KASPERSKY SECURITY FOR MOBILE

KASPERSKY lab

KASPERSKY SECURITY FOR MOBILE

Zehn Jahre Expertise in der mobilen Sicherheit

Die Technologie - und auch die Bedrohungen - werden beständig weiterentwickelt.

Seit 2004, als mit Cabir zum ersten Mal ein mobiler Virus in unseren Analysesystemen auftauchte, beschäftigt sich Kaspersky Lab mit der Erkennung, Offenlegung und Analyse von mobiler Malware.

Ein Jahrzehnt später, 2014, musste sich Kaspersky Lab mit fast **1,4** Millionen singulärer Attacken durch mobile Malware befassen[1] – ein erheblicher und immer noch anhaltender Anstieg im Vergleich zu den 335.000 Vorfällen, die im Jahr zuvor verzeichnet wurden.

Je mehr Smartphones und Tablets Teil unserer alltäglichen Arbeits- und Geschäftsroutinen geworden sind, umso größer ist auch die Bedrohung geworden, die mit ihnen einhergeht:

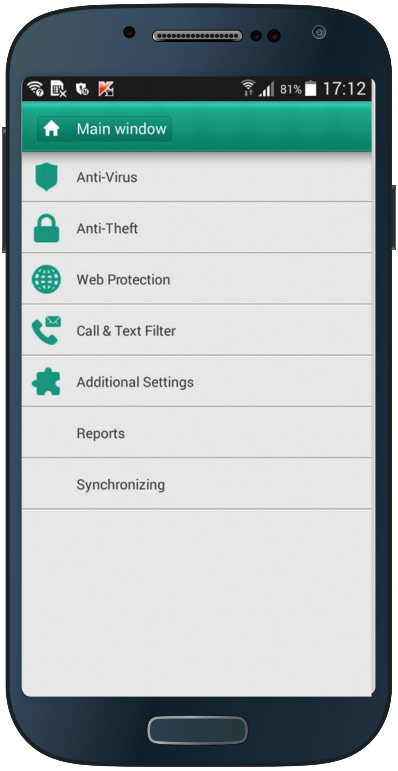
- **Mobile Malware**: Verzeichnet ein exponentielles Wachstum, sowohl für Android- als auch iOS-Plattformen. Allein im Jahr 2014 machte Kaspersky Lab die folgenden Funde:
  - **4.643.582** schädliche Installationspakete
  - **295.539** neue mobile Schadprogramme
- **BYOD**: Birgt fast genauso viele Risiken wie Vorteile: ungesicherte Geschäftsdaten sowie die Mischung aus persönlichen und geschäftlichen Programmen und Nutzungsgewohnheiten führen zu Problemen mit der Datenintegrität.
- **Unkontrollierter Zugriff auf vertrauliche Daten**: Nicht abgesicherte Geräte erhalten unkontrollierten Zugriff auf Unternehmensdaten. Schwache Kennwörter, keine Verschlüsselung, per Jailbreak entsperrte Geräte und keine Technologie, die kontrolliert, was mit vertraulichen Daten passiert, wenn ein Gerät gestohlen oder verloren wird, schaffen Probleme.
- **IT-Komplexität**: Ein Mitarbeiter besitzt durchschnittlich mindestens drei Endgeräte. Unterschiedliche Plattformen, unterschiedliche Geräte und unterschiedliche Management-Programme führen insgesamt zu einem enormen IT-Verwaltungsaufwand.

Kaspersky Security for Mobile bietet Ihnen proaktive Sicherheit, Verwaltung und Kontrolle über **sämtliche mobilen Endpoints**. Mit unserer Lösung haben Sie die Gewissheit, dass Ihr Gerät gut geschützt ist, egal wo es sich gerade befindet.

Kaspersky Security for Mobile bietet Ihnen Schutz vor sich ständig weiterentwickelnder mobiler Malware. Sie erhalten den vollständigen Überblick und die Kontrolle über alle Smartphones und Tablets innerhalb Ihrer Infrastruktur. Alles von einer zentralen Konsole aus, bei minimaler Beeinträchtigung.

