INFORMATIONSSICHERHEIT

Titok M. A., Loshetschnik S. A.

Belarussische Staatliche Universität für Informatik und Radioelektronik

Minsk, Republik Belarus

Mataliga S. A.

Kandidatin für pädagogische Wissenschaften, Dozentin

In diesem Artikel ist die Analyse moderner Angriffsmethoden auf Informationssysteme vorgestellt.

Als Informationssicherheit bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden (technischen oder nicht technischen) Systemen, die die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen. Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken.

Angriffe und Schutz

Unter einem Angriff auf den Datenschutz oder Datensicherheit (repräsentiert durch zum Beispiel ein Computersystem) versteht man jeden Vorgang, dessen Folge oder Ziel ein Verlust des Datenschutzes oder der Datensicherheit ist. Auch technisches Versagen wird in diesem Sinne als Angriff gewertet.

Statistische Sicherheit: Ein System wird dann als sicher bezeichnet, wenn für den Angreifer der Aufwand für das Eindringen in das System höher ist als der daraus resultierende Nutzen. Deshalb ist es wichtig, die Hürden für einen erfolgreichen Einbruch möglichst hoch zu setzen und damit das Risiko zu reduzieren.

Absolute Sicherheit: Ein System ist dann absolut sicher, wenn es jedem denkbaren Angriff widerstehen kann. Die absolute Sicherheit kann nur unter besonderen Bedingungen erreicht werden, die die Arbeitsfähigkeit des Systems oft erheblich einschränken (isolierte Systeme, wenige und hochqualifizierte Zugriffsberechtigte).

Der Mangel an Computersicherheit ist eine vielschichtige Bedrohung, die nur durch eine anspruchsvolle Abwehr beantwortet werden kann. Der Kauf und die Installation einer Software ist kein Ersatz für eine umsichtige Analyse der Risiken, möglicher Verluste, der Abwehr und von Sicherheitsbestimmungen, Viren, Würmer, Trojanische Pferde.

Während im Firmenumfeld die ganze Themenbreite der Computersicherheit Beachtung findet, verbinden viele Privatanwender mit dem Begriff primär den Schutz vor Viren und Würmern oder Spyware wie Trojanischen Pferden.

Die ersten Computerviren waren noch recht harmlos und dienten lediglich dem Aufzeigen diverser Schwachstellen von Computersystemen. Doch recht bald erkannte man, dass Viren zu weitaus mehr in der Lage sind. Es begann eine rasante Weiterentwicklung der Schädlinge und des Ausbaus ihrer Fähigkeiten – vom simplen Löschen von Dateien über das Ausspionieren von Daten (zum Beispiel von Passwörtern) bis hin zum Öffnen des Rechners für entfernte Benutzer (Backdoor).

Mittlerweile existieren diverse Baukästen im Internet, die neben einer Anleitung auch alle notwendigen Bestandteile für das einfache Programmieren von Viren liefern. Nicht zuletzt schleusen kriminelle Organisationen Viren auf PCs ein, um diese für ihre Zwecke (DoS-Angriffe) zu nutzen. So entstanden bereits riesige Bot-Netze, die auch illegal vermietet werden.

Phishing

Unter dem Begriff Phishing versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Ziel des Betrugs ist es, mit den erhaltenen Daten beispielsweise Kontoplünderung zu begehen und den entsprechenden Personen zu schaden. Es handelt sich dabei um eine Form des Social Engineering, bei dem die Gutgläubigkeit des Opfers ausgenutzt wird.

Homographischer Angriff ist eine Methode des Spoofing, bei der der Angreifer das ähnliche Aussehen verschiedener Schriftzeichen dazu benutzt, Computernutzern eine falsche Identität vorzutäuschen, insbesondere bei Domains. Der Angreifer lockt den Nutzer zu einem Domainnamen, der fast genauso aussieht wie ein bekannter Domainname, aber woanders hin führt, zum Beispiel zu einer Phishing-Website.

