TRUST IN GERMAN SICHERHEIT

G DATA TechPaper #0173

Mobile Device Management

G DATA CyberDefense AG | September 2019

Inhalt

1. Einführung

Bisher haben Administratoren von Unternehmensnetzwerken und Systemadministratoren immer homogene Gruppen von Client-Geräten administriert. Bei der Planung und Bereitstellung von Netzwerk-Clients befasste man sich fast ausschließlich mit Desktop-Computern. Diese voraussehbaren Gegebenheiten vereinfachten die Bereitstellung der Netzinfrastruktur, der Client-Hardware und der Anwendungen. So war die Einheitlichkeit bei allen Netzwerkgeräten gewährleistet. Seit jedoch Smartphones und Tablets den Bereich Consumer Electronics im Sturm erobert haben, ist die Technologielandschaft erheblich komplizierter geworden. Durch Trends wie die Consumerization der IT und „Bring Your Own Device“ (BYOD) hat eine Vielzahl unterschiedlicher Geräte in Unternehmen Einzug gehalten. Administratoren sehen sich nun mit der Aufgabe konfrontiert, einen breitgefächerten Zugang zu den Ressourcen anzubieten und gleichzeitig die Sicherheit zu gewährleisten. Dieses technische Dokument soll Trends in der Nutzung von Smartphones und Tablets in Unternehmensnetzwerken darlegen (Kapitel 2) und praktische Management-Strategien für Administratoren aufzeigen, die sich mit der wachsenden Nutzung von Mobilgeräten beschäftigen müssen (Kapitel 3). Kapitel 4 beschreibt die Nutzung von G DATA Mobile Device Management.

2. Mobile Endgeräte im Unternehmen

Neue Technologien halten in Unternehmen wesentlich langsamer Einzug als bei privaten Anwendern. Selbst wenn ein Produkt auf einfache Weise in Workflows integriert werden kann, muss es auf Kompatibilitätsprobleme mit der Unternehmensinfrastruktur getestet werden – ein Prozess, der sehr kostenintensiv und zeitaufwändig sein kann. Seit Apple die Kategorie der Mobilgeräte mit den Produkteinführungen von iPhone und iPad populär gemacht hat, zeigen sich Hunderte Millionen Privat- und Geschäftskunden gleichermaßen begeistert von der Kombination aus fortschrittlicher Technologie und Benutzerfreundlichkeit der Geräte. Viele Unternehmen tun sich jedoch noch immer schwer damit, diese Geräte auf angemessene Weise in die Unternehmensumgebung zu integrieren. Diese Verzögerungen bei der Einführung führen häufig zu Spannungen, da sich die Erwartungen der Endanwender nicht mit der derzeit gebotenen Funktionalität der Unternehmenslösungen decken. Zwei wichtige Trends in der IT-Landschaft der Unternehmen veranschaulichen dieses Dilemma: Consumerization der IT und „Bring Your Own Device“ (BYOD).

Die Consumerization der IT, also der Einfluss privat genutzter Consumer-Geräte auf IT-Lösungen von Unternehmen, ist immens gewachsen. Die Endanwender sind mittlerweile daran gewöhnt, ständig mobilen Zugang zum Internet zu haben und cloud-basierte Messaging- und E-Mail-Lösungen sowie zahlreiche Apps zu nutzen, mit denen die mobile Gerätenutzung den eigenen Anforderungen entsprechend gestaltet werden kann. Obwohl kein Administrator die sehr praktische Seite dieser Dienste bestreiten würde, stehen einige der dadurch erzielten Vorteile im Widerspruch zu den IT-Strukturen im Unternehmen. Die Geschwindigkeit, mit der neue Apps für mobile Plattformen auf den Markt kommen, übersteigt bei weitem die Möglichkeiten der Administratoren, einzelne Apps auf Kompatibilität und Sicherheit zu testen. Beim Einsatz von Cloud-Diensten werden Daten oft auf Servern gespeichert, die von dritter Seite administriert werden. Obgleich die Endanwender mittlerweile solche Dienste von ihren Geräten erwarten, sind nicht alle Unternehmen technisch gerüstet, diese in einer mit den IT-Richtlinien konformen Weise bereitzustellen.

Auch wenn mobile Geräte und Dienste nicht aktiv in einer Unternehmensumgebung implementiert werden, gibt es für Administratoren Mittel und Wege, mit denen diese Geräte und Dienste im Unternehmen genutzt werden können. Dieser Trend ist unter der Bezeichnung „Bring Your Own Device“ (BYOD) bekannt: Die Endanwender bringen ihre eigenen Geräte mit zur Arbeit und erwarten, dass sie die Unternehmensinfrastruktur wie etwa WLAN-Zugang und Netzwerkfreigaben nutzen können. Ebenso gestatten viele E-Mail-Serverkonfigurationen den Fernzugriff über mobile Geräte, unabhängig davon, ob das Gerät verwaltet wird oder nicht. BYOD führt oft zu reflexartigen Reaktionen: Um sicherzustellen, dass keine sensiblen Daten nach außen dringen und dass keine schädliche Software in das Netzwerk gelangen kann, werden mobile Geräte von der Unternehmensinfrastruktur vollständig blockiert, oder die Funktionalität der Geräte wird durch restriktive Richtlinien stark eingeschränkt.

So seltsam dies auch klingen mag: Es ist wichtig zu erkennen, dass bei der Nutzung von Mobilgeräten in Unternehmen kein Schwarzweiß-Denken angebracht ist. Die Konzepte BYOD und die Consumerization der IT erwecken den Eindruck, dass sie eine perfekt organisierte Umgebung destabilisieren. Doch es gibt mehrere Gründe, die für die Bereitstellung unternehmenseigener Mobilgeräte oder die Nutzung privater Mobilgeräte sprechen. Die Nutzung einer MDM-Lösung (Mobile Device Management) kann dazu beitragen, die Vorteile von Mobilgeräten zu nutzen und gleichzeitig deren Auswirkungen auf die übrige Unternehmensinfrastruktur zu begrenzen.

2.1. Vorteile

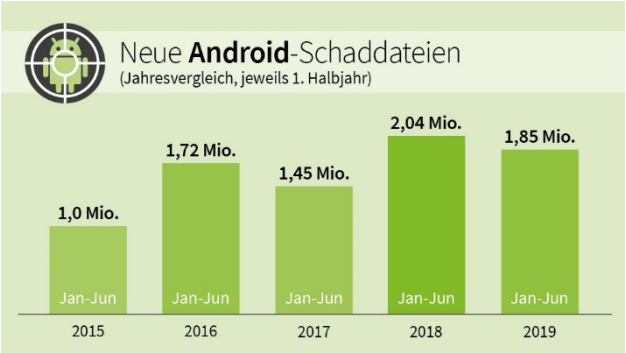
Die Integration von Smartphones und Tablets in die Arbeitsabläufe von Unternehmen bringt deutliche Vorteile, und zwar unabhängig davon, ob diese zentral bereitgestellt oder von den Mitarbeitern mitgebracht werden. Bietet man Mitarbeitern und Dienstleistern, die sich nicht am Unternehmensstandort befinden, mobilen Zugriff auf Unternehmensressourcen, kann dies deren Produktivität deutlich steigern. Eine Kombination aus Zugangskontrollen und Gerätemanagement ermöglicht eine sichere, effiziente Nutzung der Geräte für den Remote-Zugriff auf Unternehmensressourcen. Auch auf Geschäftsreisen ist die Kommunikation nicht länger eingeschränkt: Die Mitarbeiter können aus der Ferne ihre E-Mails, Kalender und Benachrichtigungen abrufen.

In vielen Fällen sind Geräte und Anwendungen im Unternehmen nicht gerade für ihre Benutzerfreundlichkeit bekannt. Die Consumer-Technologie wird hingegen oft so entwickelt, dass sie Endanwendern eine gewisse Vertrautheit bietet. Daher sind nur kurze Einarbeitungszeiten für die Mitarbeiter erforderlich, die sich schnell an die vom Unternehmen bereitgestellten Geräte gewöhnen können.

Außerdem sparen Unternehmen mit einer BYOD-Umgebung Geld, da sie keine umfangreichen Investitionen für die Bereitstellung der Geräte tätigen müssen. Statt neue Smartphones und Tablets kaufen und bereitstellen zu müssen, können die Geräte der Mitarbeiter mit MDM-Software ausgestattet und direkt für Unternehmenszwecke eingesetzt werden. Zudem sind nicht die Unternehmen für Ersatzgeräte verantwortlich, falls ein Mitarbeiter sein Smartphone oder Tablet verliert oder beschädigt.

