Основни типове заплахи за компютърните системи и мрежи

Валентина Войноховска, Светлозар Цанков

Abstract: Basic Types of Threats inCcomputerSsystems and Networks: *The purpose of the paper is to describe the Basic types of threats in computer systems and networks. The security and hacking terms in this paper are merely an introduction to computer security terminology, but they are a starting point to help person prepare for learning more about computer security. The present document has been produced with the financial assistance of the European Social Fund under Operational Programme "Human Resources Development". The contents of this document are the sole responsibility of "Angel Kanchev" University of Ruse and can under no circumstances be regarded as reflecting the position of the European Union or the Ministry of Education and Science of Republic of Bulgaria. Project № BG051PO001-3.3.06-0008 "Supporting Academic Development of Scientific Personnel in Engineering and Information Science and Technologies"*

Key words: *threats, computer security, network security*

ВЪВЕДЕНИЕ

Сигурността е свойство на една система да противостои на външни или вътрешни дестабилизиращи фактори, които могат да доведат до нейното нежелателно състояние или поведение.

Термините информационна сигурност, компютърна сигурност и защита на информацията често се използват, като синоними. Тези термини са свързани и имат общи цели, като конфиденциалност, интегритет и достъпност на информацията, но между тях има разлика:

- Информационната сигурност е защитата на информацията, независимо от нейната форма – електронна, печатна или друга.
- Компютърната сигурност се фокусира върху коректната работа на компютърните системи и мрежи и обработваната от тях информация.
- Информационна защита са практиките по управление на рисковете, свързани с използването, работата, съхранението и предаването на информацията, както и системите и процесите използвани за тези цели.

По отношение на компютърната сигурност има два типа заплахи: вътрешни (служители, оператори и потребители на системата, програмисти, технически персонал, ръководители с различни длъжности, служители по сигурността на информационната система) и външни (клиенти и посетители, бивши служители, агенти на конкурентни организации и чужди разузнавания, криминално проявени лица).

Съществуват много различни типове компютърни заплахи за сигурността, които могат да бъдат класифицирани в три големи класа по следния начин [1]:

Физическа сигурност – кражба на компютър или компютърно оборудване, пожар, токов удар или наводнение могат да повредят компютърния хардуер и мрежовите връзки и могат да причинят загуба на данни.

Фалшив софтуер – компютърни вируси. Малки програми, които нахлуват в компютъра и се разпространяват бързо и незабележимо. Вирусите са само един аспект от общата заплаха породена от фалшивия софтуер.

Мрежова сигурност Голяма част от компютрите са свързани в мрежа, а повечето локални мрежи са свързани с Интернет. Следователно, има голям клас на заплахи за компютърната сигурност, свързани с мрежите, които се отнасят към категорията на **мрежовата сигурност**. Тази широкообхватна област за сигурността включва заплахи като сканиране на портове, spoofing[5], разкриване на пароли, шпиониране и кражба на самоличност.

[5] Spoofing – в контекста на мрежовата сигурност spoofing атака представлява ситуация, в която един човек или програма, успешно се маскира като друг чрез фалшифициране на данни.

ОСНОВНИ ТИПОВЕ ЗАПЛАХИ

Повечето атаки могат да бъдат категоризирани в един от следните шест класа:

- Злонамерен софтуер (Malware): това е основен термин за софтуер, който е създаден със злонамерени цели. Той включва вирусни атаки, червеи, рекламен софтуер, троянски коне и шпионски софтуер. Това са най-често срещаните опасности за една компютърна система.
- Пробив в сигурността: тази група атаки включва всеки опит за получаване на неоторизиран достъп до системата. Това включва разкриване на пароли, превишаване на права, проникване в сървър, всички дейности, които най-често се свързват с термина „хакерство“.
- Атаки от тип „отказ от услуга“ (DoS): вид атака, която причинява загуба на услуга или невъзможност на мрежата да функционира.
- Уеб атаки: това е всяка атака, която се опитва да наруши/промени даден уеб сайт. Две от най-често срещаните такива атаки са: SQL injection (SQLi) Това е метод за уеб атака, чрез която хакерът може да внедри и изпълни SQL команди върху базата данни на даденият сайт и XSS (cross-site scripting) атака, която използва уязвимост на приложението, за да “вмъкне“ нежелан код, който се изпълнява в браузъра на крайния потребител.
- “Отвличане” на HTTP сесии (Session hijacking): тези атаки представляват отвличане на идентификатора на потребителската сесия (session hijacking), при което е възможно злонамерени потребители да осъществят достъп до чужди данни, принадлежащи на даден потребител.
- DNS отравяне (DNS poisoning): този тип атаки компрометират DNS сървъра така, че потребителите могат да бъдат пренасочени към зловредни уеб сайтове, включително и към уеб сайтове с цел фишинг. Фишинг атаките са най-разпространената форма на интернет измама. Това е широко използван похват от компютърни престъпници за получаване на важна информация.Те целят да подмамят хората да предоставят важна лична информация, най-често подробности по кредитни карти и банкови сметки.

