem einzigen Angriff vereint werden. Zudem kommen auch immer häufiger Social-Engineering-Techniken zum Einsatz. Eine Sicherheitslösung muss also viele verschiedene Komponenten bündeln, um mit jeglicher Art von Cyber-Bedrohung fertig zu werden – Viren, Spyware, Rootkits, Hacker-Angriffe, Phishing-Attacken und Spam eingeschlossen.
- ✓ **Schnelle Reaktion.** Der globale Charakter gegenwärtiger Bedrohungen macht sofortige Reaktionen zur absoluten Notwendigkeit. Um auf die steigende Zahl und Vielfalt von Angriffen adäquat reagieren zu können, sind eine schnelle Entdeckung, Analyse und Verbreitung von Gegenmitteln Voraussetzung. Bei immer raffinierteren Schadprogrammen in Verbindung mit globalen Hochgeschwindigkeits-IP-Netzwerken können Zeitverzögerungen die Infektion von weltweit vielen tausenden Systemen innerhalb weniger Minuten nach sich ziehen.

Kaspersky Open Space Security setzt neue Standards in Entdeckungsrate und Reaktionsgeschwindigkeit gegenüber diesem wachsenden Bedrohungspotential. Durch einzigartige Prozesse und innovative Technologien bietet Kaspersky Lab die höchste Entdeckungsrate der Branche, die kürzeste Reaktionszeit auf Ausbrüche und standardmäßig stündliche Updates der Bedrohungs-Signaturen.

- ✓ **Kombinierte Technologien.** Für einen umfassenden Schutz vor IT-Bedrohungen ist die richtige Kombination der verschiedenen Technologien außerordentlich wichtig, damit diese effektiv interagieren können. Während sich der Virenschutz bisher vor allem auf Signaturen stützte, rücken mittlerweile – da sich Bedrohungen teilweise innerhalb von Minuten ausbreiten – proaktive Technologien und heuristische Algorithmen in den Vordergrund. Proaktive Technologien erkennen Schadprogramme allein auf Grund ihres Verhaltens und sind daher nicht auf Signatur-Updates angewiesen.

Kaspersky Open Space Security kombiniert den Signaturen-Schutz mit neuesten proaktiven Technologien, die Schadcodes in kurzer Zeit erkennen, den User oder Administrator darauf aufmerksam machen und im Ernstfall die vom Schadprogramm vorgenommenen unerwünschten Änderungen wieder rückgängig machen.

Eine Sicherheitslösung sollte die neuesten mobilen Technologien nicht nur berücksichtigen, sondern diese auch nutzen – zum Vorteil der Benutzer und in Hinblick auf die Sicherheit des gesamten Netzwerks.

- ✓ **Sicherheit im Umbruch.** Erreichbar zu sein und in Kontakt zu bleiben – egal in welchem Winkel der Welt man sich befindet – ist in der heutigen Geschäftswelt eine Grundvoraussetzung. Daher ist der Schutz von Mitarbeitern, die außerhalb des Büros arbeiten, von ganz besonderer Dringlichkeit. Eine Sicherheitslösung muss in der Lage sein, den Betriebsmodus auszuwählen, der den Bedingungen, unter denen Notebooks oder Smartphones arbeiten, gerecht wird.

Kaspersky Open Space Security verwendet eine eigens für Laptop-User entworfene Policy, die sich automatisch aktiviert, sobald der Laptop vom Unternehmens-Netzwerk getrennt wird. Die Regeln dieser Policy wurden sehr sorgfältig angepasst, um auch für Laptops, die nicht mit ihrem Heimnetzwerk verbunden sind, höchsten Schutz zu gewährleisten. Unter anderem, indem die Quelle und die Häufigkeit von Updates, die Scan-Zeitpläne und die Firewall-Konfiguration vorgegeben werden. Verbindet sich der Benutzer wieder mit dem Unternehmens-Netzwerk, werden die Laptop-Daten und die des Administrations-Servers synchronisiert, wobei der Administrator über Anti-Malware-Aktivitäten informiert wird und die aktuellen Neuerungen in der Unternehmens-Sicherheitspolitik auf den Laptop überspielt werden.

Mit dem Schutz von Kaspersky Open Space Security können Anwender sicher in jeder Art von Netzwerk – unter anderem auch WiFi – arbeiten und bleiben dabei für Hacker unsichtbar. Stellt das Programm eine Verbindung zu einem Netzwerk her, fragt es den Benutzer, ob es sich dabei um das Internet, ein Intranet oder ein vertrauenswürdigen Netzwerk handelt und wählt dementsprechend den passenden Betriebsmodus der Firewall aus. Das Programm erstellt eine Liste aller Netzwerke, zu denen eine Verbindung hergestellt wurde, und bietet die Möglichkeit, für jedes einzelne dieser Netzwerke den Stealth Modus zu aktivieren bzw. zu deaktivieren.