2.2. Risiken

Die Nutzung mobiler Geräte kann sich in vielerlei Hinsicht positiv auf die Produktivität im Unternehmen auswirken, birgt jedoch auch einige Gefahren. Mobile Geräte werden konsequent als das schwächste Glied der Unternehmensinfrastruktur wahrgenommen (CyberEdge 2017 Cyberthreat Defense Report). Wie PCs sind auch mobile Geräte anfällig für Malware. Insbesondere Android und iOS sind großen Risiken



ausgesetzt: Mit einem gemeinsamen Marktanteil von 99,1 Prozent (Gartner) sind diese Plattformen das bevorzugte Angriffsziel Krimineller. Im 1. Halbjahr 2019 untersuchten die Sicherheitsexperten von G DATA mehr als 1,85 Millionen neue Android-Malware-Samples. Android-Malware wird für eine Vielzahl krimineller Zwecke eingesetzt, z. B.:

- Ausspähen von Daten, zum Beispiel von E- Mails, Anmeldedaten und vertraulichen Dokumenten
- Verursachung hoher Kosten durch den Versand von SMS-Nachrichten an (ausländische) Telefonnummern von Premiumdiensten
- Ausspähen mobiler Banking-Apps
- Sperren von Geräten, um Lösegeld zu erpressen (Ransomware)

Malware ist jedoch nicht die einzige Bedrohung für mobile Geräte. Beim Surfen im Internet können Phishing-Webseiten versuchen, den Benutzer dazu verleiten, persönliche Daten in ein scheinbar harmloses Formular einzugeben. Auch wenn das Gerät selbst sicher ist, bedeutet dies noch lange nicht, dass es im geschäftlichen Umfeld auf sichere Weise genutzt werden kann. Wenn Mitarbeiter mit mobilen Geräten auf Unternehmensdokumente zugreifen, muss sichergestellt sein, dass keine vertraulichen Informationen nach außen dringen können, sei es versehentlich (z. B. durch Hochladen der betreffenden Dateien auf einen Filesharing-Dienst) oder absichtlich (Insider-Bedrohung).

Mobilgeräte können nicht nur Sicherheitsrisiken darstellen, sondern auch zur Senkung der Produktivität führen. Die Nutzung von Apps sollte auch dahingehend eingeschränkt werden, dass die Mitarbeiter nicht übermäßig viel Zeit mit Spielen oder anderen Freizeitbeschäftigungen verbringen. Mithilfe des Kontakte-Managements kann die Nutzung der Telefonfunktionen auf die absolut notwendigen Ansprechpartner beschränkt werden; das spart Zeit und Kosten.

Die Vorteile der Nutzung von Mobilgeräten im Unternehmen überwiegen die Risiken. Dennoch müssen letztere entschärft werden. Integrierte MDM-Richtlinien (Mobile Device Management) können dazu beitragen, Sicherheitsrisiken und Produktivitätsproblemen Herr zu werden und die sichere, effiziente Nutzung von Smartphones und Tablets zu gewährleisten.

3. Mobile Device Management (MDM)

Als Administrator ist es praktisch unmöglich, die Phänomene Consumerization und BYOD zu ignorieren. Die Endanwender werden im Unternehmen auch künftig auf Smartphones und Tablets pochen, an deren Benutzerfreundlichkeit sie sich gewöhnt haben. Wenn solche Geräte nicht aktiv bereitgestellt werden, werden die Mitarbeiter eigene Geräte mitbringen. Angesichts der potenziellen Vorteile mobiler Geräte für

die Produktivität sollte es das Ziel des Mobile Device Management sein, die Produktivität zu maximieren und gleichzeitig die Sicherheit zu gewährleisten und Kosten zu senken.

3.1. Implementierung und Administration

Bevor Smartphones oder Tablets mit einer MDM-Lösung verwaltet werden können, müssen sie implementiert werden. Die Implementierung erfordert eine einmalige anfängliche Anmeldung des Gerätes am Server. Später meldet sich das Gerät dann in regelmäßigen Abständen beim Server und kann aus der Ferne verwaltet werden. Die Kommunikation zwischen Server und Gerät erfolgt in Form von Internet-Datenverkehr (wenn eine direkte Verbindung zum Server aufgebaut werden kann), Push-Nachrichten (welche oft auf anbieterspezifischen Cloud-Messaging-Lösungen basieren) oder SMS-Nachrichten (wenn keine mobile Internetverbindung verfügbar ist). Eine dauerhafte Verbindung zwischen Gerät und Server ist nicht erforderlich: Das Gerät kann die Serverrichtlinien auch dann umsetzen, wenn kein Kontakt zum Server besteht. Auf diese Weise sind die Geräte jederzeit geschützt, auch außerhalb der Unternehmensumgebung.

Die Implementierung sollte so weit wie möglich optimiert werden. Neue vom Unternehmen verwaltete Geräte sollten immer mit MDM-Funktionen ausgestattet werden, bevor sie den Mitarbeitern ausgehändigt werden. BYOD-Geräten sollte der Zugang zum Unternehmensnetzwerk und dessen Ressourcen verweigert werden, bevor sie mit MDM-Funktionen ausgestattet wurden. Optional kann für Geräte, die den Anforderungen nicht entsprechen, oder für Geräte von Besuchern ein Gastnetzwerk genutzt werden.

Um eine erhöhte Arbeitsbelastung zu vermeiden, sollten die Administratoren eine MDM-Lösung wählen, die sich in die vorhandenen Administrationsstrukturen integrieren lässt. Die Nutzung mehrerer Backends ist zu vermeiden. Im Idealfall können mobile Geräte mit derselben Benutzeroberfläche und mit denselben Berichtfunktionen administriert werden, die für andere Gerätetypen im Netzwerk verfügbar sind. Dies vereinfacht einen integrierten Workflow und eine konsistente Konfiguration.

Bei BYOD-Geräten ist der rechtliche Aspekt der Geräteverwaltung zu berücksichtigen. Da diese Geräte nicht Eigentum des Unternehmens sind, sind die Administratoren nicht automatisch zu deren Verwaltung berechtigt.

Problematisch können sich insbesondere Berechtigungen wie etwa das Fernlöschen erweisen. Je nach Gesetzeslage müssen die Unternehmen vor der Registrierung der Geräte für das Mobile Device Management ggf. die Erlaubnis der Endanwender einholen. Es wird empfohlen, in einem Endbenutzer-Lizenzvertrag (EULA) die Maßnahmen zu erläutern, welche das Unternehmen auf dem Gerät durchführen können muss. Der Endanwender kann den Vertrag dann entweder annehmen oder ablehnen. Der Zugriff auf die Unternehmensressourcen wird jedoch nicht gewährt, wenn der EULA-Vertrag abgelehnt wird. Auch für Nicht-BYOD-Geräte kann sich ein EULA-Vertrag als nützlich erweisen.

3.2. Diebstahlschutz

Mobile Geräte erhöhen das Risiko für die Geräteinfrastruktur und für datenbasierte Workflows. Wenn Mitarbeiter vertrauliche Dateien unterwegs dabei haben oder wenn mobile Geräte verloren gehen oder gestohlen werden, kann es sehr leicht geschehen, dass vertrauliche Informationen versehentlich nach

außen gelangen. Um sicherzustellen, dass auf geschäftliche E-Mails, Dokumente und andere Kommunikationsinhalte nicht zugegriffen werden kann, wenn ein Gerät verloren geht oder gestohlen wird, kann eine Reihe von Maßnahmen getroffen werden. Zunächst sollte man versuchen, das Gerät wieder zu finden. Die Ortung des Geräts mithilfe der GPS-Technologie oder das Auslösen eines Alarmtons kann dabei helfen. Wenn die Ortung des Geräts nicht möglich ist oder keine brauchbaren Ergebnisse liefert, kann das Gerät durch Sperren unbrauchbar gemacht werden. Als letzte Maßnahme können die Geräte auf die Werkseinstellungen zurückgesetzt werden, wobei alle Daten von dem Gerät gelöscht werden.

3.3. Apps

Mobile Geräte sind auch deshalb so attraktiv, weil die werksseitigen Funktionen durch die Installation von Apps erweitert werden können. Auch im geschäftlichen Umfeld kann sich diese Tatsache als sehr nützlich erweisen: Produktivitäts-Tools oder Konfigurations-Apps können die Einsatzmöglichkeiten für mobile Geräte deutlich erweitern. Gleichzeitig sollten geschäftlich genutzte Geräte eine kontrollierte Umgebung bereitstellen, um sicherzustellen, dass Apps nicht zu Kompatibilitätsproblemen führen, keine vertraulichen Informationen preisgeben oder Malware verbreiten. Das App-Management ist eine leistungsfähige Methode, um die Funktionalität mobiler Geräte zu steuern, wobei ein ausgewogenes Verhältnis von Sicherheit und Benutzerfreundlichkeit angestrebt werden sollte.

Die Trennung der guten von den schlechten Apps kann eine schwierige Aufgabe darstellen. Einige Apps, wie etwa Spiele, sind für Unternehmensumgebungen zweifellos ungeeignet. Andere können möglicherweise nützlich sein, bergen aber u. U. Datenschutzrisiken, wie zum Beispiel Online-Filehosting-Dienste. Auch Apps, die risikolos erscheinen, können sich später als manipuliert erweisen, sei es, weil die App selbst Sicherheitslücken enthält, weil ihre Backend-Dienste manipuliert sind oder weil sie Informationen auf unsichere Weise überträgt. Auch die Produktivität ist zu berücksichtigen: Beispielsweise kann man Mitarbeitern, die ein Smartphone allein zum Telefonieren oder für Terminvereinbarungen benötigen, nur Zugang zu den Telefon- und Kalenderfunktionen gewähren. Mitarbeiter, die unterwegs auch Dokumente bearbeiten, erhalten Zugriff auf Browser, Office-Apps und andere erforderliche Komponenten.