Злонамерен софтуер (Malware)

Вредното програмно осигуряване е общ термин за програми, които умишлено нанасят вреда на компютърните системи и мрежи. *Malware* е основен термин за софтуер, който има злонамерени цели. Следва описание на трите типа злонамерен софтуер: вируси, троянски коне и шпионски софтуер.

Вируси

Според Symantec (създателите на Norton antivirus и други софтуерни продукти) вирусът е „малка програма, която се размножава и се скрива в други програми, обикновено без знанието на потребителя“ [3].

Троянски кон

Троянският кон получава името си от мита за Троянската война. Компютърният троянски кон изглежда привидно като нормален софтуер, а всъщност тайно прехвърля вируси или друг тип зловреден софтуер на компютъра. Троянските коне най-общо казано са програми, които работят като скрити процеси на даден компютър и дават пряк или косвен достъп на външни лица до личната информация на потребителя. Много често се използват за получаване на таен достъп до системата, на която са инсталирани, т.е. някой отдалечено контролира компютъра.

Троянските коне са тип зловреден код с универсално приложение – първоначално представящ се за легитимно и полезно приложение, което всъщност извършва подмолни действия. Постепенно се появяват и такива, които не изискват потребителят да ги стартира, а се възползват от уязвимостите в операционната система и определени програми, за да се наместят незабелязано в системата.

Троянските коне могат да изпълняват различни задачи: отваряне на задна врата, следене на натиснати клавиши и/или запис на екрана (ако разполага с вграден метод за това), изтегляне или публикуване на файлове на/от компютъра, кражба на ценни данни, изтриване на файлове, забавяне и/или блокиране на системата и др. Именно затова са и много често срещани във виртуалното пространство.

Шпионски софтуер

Друга категория зловреден софтуер е шпионският софтуер (spyware). Това е софтуер, който следи какво прави потребителя на компютъра си. Той може да бъде под формата на обикновена бисквитка (cookie), която уеб сайтът, който потребителят посещава, поставя на компютъра му и използва, за да го разпознае, когато той го посети отново.

Друга форма на шпионския софтуер са програмите, които записват натиснатите клавиши на клавиатурата. Действието се нарича *keystroke logging*, а програмите - *keylogger*. Подобни програми са тези за запис на екрана – това са най-често снимки на определена област около курсора. Данните се съхраняват, за да се изпратят по-късно на източника, инсталирал шпионския софтуер или директно се изпращат чрез e-mail. Това е един от най-често срещаните начини за кражба на акаунти и/или пароли, номера на кредитни карти и други лични за даден потребител данни. Програмите за запис на дейности (най-често натиснати клавиши) често се инсталират от шпионския софтуер.

Логическа бомба

Логическата бомба е софтуер, който остава скрит докато не настъпи някакво специфично събитие. Това събитие може да е дата и време. При настъпване на това събитие софтуерът извършва злонамерени дейности като например, изтриване на файлове, промяна на системните конфигурации или дори пускане на вирус.

Компрометиране сигурността на системата

Следва да бъдат разгледани атаките, които нарушават сигурността на системата. Тези дейности най-често се свързва с думата „хакерство“, макар, че това не е терминът, който самите хакери използват.

Професионалистите, които се занимават с информационна сигурност се разделят на хакери (hackers) и кракери (crackers). И едните, и другите се занимават с решаване на една и съща задача – търсене уязвимостта в информационната система. Разликата между тях е в гледната им точка относно този проблем:

- Хакерът изследва информационната система с цел откриване на слабите й места (уязвимостта) и информира потребителите за отстраняването им. Той анализира текущата сигурност на системата, формулира необходимите изисквания и условия за повишаване нивото й на защита.
- Кракерът осъществява несанкциониран достъп до системата с цел кражба, подмяна, унищожаване на информация или обявяване наличието на достъп.