Ist eine Verbindung zum Administrations-Server nicht möglich, wird die Aktualität der Sicherheitsfunktionen trotzdem aufrechterhalten, indem (via Internet) eine andere Update-Quelle ausgewählt wird. Außerdem sind die proaktiven Technologien ebenfalls ständig eingeschaltet, so dass der Rechner auch vor unbekanntem Gefahren geschützt ist.

- ✓ **Überprüfung zurückkehrender und fremder Laptops.** Loggt sich ein Mitarbeiter nach einer Geschäftsreise mit seinem Laptop wieder in das Firmen-Netzwerk ein, überprüft Kaspersky Open Space Security den Rechner auf die Einhaltung der Sicherheits-Policy, um das Netzwerk und die anderen Anwender zu schützen. Genauso wird auch mit Gastcomputern im Netzwerk verfahren.

Auch Cisco NAC (Network Admission Control)¹ wird von Kaspersky Open Space Security unterstützt, wodurch Computer, die nach Abwesenheit erneut mit dem Netzwerk verbunden werden, auf die Sicherheits-Policy überprüft werden können. Entdeckt das Programm einen infizierten Computer, blockiert es dessen Verbindungen, so dass der Administrator die Quelle der Infektion auffindig machen kann.

¹ voraussichtlich ab Februar 2007

Das ständige Kräftemessen zwischen Antivirus-Industrie und Cyber-Kriminellen zwingt die Viren-Autoren, ständig neue Methoden zur Umgehung des Virenschutzes zu entwickeln. Eine weitere Anforderung an moderne Sicherheitslösungen ist daher auch das Erkennen neuer Malware-Techniken.

- ✓ **Schutz vor Rootkits.** Rootkits zielen darauf ab, Dateien, Ordner, Registry-Schlüssel, laufende Programme, Services, Treiber und Netzwerkverbindungen/Aktivitäten vor dem Benutzer zu verbergen. Für einen wirksamen Schutz vor dieser Art von Malware müssen hoch spezialisierte Technologien eingesetzt werden.

Kaspersky Open Space Security verwendet Anti-Rootkit-Technologien, die verborgene Prozesse im System entdecken, indem zum einen alle kritischen Bereiche – unter anderem des Betriebssystems - gescannt werden, die besonders anfällig für Infektionen sind. Zum anderen werden alle Systemprozesse analysiert und der User oder Administrator gewarnt, sobald ein gefährlicher, verdächtiger oder verborgener Prozess gestartet wird.

- ✓ **Schutz vor Identitätsdiebstahl.** Einige Schadprogramme stehlen unbemerkt vertrauliche Informationen vom Computer eines Benutzers, unter anderem LogIns und Passwörter.

Kaspersky Open Space Security verwendet heuristische Algorithmen, die extra entwickelt wurden, um den Diebstahl von Passwörtern oder anderen Daten zu verhindern. Zusammen mit einer persönlichen Firewall überwachen IDS (Intrusion Detection System) und IPS (Intrusion Prevention System) alle Netzwerkaktivitäten und verhindern Datenlecks oder das Eindringen von Hackern in das System.

- ✓ **Zurücksetzen der durch Malware hervorgerufenen Änderungen.** Ein recht neuer Trend in der Entwicklung der Schadprogramme ist der Einsatz von Ransomware, die Daten auf einem Computer beschädigt oder verschlüsselt und anschließend ein Lösegeld für deren Wiederherstellung fordert.

Kaspersky Open Space Security wehrt diese Angriffe zuverlässig ab. Das Programm blockiert alle verdächtigen Aktivitäten im System, entfernt Malware und macht alle schädlichen Veränderungen im System rückgängig.

- ✓ **Selbstverteidigung.** Der Einsatz hoch entwickelter Schutztechnologien ist nur sinnvoll, wenn diese nicht von Schadprogrammen außer Kraft gesetzt werden können.

Kaspersky Open Space Security verfügt über eine Reihe effektiver Selbstverteidigungs-Mechanismen: Das Programm überwacht seine eigenen Prozesse, Dateien sowie Registry-Schlüssel und blockiert alle Attacken gegen sich selbst.

Schließlich darf man bei der Entwicklung einer gut balancierten Sicherheitslösung nicht die Notwendigkeit einer einfachen, transparenten und leistungsfähigen Administration ausser Acht lassen.

