CIT Ebikon Consulting

State of the Art aus einer Hand

Wie sie Android Geräte gezielt gegen Ransomware absichern

Der Einsatz von Android und insbesondere auch in Unternehmen, ist nicht mehr wegzudenken. Android hat mittlerweile einen Marktanteil von 84 Prozent erreicht. Zwei große Probleme sind die hohe Zahl an bösartigen Apps und die relativ große Offenheit des Android-Systems. Mit dem Grad der weltweiten Markdurchdringung von Android wächst auch dessen Attraktivität für bösartige Software (99 Prozent aller Malware wird für Android und seine Open Source-Architektur programmiert), insbesondere RANSOMWARE, die in die Privatsphäre der Smartphone-Nutzer eingreift und beispielweise Daten stehlen kann oder Gespräche mitschneidet.

Was den Einsatz von Android-Geräten so gefährlich macht

Egal, ob in Ihrem Unternehmen die Politik „Bring your own device (BYOD)" vorherrscht oder sich die Geräte im Unternehmensbesitz befinden: grundsätzlich gilt: Alle Tablets und Smartphones sind mit den gleichen Sicherheits-Features auszustatten. Auf die Fragen, was den Einsatz so heikel macht, gibt es eine ganze Reihe von Antworten auf den unterschiedlichsten Ebenen. Android ist in der Welt der offenen Systeme vollständig angekommen.

Eine Verschlüsslung der Hardware fehlt gänzlich. Vergegenwärtigen Sie sich, dass Smartphones letzten Endes einen handlichen PC darstellen.

Ein weiteres Problem ist wie immer der Mensch selbst. Die im Store angebotenen Apps werden von Google nicht geprüft und die bei der Installation von neuen Anwendungen abgefragten Privilegien verführen dazu, der neuen App ohne weiteres Nachdenken zu viele Rechte einzuräumen.

Die schlechte Update-Versorgung bleibt eines der größten Probleme für Android-Benutzer. Nur 0,7 Prozent aller aktiven Geräte liefen laut Google Anfang Januar mit der aktuellen Android-Version 6.0. Zwei Drittel aller Benutzer verwenden sogar Android 4.4.4 und noch ältere Versionen – und haben damit ein deutlich veraltetes Betriebssystem sowie stehen damit Tür und Tor für Schädlinge, insbesondere für Ransomware offen.

Welche Sicherheits-Features für Android zur Verfügung stehen, sehen Sie in der Tabelle.

Sicherheits-Feature	Beschreibung
App Store	Google Play Store sowie alternative App Stores sind erlaubt, Standardeinstellung ist aber Play Store. Bleiben Sie auf dem Play Store. Damit sind sie einigermassen sicher.
Apps	Prüfung im Google Play Store automatisch mit Google Bouncer.
App-Berechtigungen	Der Benutzer gewährt bei der Installation die Zugriffsrechte. Ab Android 6 können Sie die Freigaben selbst steuern
App-Code	Der App-Code lässt sich auch mit eigenen Zertifikaten signieren
Sand Box	Apps können nicht auf Daten anderer Apps zugreifen; einzige Ausnahme sind Daten auf externen Speicherkarten
Orten/Sperren/Löschen verlorener Geräte	Möglich über Android-Device-Manager
Betriebssystem-Updates	Unbedingtes Muss, da Verbesserungen einfliessen
Verschlüsselung	Optional, nicht voreingeschaltet.
Zugriffsschutz	PINs, Passwörter oder Muster
Security-Apps	Breites Angebot der führenden Antivirenfirmen. Unbedingtes Muss für ihr Smartphone.
Sicherheitslücken	In 2016 wurden bis Juli 40 Sicherheitslücken dokumentiert und geschlossen. Achten Sie daher auf Updates.
Speicherschutz	Address Space Layout Randomization (ASLR) und Data Execution Prevention (DEP) sind spezielle Schutztechniken gegen Angriffe
Digitale Zertifikate	Erschwert es Angreifern, Man-in-the-Middle-Attacken durchzuführen
Härtung des Betriebssystems	Verhinderung von Root-Zugriff beim Versuch von Exploits

Wie Sie Android-Geräte in 10 Schritten sicher in Ihrer Unternehmensstruktur einsetzen können

Schritt 1: Setzen Sie die Sicherheitsrichtlinien auch für Ihre Android-Tablets konsequent durch, so wie Sie Ihre bisherige Unternehmensstruktur abgesichert haben. Bei Android-Tablets und Android-Smartphones gilt es, erhöhte Sicherheitsmaßnahmen anzuwenden. Bedenken Sie auch die IT-Compliance-Vorgaben. Schalten Sie wenn möglich auch die GPS-Ortung ab, sofern Sie diese nicht unbedingt benötigen.

Schritt 2: Sichern Sie die Verbindungen per SSL oder VPN ab.

Schritt 3: Setzen Sie auf Sandboxing-Apps. Durch das Downloaden von Apps von Drittanbietern kann unter Umständen Schad-Software mitgeladen werden.

Schritt 4: Installieren Sie Security-Apps für die E-Mail und Geräte-Security.

Schritt 5: Setzen Sie digitale Zertifikate ein. Android ab Version 4.4 warnt den User, wenn dem Gerät eine neue Zertifizierungsstelle (Certificate Authority, CA) hinzugefügt wird, was die Identifizierung von Man-in-the-Middle-Attacken innerhalb des lokalen Netzwerks erleichtert. Gleichzeitig erschwert Google es raffinierten Angreifern mit dem Certificate Pinning, den bei Google-Services ein- und abgehenden Netzwerk-Traffic abzufangen, indem sichergestellt wird, dass nur SSL-Zertifikate aus der Weißen Liste sich mit bestimmten Google-Domains verbinden können.