Mit der Einführung internationalisierter Domainnamen steht außer dem ASCII-Zeichensatz eine Vielzahl von Schriften für Domainnamen zur Verfügung, die zum Teil eine Reihe ähnlicher Schriftzeichen enthalten. Damit vervielfachen sich die Möglichkeiten für homographische Angriffe.

Ein Botnet ist eine Gruppe automatisierter Schadprogramme, sogenannter Bots. Die Bots laufen auf vernetzten Rechnern, deren Netzwerkanbindung sowie lokale Ressourcen und Daten ihnen, ohne Einverständnis des Eigentümers, zur Verfügung stehen. Betreiber illegaler Botnetze installieren die Bots

ohne Wissen der Inhaber auf Computern und nutzen sie für ihre Zwecke. Die meisten Bots können von einem Botnetz-Operator über einen Kommunikationskanal überwacht werden und Befehle empfangen.

Ein Bot stellt dem Betreiber eines Botnetzes je nach Funktionsumfang verschiedene Dienste zur Verfügung. Derweil mehren sich multifunktional einsetzbare Botnets. Der Botmaster kann so flexibel auf andere Einsatzmöglichkeiten umschwenken. Das Botnet kann wie folgt angewendet werden:

Proxy

Proxys bieten die Möglichkeit, eine Verbindung zu einem dritten Computer über den Zombie herzustellen, und können damit die eigentliche Ursprungs-Adresse verbergen. Der so geschaffene Zwischen-Host kann dann für weitere Angriffe auf andere Rechner genutzt werden. Aus Sicht des Ziel-Computers kommt der Angriff vom Proxy-Host.

Ausführen von DDoS-Attacken und DRDoS-Attacken

Denial of Service (DoS) ist in der Informationstechnik die Nichtverfügbarkeit eines Internetdienstes, der eigentlich verfügbar sein sollte.

Obwohl es verschiedene Gründe für die Nichtverfügbarkeit geben kann, ist die häufigste Art die Folge einer Überlastung des Datennetzes. Dies kann durch unbeabsichtigte Überlastungen verursacht werden oder durch einen konzentrierten Angriff auf die Server oder sonstige Komponenten des Datennetzes.

Im Fall einer durch eine Unmenge von Anfragen verursachten Dienstblockade spricht man von einer durch Vielanfragen verbreiteten Verweigerung des Dienstes.

Zugriff auf lokal gespeicherte Daten durch Einsatz von Sniffern und Password-Grabbern

Die privaten Daten der mit Bots infizierten Rechner sind lukrativ. Die meisten Bots bieten Möglichkeiten, auf lokal gespeicherte Zugangsdaten verschiedener Anwendungen zuzugreifen. Auf den Diebstahl von Daten spezialisierte Bots bieten auch Funktionen, um Daten aus Webformularen zu lesen, und können dadurch Informationen ausspionieren, die in SSL-gesicherten Webseiten eingegeben wurden, darunter beispielsweise auch Passwörter oder Kreditkartennummern. Viele IRC-Bots können den Netzwerkverkehr des Rechners protokollieren.

Einsatz als Ransomware

Speichermedium für die Verbreitung illegaler Inhalte (z. B. Filesharing von geschütztem Material)

Nutzung der Rechenleistung (z. B. für Bitcoin-Mining)

Absichtlich herbeigeführte Serverüberlastungen

Wird eine Überlastung mutwillig herbeigeführt, geschieht dies in der Regel mit der Absicht, einen oder mehrere bereitgestellte Dienste funktionsunfähig zu machen. War dies ursprünglich vor allem eine Form von Protest oder Vandalismus, werden Denial-of-Service-Attacken mittlerweile von Cyber-Kriminellen zum Kauf angeboten, um Konkurrenten zu schädigen. Ebenso werden Serverbetreiber zu einer Geldzahlung erpresst, damit ihr Internetangebot wieder erreichbar wird.

Literaturquellen:

1. Informationssicherheit [technische Ressource] – Zugriffsmodus: https://de.wikipedia.org/wiki/Informationssicherheit – Zugangsdatum 09.03.2019.