IKARUS mobile.security for MDM Handbuch

IKARUS mobile.security for MDM

IKARUS Security Software GmbH
Blechturmgasse 11
1050 Wien
Austria

© IKARUS Security Software GmbH

www.ikarussecurity.com

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

1

Einführung

Dies ist das Handbuch für IKARUS mobile.security for MDM, die Android AntiViren und Web-Security Lösung entwickelt von IKARUS Security Software für Mobile Device Management (MDM) Systeme. Die Zielgruppe dieses Dokuments sind IT Administratoren von Unternehmen welche IKARUS mobile.security for MDM entweder in Ihr eigenes oder in ein MDM System von Drittanbietern integrieren wollen.

Die Version der IKARUS mobile.security, welche man auf Google Play und auf der IKARUS Website findet, ist für Endkunden. Das Endkundenprodukt ist nicht für gewerbliche geeignet Zwecke und unterscheidet sich von der MDM Version in folgenden Aspekten:

- Um alle Features der Vollversion nach einer 30-Tage Testversion zu nutzen, muss eine Lizenz über Google Play gekauft werden oder man erwirbt einen Aktivierungscode direkt bei IKARUS oder einem unserer Partner. In der MDM Version wird ein signiertes Lizenz-File auf das Gerät gepusht. Das Auslaufdatum der Lizenz wird vorher mittels eines Vertrags festgelegt.
- Features welche:
  - ✓ im Endkundenbereich von Nutzen sind
  - ✓ viele Eingriffe durch den User benötigen um sie korrekt zu konfigurieren
  - ✓ bereits in ein MDM System integriert sind

wurden aus der IKARUS mobile.security for MDM entfernt. Konkret sind die Remote Control Funktionen per SMS (Gerät sperren, lokalisieren, zurücksetzen und Alarm auslösen), die SMS-Blacklist, die SIM-Card-Tauscherkennung und der USSD Schutz nicht mehr enthalten.

- Das User Interface ist einfacher in der MDM Version.
- In der MDM Version hat der User nicht die Möglichkeit Einstellungen zu verändern; stattdessen übermittelt der MDM Administrator ein signiertes Configuration-File auf das Gerät welches durch die App erkannt wird.
- Es gibt kein System für automatische Upgrades der MDM Version, da dies normalerweise vom Google Play Dienst der Android Plattform übernommen wird. Das MDM muss neue Versionen der App selbst an die Endgeräte verteilen sobald sie die neue Version von IKARUS erhalten haben. Normalerweise passiert dies ein paar Mal im Jahr um Verbesserungen und Optimierungen einzubauen.
  Dies ist unabhängig von den Datenbankupdates (z.B. Virendatenbank), welche automatisch mehrmals am Tag stattfinden.
- Die MDM App ist nicht auf Google Play zum Download verfügbar.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

- In der MDM Version gibt es bei der Funktion URL-Filtering zusätzlich kundenspezifische Black- und Whitelists
- In der MDM Version wurden zusätzlich Bedrohungsstatistiken inkludiert.

Deswegen sind IKARUS mobile.security und IKARUS mobile.security for MDM zwei komplett unterschiedliche Produkte, mit gewissen gleichen Basiskomponenten, aber mit zwei unterschiedlichen Zielen und Zielgruppen und mit unterschiedlichem Handling.[1]

In Kapitel 2 finden sie alles zu Lizenzmöglichkeiten, in Kapitel 3 werden die Features (Virus-Scan, URL-Filtering und Bedrohungsstatistiken) der App erklärt und in Kapitel 4 werden Strategien wie man Lizenzen und App-Konfigurationen zum Endgerät bringt erklärt und ein Hilfstool von IKARUS zur Vereinfachung dieser Aufgaben beschrieben.

```
----- BEGIN IKARUS SOFTWARE LICENSE -----
product IMSMDM
serialnumber HF2517216
owner Your Company
describtion IKARUS mobile.security MDM
startdate 2013-11-20
enddate 2014-11-30
features scanonaccessapp ; scanondemandapp ; scanondemandfull
----- SIGNATURE -----
PLGdDZIzjDhX8ANF28CwW7jAp8LWfZ++2q1xGN6xkHMej2Ac+8gLl l ro fpT /9VpiJQ0
h6VMwjXAD5qVYVnpyO4FV7MdNyofFkXvbw0l6RN4kexMnOmihDTeDslFObfB4xtRuak
uxhZJAsadzeq8lhJnt9wqjkTgOmS+FHEHqC1E=
----- END IKARUS SOFTWARE LICENSE ------
```

Abbildung 1: Ein Beispiel eines Lizenz-Files

Es ist ein Textdokument mit integrierter digitaler Signatur. Sie erhalten dieses Dokument wenn Sie die Software bei IKARUS gekauft haben und müssen diese später auf den Endgeräten verteilen.

