

Man in the Middle 2.0

Das Thema scheint sich langsam zu einem Dauerbrenner zu entwickeln... Da habe ich wohl bei vielen einen Nerv getroffen. Nachdem ich heute auf der IT-SecX an der FH St. Pölten einen Vortrag zum Thema "Man-In-The-Middle- Attacken und DNS Spoofing" gehalten habe, gibt's hier nochmal für alle, die vielleicht keine Zeit hatten, das Paper zum Nachlesen.

Viel Spass und wie immer freue ich mich natürlich über Kommentare, Fragen und Anregungen...

Einleitung

Sicherheit im IT Bereich ist immer noch ein vernachlässigtes Thema, bei Privatanwendern sowieso, aber auch bei Unternehmen werden die Gefahren oft unterschätzt. Das gängige Motto hier scheint "Mir wird schon nichts passieren" zu sein. Und dann wundern sich die Leute wie sie Opfer eines Angriffs werden konnten...

"Not to know is bad – not to wish to know is worse!"

Immer wieder werde ich mit Vorwürfen konfrontiert, allein aufgrund der Kenntnis solcher Angriffstechniken ein "böser Hacker" zu sein, oder mit der Veröffentlichung solcher Methoden den Kriminellen nur das Werkzeug in die Hand zu geben und alles nur noch schlimmer zu machen.

Dazu möchte ich hier kurz Stellung nehmen.

"Security by obscurity" ist in der IT einer der schlechtesten Ansätze, die es gibt.

Unwissen ist extrem gefährlich. Unwissen sorgt letztendlich nur dafür, dass diejenigen, die solche Angriffe durchführen ein leichtes Spiel haben und mit keinerlei Gegenwehr rechnen müssen.

Nur wenn ich weiß was die Bedrohung ist und wie sie funktioniert kann ich wirksame Gegenmaßnahmen einleiten. Durch Wissen um die Bedrohung und Kenntnis der Methoden bin ich erst in der Lage mich entsprechend zu schützen.

Das ist der Grund, warum ich denke, dass man solche Themen nicht geheimhalten soll und darf.

Hinweis

Bevor ich jetzt zu den Techniken und konkreten Beispielen einer Man-In-The-Middle- Attacke übergehe noch ein kleiner Hinweis.

Für alle "neugierigen Spielkinder" an dieser Stelle der Hinweis, dass es schon aus rechtlicher Sicht ratsam ist, die vorgestellten Techniken in einer Testumgebung auszuprobieren.

Ein Angriff im Live- Betrieb kann zu unerwünschten und unbeabsichtigten Nebenwirkungen führen. Fragen Sie dazu Ihren Admin oder einen IT-Sicherheitsexperten Ihres Vertrauens.

Was ist eine Man-In-The-Middle- Attacke?

Einfach gesagt, versteht man unter einer Man-In-The-Middle- Attacke, dass der Datentransfer zwischen zwei Kommunikationspartnern (transparent) über einen dritten – den Angreifer – läuft. Transparent meint hier, dass weder der Absender noch der Empfänger davon etwas merken. Die Kommunikationspartner sind also nicht direkt miteinander verbunden, sondern über einen unbemerkten Dritten, der ähnlich wie ein Gateway, die Anfragen weiterleitet.

Der Angreifer ist damit in der Lage unbemerkt jegliche Kommunikation mitzulesen und zu manipulieren. Solch ein Angriff ist sowohl für den Sender als auch für den Empfänger extrem schwer zu erkennen. Sie sehen ihre gewohnten und erwarteten Inhalte, schließlich sind sie ja, wenn auch über einen Umweg, mit dem richtigen Adressaten verbunden.

Der Angriff im Detail

Ziel einer Man-In-The-Middle- Attacke ist, wie gesagt, sich unbemerkt in die Kommunikation einzuschalten um diese mitzulesen oder zu manipulieren.

Der Angreifer spielt dabei dem Sender vor der Empfänger zu sein und dem Empfänger der Sender zu sein.

Der Ablauf sieht immer in etwa gleich aus:

Man in the Middle 2.0

Das Opfer (nennen wir sie Heidi) sendet eine Anfrage an den Empfänger (etwa an Peter) die vom Man-In-The-Middle abgefangen wird. Der Angreifer kann die Anfrage von Heidi in Ruhe lesen und modifizieren. Als zweiten Schritt baut der Angreifer eine Verbindung mit dem eigentlichen Empfänger, Peter, auf und leitet die Anfrage an ihn weiter. Auf die Antwort von Peter hat der Man-In-The-Middle natürlich auf die selbe Art ebenfalls Zugriff.

Der schwierigste Teil des Angriffs ist dabei die Verbindung auf den eigenen Rechner umzuleiten. Hilfreich dabei sind Methoden wie ARP Spoofing und DNS Manipulation.