[1] http://securelist.com/analysis/kaspersky-security-bulletin/68010/kaspersky-security-bulletin-2014-overall-statistics-for-2014/

HOCHENTWICKELTER MOBILER MALWARE-SCHUTZ



MEHRSTUFIGER MALWARE-SCHUTZ

Die mobilen Sicherheitstechnologien von Kaspersky Lab verbinden leistungsstarken, signaturbasierten Malware-Schutz mit proaktiven und cloud-basierten Technologien (Kaspersky Security Network). Das Ergebnis sind ausgezeichnete Erkennungsraten und ein Schutz vor bekannten wie unbekannten Bedrohungen durch Malware.

Bedarfsorientierte und planmäßige Überprüfungen gepaart mit automatischen OTA-Aktualisierungen sorgen für noch besseren Schutz der mobilen Geräte und der auf ihnen gespeicherten Daten.

WEBFILTER

Die integrierte mobile Web-Kontrolle garantiert sicheren Online-Zugang auf Smartphones und Tablets, denn die Technologie von Kaspersky Lab blockiert den Zugriff auf schädliche Websites.

Gestützt durch unser cloud-basiertes Kaspersky Security Network (KSN), liefert die Funktion „Sicherer Browser“ eine stets aktuelle Reputationsanalyse von Webressourcen und schützt den Benutzer so vor Phishing und anderen Angriffen aus dem Internet.

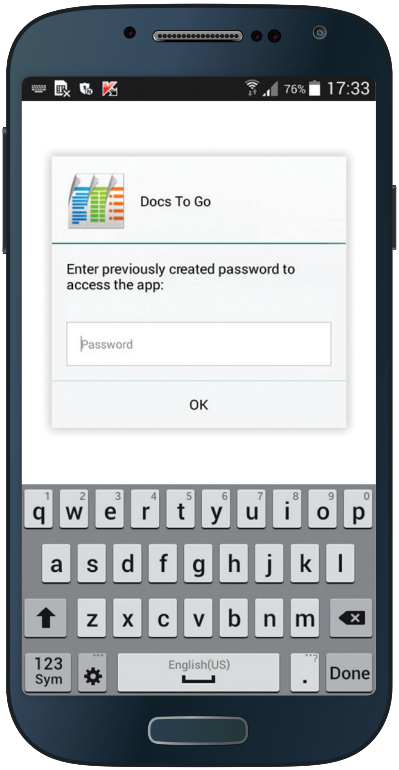
TRENNUNG VON GESCHÄFTLICHEN UND PERSÖNLICHEN DATEN FÜR BYOD

CONTAINERISIERUNG

Die Trennung von persönlichen und geschäftlichen Daten auf beliebigen Geräten bietet zusätzliche Sicherheit, besonders in Umgebungen, in denen BYOD-Geräte eingesetzt werden.

Kaspersky Security for Mobile ermöglicht eine „Containerisierung“, d. h. die Kapselung von geschäftlichen Programmen in eigene sichere Container, auf die zusätzliche Richtlinien, z. B. für die Verschlüsselung, angewendet werden können, um vertrauliche Geschäftsdaten zu schützen. Die Daten innerhalb des Containers können nicht in einen anderen Speicherort kopiert werden.

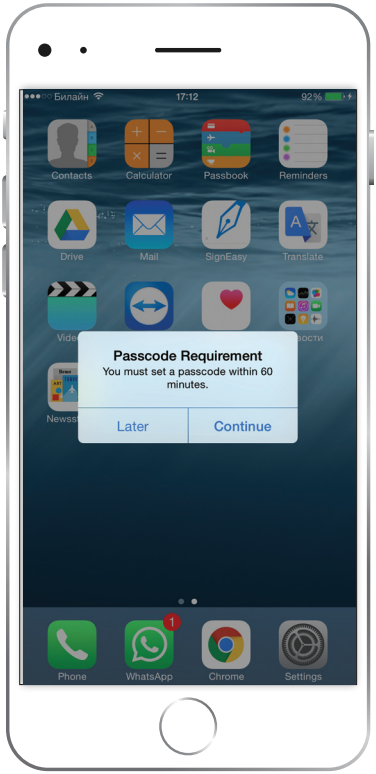
Das System kann so konfiguriert werden, dass der Benutzer sich zum Starten eines Programms bei allen Containern authentifizieren muss. Durch die Überwachung des Inaktivitätszeitraums von Programmen kann eine erneute Anmeldung durch den Benutzer erzwungen werden, falls für einen vorgegebenen Zeitraum keine Benutzereingabe erfolgt ist. Auf diese Weise sind die Daten zusätzlich geschützt, selbst wenn ein Programm geöffnet ist und das Gerät abhanden kommt oder gestohlen wird.