1 Es ist technisch möglich beide Versionen am selben Gerät zu betreiben. Trotz eines nach außen hin identisch angezeigten Namens unterscheiden sich die beiden Versionen in der Art wie sie sich im Betriebssystem registrieren. Wir haben jedoch bisher keinen praktischen Nutzen erkannt, wieso dies sinnvoll sei.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

2

Lizenzierung

Im Vorfeld einigen sich IKARUS und der Kunde in einem Vertrag auf eine Lizenz für IKARUS mobile.security for MDM. IKARUS übermittelt dann ein digital signiertes Lizenzfile, wie in Abbildung 1 abgebildet, welches das vorher vereinbarte Ablaufdatum der Lizenz festlegt. Das File muss zu jedem Endgerät, welches IKARUS mobile.security for MDM nutzt oder nutzen wird, transferiert werden. In Kapitel 4 werden mögliche Strategien zu diesem Thema erläutert.

Aber die Lizenz beinhaltet nicht nur das Ablaufdatum, sondern legt auch fest welche Features gekauft und genutzt werden können. Jedoch ist es nicht sehr wichtig weil normalerweise Lizenzen mit allen Features gekauft werden. Wenn Sie denken, dass Sie von einer detaillierteren Lizenzierung profitieren, kontaktieren Sie bitte die IKARUS Sales Abteilung. Kapitel 3 erklärt alle verfügbaren Features im Detail.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

3

App Features

IKARUS mobile.security for MDM bietet Ihnen drei Möglichkeiten Sie beim Schutz Ihrer Endgeräte zu unterstützen: Virenscanner, URL-Filter und Bedrohungsstatistiken (Interface). Der Virenscanner, welcher in Kapitel 3.2 genauer erklärt wird, scannt auf dem Endgerät nach Viren. Mithilfe des URL-Filters, welcher in Kapitel 3.3 genauer erklärt wird, werden gefährliche Websites blockiert. Bei den Bedrohungsstatistiken, erklärt in Kapitel 3.4, kontaktieren die Endgeräte den Server, um ihn über Virenfunde oder gefährliche URL-Aufrufe zu informieren.

Sie werden feststellen, dass das grafische User-Interface, gezeigt in Abbildung 2, der App sehr schlank gehalten ist. Da die App dafür gedacht ist mit einer MDM Software konfiguriert und administriert zu werden, hat der End-User fast nichts zu tun. Auf dem Endgerät können nur weitere Scans und Datenbankupdates gestartet werden, alles andere kann nur der Administrator erledigen.

3.1 Updates

Beides, der Virenscanner und der URL-Filter funktionieren nur zuverlässig wenn sie regelmäßig an die aktuellen Bedrohungsszenarien angepasst werden. Um dies zu erreichen, bietet IKARUS mehrmals am Tag ein Datenbank-Update zum Download an, welches sich die App jederzeit herunterladen kann. Die Datenbank beinhaltet Virendefinitionen und URLs welche als gefährlich eingestuft werden.[2] Der Transfer der Datenbank vom IKARUS Webserver funktioniert mit einer gewöhnlichen Internetverbindung. Beim Update-Vorgang ist die MDM-Software nicht involviert. Updates können manuell durch den Enduser ausgelöst werden oder der MDM-Administrator konfiguriert einen automatischen Update-Intervall, wie in Kapitel 4.2 erklärt. Wenn der User die App manuell aktualisiert, klickt er in der App auf den Button „AntiVirus“ und klickt dort auf „Update“. Automatische Updates sind jedoch in Unternehmensumgebungen sinnvoller. Dieser Vorgang wird von der MDM Software erledigt. Dort wird ein bestimmtes Intervall definiert, indem die App beim IKARUS Server überprüft ob neue Updates zur Verfügung stehen. Siehe dazu Kapitel 4.2.

[2] Manchmal werden zusätzlich auch die IKARUS T3.scan.engine und die AntiSPAM Engine, welche für das URL-Filtering benötigt werden, aktualisiert. Diese beiden Komponenten werden nicht sehr häufig, normalerweise ein paar Mal im Jahr, aktualisiert.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Die letzte Version mit allen aktualisierbaren Komponenten wird vom IKARUS Server beim ersten Start der App heruntergeladen.

Beachten Sie bitte, dass das Upgrade der App selbst eine völlig andere Angelegenheit ist! App-Upgrades sind sehr selten und die MDM Software muss diese verteilen. Dies erfordert einen Gerätemanagement-Mechanismus welcher dafür geeignet ist. IKARUS wird Sie kontaktieren wenn eine neue Version der App für die Kunden verfügbar ist.

3.2 Virenscanner

Der Virenscanner analysiert installierte Apps auf dem Gerät und untersucht alle Files in öffentlich zugänglichen Dateisystem (wie die SD-Card oder heruntergeladene Dateien von Websites). Um dies erledigen zu können wird eine Virendatenbank (VDB) verwendet. Diese wird ständig aktuell gehalten und warnt den Nutzer im Falle eines Fundes.

