PROTEUS SOLUTIONS
IT-Lösungen für den Mittelstand

Die klassischen Angriffsformen

Heutzutage ist eigentlich jeder der einen PC, ein Mobilfunktelefon oder Smart-Phone, das Internet, Bank- oder Kreditkarten benutzt für viele Angreifer ein potentielles Opfer. Seit Jahren sind die klassischen Angriffsformen bekannt, die Angreifer benutzten um ihr Ziel zu erreichen.

Ich möchte Ihnen heute diese Angriffsformen einmal einzeln definieren und einige kurze Erläuterungen dazu machen.

1. Impersonifizierung

Der Angreifer will durch den Angriff die Rechte erlangen, die einem legitimen Benutzer gewährt wurden. Er gibt sich dem System gegenüber als autorisierte Person aus. Diese Angriffsform basiert in der Regel auf der Ausspähung von Geheimnissen (z.B. Passwörtern).

Das Ausspähen von Kennwörter oder Zugangs-IDs ist eine recht einfache Methode. Sei es der berühmte Zettel unter der Tastatur oder in der obersten Schublade des Schreibtisches mit dem aktuellen Kennwort oder das Eingeben des PINs in den Bankautomaten, wenn jemand neben dran steht.
Aber auch etwas technischere Systeme wie z.B. Keylogger, Schadprogramme, die alle Tastatureingaben mitschneiden, sind Möglichkeiten, um an fremde Kennworte zu gelangen. Hierbei empfiehlt es sich ein gewisses Misstrauen an den Tag zu legen und auch Passwörter mal häufiger zu wechseln.

2. Systemlöcher

Der Angreifer möchte eine Applikation oder das Betriebssystem dazu veranlassen, eine Aktion durchzuführen, zu der er selbst nicht berechtigt ist. Dieser Angriff zielt in der Regel darauf ab, einen privilegierten Zugriff auf ein System zu erlangen. Der Angreifer erzeugt Eingaben, die bei der Erstellung der angegriffenen Software nicht vorgesehen waren. Bei schlechter Programmierung führt dies dazu, dass eine nicht vorhergesehene Ausnahmesituation eintritt, die z.B. dazu führt, dass anstelle einer Ausgabe einer Fehlermeldung, vom Angreifer übermittelter Programmcode ausgeführt wird.

Die merkt man z.B. wenn man sich die Logfiles seines Webservers genauer ansieht: hier werden im Regelfall alle aufgerufenen URLs gespeichert, und viele von denen sind teilweise länger als 1024 Zeichen und enthalten Parameter, die den Webserver veranlassen sollen Befehle auszuführen.
Aber auch immer wieder bekannt gewordene Lücken in Browsern, Büro- oder Anwendungssoftware bieten solche Systemlöcher. Daher sollte man bei bekannt werden dieser sofort auf die entsprechenden Patches oder Bugfixes der Hersteller zurückgreifen.

3. Transitives Vertrauen

Der Angreifer möchte den Zugriff auf ein System A (egal ob dieser legitim ist oder nicht) dazu nutzen, Zugriff auf ein System B zu erlangen. Dabei bedient er sich der Tatsache, dass das System A auf dem System B besonderes Vertrauen und damit unfangreiche Rechte genießt.

Wenn ein Angreifer in ein ansonsten gut gesichertes Netz eindringen will, sucht er häufig nach Rechnern oder Netzen, denen das Zielsystem vertraut (z.B. der

Arbeitsplatz des Chefs). Sind diese weniger stark gesichert, so verwendet er sie als Sprungstelle für den Angriff. Es ist bekannt, dass solche Vertrauensketten in einer Länge von über zehn Stationen verwendet wurden, um ein vorher ausgewähltes Zielsystem anzugreifen.