GEZIELTES LÖSCHEN

Wenn ein Mitarbeiter zu einem anderen Unternehmen wechselt, sollten Sie sicherstellen, dass er keine Geschäftsdaten dorthin mitnimmt. Kaspersky Security for Mobile ermöglicht die Löschung von containerisierten Geschäftsdaten, lässt aber private Daten wie Fotos, Wiedergabelisten, Kontakte und andere Einstellungen intakt.

VERWALTEN UND KONTROLLIEREN DES ZUGRIFFS AUF GESCHÄFTSDATEN



MOBILE DEVICE MANAGEMENT (MDM)

Einheitliche MDM-Richtlinien für Microsoft Exchange ActiveSync und iOS MDM unterstützen die Durchsetzung von Kennwörtern, Geräteverschlüsselung, den Einsatz der Kamera und anderer Gerätefunktionen. Die Bedienoberfläche für die Verwaltung von Android, iOS und Windows Phone ist dabei einheitlich für alle Geräte.

UNTERSTÜTZUNG VON SAMSUNG KNOX

Kaspersky Security for Mobile unterstützt Samsung KNOX 1.0 und 2.0 und ermöglicht so die Konfiguration von Firewalls und APN/VPN sowie der Microsoft Exchange Server-Einstellungen für Smartphones und Tablets von Samsung.

KONTROLLTOOLS

Dank Programmkontrolle können Administratoren die Programmnutzung verwalten und auf innerhalb des Unternehmens genehmigte Programme beschränken. Unsichere oder nicht autorisierte Programme können so blockiert werden, während bestimmte Gerätefunktionen von der Installation von innerhalb des Unternehmens vorgegebenen Programmen abhängig gemacht werden. Durch die Überwachung des Inaktivitätszeitraums von Programmen kann eine erneute Anmeldung durch den Benutzer erzwungen werden, falls für einen vorgegebenen Zeitraum keine Benutzereingabe erfolgt ist.

Mithilfe der Web-Kontrolle können Administratoren den Zugriff auf Websites kontrollieren, die nicht den unternehmensinternen Sicherheits- oder Nutzungsrichtlinien entsprechen, z. B. Social Media, Glücksspiele, Erotik, Proxyserver oder andere unerwünschte Inhalte.

ERKENNUNG VON „ROOTING“ UND „JAILBREAK“

Gerootete oder per Jailbreak entsperrte Geräte stellen erhebliche Sicherheitsrisiken für ein Unternehmen dar, egal ob sie Teil einer BYOD-Initiative sind oder dem Unternehmen gehören. Da ihnen naturgemäß wichtige Sicherheitsschichten fehlen, ist das Risiko, die Kontrolle über diese Geräte zu verlieren, erheblich. Kaspersky Security for Mobile erkennt automatisch per Jailbreak entsperrte Geräte, alarmiert den Administrator und kann sogar Gerätedaten per Fernzugriff löschen.

HOCHENTWICKELTE SICHERHEITSFUNKTIONEN FÜR VERLORENE ODER GESTOHLENE GERÄTE

DIEBSTAHLSCHUTZ

Kaspersky Security for Mobile bietet eine Reihe von Diebstahlschutz-Funktion:

- Sperren/Entsperren des Geräts per Fernzugriff
- Geräteortung – Anzeige des Gerätestandorts auf einer Karte
- Alarm- und Fahndungsfoto-Funktionen zum Auffinden des Geräts
- SIM-Kontrolle – Benachrichtigt den Eigentümer bei Austausch der SIM-Karte
- Löschen von Gerätedaten – Löschen von bestimmten Daten in Containern oder Löschen des gesamten Geräteinhalts

Alle diese Funktionen können je nach Situation entweder vom Administrator oder Geräteeigentümer per Fernzugriff ausgelöst werden. Dank Integration mit Google Cloud Messaging können Administratoren Befehle umgehend per Push absetzen. Über das Self-Service-Portal von Kaspersky Lab kann der Benutzer die Diebstahlschutz-Funktion eigenständig aktivieren und so schnell auf den Verlust oder Diebstahl seines Geräts reagieren.