Социално инженерство

Социалното инженерство е техника за нарушаване сигурността на системата с използване на човешката същност, а не чрез технологията. Това е начинът, който използва известният хакер Кевин Митник. Социалното инженерство представлява получаване на несанкциониран достъп до информация без намеса в програмното осигуряване. Целта е да се провокират хората, за да се получат паролите за достъп до системата или друга информация, която би спомогнала за нарушаване на сигурността й.

Нарастващата популярност на безжичните мрежи дава възможност за създаване на нови видове атаки. Една такава е т.нар. wardriving.

Wardriving се използва за намиране на уязвими wireless мрежи. В този сценарий зложелателите обикалят и опитват да намерят wireless мрежи, създавайки карта на

всички отворени точки за достъп в тях. Обикновено wireless мрежите могат да предават сигнал до около 3000 метра.

Wardriving може да се извърши с помощта на програмата NetStumbler. Основното предназначение на този Wi-Fi инструмент е да състави схема на мрежата и да покаже „кой, кой е в нея“. Освен, че спомага за намиране на незащитени мрежи, „мъртви точки“, в които сигналът е слаб“, както и вредни точки за достъп, които заблуждават нищо неподозиращите потребители, този софтуер може дори да сортира смущенията в безжичната мрежа.

NetStumbler показва много детайли за съседни безжични мрежи - MAC адрес, SSID, канал, скорост, вид криптиране, както и подробни данни за отношението сигнал/шум, филтри за сортиране според силата на сигнала, състояние на криптиране и др. характеристики. Освен това с помощта на GPS устройство, NetStumbler може да покаже точно къде физически е разположена всяка точка за достъп.

Атака от тип „отказ от услуга“ – DoS

При тази атака зложелателите нямат достъп до системата, а блокират достъпа на легитимните потребители. Един от начините да се блокира дадена легитимна услуга е да се наводни целевата система с множество фалшиви заявки за свързване. При това тя неможе да отговори на легитимните заявки. DoS е най-често срещаната атака в уеб.

Уеб атаки

По своята същност уеб сървърите трябва да осигуряват комуникация. Много често уеб сайтовете позволяват на потребителите да взаимодействат с тях. Всяка част от уеб сайта, която позволява взаимодействие на потребителите е също потенциална точка за уеб атака. SQL injections представлява въвеждане на SQL (Structured Query Language) команди във формите за вписване (полетата за потребителско име и парола) в опит да се излъже сървъра да изпълни тези команди. Най-често срещаната цел е да се накара сървъра да регистрира зложелателя въпреки, че той няма легитимни потребителско име и парола.

“Отвличане” на чужди HTTP сесии (Session hijacking)

Session hijacking може да е много сложна за изпълнение. Поради тази причина не е много често срещана форма на атака. По-просто казано, зложелателят наблюдава сесии между клиентската машина и сървъра и поема контрола над тази сесия.

DNS отравяне (DNS poisoning)

По-голяма част от комуникациите в интернет включват DNS (Domain Name Service). DNS е това, което превежда домейн имената, които обикновените потребители разбират (например www.abv.bg) в IP адрес, който компютрите и рутерите разбират. DNS poisoning използва няколко техники за компрометиране на този процес и пренасочване на трафика към незаконен сайт. Това най-често се прави с цел кражба на лична информация.

ХАКЕРСКИ ЖАРГОН

Всеки човек познава термина хакер, с който се визира човек, проникващ в чужди компютърни системи. В хакерското общество, обаче, хакерът е:

- компютърен експерт неучастващ в криминална дейност;
- човек, който просто иска да усъвършенства своите знания и умения;
- човек, който с проникване в компютърни системи цели да открие пропуски в сигурността им.

Терминът е обект на дългогодишни дискусии, целящи да дадат подходящо определение на думата "хакер". Компютърни програмисти твърдят, че някой, който прониква с криминални цели в чужди компютри, е по-добре да бъде наречен кракер (от англ. crack-чупя), а не хакер.