Ein kleines Beispiel sollte auch hier zeigen, wie einfach dies in der Praxis sein kann. Ihr Dienstleister, der Ihr Netzwerk betreut erhält der Einfachkeit halber Zugriff per Remote Desktop Verbindung auf Ihr System. Ist das Netzwerk des Dienstleisters nur ungenügend gesichert, so könnte jemand in dieses eindringen, sich mit Ihrem Netzwerk verbinden und bei Ihnen im System nach vertraulichen Daten suchen, oder auch nur eine Bestellung im Internet tätigen. Ihre IP-Adresse wird dann zum Shopsystem übermittelt.

4. Programmbasierte Angriffe

Der Angreifer lässt sein Opfer (System oder Benutzer) ausführbare Programme zukommen, die den Angriff ausführen sollen (z.B. Trojanische Pferde).
Ein Benutzer kann durch gutes Zureden oder Vortäuschung eines bestimmten Absenders (Chef, Software Hersteller) dazu veranlasst werden, Software, die er via E-mail, WWW-Seite oder per USB-Stick mittels Briefpost bekommen hat, auszuführen. Dieses Programm nutzt dann die Rechte des Benutzers z.B. dazu, das System auszuspionieren oder dem Angreifer eine Tür zu öffnen.

Die ist eigentlich die klassische Methode: einem potentiellen Opfer Software als Anlage in einer EMail zukommen zu lassen und darauf vertrauen, dass diese ausgeführt wird. Man sollte meinen, dass es sich mittlerweile rumgesprochen hat, nicht angeforderte Anlagen zu öffnen. Es gibt jedoch immer noch eine erschreckend große Anzahl von Usern, die hier nicht an eine Bedrohung denken. Ausführbare Programme oder Makros in Dokumenten werden zwar weniger, weil die Hersteller immer mehr Möglichkeiten dichtmachen - teilweise so weit, das ein vernünftiges Arbeiten kaum mehr mögliche ist -, dafür verlagern die Angreifer die Verteilung ihrer Software immer mehr auf Websites, die geknackt worden sind. Und das sind nicht nur private Sites, sondern nicht selten Internetauftritte von renommierten Firmen. Hier empfiehlt sich unter anderem der Einsatz eines aktuellen Virenscanners.

5. Infrastrukturbasierte Angriffe

Der Angreifer nützt Lücken oder Fehler der verwendeten Protokolle aus, um eigene Daten in existierende Verbindungen einzuschmuggeln.
Hat der Angreifer Zugriff auf die Infrastruktur, über die zulässige Verbindungen geführt werden, so kann er dies dazu nutzen „Verbindungen berechtigter Benutzer zu „kapern" oder den Platz vertrauenswürdiger Systeme einzunehmen.

Ein Beispiel hierzu ist die aktuelle Diskussion der Experten, dass DNS-Protokoll entsprechend zu ändern. Tippen Sie in Ihren Browser eine Adresse ein, wird zuerst diese an einen DNS-Server weiter gegeben. Dieser antwortet dann mit einer IP-Adresse, die dann von Ihrem Browser aufgerufen wird. Dabei enthält das DNS-Protokoll keinerlei Sicherheitsmechanismen. Damit ist es möglich, sich beispielsweise innerhalb eine bestehenden Internetverbindung als DNS-Server auszugeben und mit IP-Adressen zu antworten, die gefälscht sind. Damit könnte ein User annehmen, er wäre z.B. auf der Seite seiner Bank, ist jedoch auf der Seite eines Angreifers. Noch einfacher wäre ein Szenario, wenn ein Angreifer z.B. einen Proxy-Server in die Verbindung einbringen kann.

6. Denial-of-Service (DoS)

Der Angreifer legt ein bestimmtes System oder eine bestimmte Applikation dadurch lahm, dass er eine Überlast- oder Ausnahmesituation herbeiführt.

Dieser Angriff ist vom Prinzip her rein destruktiv. Der Angreifer schickt einer Applikation z.B. unerwartete Daten oder stellt Tausende von gleichzeitigen Anfragen und bringt so die Applikation entweder zum Abstützen oder verlangsamt sie derart, dass sie nicht mehr benutzbar ist. Ein solcher Angriff wird gerne zusammen mit infrastrukturbasierte Angriffen verwendet, um danach den Platz des Systems selber einzunehmen. Eine Abwehr solcher Angriffe ist extrem schwierig.