WENIGER AUFWAND FÜR DIE IT-VERWALTUNG

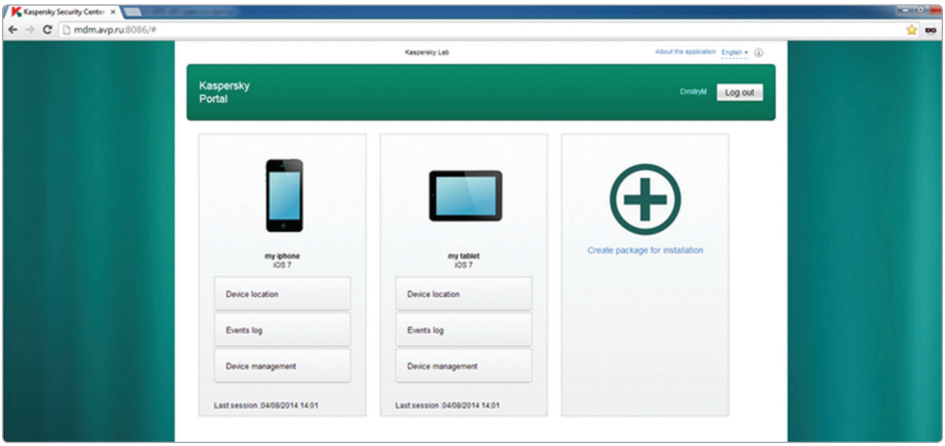
SELF-SERVICE-PORTAL

Kaspersky Security for Mobile ermöglicht die Einrichtung eines Self-Service-Portals, über das zeitraubende Routineaufgaben an den Endbenutzer delegiert werden können. So können Mitarbeiter beispielsweise ihre freigegebenen Endgeräte mit nur wenigen Mausklicks im Netzwerk registrieren. Alle erforderlichen Zertifikate können über das Portal automatisch installiert und aktiviert werden.

Bei Verlust oder Diebstahl seines Geräts kann der Benutzer Diebstahlschutz-Funktionen wie die Gerätesperrung, das Löschen von Daten oder die Geräteortung über das Self-Service-Portal aktivieren und so die Reaktionszeiten verkürzen.

WEBKONSOLE

Sämtliche mobilen Endgeräte (und normalen Endpoints) lassen sich wahlweise auch per Fernzugriff über einen Webbrowser verwalten. Die Webkonsole des Kaspersky Security Center wurde entsprechend erweitert und erlaubt nun auch die Verwaltung von Sicherheits- und Management-Funktionen für mobile Endgeräte.



INTEGRIERTE IT-SICHERHEITSPLATTFORM – EINE VERWALTUNGSKONSOLE

Im Gegensatz zu den meisten anderen IT-Sicherheitsanbietern ist das breite Produktportfolio von Kaspersky Lab das Ergebnis einer beträchtlichen Investition in die interne Forschung und Entwicklung und nicht durch den Zukauf von fremden Unternehmen entstanden.

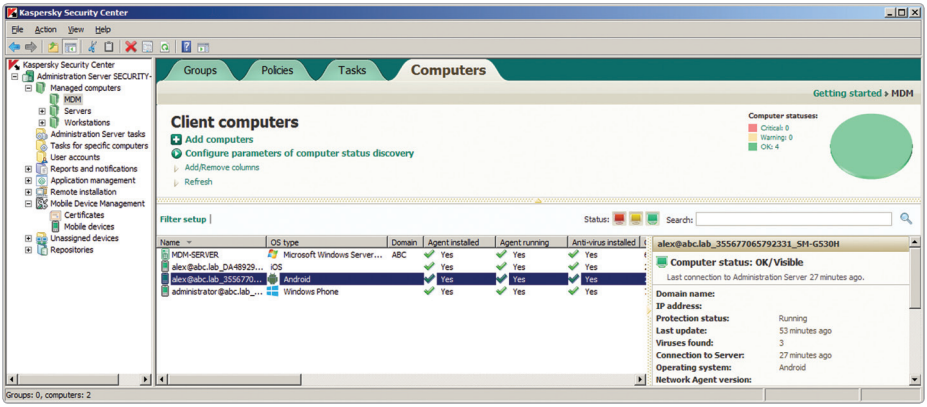
Alle unsere Technologien werden intern von Teams aus eigens dafür beschäftigten Sicherheitsexperten entwickelt. Das Ergebnis ist eine integrierte Technologieplattform, mit der jeder Aspekt der IT-Sicherheit in Unternehmen verwaltet werden kann.