Es gibt verschiedene Techniken sich in der Art in die Verbindung zwischen zwei Rechnern einzuklinken. Die Durchführung ist dabei abhängig von verschiedenen Faktoren, wie z.B. den Netzwerken, der Verbindung, Verschlüsselung etc... Der Man-In-The-Middle kann auf verschiedenen Ebenen seinen Angriff ansetzen, direkt am Rechner des Opfers oder aber auf Netzwerkebene etc.

Grundsätzlich unterscheidet man zwei Arten von Angriffen: den physikalischen (mittels Kabelverbindung) und den logischen Zugriff.

Ausgewählte Beispielszenarios

Der Postbote, öffentliche WLAN Hotspots und andere Kriminelle

Zur Veranschaulichung des Themas ein Beispiel aus der "analogen Welt":

Der Postbote ist der Man-In-The-Middle zwischen Sender und Empfänger. Er kann die Post des Empfängers lesen, seine eigenen Grüße auf der Postkarte von Tante Erna hinterlassen. Der Postbote hat physikalischen Zugang zur Kommunikation und kann sie auf diesem Weg manipulieren.

Bei Computerangriffen handelt es sich in der Regel nicht um einen physikalischen sondern um einen logischen Zugang zur Kommunikationsverbindung.

WLAN Hotspots oder Noch einfacher geht's nicht

Eine klassische Variante wäre der Angriff über einen öffentlichen WLAN Hotspot. WLANs allgemein und öffentliche Hotspots im speziellen sind sehr beliebte Angriffspunkte. Bei kostenlosen Hotspots am Flughafen etc. ist es recht einfach. Der Angreifer spielt allen Usern im WLAN Netzwerk vor, der Router zu sein. Das heißt alle Anfragen gehen zuerst an den Angreifer, der sie bequem mitlesen etc. kann und leitet sie an den tatsächlichen Adressaten weiter. Gibt sich der Angreifer als Gateway aus kann er die Verbindungen auch ganz leicht manipulieren. Er kann also Verbindungen verweigern, abbrechen, etc...

Mittels DNS Spoofing ist es dem Angreifer möglich, einer Domain andere IP Adressen zuzuordnen. So kann beispielsweise das Opfer, dass eigentlich auf google.com zugreifen wollte auf eine beliebige andere Seite leiten.

Intranet, Firmennetzwerke und Spass mit Studenten

In diesem Beispiel hat der Chef Zugriff auf den Router, der das Intranet mit dem Internet verbindet. Er leitet alle Anfragen, die nach draußen gehen auf einen transparenten Proxy um. Jede Verbindung wird also mitgeloggt. Der Chef sieht genau von wo, wann auf welche Seiten zugegriffen wird. Die Opfer (in dem Fall die Mitarbeiter) können ganz normal surfen und bekommen davon in der Regel nichts mit.

Sollte der "böse Chef" wenig begeistert von "YouPorn" surfenden Mitarbeitern sein, ist es für ihn natürlich ein leichtes diese Anfragen zu unterbinden.

Es können auch unbemerkt Bilder, Wörter oder ganze Texte ausgetauscht und manipuliert werden.

Diese Möglichkeit hat natürlich nicht nur ein Firmenchef, das kann auch UPC z.B. und sie machen das auch, aber das ist eine andere Geschichte....

Dazu gab es ein interessantes Experiment an der Hochschule für Gestaltung in Stuttgart. Hier haben Studenten im Rahmen ihrer Diplomarbeit den gesamten Internettraffic ihrer Uni manipuliert. So wurde z.B. der Name des Politikers Al Gore mit Al Bundy ausgetauscht. Die Reaktion der Benutzer war überraschend, oder auch nicht, denn bis auf einen Fall hat niemand die Manipulationen bemerkt, auch wenn sie noch so offensichtlich

Man in the Middle 2.0

waren. <http://www.fitug.de/debate/0012/msg00249.html>

Abschließend bleibt zu vermerken, dass keine Verbindung als "sicher" anzusehen ist. Potenziell kann jede Verbindung mitgelesen und manipuliert werden. Daher ist prinzipiell immer davon auszugehen, dass jemand den Quatsch mitliest den man so von sich gibt.

Google Phishing oder Wo bitte geht's nach Fidji?

Die meisten bisher üblichen Phishing Angriffe sind keine Man-In-The-Middle- Attacken. Sie sind noch einfacher gestrickt und verlassen sich ausschließlich auf das "Look and Feel" Prinzip. Die Phisher leiten ihre Opfer direkt auf eine manipulierte Webseite auf ihrem eigenen Server. Sie spielen dem Opfer vor, der Adressat zu sein und interagieren direkt.

Die Zukunft des Phishing geht aber stark in Richtung Man-In-The-Middle- Attacke. Der Angreifer braucht keine lästigen Emails verschicken, keine URL Manipulation und gefälschten Webseiten mehr, er fängt die Anfrage ab und leitet sie schließlich an den tatsächlichen Empfänger weiter.