3.4. Echtzeit-Schutz und On-Demand-Schutz

Wie Desktop- und Laptop-Computer sind auch Mobilgeräte anfällig für Online-Angriffe. Insbesondere gerootete Android-Geräte verfügen nicht über ausreichende Schutzmechanismen gegen Malware-Apps aus unbekannten Quellen. Aber auch Malware-Apps, die sich in offizielle App-Stores einschleichen, können schwerwiegende Folgen verursachen. In ähnlicher Weise könnten auch Websites versuchen, Malware zu verbreiten, Schwachstellen im Betriebssystem auszunutzen oder den Endanwender auf andere Weise zu täuschen. Wie bei Desktop-Computern können Phishing-Websites versuchen, Benutzern Kennwörter oder andere vertrauliche Daten zu entlocken. Um diesen Bedrohungen zu begegnen, sollten Schutzmaßnahmen für alle verwalteten Mobilgeräte konfiguriert werden.

Der Echtzeitschutz schützt Geräte jederzeit ganz ohne Benutzereingriff. Dazu zählen Technologien wie Phishing-Schutz und automatische Virenprüfungen. Der On-Demand-Schutz wird hingegen nur dann

aktiviert, wenn ein Endanwender oder Administrator diesen auslöst. Beispielsweise kann eine Virenprüfung manuell gestartet werden, um sicherzustellen, dass auf dem Gerät nicht bereits Malware-Apps installiert wurden.

Lösungen für den Echtzeit-Schutz und On-Demand-Schutz unterscheiden sich je nach Client-Plattform deutlich voneinander. Android-Geräte sind besonders anfällig für Malware-Apps, während iOS-Geräte anfälliger für Datenverlust oder Phishing-Angriffe sind. MDM-Lösungen sollten Maßnahmen bieten, die speziell auf die jeweilige mobile Plattform zugeschnitten sind: Ein Universalmodul wird den vielfältigen Bedrohungen, denen die Geräte ausgesetzt sind, nicht gerecht.

3.5. Kontakte-Management und -Filterung

Bei Geräten, die im geschäftlichen Umfeld genutzt werden, kann die Kontrolle der Kommunikationsströme von entscheidender Bedeutung sein. Das Blockieren von Apps kann dann sinnvoll sein, wenn die Kommunikation gänzlich verhindert werden soll. In anderen Fällen müssen jedoch feinmaschigere Filter eingesetzt werden. Anstatt die Telefonanwendung vollständig zu blockieren, wenn ein Gerät nur für die geschäftliche Kommunikation genutzt werden soll, können ankommende und abgehende Anrufe gefiltert werden, wenn sie nicht den Kriterien des Unternehmens entsprechen. So könnte beispielsweise ein Unternehmen, das seinen Mitarbeitern Mobiltelefone zur Verfügung stellt, damit diese unterwegs mit der Zentrale telefonieren können, sämtliche Anrufe blockieren, mit Ausnahme derjenigen Nummern von Gesprächspartnern, die vorab vom Unternehmen genehmigt wurden.

Von zentraler Bedeutung für das Kontakte-Management ist ein verwaltetes Telefonbuch. Die auf dem Gerät gespeicherten Kontakte können mit dem zentralen Server synchronisiert werden, und die Administratoren können die aktuellsten Telefonnummern per Push-Technologie auf die Geräte übertragen. Wie das App-Management kann auch das Kontakte-Management für einzelne Geräte verwendet werden. Idealerweise wird das Kontakte-Management jedoch mit einem gruppenbasierten Management kombiniert. Einzelne Rufnummern können für Gerätegruppen in einem Vorgang zugelassen oder gesperrt werden. Es kann aber auch das gesamte Telefonverzeichnis des Unternehmens auf alle Geräte übertragen werden.

4. Nutzung von G DATA Mobile Device Management

G DATA bietet im Rahmen seiner Unternehmenslösungen ein MDM-Modul an. Im Lieferumfang der Produkte G DATA Antivirus Business, G DATA Client Security Business, G DATA Endpoint Protection Business und G DATA Managed Endpoint Security ist die MDM-Komponente mit Unterstützung für iOS und Android enthalten. Das Modul ist vollständig in die anderen Komponenten der Business-Lösungen integriert und kann mit derselben Anwendung (G DATA Administrator) verwaltet werden. Dies ist im Vergleich zu eigenständigen Lösungen ein entscheidender Vorteil, erfordern diese doch eine separate Administration und einen hohen Einarbeitungsaufwand.

4.1. Android

G DATA Mobile Device Management für Android wird über G DATA Mobile Internet Security ausgeführt. Die Funktionalität der App wird zentral über G DATA Administrator verwaltet und bietet umfassende Sicherheits- und Produktivitätsfunktionen für alle Geräte mit Android 4.0 oder neuer.

4.1.1. Verteilung und Administration

Der erste Schritt ist die Verteilung von G DATA Mobile Internet Security an alle Android- Geräte. Um sicherzustellen, dass sich nur autorisierte Netzwerk-Clients mit dem Server verbinden können, muss vor der Bereitstellung der Clients serverseitig ein Passwort definiert werden. Dasselbe Passwort muss später dann in der App eingegeben werden, damit diese sich beim G DATA Management Server authentifizieren kann. Die Client-Installationen werden mithilfe von G DATA Administrator initiiert. Der Implementierungsprozess wird per E-Mail durchgeführt. Die Aktivierung erfolgt über eine E-Mail mit einem Link zur Installationsdatei. Diese kann an eine oder mehrere E-Mail-Adressen versendet werden. Nach dem Download der Datei auf den Android-Client und der Bestätigung der dabei angeforderten Berechtigungen wird G DATA Mobile Internet Security installiert und kann aus dem Android-App-Menü gestartet werden. Die Implementierung wird abgeschlossen, indem die Android-App mit dem Management Server verbunden wird. Diese lädt dann vom Server unverzüglich die standardmäßige MDM-Konfiguration herunter.

Unmittelbar nachdem das Gerät mit dem Management Server verbunden ist, wird es automatisch in G DATA Administrator angezeigt. Da Android-Geräte in der regulären Clientliste als Clients angezeigt werden, können sie Gruppen zugeordnet werden. Es wird empfohlen, für die Android-Geräte eine eigene Gruppe mit Untergruppen für die verschiedenen Gerätezugriffstypen (Unternehmen, private oder gemischte), für die verschiedenen Abteilungen, die Android-Geräte nutzen, sowie für etwaige andere Geschäftsbereiche zu erstellen. Dies ermöglicht eine effiziente Verwaltung; die korrekten Einstellungen für die Geräte können dann jeweils automatisch übernommen werden.

Für jedes Gerät und jede Gruppe kann unter ANDROID-EINSTELLUNGEN > POLICIES ein Telefontyp definiert werden. Für Geräte, die vom Unternehmen bereitgestellt wurden und nur für die geschäftliche Nutzung gedacht sind, wird der Telefontyp GESCHÄFTLICH empfohlen. Dadurch werden die clientseitigen Einstellungsmenüs von Mobile Internet Security gesperrt, sodass die Benutzer nicht versehentlich zentral verwaltete Einstellungen ändern können, während sie mit dem Unternehmensnetzwerk verbunden sind. Der Telefontyp PRIVAT kann für Geräte verwendet werden, die nicht vom Unternehmen bereitgestellt wurden. Dies gewährt dem Benutzer vollen Zugriff auf die Einstellungen von Mobile Internet Security. Der Telefontyp GEMISCHT ist für Geräte gedacht, die vom Unternehmen bereitgestellt wurden und sowohl für die geschäftliche als auch für die private Kommunikation genutzt werden.

Einige grundlegende Einstellungen sollten direkt nach der Bereitstellung eines neuen Geräts konfiguriert werden. Es empfiehlt sich in jedem Fall, einen Zeitplan für Updates und für die Synchronisation festzulegen. Beide Einstellungen sind vom Nutzungsmuster des Geräts abhängig. Geräte, die oft mit einem drahtlosen Netzwerk (WLAN) verbunden sind, können so konfiguriert werden, dass automatisch alle paar Stunden eine Aktualisierung der Virensignaturen und eine Synchronisierung der Daten mit dem Management Server erfolgt. Geräte, die meist außerhalb des Unternehmensnetzwerks eingesetzt werden

oder eine Internetverbindung mit einem Mobildatentarif nutzen, können so konfiguriert werden, dass sie weniger häufig, nur manuell oder nur dann, wenn sie per WLAN verbunden sind, aktualisiert werden. Dasselbe gilt für die Synchronisierung: Es können verschiedene Einstellungen für WLAN und Mobildatentarife konfiguriert werden. Bei Bedarf kann den Geräten ein Endbenutzer-Lizenzvertrag zugeordnet werden. Aufgrund gesetzlicher Verpflichtungen kann es erforderlich sein, dass das Unternehmen die Endanwender darüber informieren muss, dass ihre Geräte zentral verwaltet werden können.

