Wer hat nicht schon von Ungeziefern wie Viren, Würmern oder Trojanern gehört bzw. unangenehme Erfahrung damit gemacht? Längst gibt es aber weitere Angriffe wie Spoofing, Phishing und Co., vor denen sich jeder Nutzer schützen sollte. Dieser Artikel gibt eine kurze Übersicht über die einzelnen Angriffe auf die IT-Sicherheit, die jeden Tag den Rechner bzw. das Netzwerk gefährden.

1. Malware (Schadprogramme)

Im alltäglichen Sprachgebrauch werden Viren, Trojaner und Würmer als Synonyme verwendet, wobei sich die Schädlinge deutlich in ihrer Funktion und dem Schaden unterscheiden:

Viren, Würmer, Trojaner

Viren vermehren sich selbst lokal, wobei sie einen Wirt (Betriebssystem/Programm/Datei) benötigen. Viren stecken also in Programmen und werden erst aktiv, wenn das befallene Programm ausgeführt wird. Erhält man also eine E-Mail mit einem virenverseuchten Anhang, ist der Virus solange inaktiv bis der Anhang geöffnet wird. Deswegen sollten solche E-Mails sofort gelöscht werden.

Würmer benötigen im Gegensatz zu den Viren keinen Wirt. Würmer können sich selbst von einem Rechner auf den anderen kopieren, indem sie z.B. alle E-Mailadressen in Adressbüchern durchforsten und selbständig E-Mails mit einer Kopie von sich selbst an alle Kontakte verschicken. Auch Sicherheitslücken werden gerne von Würmern ausgenutzt.

Trojaner verbreiten sich nicht selbst sondern verstecken sich in scheinbar nützlichen Programmen oder Dokumenten. Wird das Programm oder das Dokument mit dem Trojaner aufgerufen, kann auch der Schädling (meist ein Spionageprogramm) unabhängig von dem Programm sein Unwesen treiben. Die üblichen Trojaner zielen darauf ab, Daten wie Passwörter oder Kreditkartennummern auf dem verseuchten Rechner auszuspähen und an den Urheber des Trojaners zu übermitteln.

Genauso wie es den trojanischen Einwohnern nichts mehr genutzt hat das Trojanische Pferd zu zerstören, als die Griechen Troja stürmten, ist es auch in der Computerwelt nicht ausreichend nur den Trojaner zu löschen.

Im Gegensatz zu Viren oder Würmern verbreiten sich Trojaner meist nicht fort und kopieren sich auch nicht selbst.

Backdoor, Spyware, Scareware

Backdoor richtet eine versteckte Hintertür zu einem System ein, um Zugang zu einem Rechner, unter Umgehung der Sicherheitseinrichtungen des Betriebssystems, zu ermöglichen.

Spyware ist ein Programm, das Informationen über Nutzeraktivitäten ausspäht. Hierunter fallen z.B. Keylogger, die jeden Tastaturschlag des Nutzers aufzeichnen und weiterleiten. Zu dieser Gruppe gehören auch Programme, die in regelmäßigen Abständen im Hintergrund Bildschirmfotos anfertigen und diese dann an den Angreifer übermitteln.

Scareware sollen den Nutzer mit Warnmeldungen über angebliche Sicherheitsgefahren verunsichern und dazu bewegen, das angebotene Produkt zu kaufen. Dem Nutzer wird vorgegaukelt, dass dieses Produkt angeblich die Schadsoftware beseitigen kann.

2. Angriffe auf Passwörter

Neben dem Raten und Ausspionieren von Passwörtern ist die Brute Force Attacke weit verbreitet. Bei dieser Attacke versuchen Hacker mithilfe einer Software, die in einer schnellen Abfolge verschiedene Zeichenkombinationen ausprobiert, das Passwort zu knacken. Je einfacher das Passwort gewählt ist, umso schneller kann dieses geknackt werden.

Bei einem aus 5 Zeichen (3 Kleinbuchstaben, 2 Zahlen) bestehenden Passwort kann durch automatisches Ausprobieren aller Kombinationen innerhalb von 0,03 Sekunden einen Treffer bedeuten.