Der Denial-of-Service kann heute durchaus von Sicherheitssystemen erkannt und geblockt werden. Allerdings gibt es noch eine heftigere Form: den **Distributed Denial-of-Service** (DDos).

Auch diese Form von Angriffen wurde schon mehrfach beobachtet. Haben Angreifer z.B. großen Erfolg damit Schadprogramme per Mail zu verteilen oder viele User via Website mit Schadsoftware zu infizieren, so gibt es unter Umständen Tausende von PCs, die diese Schadsoftware enthalten. Zu einem bestimmten Zeitpunkt starten dann nahezu alle Programme synchron und jedes einzelne löst einen DoS aus. Mit der Summe der Angreifer kommt dann kaum noch ein Zielsystem zurecht. Als Ergebnis muss nicht immer die Übernahme eines Systems geplant sein. Oft reicht es den Angreifern eine Website oder einen Dienst völlig außer Funktion zu setzen.

7. Sozialarbeit (Social Engineering)

Der Angreifer nutzt seine sozialen Fertigkeiten (z.B. Redegewandtheit, sicheres Auftreten), um jemanden zu überzeugen, ihm seine Kennung zu überlassen oder bestimmte Operationen für ihn vorzunehmen. Der Angreifer gibt sich am Telefon als Vorgesetzter Kollege oder Systemadministrator aus. Meist erzeugt er eine künstliche Dringlichkeit *(„ich stehe hier mit einem potentiellen Großkunden und muss ihm das System zeigen*") um sein Opfer davon zu überzeugen, ihm ohne Überprüfung sein Passwort zu geben.

Aber auch indirekt ist Sozialarbeit die wohl effektivste Methode an Wissen zu gelangen und damit immer näher an ein gesetzten Ziel heran zu kommen.

Klassische Möglichkeiten, wie den Papiermüll durchsuchen, Gespräche über das interne Haustelefon zu führen oder die zufällige Bekanntschaft in der Stammkneipe werden immer noch gerne und häufig genutzt.

Fazit

Diese Liste soll Ihnen einen kleinen Überblick über die verschiedenen Arten geben, mit der es Angreifern möglich ist, in ein Zielsystem einzudringen oder ganz einfach nur ein Opfer zu schädigen. Die Beispiele können fast endlos erweitert werden, zumal hier ganz pragmatisch nur die Definitionen angesprochen werden. Im Regelfall werden verschiedene Angriffsformen immer in einem Mix aus diesen verwendet.

Stellt man - insbesondere bei kleinen und mittelständischen Unternehmen - Unternehmensinhabern, Geschäftsführern oder auch EDV-Verantwortlichen die Frage, ob das Unternehmen denn schon mal Ziel eines Angriffes war, kommt nicht selten ein "**Nein**". Fragt man dann weiter, wie denn potentielle Angriffe z.B. auf die

Infrastruktur erkannt und ausgewertet werden, so wird in vielen Fällen die Situation unangenehm; vor allen für die Befragten.

Angriffe beziehen sich heute nicht mehr nur auf den einzelnen PC oder das Firmennetzwerk. Vielmehr ist jedes Unternehmen und auch jeder Privatbürger ein potentielles Opfer. Die Schlagzeilen in den Medien zeigen uns immer nur die Spitze des Eisberges.

Phishing-Mails, Kreditkartenmissbrauch, Viren, Trojaner und Schadsoftware sind heute Themen im Internet und auch in den Printmedien. Hierbei den Durchblick zu behalten und nicht aus Unwissenheit zum Opfer zu werden, ist nicht immer ganz einfach.

Um sich einen vollständigen Überblick über die Beispiele und technischen Möglichkeiten zu verschaffen, empfehlen wir Ihnen gerne einen ganzen Stapel an Literatur oder bieten Ihnen auch eine persönliche Beratung an, die auf Ihre Umgebung zugeschnitten ist.

Björn-Lars Kuhn
BLK@proteus-solutions.de

FREECALL
0800
50506055