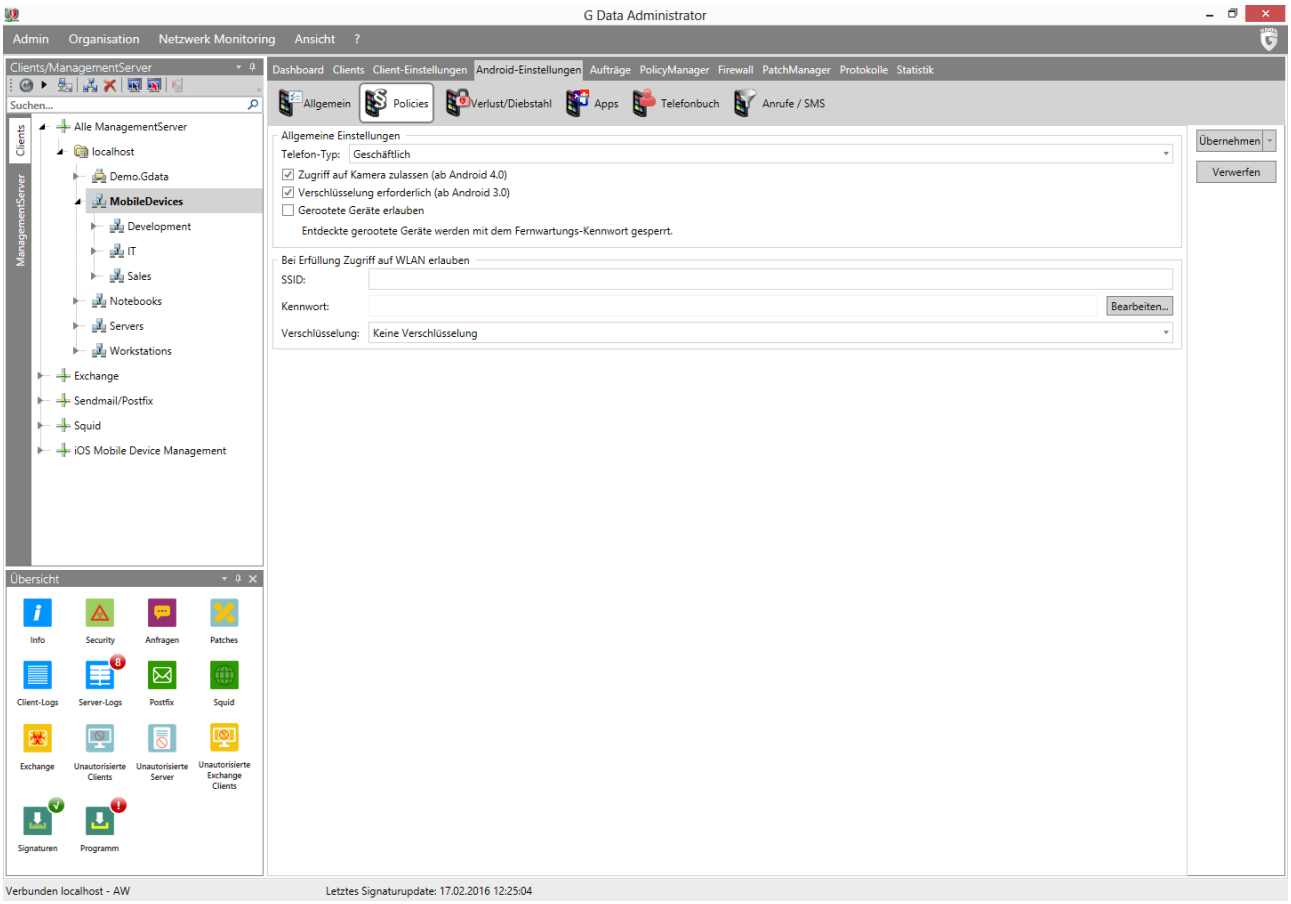


Abbildung 1: G DATA Administrator, Android-Einstellungen, Policies

4.1.2. Diebstahlschutz

Diebstahlschutzmaßnahmen können sowohl automatisch als auch manuell ausgelöst werden. Einige Maßnahmen können so konfiguriert werden, dass sie ausgeführt werden, wenn am Gerät bestimmte Änderungen vorgenommen werden (z. B. wenn die SIM-Karte gewechselt wird). Andere Maßnahmen können mit G DATA Administrator ausgelöst werden, damit ein Befehl über Google Firebase Cloud Messaging gesendet wird. Außerdem können Befehle auch per SMS gesendet werden.

Um alle Maßnahmen zu aktivieren, müssen unter ANDROID-EINSTELLUNGEN > VERLUST/DIEBSTAHL verschiedene Einstellungen konfiguriert werden. Um SMS-Befehle nutzen zu können, muss ein Fernwartungspasswort (ein numerischer PIN-Code) eingegeben werden. Dieser Code fungiert auch als Passwort für den Sperrbildschirm, falls dieses nicht separat festgelegt wurde. Es muss eine vertrauenswürdige Telefonnummer eingegeben werden, um sicherzustellen, dass keine Unbefugten den Befehl zum

Zurücksetzen des Passworts versenden können und dass ein solcher Befehl nur dann ausgeführt wird, wenn er von der vertrauenswürdigen Telefonnummer aus gesendet wurde. Zudem sollte eine E-Mail-Adresse eingegeben werden, um Feedback von Maßnahmen zu erhalten, die diese Funktion unterstützen.

Wenn ein Gerät verloren geht oder gestohlen wird, ist die schnellste Möglichkeit, einen Befehl auf dem betreffenden Gerät auszulösen, diesen per SMS-Nachricht an das Gerät zu senden. Administratoren können die jeweiligen Befehle, die an das Gerät gesendet werden können, einzeln auswählen. Die folgenden Maßnahmen sind verfügbar:

- Dem Administrator eine E-Mail mit Standortdaten senden
- Gerät auf Werkseinstellungen zurücksetzen. Alle persönlichen Daten werden gelöscht
- Alarmton auslösen
- Alle Klingeltöne stummschalten, mit Ausnahme desjenigen, der durch die Alarmtonfunktion ausgelöst wird
- Mit dem Sperrbildschirmpasswort den Sperrbildschirm aktivieren
- Sperrbildschirmpasswort festlegen

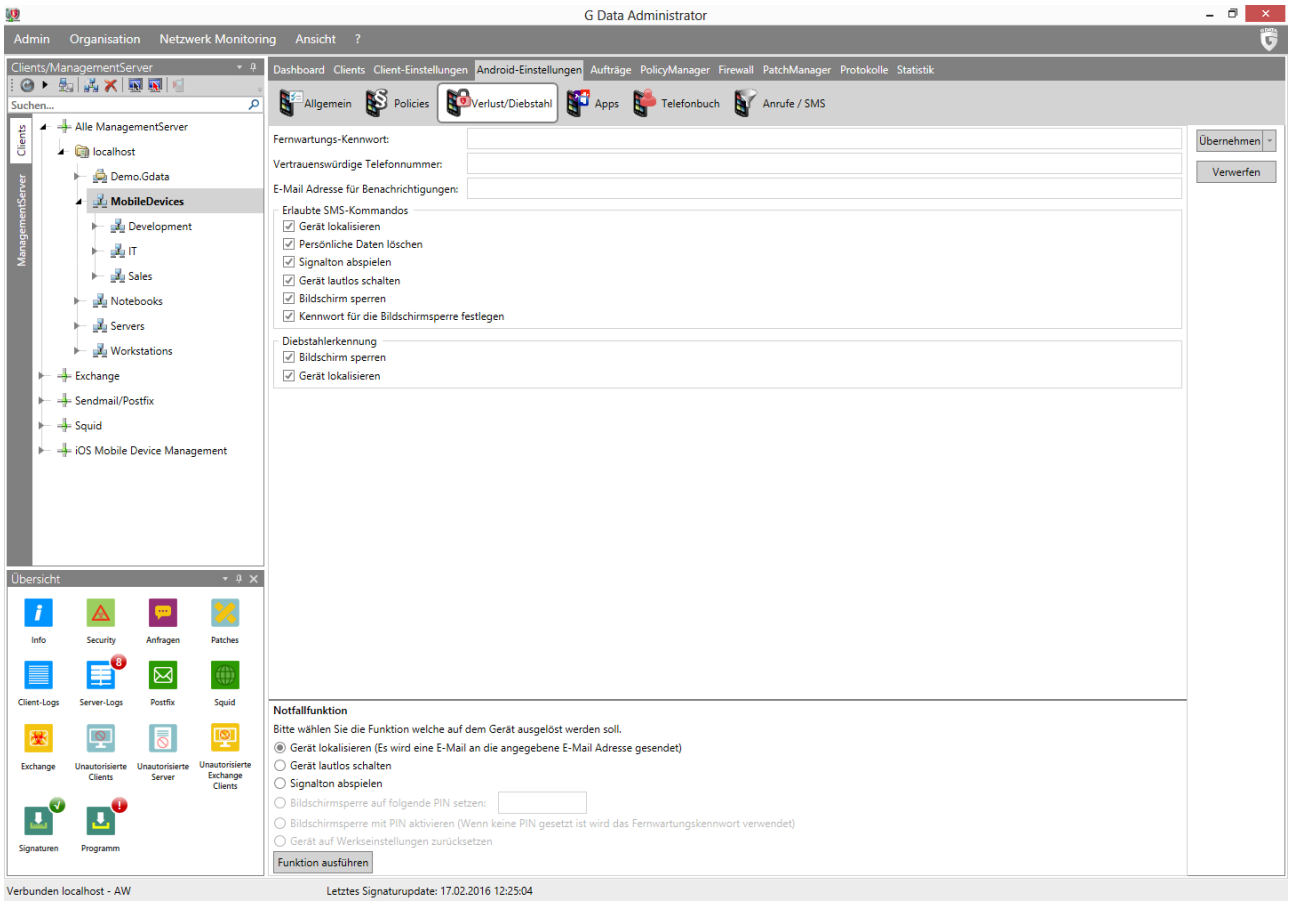


Abbildung 2: G DATA Administrator, Android-Einstellungen, Verlust/Diebstahl

Wenn ein Gerät gestohlen wird, wird häufig die SIM-Karte entfernt, damit der rechtmäßige Eigentümer das Gerät nicht über die entsprechende Telefonnummer kontaktieren kann. Dies bedeutet auch, dass keine SMS-Nachrichten an das Gerät gesendet werden können. Als Gegenmaßnahme können Sie Maßnahmen festlegen, die automatisch getroffen werden, wenn die SIM-Karte ausgewechselt wird. Der

Sperrbildschirm des Telefons kann aktiviert werden, sodass nicht mehr auf das Gerät zugegriffen werden kann und das Gerät geortet werden kann. Neben Maßnahmen, die auf der SIM-Karte und auf SMS-Nachrichten basieren, können auch über G DATA Administrator verschiedene Maßnahmen initiiert werden. Das Gerät muss nicht mit dem Management Server-Netzwerk verbunden sein, damit diese Maßnahmen greifen: Für diese Funktionen wird Google Firebase Cloud Messaging genutzt, ein Online-Service von Google, mit dem man Befehle an Android-Geräte senden kann. Dies erfordert einen Account für Google Firebase Cloud Messaging. Dieser kann kostenlos bei Google unter https://firebase.google.com registriert werden.