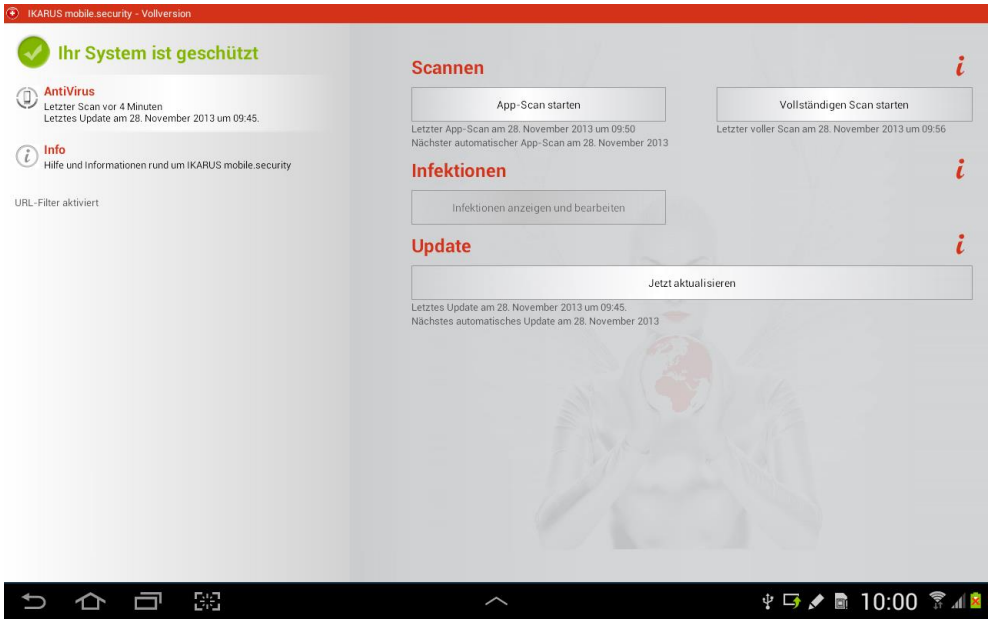

Abbildung 2: Startbildschirm der App auf einem Android Tablet

Die App bietet wenige Enduser-Mitwirkungsmöglichkeiten weil die App dafür gedacht ist über ein MDM administriert zu werden. Trotzdem kann der User weitere Scans und Datenbankupdates jederzeit starten.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Die folgenden Scans werden unterstützt:

- On-Demand-Scan durch den User
  Der User navigiert in der App zum Punkt „AntiVirus“ und klickt auf „App-Scan starten“ oder „Vollständigen Scan starten“. Der erste scannt nur die Apps welche auf dem Gerät installiert sind und der zweite scannt zusätzlich auch noch alle öffentlich zugänglichen Dateien (wie von der SD-Card oder dem internen Speicher).
- Automatische On-Demand-Scans mit gewissen Intervallen durch den MDM-Administrator festgelegt
  Auch hier können Sie zwischen einen App-Scan oder einen Vollständigen Scan auswählen.
- On-Access-Scan
  Die App überprüft proaktiv Apps wenn sie heruntergeladen oder aktualisiert werden und scannt alle neuen Dateien auf dem Endgerät (wie Dateien die auf die SD-Karte kopiert werden oder mit einem Web-Browser heruntergeladen werden).

Wenn ein Virus gefunden wird, erscheint eine Vollbild-Warnung, wie in Abbildung 3 gezeigt, und der User wird gefragt ob die infizierte Datei gelöscht werden soll. Alle Virenscans basieren auf der Datenbank und der IKARUS T3.scan.engine, welche auf dem Gerät vorhanden sind.

Andere Möglichkeiten im Falle einer Infektion sind:

- Ignorieren
  Wenn der User sich der Gefahr bewusst ist oder sich absolut sicher ist, dass das Scan-Ergebnis falsch ist kann die App oder die Datei auf die Whitelist gesetzt werden sodass sie beim nächsten Scan ignoriert wird.
- Datei zu MDM-Administrator senden
  Der User kann eine infizierte Datei als E-Mail Anhang zu einer E-Mail-Adresse, die vorher in der MDM Software festgelegt wurde schicken. Sie können eine manuelle Analyse durchführen oder Sie konfigurieren die App, sodass die Infektionen direkt in das IKARUS Malware-Analyse-Labor geschickt werden können. Siehe dazu Kapitel 4.2.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

