sicherer Apple Geräte-Transport

> TL;DR - nur Apple kann dauerhafte Gerätesperren setzen, für eine dauerhafte Gerätesperre benötigt Apple die Geräte-Verknüpfung zu einer Apple ID.
> MDM-Gerätesperren sind ab MDM-Entfernung aufgehoben was genau das Ziel der Diebe ist.

Voraussetzungen

- Apple Business Manager
- Händler, welche Geräte vorregistriert
- Händler, welcher Freigabeprozesse zwischen Vorregistrierung und Versand ermöglicht
- MDM mit Profilen (z.B. Intune)

Doings

1. Klassische Apple ID anlegen (z.B. transportdevices@company.com)
2. MDM profil anlegen, enforcing der Apple ID auf iOS
3. Shop bitten Geräteregistrierung zu machen
4. Geräte im Apple Business Manager zum MDM server hinzufügen
5. MDM profil für neu registriertes Gerät setzen
6. Freigabe zum Versand erteilen

Reaktion bei ordnungsgemäßem Empfang

1. Vor erstem Anschalten das MDM-Profil ändern
2. Gerät einsetzen

iPhone Prozess bei Dieb

1. Dieb oder Käufer der Hehlerware schalten das Gerät ein
2. Einrichtungsprozess kann durchgangen werden
3. Dieb sorgt für Internetzugriff, durch SIM oder WLAN
4. Im Einrichtungsprozess wird keine Möglichkeit gegeben eine Apple ID anzugeben
5. Die durch das MDM Profil vergebene PIN ist aktiv
6. Durch die Apple ID können die Geräte von Apple selbst verwaltet werden, weil Apple den MDM Herstellern weniger Zugriff gestattet.
   (z.B. Komplett-Deaktivierung des gesamten Geräts, auch nach Entfernung aus MDM)

Nachsorge nach Diebstahl

Voraussetzung: Dieb oder sein Käufer muss das Gerät eingeschaltet haben. Sieht man im MDM.

- Als Apple ID transportdevices@company.com mit Apple kommunizieren.
- Apple über Diebstahl und polizeiliche Anzeige aufklären.
- Anzeige erstatten
- Polizei den Umstand mit der Apple ID erklären
- Polizei Zugriff auf eure transportdevices Apple ID geben. (Geolokation über "Wo ist" Netzwerk)
- Nach Bestätigung von Apple und Zeitablauf der Anzeige dass dieses Gerät komplett deaktiviert wurde aus dem MDM entfernen.

Die meisten Anzeigen werden nicht weiterverfolgt, da es sich nicht um Diebstähle in großem Maß handelt und die Jurisdiktion von Polizeiarbeit über Ländergrenzen hinweg deutlich schwieriger ist.

Warum?

Apple erlaubt ohne Apple ID keine dauerhafte Gerätesperre.
Das Ziel der Diebe ist nicht das iPhone, sondern der Erlös des Verkaufs von diesem.

Der Hehler hat keine Kundschaft, wenn er Geräte verkauft die für seine Kunden nicht einsetzbar sind, und fordert demzufolge auch keine neuen Geräte vom Dieb an.

Drittanbieter-MDM's können keine dauerhaften Gerätesperren setzen! Auch Intune ist in der Hinsicht Drittanbieter.
Dauerhaft bedeutet ein kompletter Soft-Brick der Geräte. Egal nach welcher Methode, diese Seriennummer hat keine Betriebserlaubnis bei Apple mehr...

Wie kann der Dieb mit den Geräten umgehen?

- SMD-Lötstation haben
- Zugriff auf Spare-Part-Chips aus gleicher Modellserie haben
- SMD-Chip auslöten und anderen einlöten

Dies ist ein Prozess der fast ausschließlich nur im Produktionsland der iPhones gemacht werden kann.
Die Endpunkte der Hehlereiware sind in der Regel nicht die Produktionsländer.

Quirks and Features

- Mit eurem MDM hat Apple nichts zu tun

- Apple kann erst Geräte sperren, wenn sie Internetverbindung hatten, und eine Apple ID auf dem Gerät aktiv war
- Über das Enforcing der Apple ID sorgt ihr dafür dass ein Apple Device ab dem ersten einschalten im "Wo ist" Netzwerk von Apple ist.

Version #12
Erstellt: 2024-04-09 11:11:05 UTC von Konstantin
Zuletzt aktualisiert: 2025-07-08 11:27:42 UTC von Konstantin