Da die Diebstahlschutzmaßnahmen die Nutzbarkeit des Mobiltelefons stark beeinträchtigen können (beispielsweise wenn die Daten vom Gerät gelöscht werden), ist es empfehlenswert, dass der Endanwender in einem EULA-Vertrag über diese Möglichkeit informiert wird.

4.1.3. Apps

G DATA Mobile Device Management für Android bietet innovative Funktionen für die App-Verwaltung. Zunächst einmal können diese dazu genutzt werden, um eine Bestandsliste aller Apps zu erstellen, die auf Mobilgeräten im Netzwerk genutzt werden. Jede installierte App wird mit Name, Version und Größe aufgeführt. Zu jeder App sollten die Administratoren Informationen über den Hersteller, die Funktionen und den Versionsverlauf erhalten, sofern entsprechende Informationsquellen zur Verfügung stehen. Bei vielen Apps bieten die offiziellen App-Stores hinreichende Detailinformationen. Bei manchen Apps kann es erforderlich sein, auf der Website des Herstellers nachzuschauen. Anhand dieser Informationen und ausgehend von der beabsichtigten Nutzung des Geräts (je nach Gerätegruppe und -art sowie nach Netzwerkbereich) können Apps auf die Whitelist oder die Blacklist gesetzt werden. Dadurch werden die betreffenden Apps freigeschaltet bzw. gesperrt. Wenn das vordefinierte Passwort eingegeben wird, wird die Ausführung der betreffenden Apps gesperrt.

Ob ein Blacklist- oder Whitelist-Konzept genutzt wird, hängt davon ab, in welchem Ausmaß das Gerät gesperrt werden soll. Wenn für das App-Management das Blacklist-Verfahren verwendet wird, stellt diese eine einfache Konfigurationsmöglichkeit für Mehrzweckgeräte dar, bei denen der Endanwender in der Lage sein soll, neue Apps ohne vorherige Genehmigung zu installieren. Die Gefahr besteht darin, dass praktisch alle Apps installiert und ausgeführt werden können. Erst nachdem ein Administrator bestimmte Apps manuell blockiert hat, ist der Zugriff für den Benutzer gesperrt. Eine sichere, aber restriktivere Methode ist das Whitelist-Verfahren: Es können keine Apps verwendet werden, die nicht in der Whitelist aufgeführt sind. Dies ist besonders in den Fällen nützlich, in denen die Geräte nur für einen einzigen Zweck konfiguriert werden. Die Administratoren können dann die erforderlichen Apps vorinstallieren, auf die Whitelist setzen und so den Zugriff auf alle anderen Apps sperren.

Wenn beabsichtigt wird, nur einige wenige, bekanntermaßen unerwünschte Apps zu sperren, ansonsten dem Benutzer aber relative Freiheit zu gewähren, reicht das Blacklist-Verfahren aus. Zumindest die App mit den Android-Einstellungen und Mobile Internet Security selbst sollten aber in jedem Fall passwortgeschützt werden. Dadurch wird verhindert, dass der Anwender Einstellungen manipulieren kann. Wird der offizielle App-Store auf die Blacklist gesetzt, ist sichergestellt, dass keine anderen Apps installiert werden können. Um die App-Nutzung auf einem Gerät vollständig zu kontrollieren, ist das Whitelist-Verfahren die zuverlässigste Option. Die in der Whitelist aufgeführten Apps können ohne

Einschränkungen genutzt werden; alle anderen Apps sind hingegen gesperrt. Dies ist vor allem für Geräte empfehlenswert, die für maximale Sicherheit oder für nur einen einzigen Workflow konfiguriert werden. Beispielsweise kann ein Gerät, das nur von Außendienstmitarbeitern genutzt wird, im Whitelist-Modus eingesetzt werden, sodass nur die Telefonfunktion und das Frontend der Vertriebsdatenbank genutzt werden können.

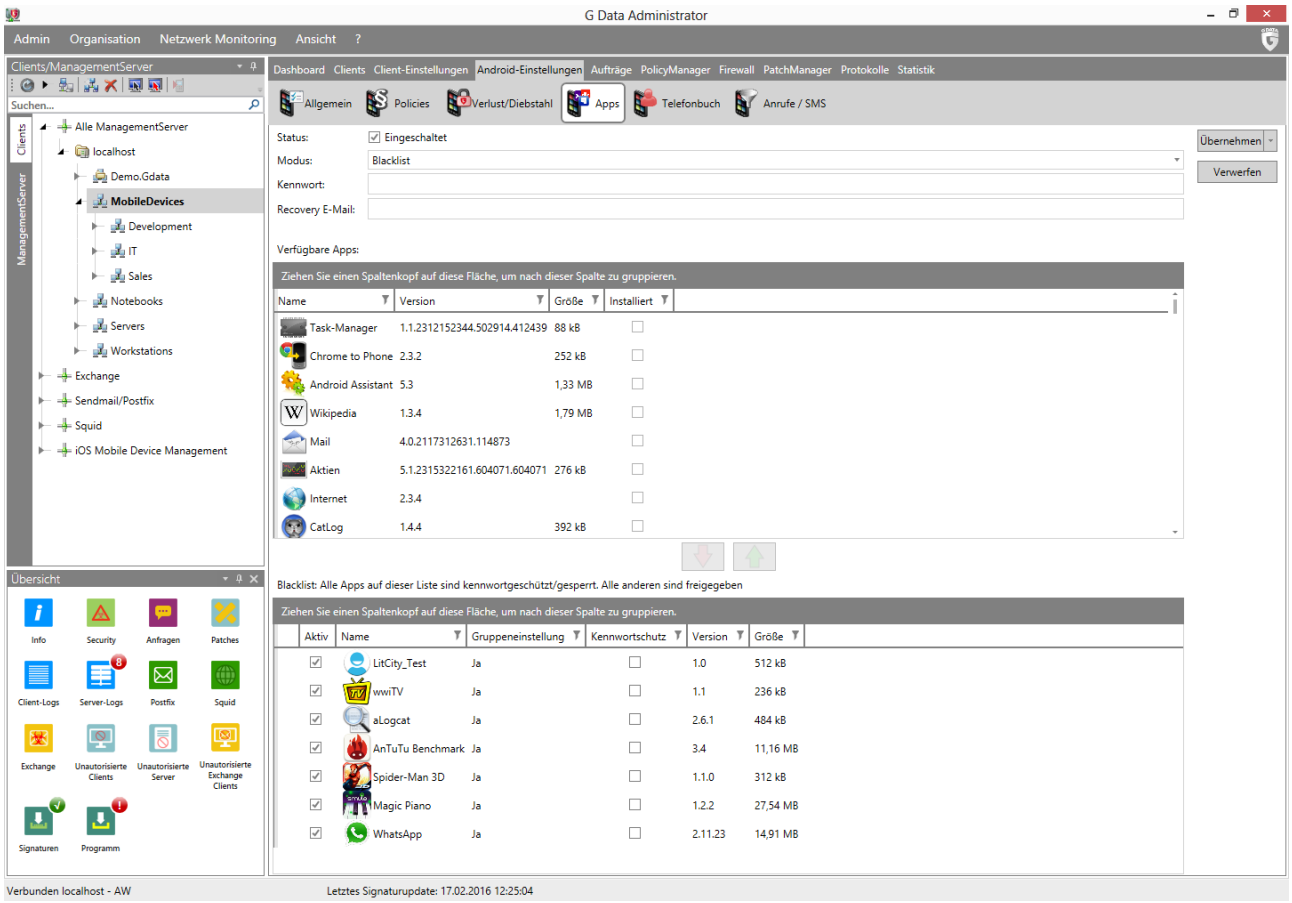


Abbildung 3: G DATA Administrator, Android-Einstellungen, Apps

4.1.4. Echtzeit-Schutz und On-Demand-Schutz

Echtzeit-Malware-Schutz ist über die Module WEB-SCHUTZ und VIRENPRÜFUNG verfügbar. Darüber hinaus kann die Funktionalität in G DATA Administrator auf der Registerkarte POLICIES eingeschränkt werden.