Bei einem Passwort bestehend aus 9 Zeichen (bestehend aus 2 Großbuchstaben, 3 Kleinbuchstaben, 2 Zahlen, 2 Sonderzeichen) benötigt das System ca. 9 Jahre bis es geknackt ist. In der Zwischenzeit hat man hoffentlich das Passwort gewechselt.

3. Phishing

Bei einem Phishing versucht der Angreifer über gefälschte E-Mails, Internetseiten, SMS usw. an persönliche Daten eines Nutzers heranzukommen. Beispielsweise wird die Startseite einer Onlinebanking-Seite nachgebaut, auf die der Nutzer verwiesen wird, z.B. über einen Link in einer vermeintlich von der eigenen Bank stammenden E-Mail. Sobald sich der Nutzer mit seinen Daten einloggt, werden seine Anmeldedaten ausspioniert und für kriminelle Aktivitäten genutzt.

Da sich die gefälschten von den echten Seiten kaum unterscheiden gilt: Augen auf im Internetverkehr!

4. Man-in-the-Middle Attacke

Bei der „Man in the Middle“-Attacke nistet sich ein Angreifer zwischen den miteinander kommunizierenden Rechnern. Diese Position ermöglicht ihm, den ausgetauschten Datenverkehr zu kontrollieren und zu manipulieren. Er kann z.B. die ausgetauschten Informationen abfangen, lesen, die Weiterleitung kappen usw. Von all dem erfährt der Empfänger aber nichts.

5. Sniffing

Unter Sniffing (Schnüffeln) wird das unberechtigte Abhören des Datenverkehrs verstanden. Dabei werden oft Passwörter, die nicht oder nur sehr schwach verschlüsselt sind, abgefangen. Andere Angreife bedienen sich dieser Methode um rausfinden zu können,

welche Teilnehmer über welche Protokolle miteinander kommunizieren. Mit den so erlangten Informationen können die Angreifer dann den eigentlichen Angriff starten.

6. Spoofing

Bei einem Spoofing (die Verschleierung, Vortäuschung) wird eine falsche Identität vorgetäuscht. Dabei gibt es mehrere Arten von Spoofing, von denen wir vier Vertreten vorstellen möchten:

IP-Spoofing:

gehört zu der Man-in-the Middle-Angriffen. Dabei wird eine falsche IP-Adresse vorgespiegelt, so dass der Angreifer vortäuscht, dass seine Datenpakete von einem Rechner kommen, denen der angegriffene Rechner vertraut.

DNS-Spoofing:

Hier wird die Zuordnung der IP-Adresse zu dem zugehörigen Domainnamen verfälscht. So wird der Datenverkehr zu einem anderen Rechner umgeleitet, um z.B. einen Phishing-Angriff starten zu können.

Mail-Spoofing:

Bei einem Mail-Spoofing wird ein falscher E-Mail-Absender vorgegaukelt.

Call ID Spoofing:

Hier wird die Telefonnummer „gespooft“, indem der Anruf mit einer vorgetäuschten oder geklauten Telefonnummer anruft. Während des Telefonates wird nicht die Originalrufnummer des Anrufers angezeigt, sondern die geklaute Telefonnummer, um die wahre Identität des Anrufers zu verschleiern.

7. DoS – Denial of Service

Bei einer DoS-Attacke wird ein Infrastruktursystem absichtlich mit so vielen Anfragen belastet, damit das System zusammenbricht, weil die Aufgaben nicht mehr abgearbeitet werden können. Auf diese Weise wurden schon Web-Server von Amazon oder Yahoo lahmgelegt und waren nicht mehr verfügbar. Längst hat sich die DoS-Attacke zu einem Instrument des Online-Protestes etabliert, indem kritische Seiten attackiert werden.

8. Social Engineering

Als Social Engineering werden alle Angriffe auf Systeme bezeichnet, bei der der Angreifer Personen durch psychologische Tricks manipuliert, um an Informationen zu gelangen. Nähere Informationen finden sie hier.