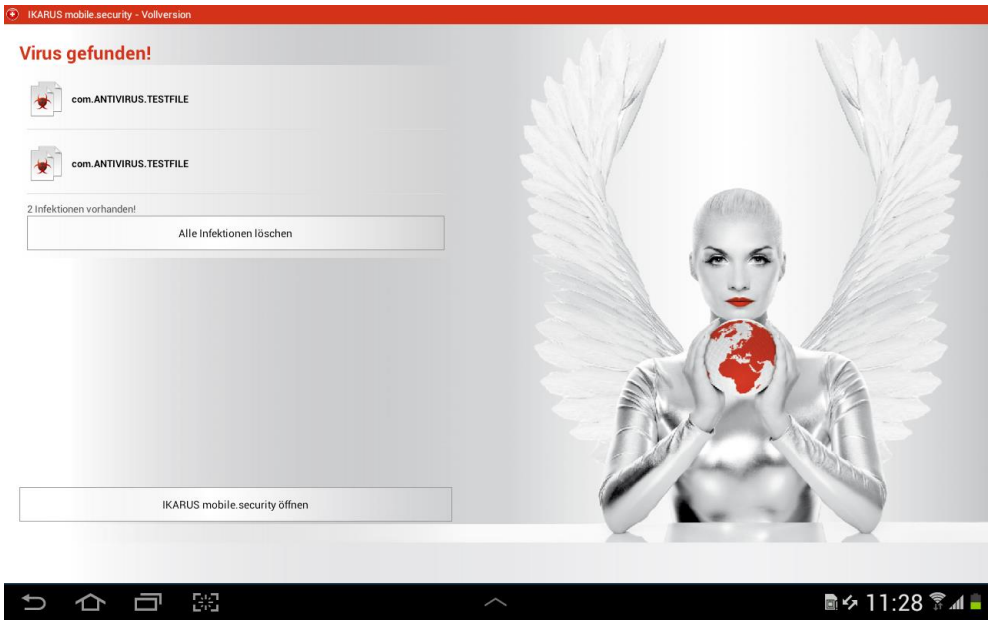

Abbildung 3: Warnung bei Virusfund

Wenn ein Virus durch die IKARUS App gefunden wird, sieht der User eine Vollbild-Warnung und kann die infizierte Datei oder App sofort löschen. Er kann die Infektion aber auch temporär ignorieren oder die Infektion zur Analyse an den MDM-Administrator oder an das IKARUS-Malware-Analyse-Labor senden.

Der Bereich „AntiVirus“ in der App beinhaltet auch eine Infektionsliste welche dem User mögliche Viren am Gerät anzeigt. Hier können auch Dateien, welche eindeutig keine Gefahr für das Gerät darstellen, wieder aus der Infektionsliste entfernt werden.

Auf Anfrage (siehe Kapitel 4.2), kann im Hintergrund ein Service namens „Signature Quality Assurance“ aktiviert werden. SigQA ist ein Tool zur anonymem Verarbeitung von Virusstatistiken, durch unsere Malwareanalysten um die Scanqualität zu verbessern. Wenn SigQA aktiviert ist, werden im Hintergrund anonyme Daten an einen IKARUS Server übertragen.

Dateien und Apps werden möglicherweise als Virus klassifiziert weil sie in einer Internet-URL enthalten sind, die als Adware kategorisiert ist. Wenn eine Infektion aufgrund einer Internet-URL erkannt wurde, wird die betreffende URL neben der Datei in der Infektionsliste angezeigt.

3.3 URL-Filter

Der URL-Filter ist ein voll automatisierter Webschutz-Mechanismus. Die Klassifikation ob eine Website gefährlich ist basiert auf einer URL Datenbank. Die App nutzt prinzipiell die aktuelle Version der Datenbank und der AntiSPAM Engine am Endgerät.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

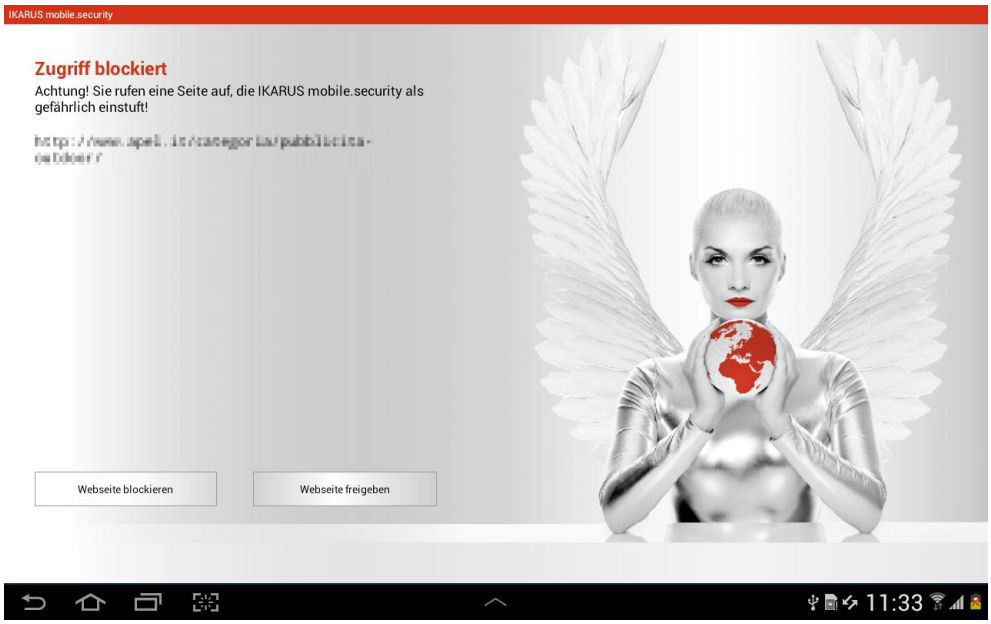

Abbildung 4: Zugriff blockiert – gefährliche Website erkannt

Die App erkennt verdächtige Seiten aus der IKARUS Datenbank oder von der eigenen Blacklist wenn der User versucht diese mit dem Browser zu öffnen. Eine Vollbild-Warnung wird angezeigt und der User hat die Möglichkeit trotzdem die Seite anzeigen zu lassen oder die Website zu blockieren. Diese Auswahl wird solange gespeichert bis das Gerät neugestartet wird.