- ✓ **Zentrale Administration.** Moderne Firmen-Netzwerke werden immer komplexer und während der durchschnittliche Anwender aus neuen Tools einen großen Nutzen zieht, fehlt ihm andererseits möglicherweise die IT-Sicherheitskompetenz. Eine professionelle, zentrale Administration ist daher unerlässlich, soll das Netzwerk erfolgreich vor Viren und Schadprogrammen geschützt werden. Um die Bedrohungs-Datenbanken und Programm-Module auf dem neuesten Stand zu halten und wirksam auf Vorfälle im Netzwerk reagieren zu können, sind vollständige und fortlaufende Informationen über den Systemstatus wichtig.

Kaspersky Open Space Security bietet mit dem kostenlosen Kaspersky Administration Kit eines der umfangreichsten und flexibelsten Administrations-Werkzeuge, das derzeit im Security-Bereich erhältlich ist. Es ermöglicht die zentrale Administration dynamischer Netzwerke mit bis zu zehntausenden Knoten, inklusive mobiler Anwender und Remote-Reparatur.

- ✓ **Kompatibel mit Technologien von Drittanbietern.** Um höchste Effektivität zu erzielen, sollte eine moderne Sicherheitslösung die technischen Features von anderen im System installierten Produkten berücksichtigen.

Da Kaspersky Open Space Security das Intel Active Management (Intel vPro) unterstützt, ist auch eine Remote-Bearbeitung von Workstations möglich. Über Cisco NAC (Network Admission Control) können zudem einzelne Computer isoliert und auf Einhaltung der Sicherheits-Policy geprüft werden. Die Unterstützung der Centrino-Duo-Technologie ermöglicht den sparsamen Umgang mit den Ressourcen von Laptops.

- ✓ **Effizienter Einsatz von Netzwerk-Ressourcen.** Eines der wichtigsten Kriterien für Unternehmen bei der Wahl einer Sicherheitslösung ist deren Einfluss auf die Netzwerk-Ressourcen und die Betriebsgeschwindigkeit.

Kaspersky Open Space Security wurde zur Verbesserung der Systemperformance entwickelt. Dank der innovativen iSwift-Technologie werden unnötige Scans von Dateien auf Arbeitsplätzen oder File-Servern vermieden, so dass die Anwender schneller Zugriff auf Dateien des Servers bekommen.

Work Space Security

Erhältliche Anwendungen

Anti-Virus für Windows Workstation
Anti-Virus für Linux Workstation

Geschützte Plattformen/Betriebssysteme

Workstations: Windows (einschließlich x64), Linux

Business Space Security

Erhältliche Anwendungen

Anti-Virus für Windows Workstation
Anti-Virus für Linux Workstation
Anti-Virus für Windows File Server
Anti-Virus für Linux File Server
Anti-Virus für Novell NetWare File Server

Geschützte Plattformen/Betriebssysteme

Workstations: Windows (einschließlich x64), Linux
Datei-Server: Windows (einschließlich x64),
Novell NetWare, Linux

Enterprise Space Security

Erhältliche Anwendungen

Anti-Virus für Windows Workstation
Anti-Virus für Linux Workstation
Anti-Virus für Windows File Server
Anti-Virus für Linux File Server
Anti-Virus für Novell NetWare File Server
Anti-Virus für Microsoft Exchange Server
Anti-Virus für Linux Mail Server
Anti-Virus für Linux Mail Gateway
Anti-Virus für IBM Lotus Domino

Geschützte Plattformen/Betriebssysteme

Workstations: Windows (einschließlich x64), Linux
Datei-Server: Windows (einschließlich x64), Novell
NetWare, Linux
Mail-Server und Server zur gemeinsamen Arbeit:
Microsoft Exchange, IBM Lotus Domino, Linux
(Sendmail, Qmail, Postfix und Exim)

Total Space Security

Erhältliche Anwendungen

Anti-Virus für Windows Workstation
Anti-Virus für Linux Workstation
Anti-Virus für Windows File Server
Anti-Virus für Linux File Server
Anti-Virus für Novell NetWare File Server
Anti-Virus für Microsoft Exchange Server
Anti-Virus für Linux Mail Server
Anti-Virus für Linux Mail Gateway
Anti-Virus für IBM Lotus Domino
Anti-Virus für Microsoft ISA Server
Anti-Virus für Proxy Server
Anti-Virus Mobile
Anti-Spam für Linux

Geschützte Plattformen/Betriebssysteme

Workstations: Windows (einschließlich x64), Linux
Mobile Geräte: Symbian, Windows Mobile
Datei-Server: Windows (einschließlich x64), Novell
NetWare, Linux
Mail-Server und Server zur gemeinsamen Arbeit:
Microsoft Exchange, IBM Lotus Domino, Linux
Internet-Gateways: Microsoft ISA Server, Squid
Proxy Server

Weitere Lösungen

Anti-Virus Mobile
Anti-Virus für Clearswift MIMESweeper for SMTP
Anti-Virus S.O.S.

