Man-in-the-Middle-Angriffe

Netzwerkangriffe auf Mobilgeräten verhindern

Da Mobilgeräte verstärkt auf sensible Daten zugreifen, werden mobile Bedrohungen immer häufiger und zunehmend ausgeklügelter. Man-in-the-Middle-Angriffe sind ein Beispiel für diese Art von Bedrohungen. Laut einer kürzlich veröffentlichten Studie berichten 24 % aller Unternehmen, dass unternehmensintern genutzte Mobilgeräte bereits mindestens einmal eine Verbindung zu einem bösartigen WLAN-Netzwerk hergestellt haben.[1]

Ablauf von Man-in-the-Middle-Angriffen

Man-in-the-Middle-Angriffe auf Unternehmensdaten erfordern in der Regel zwei Schritte:

1. Zugang zum Netzwerkverkehr
2. Entschlüsselung der Daten

Der zweite Schritt ist wichtig, da Unternehmensdaten fast immer verschlüsselt sind und das Einschalten in den Netzwerkverkehr somit nicht unbedingt einen Datendiebstahl zur Folge haben muss.

1. Zugang zum Netzwerkverkehr

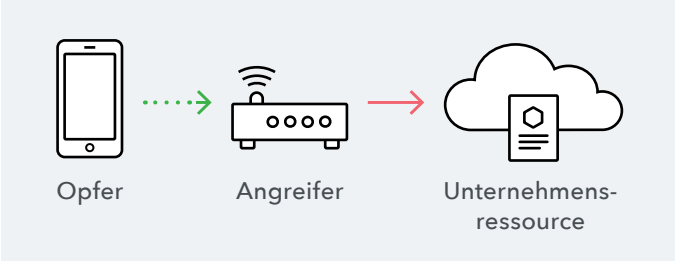
Angreifer können sich auf unterschiedliche Art und Weise Zugang zum Netzwerkverkehr verschaffen, zum Beispiel:

A. durch Vortäuschen eines WLAN- oder Mobilfunknetzes

B. indem Sie ein VPN anweisen, den Datenverkehr über ihr Netzwerk zu leiten

C. durch Einrichtung einer Proxy-Verbindung, die den Datenverkehr zu ihrem Netzwerkpfad umleitet

D. durch ARP-Spoofing (Address Resolution Protocol), bei dem der Angreifer anstelle eines Gateways die eigene Hardwareadresse angibt



2. Entschlüsselung der Daten

Hat ein Angreifer Zugriff auf einen Netzwerkpfad, muss er im nächsten Schritt entweder die Verbindung oder den Anwender manipulieren, um verschlüsselte Daten einsehen zu können. Dies erfolgt gewöhnlich über eine der folgenden Methoden:

Host Certificate Hijacking

Der Angreifer installiert eine von ihm kontrollierte bösartige Zertifizierungsautorität im vertrauenswürdigen Root Certificate Authority Store des attackierten Geräts und kann sich so als Unternehmensressource ausgeben, mit der das Opfer sicher kommunizieren kann.

SSL-Stripping

Der Angreifer unterwandert unverschlüsselte Verbindungen des Opfers, entfernt das „S" in HTTPS-Verbindungen und kann dadurch üblicherweise verschlüsselte Daten im einfachen HTTP-Textformat anzeigen lassen.

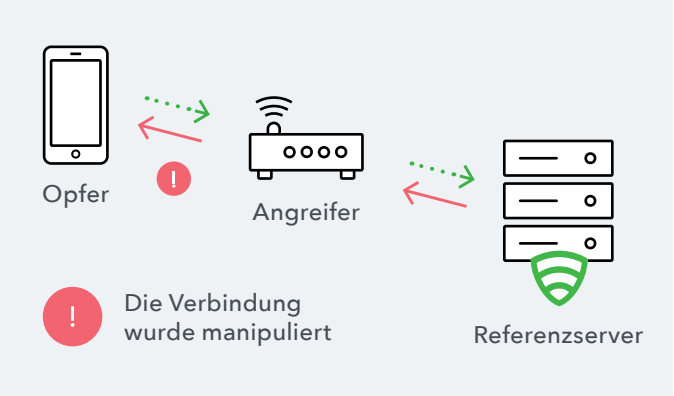
TLS-Protocol-Downgrade

Der Angreifer manipuliert die bestehende Verbindung, um das verwendete Protokoll oder die Cipher-Suites herabzustufen und die Verbindungssicherheit zu schwächen.

[1] CIO.com, „One-fifth of IT pros say their companies had mobile data breach", 2016

Das Sicherheitskonzept von Lookout

Unsere On-device-App überprüft die Referenzserver anhand bekannter Zertifikateigenschaften und Sicherheitsprotokollkonfigurationen. Auf diese Weise können wir die *erwarteten* Netzwerkkonfigurationseigenschaften mit den *beobachteten* Eigenschaften vergleichen. Indem wir analysieren, ob die beobachteten den erwarteten Eigenschaften entsprechen, können wir feststellen, ob Verbindungen von einem Angreifer mithilfe der zuvor beschriebenen Methoden manipuliert wurden.



Der Ansatz von Lookout minimiert False-Positives

Lookout-Warnmeldungen beschränken sich NICHT nur auf:

- Captive Portals in Cafés oder Hotels
- Proxy-Verbindungen
- VPN-Verbindungen

Anfällig für False-Positives

Warnungen WERDEN ausgegeben bei:

- Host Certificate Hijacking
- SSL-Stripping
- TLS-Protokoll-Downgrades

Unternehmensrelevante Bedrohungen

Lookout konzentriert sich bei seinem Ansatz auf Risiken mit der größten Relevanz für Unternehmen, d. h. auf Versuche, verschlüsselte Unternehmensdaten während der Übertragung abzufangen.

Die meisten modernen Mobilitätskonzepte schränken Verbindungen zu WLAN-Netzen in Cafés, Hotels oder Flughäfen nicht ein, weil dies die Produktivität mindern würde. Bei anderen Konzepten zur Erkennung von Man-in-the-Middle-Angriffen wiederum erhalten Administratoren bei diesen alltäglichen Aktivitäten jedesmal Warnmeldungen. Diese Ansätze führen zu einer wahren Flut von False-Positives, die IT-Organisationen üblicherweise nicht effektiv handhaben können.

Lookout konzentriert sich bei seinem Konzept auf Verbindungstypen, die verschlüsselte Daten gefährden. False-Positives für bösartige Netzwerkverbindungen werden folglich minimiert. User können eingeloggt bleiben und auch unterwegs produktiv arbeiten.