Barrierefreie Version
CSBW-Factsheet: Cybersecurity-Wissen kompakt

Zum Thema: **Man-in-the-Middle-Angriffe**

Wie kann man sich vor einem Man-in-the-Middle-Angriff schützen?

Bei einem Man-in-the-Middle-Angriff (MitM) klinken sich Cyberkriminelle in einen Kommunikationsvorgang ein. Sie haben das Ziel, sensible Daten abzugreifen oder zu manipulieren. Dabei sind die Einfallstore für Cyberkriminelle vielfältig: Sie reichen von öffentlichen WLAN-Hotspots bis zu unverschlüsseltem Datenverkehr und Infektionen mit Schadsoftware. Angriffsziel kann die tatsächliche Kommunikation zweier realer Personen bis hin zur Kommunikation zwischen Systemen sein.

Schaubild:

Kommunikationspartei 1 | Angreifende | Kommunikationspartei 2

Beschreibung des Schaubilds: Das Schaubild zeigt auf der linken Seite einen PC der Kommunikationspartei 1, in der Mitte den Angreifenden auf einem Monitor und auf der rechten Seite einen PC der Kommunikationspartei 2.
Pfeile zeigen die Kommunikationsrichtung Hin und Her zwischen den jeweiligen Kommunikationsparteien und dem Angreifenden an.

Was ist ein Man-in-the-Middle-Angriff?

Bei einer solchen Attacke greifen Cyberkriminelle in die Kommunikation zwischen zwei Parteien ein, um diese unbemerkt zu manipulieren und/oder zu überwachen.[1]

Das Ziel von Angreifenden ist es, zwischen den beiden Kommunikationsparteien zu stehen, um die Kontrolle über den Datenaustausch zu haben. Dabei können die Kriminellen die ausgetauschten Informationen einsehen und manipulieren. In manchen Fällen erlangen sie die Kontrolle, indem sie den jeweiligen Kommunikationspartnern vortäuschen, der legitime Partner am anderen Ende zu sein.[1]

Dabei handelt es sich nicht ausschließlich um die Kommunikation zweier realer Personen. Ein solcher Angriff ist auch auf IT-Systeme möglich, beispielsweise in der Kommunikation zwischen zwei Systemen.

Dadurch können sensible Informationen, wie Passwörter und TANs, in die Hände von Kriminellen fallen.[2]

Es gibt unterschiedliche Methoden, um sich unbemerkt in einem Kommunikationsvorgang zu positionieren.

Gängige Beispiele sind:

1. Das Ausnutzen unverschlüsselter WLAN-Netzwerke. Diese sorgen für einen unverschlüsselten Datenaustausch zwischen zwei Kommunikationsparteien. Angreifende können die unverschlüsselten Daten abgreifen.
2. Das Einschleusen von Malware (Schadprogrammen) oder sogenannte Spyware (Spionagesoftware). Diese Schadsoftware wird unerkannt auf einem Gerät installiert und spioniert die Zielperson aus.
3. Das Ausspähen von Netzwerkverbindungen beispielsweise durch Rouge Access Points. Hier richten Angreifende eigene unsichere WLAN-Zugangspunkte („Access Points“) ein und versuchen Geräte, die sich automatisch mit offenen WLAN-Netzen verbinden, anzusteuern und deren Netzwerkverkehr abzuhören.

Welche Folgen können Man-in-the-Middle-Angriffe haben?[3]

Abhören des Datenverkehrs:
Cyberkriminelle können Ihre Daten mithilfe unterschiedlicher Methoden abfangen. Die so gewonnenen Daten können für weitere kriminelle Aktivitäten wie beispielsweise einen Identitätsdiebstahl genutzt werden.

Umleitung des Datenverkehrs:
Ihre Daten werden von den Cyberkriminellen ohne Ihr Wissen weitergeleitet. Die Empfänger können beispielsweise andere Kriminelle sein.

Manipulation der Kommunikation:
Cyberkriminelle manipulieren Ihre Kommunikation, indem beispielsweise Ihre

persönlichen Informationen gestohlen werden oder gefälschte Daten (z.B. falsche Bankverbindungen in Rechnungen) eingeschleust werden.

Tipps zum Schutz vor Man-in-the-Middle-Angriffen:

Verschlüsselung verwenden:
Nutzen Sie Verschlüsselungstechniken wie beispielsweise TLS (Transport Layer Security) als Transportverschlüsselung oder insbesondere in der -E-Mail-Kommunikation eine Ende-zu-Ende-Verschlüsselung.[2]

Auf Zertifikate achten:
Achten Sie darauf, ob ein (Sicherheits-)Zertifikat vorliegt. Insbesondere bei Webseiten sollten Sie nur verschlüsselte Verbindungen nutzen. Dies erkennen Sie an dem Zusatz „https“ (Hypertext Transfer Protocol Secure) in der URL-Zeile. Zusätzlich kann auch ein Schlosssymbol ein Hinweis auf eine verschlüsselte Verbindung sein.

Zwei-Faktor-Authentifizierung:
Nutzen Sie eine Zwei-Faktor-Authentifizierung, um Ihre Geräte und Accounts mit einer zusätzlichen Barriere zu schützen. Cyberkriminelle benötigen zum Zugriff auf Ihre Geräte und Accounts nicht nur Ihr Passwort, sondern noch weitere Faktoren, die einen höheren Aufwand in der Beschaffung darstellen. Weitere Informationen hierzu finden Sie auf dem Factsheet „Zwei-Faktor-Authentifizierung“.

Öffentliche WLAN-Verbindungen meiden:
Vermeiden Sie die Nutzung öffentlicher WLAN-Netzwerke, da diese häufig unverschlüsselt sind. Sie sollten bei der Nutzung öffentlicher WLAN-Netzwerke auf die Eingabe von persönlichen Daten wie z.B. beim Online-Banking oder in Online-Shops verzichten. Nutzen Sie öffentliche WLAN-Netzwerke nur mit einer VPN-Verbindung. Weitere Informationen hierzu finden Sie auf dem Factsheet „Öffentliche WLAN-Netzwerke/VPN“.

Regelmäßige Updates:
Halten Sie Ihre Programme und Anwendungen mit regelmäßigen Updates auf dem aktuellen Stand.

Schutz vor Spyware:
Bei Spyware handelt es sich um eine Schadsoftware, die Sie ausspionieren kann. Laden Sie Apps und Software stets aus sicheren und vertrauenswürdigen Quellen (z.B. offizielle Webseite des Softwareanbieters) herunter.

Quellen:

[1] Was ist ein Man-in-the-Middle-Angriff? (csoonline.com)

[2] BSI - E-Mail Verschlüsselung - E-Mail-Verschlüsselung (bund.de)

[3] Man-in-the-Middle-Attacke: Die unsichtbare Bedrohung (dr-datenschutz.de)

Weitere CSBW-Factsheets unter folgendem Link:
Wissen kompakt: Factsheets | Cybersicherheitsagentur

Oder QR-Code scannen:

www.cybersicherheit-bw.de

CSBW – Abteilung 1: Prävention – Stand 12.2024
Kontakt: schulungen@cybersicherheit.bwl.de