UNTERSTÜTZUNG ALLER GÄNGIGEN MOBILEN PLATTFORMEN

Mit Kaspersky Security for Mobile können Smartphones und Tablets unter Android, iOS und Windows Phone geschützt und verwaltet werden.

VERWALTUNG VON HERKÖMMLICHEN ENDPOINTS UND MOBILEN ENDGERÄTEN ÜBER EINE EINZIGE VERWALTUNGSKONSOLE

Als Teil einer integrierten Sicherheitsplattform ermöglicht Kaspersky Security for Mobile die zentrale Verwaltung von Smartphones und Tablets zusammen mit herkömmlichen Endpoints. Hierdurch erhält der Administrator einen besseren Überblick über alle unternehmensinternen IT-Ressourcen und kann einfacher einheitliche und universell gültige Richtlinien festlegen und umsetzen. Hinzu kommt, dass die Abteilung durch diese effizientere Verwaltung und Instandhaltung mehr Zeit hat, sich auf andere Aspekte des Unternehmens zu konzentrieren.



LIZENZIERUNG

Kaspersky Security for Mobile ist Teil von:

- **Kaspersky Endpoint Security for Business – Select**: Einschließlich Endpoint- und File-Server-Sicherheit sowie Kontrolltools und Mobilitätsfunktionen.
- **Kaspersky Endpoint Security for Business – Advanced**: Enthält alle Funktionen von Select plus zusätzliche Features, einschließlich Verschlüsselung, Patch Management, erweiterte Verwaltungsfunktionen und Mobilitätsfunktionen.
- **Kaspersky Total Security for Business**: Eine umfassende Endpoint-Schutzplattform, die sämtliche Funktionen der anderen Stufen enthält plus Schutz für Web und Messaging sowie Mobilitätsfunktionen.
- **Kaspersky Security for Mobile als Targeted Solution**: Schutz und Verwaltung von mobilen Endpoints mithilfe der mobilen Sicherheitstechnologien von Kaspersky Lab in Form einer eigenständigen, separat erhältlichen Lösung.

SICHERHEIT, ÜBERSICHT UND VERWALTUNG FÜR UNTERNEHMENSEIGENE UND BYOD-ENDGERÄTE ÜBER EINE ZENTRALE BENUTZEROBERFLÄCHE

Kaspersky Security for Mobile gewährleistet, dass Ihre Geräte sicher sind, egal wo sich diese befinden und ob es sich dabei um unternehmenseigene oder BYOD-Endpoints handelt. Schaffen Sie sich schnell und problemlos einen Überblick über die Smartphones und Tablets innerhalb Ihrer Umgebung – von einer zentralen Konsole aus, bei minimaler Beeinträchtigung.

Verschaffen Sie sich den benötigten Überblick – Ersparen Sie sich das Rätselraten, den Status jedes einzelnen Geräts zu ermitteln. Verschaffen Sie sich einen zuverlässigen Überblick über die mobilen Endgeräte, mit denen Ihre Mitarbeiter auf die Ressourcen des Unternehmens zugreifen.

Minimieren Sie das Risiko von Datenverlusten durch gestohlene Geräte oder Malware – Aktivieren Sie mobile Schutzfunktionen, die garantieren, dass die Geräte und die darauf gespeicherten Daten optimal geschützt sind.

Reduzieren Sie den IT-Verwaltungsaufwand – Schützen Sie mobile Endgeräte und herkömmliche Endpoints zusammen über ein und dieselbe zentrale Verwaltungskonsole, die Teil einer integrierten IT-Sicherheitsplattform ist.


Twitter.com/
Kaspersky_DACH


Facebook.com/
Kaspersky.Lab.DACH


Youtube.com/
KasperskyLabCE

Kaspersky Lab
www.kaspersky.de

Informationen zur
Internetsicherheit:
www.securelist.com

Informationen zu Partnern in
Ihrer Nähe finden Sie hier:
www.kaspersky.de/buyoffline

March 15/Global

KASPERSKY lab