Immer beliebter wird z.B. das google Phishing. Der Angreifer stellt nach außen ein Reisebüro dar, das über google vom Opfer gefunden wird. Das urlaubsbedürftige Opfer gibt seine Reisewünsche an den Angreifer, der sie an ein real existierendes Reisebüro weiterleitet. Das Opfer bekommt also reale Flugdaten etc. zurück. Nun geht das Opfer zur Buchung über und gibt dem Angreifer bereitwillig seine Kreditkartennummer und alles was man sonst noch so braucht.

Es wurden schon Fälle bekannt, in denen der Angreifer dem Opfer den ersehnten Urlaub nicht vorenthielt. Er leitete die Buchung an das tatsächliche Reisebüro weiter, die dem Opfer dann zwei Wochen später die Reiseunterlagen per Post zukommen ließen, inklusive einer zweiten Rechnung, denn mit dem, von der Kreditkarte abgebuchten, Geld liegt der Angreifer mittlerweile aus Fiji unter Palmen.

Auf diese Weise ist es möglich so gut wie alle Sicherheitsmechanismen, wie Passwörter, TAN, Challenge-Response verfahren etc., auszuhebeln. Das Opfer liefert sie schließlich ganz ohne Wissen "frei Haus".

Theoretische Grundlagen

Was ist das Address Resolution Protocol?

Das ARP funktioniert ähnlich wie DNS, anstatt dem Domainnamen löst ARP aber die IP zu MAC Beziehung auf. ARP ist in der untersten Schicht der nicht physikalischen Gegend des OSI Modells anzutreffen.

ARP Spoofing

Mit gefälschten ARP Paketen spiele ich den Rechnern im Netzwerk vor, das Gateway zu sein. Ich sende nun an alle Teilnehmer in dem Netzwerk die manipulierte ARP Nachricht. Damit fälsche ich die ARP Tabellen des Netzwerks und in der Folge senden die Teilnehmer ihre Anfragen an mich. Ich kann alle Verbindungen mitlesen und sie nach Lust und Laune manipulieren. Anschließend leite ich sie an den tatsächlichen Empfänger weiter. Eine abhörbare Verbindung ist zustande gekommen.

Das reine Abhören via Sniffing ist nur in ungeswitchten Netzwerken möglich, mittels ARP Spoofing ist das auch in geswitchten Netzwerken kein Problem.

Switch, Hub, Router

Ein Hub leitet die Antwort an alle Teilnehmer des Netzwerkes weiter. Ein Switch ist da schon etwas intelligenter, er merkt sich woher die Anfrage kam und sendet die Antwort nur an den Adressanten zurück. Ein Router verbindet unterschiedliche Subnetze, dabei vergisst er die Macadresse.

Software- Beispiele

Fürs ARP Spoofing gibt es unter Linux ganz nette Software wie "Ettercap" und "Dsniff".

Man in the Middle 2.0

Unter Windows wäre "Chain&Able" eine Möglichkeit.

Folgen und unvorhergesehene Nebenwirkungen

Wie Eingangs schon kurz erwähnt, kann eine Man-In-The-Middle- Attacke unvorhergesehene Effekte haben und in den seltensten Fällen kann man am Beginn die volle Tragweite abschätzen. Was einem in jedem Fall klar sein muss ist, dass bei ARP Manipulation die DNS Einträge verändert und gespeichert werden. Sprich, wenn ich den Angriff beende und meinen Rechner abhänge, denken alle anderen im Netzwerk trotzdem ich bin das Gateway, was defacto bedeutet, dass das gesamte Netzwerk steht...

Prävention

Was ich an dieser Form des Angriffs besonders kritisch finde, ist, dass es offensichtlich von den Sicherheitsexperten nicht als kritisch wahrgenommen wird. Das erste Mal habe ich eine Man-In-The-Middle-Attacke vor 6-7 Jahren durchgeführt, möglich sind diese Angriffe schon viel länger. Das heißt, dass in der Zwischenzeit sich keiner die Mühe gemacht hat, diese Gefahrenquelle auszuschließen.

Im Gegenteil, es wurde nur noch schlimmer...

Das bringt mich nun zum letzten Punkt meines Vortrags – die Prävention.

Frei nach dem Motto "selbst ist der Mann (oder Frau)" ist jeder herzlichst eingeladen gewisse vorbeugende Maßnahmen zu treffen.

Verschlüsselung des Netzwerkverkehrs bzw. Authentifizierung von Paketen, beispielsweise durch SSL oder ähnliches

Einsatz von Network Intrusion Detection / Intrusion Prevention Systemen

Überwachung des ARP-Caches (ARPWatch, XARP2)

Statisches Routing

Generell:

Keine Administrationsrechte auf Client PCs

Anwenderschulung / Benutzersensibilisierung / Sensibilisierung der Administratoren und IT-Verantwortlichen

Sichere / komplexe Kennwörter; obwohl dies bei Klartextübertragung der Kennwörter wenig nützt, "zwingt man die beteiligten Systeme jedoch zum verschlüsselten bzw. gehashten Kennwortaustausch, macht das allemal Sinn"

Man in the Middle 2.0