Manuelles hinzufügen von URLs oder Domains (Blacklists) oder URLs und Domains ausnehmen (Whitelists) ist auch möglich; Kapitel 4.2 enthält Erklärungen wie sie solche spezifischen Einträge hinzufügen können. Zum Beispiel können Sie auf ihre Blacklist die URLs „facebook.com;youtube.com“ setzen und auf ihre Whitelist „example.org;example.com;example.net“ setzen.

Die Whitelist gilt für eigene Blacklist-Einträge und die IKARUS Datenbank. Wenn also auf der Blacklist „facebook.com;youtube.com“ eingetragen ist und auf der Whitelist „example.org;youtube.com“ wird youtube.com vom URL-Filter nicht beachtet.

Wenn eine URL als gefährlich eingestuft ist und im Browser geöffnet wird, erscheint eine Warnung und der User wird gefragt ob die Seite angezeigt oder geblockt werden soll. Abbildung 4 zeigt was der User sieht wenn dies passiert. Das temporäre Freischalten der Website gilt nicht für immer, nur so lange bis das Endgerät das nächste Mal neu gestartet wird.

Der URL-Filter funktioniert mit dem Android-Standardbrowser und Google Chrome, ABER nicht mit anderen Browsern wie Firefox oder Opera.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

3.4 Bedrohungsstatistiken

Um diese Bedrohungsstatistiken zu erhalten wird zunächst im Hintergrund ein anderer Vorgang in Gang gesetzt: Die App kontaktiert einen bestimmten Server sobald ein Ereignis auftritt (z.B.: „Virus gefunden“ oder „Besuch einer gefährlichen Website“). Ein Business-Kunde kann auf einfachste Weise eine Server-Applikation schreiben um die Daten abzurufen und Statistiken von einer Device-by-Device Basis zu generieren.

Die App bietet ein Interface welches von bestimmten Server-Applikationen genutzt werden kann um Statistiken für Bedrohungen von Infektionen und gefährlichen URLs erstellen zu können. Dieses Feature funktioniert mit einer HTTP Verbindung zu der in der Konfiguration festgelegten Server-Adresse; siehe Kapitel 4.2.

Bei bestimmten Ereignissen in der App wird eine HTTP Anfrage mit bestimmten Daten inklusive Geräte-Identifikation (IMEI) generiert. Mit diesem Mechanismus ist es beispielsweise möglich zu erkennen, welche Viren auf welchen Geräten aufgetaucht sind und welche URLs blockiert wurden. Wenn der Server zur Zeit des Ereignisses nicht erreichbar ist (was im mobilen Kontext oft der Fall sein kann), werden die Daten lokal gespeichert und ein neuer Sendeversuch wird jeden Tag automatisch ausgelöst.

Erkannte Infektions-Ereignisse sind:

- Virus gefunden,
- Virus gelöscht,
- Virus ignoriert,
- Datei/App freigegeben.

Erkannte URL-Filter-Ereignisse sind:

- gefährliche URL gefunden,
- gefährliche URL blockiert,
- gefährliche URL nicht blockiert.

Es können verschiedene Server URLs für die verschiedenen Infektions- und URL-Filter-Ereignisse definiert werden.

In der URL für Infektions-Ereignisse können die folgenden Parameter, jedes mit einem vorhergehenden Dollar-Zeichen, definiert werden:

- action (= found, removed, ignored oder unignored)
- imei
- filename
- signatureName
- signatureId
- packageName
- url (wenn eine Datei als Virus erkannt wird weil sie in einer bestimmten URL enthalten ist)
- when

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Zum Beispiel wird in der Konfiguration folgende Anfrage Adresse als Template festgelegt:

```
http://www.example.com/notify?event=$action&filename=$filename&device=$imei
```

Nun nehmen wir an ein Virus „malicious file.apk“ wurde gefunden auf einem Gerät mit der IMEI 12345. Das Ergebnis der Anfrage URL würde so aussehen:

```
http://www.example.com/notify?event=found&filename=malicious\%20file.apk&
device=12345
```

URL-Filter funktionieren mit der gleichen Methode, bieten aber andere Parameter:

- action (=hit, blocked oder not blocked)
- imei
- url
- when

Um diese Funktionen vollständig zu nutzen muss der Kunde eine serverseitige Unterstützung implementieren. IKARUS stellt in diesem Fall nur die Funktionen auf der Client-Seite zur Verfügung.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

4

Verteilung

Der Verteilungsprozess für IKARUS mobile.security for MDM involviert zwei Installations-APK-Pakete:

- IKARUS mobile.security.apk

die aktuell, arbeitende Haupt-App. Diese wird direkt von IKARUS bereitgestellt.