Der Webschutz bietet Echtzeit-Schutz, wenn der Android-Browser genutzt wird. Da der Webschutz in geringem Umfang Datenverkehr verursachen kann, kann die Funktion so konfiguriert werden, dass sie nur dann aktiv ist, wenn das Gerät per WLAN verbunden ist. Die Virenprüfung überprüft auf transparente Weise die heruntergeladenen Apps auf Malware und blockiert die Installation, wenn festgestellt wird, dass es sich um Malware handelt.

On-Demand-Malware-Schutz ist in Form einer vollständigen Virenprüfung des kompletten Geräts verfügbar. Eine regelmäßige Überprüfung aller Apps wird empfohlen, um sicherzustellen, dass keine Malware auf Speichermedien (wie etwa auf einer SD-Karte) gespeichert ist. Je nachdem, wie oft das Gerät genutzt wird und wie oft neue Software installiert oder auf dem Gerät gespeichert wird, kann das Intervall auf 1 Tag, 3 Tage, 7 Tage, 14 Tage oder 30 Tage eingestellt werden. In den meisten Fällen

empfiehlt es sich, eine tägliche Prüfung durchzuführen: Der Scan verursacht keine merkliche Verlangsamung und bietet maximale Sicherheit. Um sicherzustellen, dass die Virenprüfung den Akku des Geräts nicht zu sehr beansprucht, kann sie so konfiguriert werden, dass sie nur dann ausgeführt wird, wenn das Gerät aufgeladen wird.

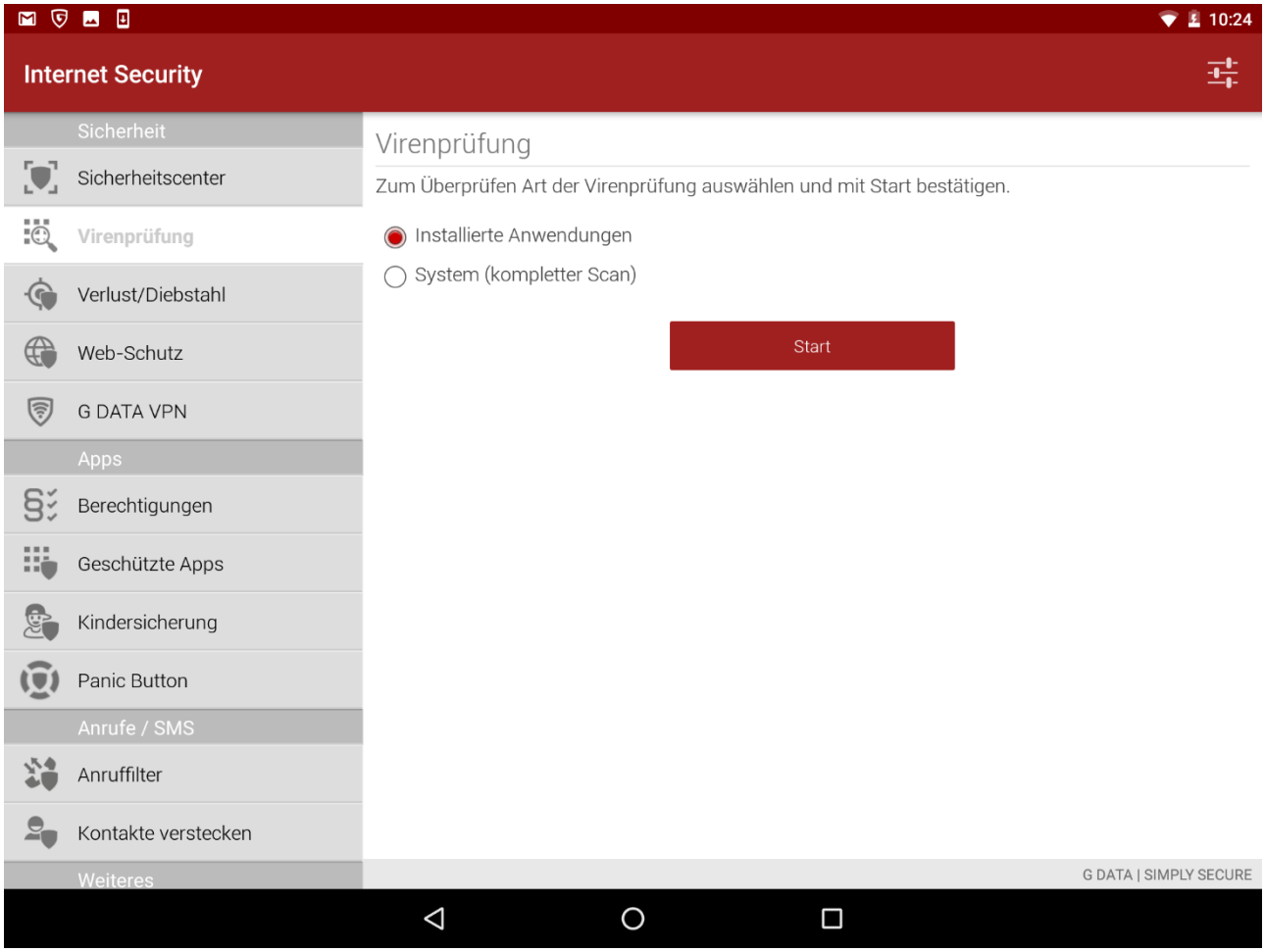


Abbildung 4: G DATA Mobile Internet Security, Sicherheit, Virenprüfung

Bei Android-Geräten stellen gerootete Geräte das größte Risiko dar. Wenn sich der Endanwender Root-Zugriff auf das Gerät verschafft hat, kann jede Sicherheitsmaßnahme auf Betriebssystem- und App-Ebene problemlos unterlaufen werden; wenn es der Malware gelingt, das Gerät zu infizieren, erhält sie nahezu unbegrenzten Zugriff auf alle Betriebssystemfunktionen. Um die Kontrolle über verwaltete mobile Geräte zu behalten, empfiehlt es sich daher, mithilfe der Registerkarte POLICIES den Netzwerkzugriff für gerootete Geräte zu sperren. Darüber hinaus kann der Administrator den Kamerazugriff aktivieren oder deaktivieren und/oder eine Datenverschlüsselung vorschreiben, um die auf dem Gerät gespeicherten Daten zu schützen.

4.1.5. Kontakte-Management und -Filterung

Das Telefonverzeichnis des Unternehmens kann zur Verwaltung der Kontakte auf Android-Geräten genutzt werden. Auch ohne den Einsatz von Filterfunktionen kann die Sperrung des im Gerät integrierten Telefonbuchs und die Nutzung des Telefonverzeichnisses des Unternehmens in Mobile Internet Security

eine effiziente Möglichkeit darstellen, die Kontrolle über Kontaktinformationen sicherzustellen. Zusammen mit dem Anruffiltermodul bietet diese Funktion umfangreiche Verwaltungs- und Filtermöglichkeiten für Kontakte.

Die Grundlage für sämtliche Funktionen dieser Art bildet die Kontaktdatenbank. Sie dient als zentraler Ausgangspunkt für alle Unternehmenskontakte. Davon ausgehend können Telefonbücher für verschiedene Geräte sowie gezielte Anruf- und SMS-Filter erstellt werden. Für Unternehmen mit einer begrenzten Anzahl an Kontakten oder für kleine, verwaltete Telefonbücher ist die manuelle Eingabe der Kontakte eine praktische Methode, um die Kontaktdatenbank schnell zu bestücken. Wenn das Netzwerk mit Active Directory arbeitet, können Kontakte importiert werden. Wenn alle Kontakte definiert sind, können sie an die entsprechenden Geräte verteilt werden. Beispielsweise kann auf allen Geräten eine vollständige Liste der Durchwahlnummern aller Kollegen gespeichert werden. Alternativ dazu kann die Standardtelefonbuch-App gesperrt und ein Anruffilter genutzt werden und Gerätegruppen nur der Zugriff auf bestimmte Telefonnummern gewährt werden, die explizit im Telefonbuch gespeichert sind.

