Deniz Kural 3DHIT

1. Was ist sicherer iOS / Android?
   iOS

   - Warum?

     Es gibt kein einziges Sicherheitsfeature von Android, dass sicherer ist als bei iOS. Das heißt aber nicht direkt das Android unsicher ist. Jedes Gerät ist sicher genug, wenn der Benutzer ein gewisses Sicherheitsbewusstsein hat. Jedoch erleichtert iOS dem Benutzer aus IT-Sicherheitsperspektive durch sein geschlossenes Betriebssystem und die streng kontrollierten Apps die Umsetzung von Sicherheitsvorkehrungen.

   - Welche Sicherheitsfeatures haben diese Betriebssysteme?

     Sicherheitsfeatures: App-Berechtigungen, Geräteverschlüsselung, Benutzerauthentifizierung, Sicherheitsupdates, App-Überprüfung, Sandboxing

   - Stelle die Sicherheitsfeatures gegenüber.

     App-Berechtigungen: Beide Betriebssysteme funktionieren hier ähnlich. Der User kann einstellen, welche Berechtigungen eine App auf dem Gerät hat.

     Geräteverschlüsselung: Bei beiden Betriebssystemen gibt es eine Verschlüsselung, jedoch ist die bei Android nicht standartmäßig aktiviert. Beide verwenden denselben Verschlüsselungsalgorithmus und funktionieren sehr ähnlich.

     Benutzerauthentifizierung: Beide Betriebssysteme über eine Benutzerauthentifizierung, wenn das Gerät verwendet wird. Bei beiden Geräten kann man sich mit einem Passwort, PIN, Fingerabdruck oder Gesicht anmelden.

     Sicherheitsupdates: Bei iOS gibt es im Vergleich zu Android eine längere Supportzeit. Da es so viele verschiedene Android Geräte gibt, ist es unmöglich für jedes Gerät ein individuelles Update zu erstellen. Bei iOS ist das anders.

     App-Überprüfung: Bevor eine App im App Store/Play Store veröffentlicht wird, wird diese auf Fehler und Sicherheitslücken überprüft. Bei iOS ist die Überprüfung jedoch strenger und genauer.

     Sandboxing: Bei beiden Betriebssystemen wird jede App in einer isolierten Umgebung ausgeführt, um Schutz zu garantieren.

2. Was kostet iOS / Android Zero-Days (Quelle)

   Der Preis für ein Zero-Day-Exploit variiert je nach Sicherheitslücke. Man kann davon ausgehen, dass man bei Android 100.000$ bis 200.000$ im Durchschnitt zahlt und bei iOS von 200.000$ bis 500.000$ im Durchschnitt zahlt.

   Quelle: https://threatpost.com/android-zero-days-worth-more-iphone-exploits/147981/#:~:text=Exploit%20broker%20Zerodium%20has%20implemented,on%20the%20global%20cyberweapons%20market

3. Was verkaufen folgende Firmen (Suche Werbematerial/Verkaufsbroschüren):

    - Zerodium: Zerodium kauft verschiedene Arten von Exploits von Privatpersonen ab und verkaufen diese wiederrum an Sicherheitsbehörden oder Regierungen.
    - NSO: NSO verkauft Überwachungs- und Spionagesoftware an Sicherheitsbehörden oder Regierungen. Ihr bekanntestes Produkt ist die Software Pegasus.
    - FinFisher: FinFisher verkauft ebenfalls Überwachungs- und Spionagesoftware. Ihr bekanntestes Produkt ist die Software FinSpy.
    - BoldIntel: BoldIntel verkauft Deep Adaptive Intelligence-Lösungen für nationale Sicherheitsbehördern.
    - DSIRF: Das Unternehmen DSIRF ist bereits geschlossen, jedoch haben Sie einen Trojaner entwickelt und wurden mit Kunden aus Russland in Verbindung gesetzt.

Quellen:

https://zerodium.com/program.html

https://de.wikipedia.org/wiki/NSO_Group_Technologies

https://de.wikipedia.org/wiki/FinFisher

https://www.nsogroup.com/

https://www.boldintel.com/

https://finder.startupnationcentral.org/company_page/bold

https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/