- MDMHelper.apk

eine Hilfs-App, welche die Haupt-App mit Lizenz- und Konfigurationsinformationen versorgt. Diese wird von Ihnen mithilfe eines IKARUS-Tools, welches in den nächsten Kapiteln erklärt wird, erstellt.

Beide Apps müssen, wie jede andere App, mithilfe der MDM Software auf die Endgeräte verteilt werden. Sie müssen sicherstellen, dass die Enduser nicht nur die App installieren sondern sie zumindest einmal nach der Installation einschalten. Die Befehle mit dem die Apps installiert und gestartet werden spielen keine Rolle.

Beachten Sie dass die Haupt-App nach einem Neustart des Geräts automatisch gestartet wird aber zuvor muss diese einmal durch den User geöffnet werden weil dies mit allen proaktiven Android-Apps so ist.

Die Hilfs-App beinhaltet eine Lizenz und eine Konfiguration. Es braucht also jede Lizenz- und Konfigurations-Kombination oder jede Änderung eine andere Hilfs-App. IKARUS stellt deswegen ein Tool zum Erstellen von Hilfs-Apps zur Verfügung.

Dieses Tool ist inkludiert wenn sie IKARUS mobile.security for MDM erhalten. Es ist ein ausführbares Kommandozeilen-Java-Programm-Tool mit dem Namen „create-ikarus-mdmhelper.jar“ und es wird eine voll funktionierende, installierbare und ausführbare Hilfs-App APK mit inkludierter Lizenz und Konfiguration erstellen, wenn Sie dem Tool drei Dinge geben:

- Ein Zertifikat für die Hilfs-App mit Password und Alias in Form einer Datei. Dies kann in nur einem Schritt mithilfe der Android SDK Tools erledigt werden. Sie können es einmal erstellen und dann immer wieder verwenden. Alternativ kann IKARUS Ihnen auch ein Zertifikat erstellen. Der Name der Datei endet normalerweise mit „.keystore“. Kapitel 4.1 erklärt diesen Schritt genauer.
- Ein gültiges Lizenz-File (vorher signiert durch IKARUS und mit der Auslieferung der IKARUS mobile.security for MDM von IKARUS erhalten). Der Name der Datei endet normalerweise mit „.ikkey“. Lesen Sie Kapitel 2 für mehr Informationen zum Thema Lizenz-File.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

- Ein Konfigurations-File welches ihre benutzerdefinierten Einstellungen enthält. Die Datei wird später automatisch mithilfe dieses Tools signiert. Der Name der Datei endet normalerweise mit „.config“. Kapitel 4.2 erläutert die Konfigurationsmöglichkeiten.

```
automaticScansEnabled=true
automaticScansInterval=50000000
automaticScansMethodFull=false
automaticUpdatesEnabled=true
automaticUpdatesInterval=5000000
appProtectionActivated=true
sdCardProtectionActivated=true
updateOnlyWifi=true
sigqaActive=false
webFilteringEnabled=true
customUrlBlacklist=facebook.com;youtube.com
customUrlWhitelist=example.org;example.com;example.net
sendInfectionRecipient=mymail@myorganisation.com
infectionProtocolUrl=http://www.myorganisation.com/notifyVirus?event=$action&filename=
$filename&device=$imei
urlFilterProtocolUrl=http://www.myorganisation.com/notifyUrl?event=$action&device=
$imei&time=&when
```

Abbildung 5: Beispiel für ein Konfigurations-File

Der MDM Administrator schreibt diese Datei und benutzt dabei die möglichen Optionen aus Tabelle 1 im parameter=value Format. Die Datei wird digital signiert und in die Hilfs-App mithilfe des Spezial-Verteilungs-Tools von IKARUS eingebettet.

Die folgenden Kapitel erklären die Schritte um eine Hilfs-App zu erstellen und zu verwenden.

4.1 Erstellen Ihres Hilfs-App Schlüssel

Die offizielle Android Dokumentation auf http://developer.android.com/tools/publishing/app-signing.html beinhaltet eine umfangreiche Anleitung zum Signieren von Apps. Das Signieren ist aufgrund der Sicherheitsrichtlinien so wichtig, denn nicht signierte Apps können normalerweise auf dem Endgerät nicht installiert oder ausgeführt werden.

Sie können entweder ein Zertifikat mit privatem Key selber erstellen oder Sie fragen bei IKARUS an. Die erste Lösung gewährt eine bessere Sicherheit für ihren Key, die zweite Lösung ist vielleicht bequemer für Ihr Unternehmen.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Das Erstellen eines eigenen Zertifikats wird einen Kommandozeilen-Befehl wie diesen voraussetzen:

```
keytool –genkey –v –keystore MDMHelper.keystore –alias MDMHelper-keyalg RSA –
keysize 2048 –validity 10000
```

Wenn Sie aufgefordert werden, vergeben Sie ein Passwort und lassen alle anderen Daten leer.

Für mehr Details ziehen Sie die Android Dokumentation heran. In jedem Fall benötigen Sie später die Datei („MDMHelper.keystore“, wenn wir das Beispiel von oben heranziehen), das Passwort und das Alias.