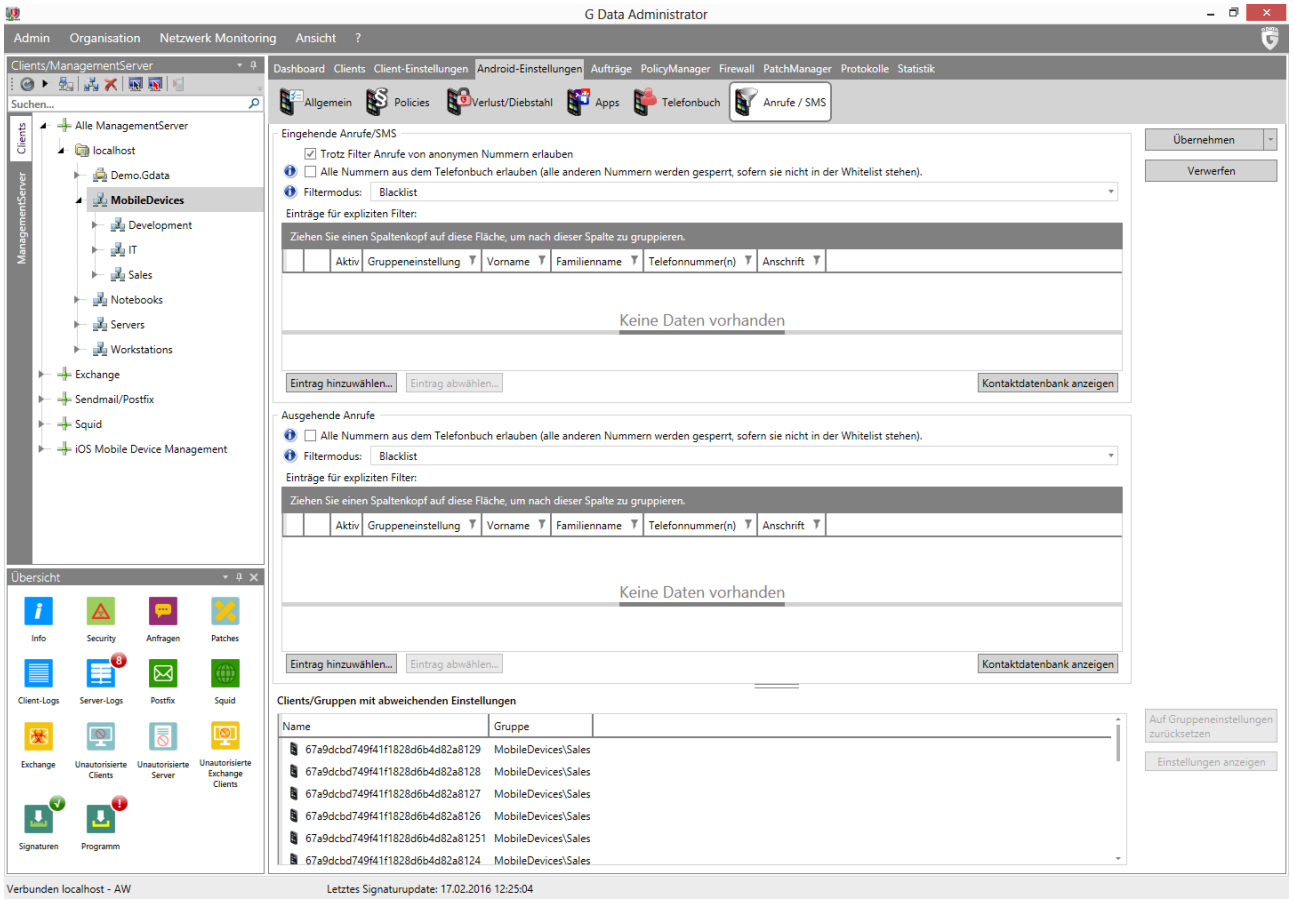


Abbildung 5: G DATA Administrator, Android-Einstellungen, Anrufe / SMS

Der Anruffilter kann auch für eine umfangreiche Filterung eingehender und ausgehender Kommunikationsverbindungen genutzt werden. Er dient als Filter für das im Gerät integrierte Telefonbuch. Anstatt die Telefonbuch-App des Android-Geräts vollständig sperren zu müssen, gestattet der Filter eine feinmaschige Kontrolle der Kommunikationsströme. Wird beispielsweise der Whitelist-Modus aktiviert, sind keine eingehenden oder ausgehenden Anrufe zugelassen, mit Ausnahme der

Nummern, die in der Whitelist aufgeführt sind. Im Blacklist-Modus ist die Kommunikation im Allgemeinen erlaubt, bestimmte Nummern können jedoch gesperrt werden.

4.2. iOS

G DATA Mobile Device Management für iOS-Geräte wurde als agentenlose Lösung für iOS 7.0 und höher konzipiert. Mit G DATA Administrator können Richtlinienprofile bei einem oder mehreren iOS-Geräten implementiert werden. Dadurch können Administratoren die Geräte flexibel verwalten und gleichzeitig maximalen Einfluss auf deren Nutzung nehmen. Die Verwaltung von iOS-Geräten setzt voraus, dass Sie sich beim G DATA Action Center registriert haben (https://ac.gdata.de; kostenfrei). Geben Sie Ihre Zugangsdaten für das Action Center im Modul ACTIONCENTER des G DATA Administrators ein, um G DATA Mobile Device Management für iOS zu aktivieren.

4.2.1. Implementierung und Administration

Implementierungen von iOS-Clients können mit G DATA Administrator initiiert werden. Der Implementierungsprozess wird per E-Mail durchgeführt. Wählen Sie dazu unter CLIENTS/MANAGEMENTSERVER > CLIENTS einen beliebigen Knoten unter IOS MOBILE DEVICE MANAGEMENT, klicken Sie in der Symbolleiste auf die Schaltfläche INSTALLATIONSLINK AN MOBILE GERÄTE SENDEN und geben Sie eine Liste mit E-Mail-Adressen ein. Um die Darstellung der MDM-Anfrage auf dem Gerät anzupassen, können einige Parameter eingegeben werden. In der MDM-Anfrage sowie später im Register ALLGEMEIN unter IOS-EINSTELLUNGEN werden NAME, BESCHREIBUNG und ORGANISATION angezeigt. Mit dem END USER LICENSE AGREEMENT kann der Endanwender darüber informiert werden, dass das Gerät zentral verwaltet wird.

Wenn der Endanwender den Link aus der Installations-E-Mail auf einem iOS-Gerät öffnet, wird das Gerät sofort in G DATA Administrator angezeigt (auf der Registerkarte CLIENTS unter SECURITY-STATUS finden sich detaillierte Angaben über den Wartestatus des Geräts). Sobald der Anwender die MDM-Anfrage akzeptiert, kann das iOS-Gerät vollständig mithilfe von G DATA Administrator verwaltet werden.

Wird ein iOS-Gerät in G DATA Administrator ausgewählt, stehen verschiedene MDM-Module für iOS zur Verfügung. Auf der Registerkarte CLIENTS (IOS) wird eine Übersicht aller verwalteten iOS-Geräte angezeigt. Zu jedem Client werden verschiedene gerätespezifische Eigenschaften angezeigt, z. B. die IMEI-Nummer, die iOS-Version und der Produktname. In der Spalte SECURITY-STATUS werden Warnungen zu Geräten ohne Richtlinienprofil sowie Statusmeldungen zur MDM-Installation angezeigt. Im Modul IOS-EINSTELLUNGEN können Administratoren Diebstahlschutzmaßnahmen (siehe Kapitel 4.2.2) sowie Richtlinienprofile (siehe Kapitel 4.2.3) konfigurieren. Im Modul PROTOKOLLE (IOS) kann der Status der verschiedenen Push-Nachrichten verfolgt werden. Dies ist die wichtigste Kommunikationsmethode zwischen dem G DATA Action Center und iOS-Geräten. Zu den Berichten zählen der Profilbereitstellungsstatus und Bestätigungen zu den Diebstahlschutzfunktionen.

4.2.2. Diebstahlschutz

Wenn ein Gerät verloren geht oder gestohlen wird, muss zu allererst sichergestellt werden, dass kein Unbefugter auf Daten zugreifen kann, die auf dem Gerät gespeichert sind. Anschließend kann es mit Hilfe von GPS geortet werden (um es zu finden und dem Benutzer zurückzugeben). Die drastischere

Maßnahme, die komplette Löschung der auf dem Gerät gespeicherten Daten, kann getroffen werden, falls keine Chance mehr besteht, das Gerät zu finden und dem Benutzer zurückzugeben. Apple bietet registrierten iCloud-Nutzern die Funktion „Mein iPhone suchen“. Es bietet den Benutzern die Möglichkeit, sich an einer speziellen Website anzumelden und ihr Gerät zu sperren, zu orten oder zu löschen.