Schritt 6: Betriebssystemhärtung unter Android ab V. 4.4. SELinux (Secure Linux) läuft nun im Enforce-Modus anstatt im Permissive-Modus. Das trägt dazu bei, Benutzerrechte durchzusetzen und Privilegieneskalationen zu verhindern, wenn etwa ein Exploit versucht, Root-Zugriff zu erhalten. Android ab V. 4.4 ist mit der „FORTIFY_SOURCE“-Einstellung in Level 2 kompiliert, was die Implementierung von Pufferüberlauf-Exploits erschwert.

Unter diesem Schritt nutzen Sie auch Mandatory Access Control (MAC).

Schritt 7: Verschlüsseln Sie Ihre Nachrichten, zum Beispiel mit OpenPGP (Pretty Good Privacy) für Android. Diese Software steht Ihnen kostenlos im App Store zur Verfügung.

Schritt 8: Setzen Sie Ihre eigenen Apps im Unternehmen ein.

Schritt 9: Spielen Sie stets aktuelle Sicherheits-Patches ein und halten Sie die Geräte mit Apps so schlank wie möglich.

Schritt 10: Schützen Sie den Lockscreen mit einem Passwort. Aus Bequemlichkeit nutzen nur wenige diese Funktion. Die Sicherung durch das Zeichnen einer Geste oder gar keine Sicherung ist weitaus beliebter. Durch Verschmierungen auf dem Bildschirm lässt sich die Geste jedoch leicht nachvollziehen.

Weitere Schutzmassnahmen

Mobile Device Management (MDM) ist eine weitere Möglichkeit, Ihre mobilen Geräte zu schützen. Das ist ein System, das sich von der automatisierten Erstkonfiguration über das Einspielen aktueller Patches und Anwendungen bis zur Überwachung der aufgespielten Daten nebst Remote Wiping beim unautorisierten Besitzerwechsel um alle Phasen des Smartphone-Lebens fürsorglich kümmert. Eine weitere Möglichkeit des Schutzes bietet Samsung KNOX. Es wurde speziell für Unternehmen entwickelt und bietet Unterstützung für VPN (Virtual Private Network), On-Device Encryption (ODE), Smart-Card-Authentifizierung und eine integrierte Diebstahlsicherungstechnologie.

Einige Whitepapers dazu finden Sie hier: „https://www.samsungknox.com/de/knox-technology/white-papers“.

Diese App-Berechtigungen sollten Sie in Ihrem Unternehmen als besonders gefährlich einstufen

- Uneingeschränkter Internetzugriff: Die App kann selbsttätig auf Up- und Download von Web-Inhalten zugreifen.
- Adressbuch lesen und verändern: Viele Malware-Apps mit dieser Berechtigung geben Kontakte an Dritte weiter.
- Protokolldaten lesen: Viele Malware-Apps mit dieser Berechtigung geben Kontakte an Dritte weiter.
- Telefonstatus lesen und identifizieren: Die App darf auslesen, ob Sie gerade telefonieren, damit sie sich gegebenenfalls automatisch abschalten kann. Allerdings liegen damit außerdem die IMEI- und IMSI Nummern Ihres Geräts offen, womit Ortung und Verfolgung möglich sind. Diese Daten werden sonst nur zu Fahndungszwecken von der Polizei verwendet.
- Bekannte Konten suchen: Die App darf auslesen, welche Konten mit dem Gerät verbunden sind.
- Kontoliste verwalten: Die App darf selbsttätig Konten löschen und hinzufügen.
- Apps installieren: Die App darf selbsttätig andere Apps installieren.
- Stand-by-Modus deaktivieren: Die App darf den Wechsel in den Stand-by-Modus sperren.
- Bilder und Videos aufnehmen: Die App darf auf die Kamera zugreifen.

Wie Sie ein Android Gerät verschlüsseln können

Klicken Sie auf „Einstellungen“ -> „Security“ und wählen Sie „verschlüsseln“. Fragen Sie sich vorher, welchen Grad Sie zur Verschlüsselung verwenden wollen. Android 3 bis 6 erlauben optional zum Schutz des Dateisystems eine Verschlüsselung von 128 Bit AES CBS und ESSIV SHA-256. Zum Vergleich: Das Apple iPad erlaubt eine Verschlüsselung von 256 Bit AES und ist mit einer Hardware-Verschlüsselung ausgestattet.

Fazit: Die Offenheit des Android-Betriebssystems birgt viele Gefahren für Ihr Unternehmen, die Sie als Administrator vor dem ersten Einsatz, so gut es geht, eliminieren bzw. reduzieren sollten. Nutzen Sie dazu die in diesem Artikel beschriebenen Sicherheits-Features. Seien Sie sich stets bewusst, dass der Einsatz mobiler Technologien in Ihrem Unternehmen ein großes Gefahrenpotenzial bergen kann. Richten Sie Ihren Fokus auf die Absicherung der Geräte. Wichtig dabei ist auch die strikte Einhaltung Ihrer Sicherheitsrichtlinien.

Dies ist ein Whitepaper von

IT Ebikon Consulting
State of the Art aus einer Hand

Internet: https://IT-Consulting-Ebikon.ch
e-mail: support@it-consulting-ebikon.ch
Telefon: +41 79 267 40 41

Adele FireWall
So sicher wie ein Fels in der Brandung