4.2 Konfiguration

Der Enduser kann keine Einstellungen am Gerät vornehmen; jede Konfiguration der App wird exklusiv nur vom MDM-Administrator vorgenommen. Wenn der Administrator ein Set von Konfigurationen erstellen möchte, dann schreibt er diese in eine Textdatei wie in Abbildung 5 gezeigt.

Tabelle 1 zeigt eine komplette Liste aller unterstützten Parameter im Konfigurations-File. Jeder Parameter hat einen Default-Wert, welcher von der App verwendet wird wenn diese im Konfigurations-File nicht anders definiert wird. Weiters hat jeder Parameter einen Typ. Bei einem „Boolean“-Typ kann man beispielsweise Optionen nur aktivieren oder deaktivieren, bei einem „Long“-Typ kann eine (möglicherweise sehr lange) Integer Nummer eingegeben werden und in ein Feld mit dem Typ „String“ können Sie Text einfügen. Für jeden Wert der im Konfigurations-File festgelegt wird, überprüft die App ob die Definition dem Parameter-Typ entspricht.

String-Werte müssen nicht unter Anführungszeichen stehen. Zum Beispiel wenn Sie festlegen möchten, dass eine Infektion zu einer bestimmten E-Mailadresse geschickt werden brauchen Sie folgendes Kommando im Konfigurations-File:

```
sendInfectionRecipient=email@example.com
```

Es würde nicht funktionieren, wenn Sie diese Zeile eintippen:

```
sendInfectionRecipient=“email@example.com“
```

Automatische Scans und Updates können auf Millisekunden genau eingestellt werden und bieten damit den Administratoren einen sehr feinkörnigen Kontrollmechanismus. Zum Beispiel bedeutet die Zahl 86400000 „täglich“, weil 1000 Millisekunden = 1 Sekunde, 60 Sekunden = 1 Minute, 60 Minuten = 1 Stunde, 24 Stunden = 1 Tag und damit 1000 x 60 x 60 x 24 = 86400000

Der User kann das Konfiguration-File unter dem Punkt „Info“ in der App einsehen (aber nicht verändern). Administratoren können diese Information verwenden um sicherzustellen, dass die Konfigurationen korrekt angewandt worden sind.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

4.3 Verteilen Ihrer Hilfs-App

Das Tool um Ihre Hilfs-App zu erstellen ist eine Java-Kommandozeilen-Anwendung mit dem Namen „create-ikarus-mdmhelper.jar“.

In seiner Grundform stützt sich das Programm auf die Standartwerte und Standartdateinamen („license.ikkey“ für das Lizenz-File und „ikarus.config“ für das Konfigurations-File) und wird mit diesem Befehl ausgeführt:

```
java –jar create-ikarus-mdmhelper.jar –storepass YourKeyStorePassword
```

“YourKeyStorePassword” ist das Passwort welches Sie beim Erstellen des Zertifikats vergeben haben.

Das Tool wird aufgrund dieses Befehls die App „MDMHelper.apk“ erstellen. Die App muss vom MDM-Administrator verteilt werden und die User müssen die App starten.

Wenn die App gestartet wird verteilt es die Lizenz und die Konfiguration am Gerät, sodass die eigentliche App diese automatisch verwendet.[3]

[3] Die technische Implementierung des Lieznz- und des Konfigurations-Files erfolgt an einem öffentlichen Dateisystem des Endgeräts. Die IKARUS mobile.security for MDM App holt sich die Daten von dort. Diese Dateien können dort in jeder technisch möglichen Weise platziert werden. Ihre MDM Software unterstützt möglicherweise einen direkten Datentransfer. Weitere Möglichkeiten sind: E-Mailversand an den User oder Anbieten eines Downloads der Dateien. Allerdings würden diese Ansätze für Ihr Unternehmen möglicherweise ungeschickt oder unangebracht sein. Die Hilfs-App hilft den technischen Aufwand zu minimieren und ist dazu wenig fehleranfällig.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Name	Beschreibung	Typ	Default
automaticScansEnabled	Sind geplante automatische Scans aktiviert?	Boolean	false
automaticScansInterval	Intervall für automatische Scans in Millisekunden	Long	86400000
automaticScansMethodFull	Sind geplante automatische Scans vollständige Scans?	Boolean	false
automaticUpdatesEnabled	Sind geplante automatische Updates aktiviert?	Boolean	true
automaticUpdatesInterval	Intervall für automatische Updates in Millisekunden	Long	43200000
appProtectionActivated	Sind automatische App-Scans aktiviert?	Boolean	true
sdCardProtectionActivated	Sind automatische Scans für externe Medien aktiviert?	Boolean	true
updateOnlyWifi	Sollen Updates nur über Wi-Fi gemacht werden?	Boolean	false
sigqaActive	Ist SigQA aktiviert?	Boolean	true
webFilteringEnabled	Ist der URL-Filter aktiviert?	Boolean	false
customUrlBlacklist	Eigene URL-Blacklist (getrennt durch einen Strichpunkt)	String	
customUrlWhitelist	Eigene URL-Whitelist (getrennt durch einen Strichpunkt)	String	
sendInfectionRecipient	Infektions-Empfänger-E-Mail – User schicken Ihnen Infektionen zur Analyse	String	
infectionProtocolUrl	Bedrohungsstatistik-URL für Infektionsereignisse	String	
urlFilterProtocolUrl	Bedrohungsstatistik-URL für URL-Filter-Ereignisse	String	