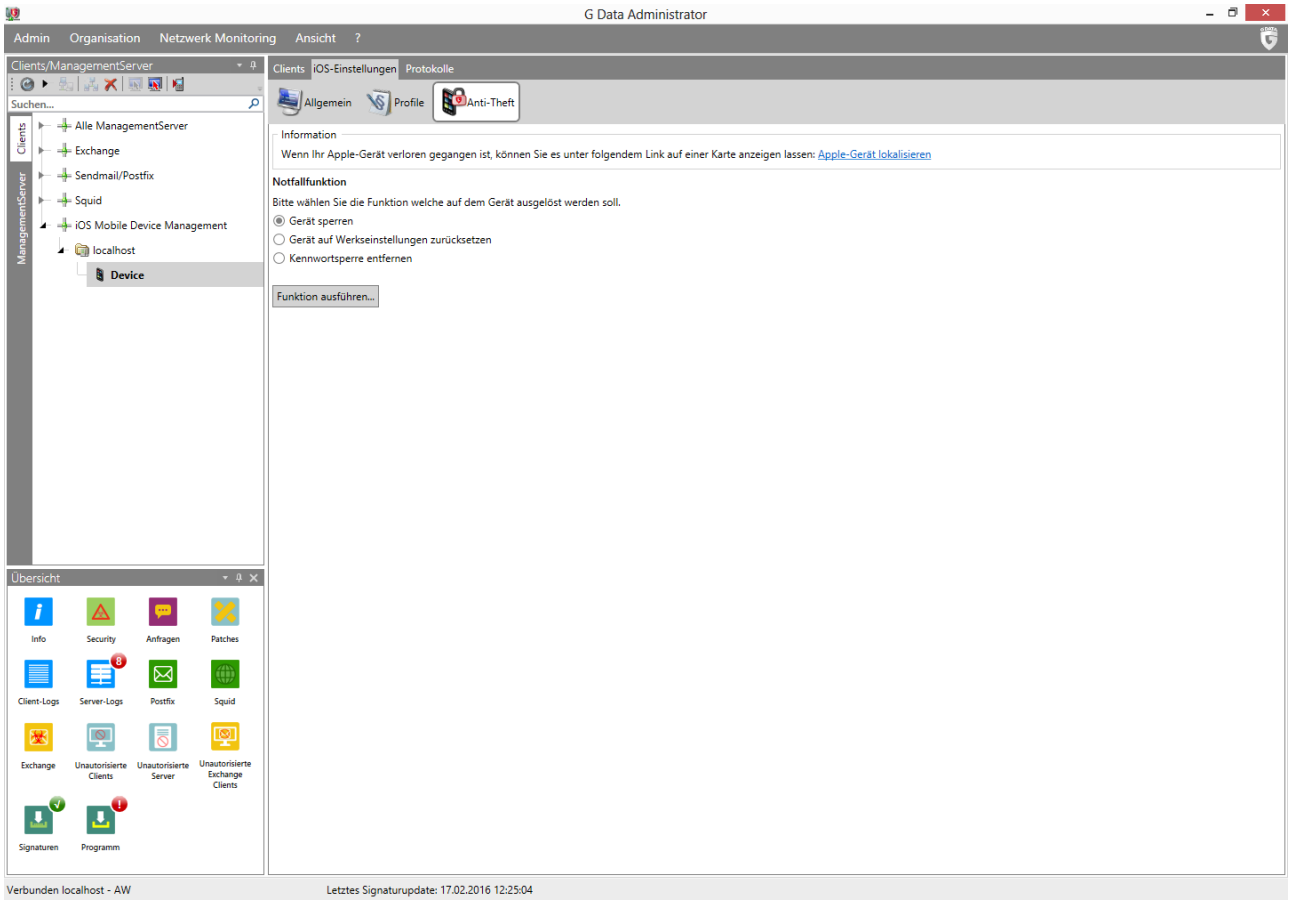


Abbildung 6: G DATA Administrator, iOS-Einstellungen, Anti-Theft

Als Alternative zur Funktion „Mein iPhone suchen“ können Administratoren mit dem Modul iOS-Einstellungen auf der Registerkarte Anti-Theft Diebstahlschutzfunktionen auslösen, ohne dass sie sich auf einer externen Website anmelden müssen. Die Funktionen zum Sperren und Zurücksetzen der Geräte können durch Auswählen der entsprechenden Option und durch Klicken auf Funktion ausführen ausgelöst werden. Verwenden Sie bei Geräten, die mit einem unbekannten Passcode gesperrt wurden, die Option Kennwortsperre entfernen.

4.2.3. Apps, Schutz und Kontakte-Management

Im Gegensatz zu Android-Geräten verfügt iOS über ein einheitliches Sicherheitsmanagementkonzept, das es Administratoren gestattet, Sicherheitseinstellungen für verschiedenste Module in einem einzigen Profil zu konsolidieren. Diese Profile können dann auf mehrere Geräte angewendet werden, wodurch die erforderliche Zeit, um alle iOS-Geräte im Netzwerk zu sichern, verkürzt wird. Die Registerkarte Profile von G DATA Administrator kann zum Erstellen und Bearbeiten von Profilen verwendet werden. Jedes Profil kann bis zu fünf Richtlinien enthalten; jede Richtlinie behandelt schwerpunktmäßig einen bestimmten Typ von Sicherheitseinstellungen:

- EINSCHRÄNKUNGEN DER FUNKTIONALITÄT: Beschränkung der iCloud-Nutzung, Gewährleistung der sicheren Nutzung des Sperrbildschirms, Steuerung verschiedener anderer Funktionen
- CODE-EINSTELLUNGEN: Vorgabe zwingender Richtlinien für die Passcode-Nutzung, wie beispielsweise Mindestanzahl komplexer Zeichen, Mindestlänge und Nachfrist für die Gerätesperre
- APP-EINSCHRÄNKUNGEN: Sperre oder Freigabe von Safari (einschließlich Funktionen wie Cookies, Pop-ups und JavaScript) sowie des iTunes Store
- EINSCHRÄNKUNGEN FÜR MEDIALE INHALTE: Steuerung, welche Arten von Multimediainhalten erlaubt sind (Apps, Filme, Fernsehsendungen)
- WLAN: Eingabe von WLAN-Netzwerkinformationen, so dass iOS-Geräte automatisch eine Verbindung zu einem bestimmten WLAN-Netzwerk herstellen können

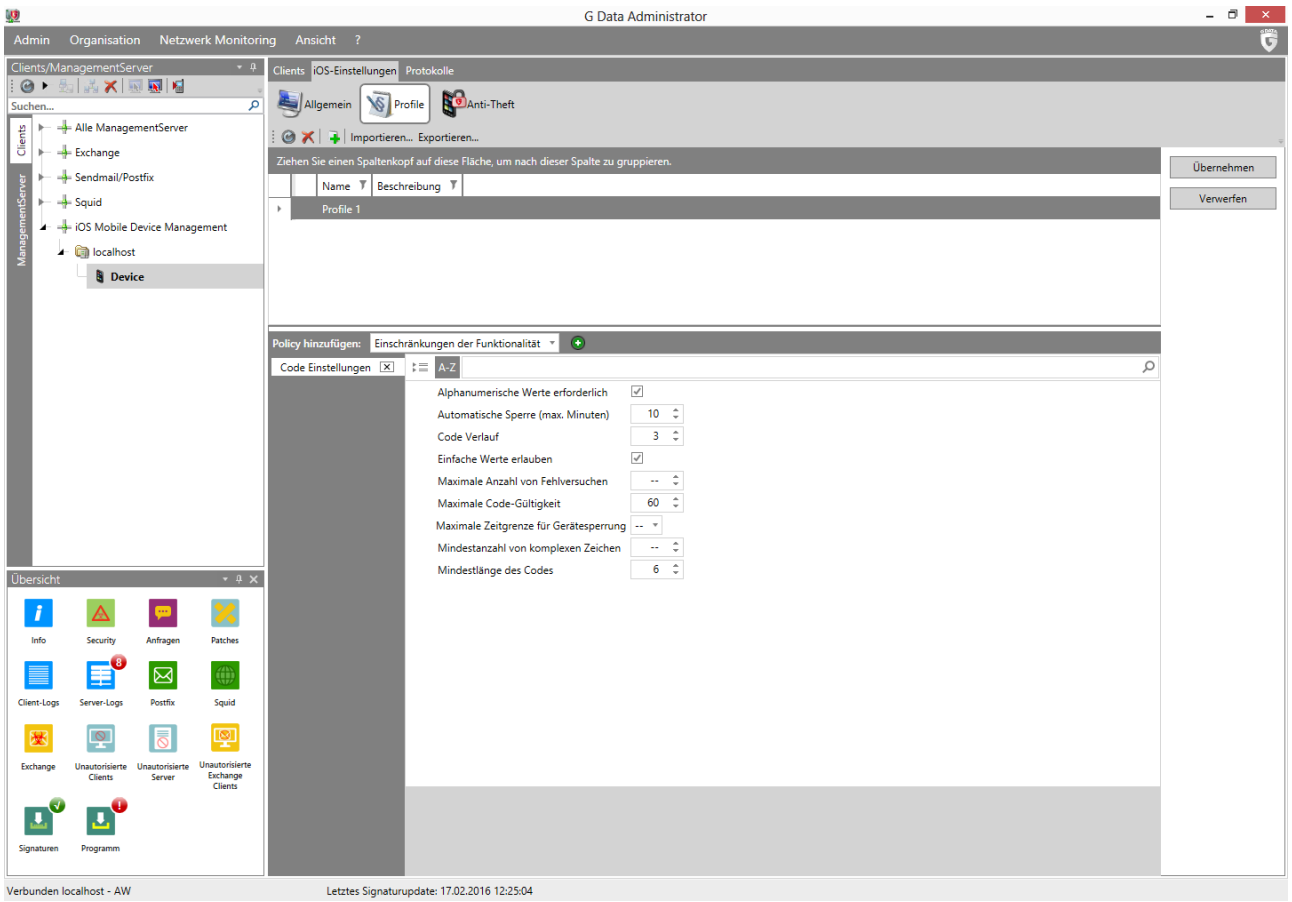


Abbildung 7: G DATA Administrator, iOS-Einstellungen, Profile

Da Apple es Benutzern ermöglicht, MDM-Profile jederzeit von ihrem Gerät zu entfernen, sollten Administratoren sicherstellen, dass ihre Sicherheitsprofile einen überzeugenden Grund enthalten, dies nicht zu tun. Es wird empfohlen, die WLAN-Richtlinie jedem Profil hinzuzufügen. Dadurch kann sich das Gerät mit dem angegebenen (geschützten) WLAN-Netzwerk verbinden. Wenn ein Endanwender versucht, Teile der Sicherheitsrichtlinien durch Entfernen des MDM-Profils von einem iOS-Gerät zu umgehen, wird automatisch auch der WLAN-Zugang entfernt, wodurch der Zugriff des Geräts auf Unternehmensressourcen stark eingeschränkt wird. So kann sichergestellt werden, dass unsichere Geräte keinen Zugriff auf vertrauliche Netzwerkfreigaben und andere vertrauliche Daten haben.