Tabelle 1: Verfügbare Konfigurationsmöglichkeiten

Diese können im Konfigurations-File durch den MDM-Administrator genutzt werden. Der Default-Wert wird von der App verwendet wenn im Konfigurations-File nichts festgelegt wird. Bei einem „Boolean“-Typ kann man Optionen nur aktivieren oder deaktivieren, bei einem „Long“-Typ kann eine (möglicherweise sehr lange) Integer Nummer eingegeben werden und in ein Feld mit dem Typ „String“ können Sie Text einfügen.
Abbildung 5 zeigt ein Beispiel eines Konfigurations-Files, welches einige dieser Optionen nutzt.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

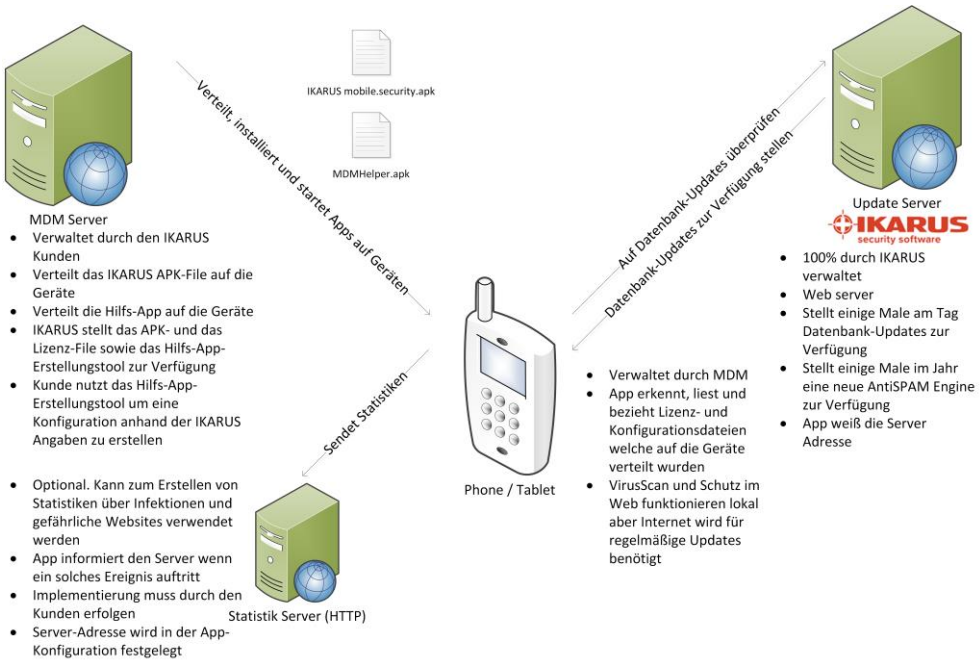

Abbildung 6: Funktionsweise IKARUS mobile.security for MDM

Die Server interagieren miteinander und mit dem Android-Gerät und bilden damit die Sicherheitsarchitektur. Der MDM-Server kümmert sich um die Verteilung der IKARUS App und die Hilfs-App auf die Endgeräte. Die IKARUS App kontaktiert in regelmäßigen Abständen den IKARUS Update Server für Datenbankupdates und optional sendet die App auch Infos für die Bedrohungsstatistiken an einen anderen benutzerdefinierten Server.

An diesem Punkt könnte die Hilfs-App auch wieder deinstalliert werden weil sie dann nicht mehr gebraucht wird. Wenn Sie die Hilfs-App auf dem Gerät lassen und der User öffnet sie wieder richtet die Hilfs-App keinen Schaden an.

Abbildung 6 stellt das MDM System mit allen wichtigen Komponenten dar: Der MDM-Server verteilt zwei Apps auf das Endgerät, der IKARUS-Update-Server versorgt die App mit aktuellen Datenbank-Updates, der Bedrohungsstatistik-Server empfängt die Statistiken des Endgeräts und das Endgerät selbst im Zentrum der Informationsfluss.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

5

Kontakt

IKARUS Security Software GmbH

Blechturmgasse 11
1050 Wien
Österreich

Telefon: +43 (0) 1 58995-0
Fax: +43 (0) 1 58995-100

office@ikarus.at
www.ikarussecurity.com

IKARUS Security Software Support Kontakt

Telefon: +43 (0) 1 58995-400
Support-Zeiten: Mo bis Do: 8.00 – 18.00 (MEZ)
Fr: 8.00 – 15.00 (MEZ)
E-Mail: support@ikarus.at

IKARUS Security Software Sales Kontakt

Telefon: +43 (0) 1 58995-500
E-Mail: sales@ikarus.at