Например, човек, който е опитен в работа с Линукс ОС, работещ с цел да разбере и установи слабостите и недостатъците на системата, може да се нарече хакер. Това не винаги означава, че при намиране на недостатък, той ще се използва за получаване на достъп до системата. Начинът на това „използване“ е това, което разделя хакерите на три основни групи [2]:

- **White hat** – хакери – този тип хакери проникват в компютри с позитивни намерения. Те са консултанти и изпитват системите за сигурност. Това са също и лица, които извършват проникване и тестове, търсейки уязвимости в рамките на договорно споразумение. Често те биват наричани етични хакери. Международният съвет за електронна търговия е разработил сертификати, курсове и онлайн обучение, обхващащи различни сфери на етичното хакерство.
- **Black hat** – хакери – този тип хакери обикновено се споменават в медиите. Наричат се още *кракери*. Това е компютърен престъпник, който прониква незаконно в компютри, нарушава компютърната сигурност без разрешение и извършва вандализъм, измами с кредитни карти, кражба на лични данни, пиратство, или други видове незаконна дейност.
- **Gray hat** – хакери – това е хакер, който не е злонамерен, но може да разруши уебсайт, напр. само за да покаже на администратора, че защитата е слаба и има пропуски в сигурността. С дейността си този тип хакери не преследват печалба или материални облаги.

Script Kiddies (скрипт киди)

Думата е название на човек, който извършва атаки над компютри с помощта на програми, написани от други (опитни хакери), и с много малко познания за начина им на работа. Представителите на тази група не са експерти или програмисти и имат повърхностни знания в компютърната област. Обикновенно уменията им стигат до обезобразяване на уебсайтове или извършване на DoS-атаки. Повечето от тях са тийнейджъри и действат мотивирани единствено от тръпката или повишаване на репутацията си сред своите връстници.

Името на този вид хакери произлиза от факта, че Интернет е изпълнен с програми и скриптове, които са свободни за ползване с цел изпълнение на хакерски дейности. Много от тези средства имат лесен за използване графичен интерфейс, който позволява на някой с много ограничени умения да борави с тях. Класически пример за това е Low Earth Orbit Ion Cannon за изпълнение на DoS атаки. Човек, който използва такива средства се нарича Script Kiddie (скрипт киди). Голяма част от хората, които считат себе си за хакери, всъщност са такива. Те използват за своите атаки предимно операционната система Windows, а по-напредналите от тях са запознати и с Linux. Програмите, които използват, са лесно откриваеми в интернет – напр. софтуера за DoS-атаки WinNuke, троянските коне Back Orifice, NetBus и Sub7, също и програми, като Metasploit, Zenmap, и др. уеб и порт-скенери.

Етични хакери: sneakers

Когато някой даде права на друг, за да влезе системата му, това най-често е с цел оценяване на системните уязвимости. Тези хора най-често се наричат сникъри. Те легално проникват в система, за да оценят пропуските в сигурността. Все повече компании се възползват от услугите на такива специалисти за оценка уязвимостта на техните системи.

Специалистите, изпълняващи такива услуги трябва да бъдат технически и етично грамотни. Назначаването на такива хора трябва да е съпътствано с предварителни проучвания относно евентуалното криминално минало на кандидата.

Phreaking

Фрийкинг (от англ. Phreaking) е жаргон, създаден от думите phone (телефон) и freak (разг. маниак), който описва дейността на хора, които изучават и експериментират с възможностите на телекомуникационните системи. Човек, които се занимава с фрийкинг, се нарича фрийкър.

Основната дейност на фрийкърите се състои в манипулирането на телефонните системи с цел осъществяване на безплатни разговори. Понастоящем фрийкингът не е толкова популярен както през 70-те и 80-те години на мин. век, тъй като телефонните мрежи вече са дигитални.

ЗАКЛЮЧЕНИЕ

В тази публикация са разгледани и систематизирани основните видове заплахи за компютърните системи и мрежи. Използваните термини за сигурност и хакерство са въведение в терминологията на компютърната сигурност. „Настоящият документ е изготвен с финансовата помощ на Европейския социален фонд. Русенският университет „Ангел Кънчев" носи цялата отговорност за съдържанието на настоящия документ, и при никакви обстоятелства не може да се приеме като официална позиция на Европейския съюз или Министерството на образованието и науката". Проект:№ BG051PO001-3.3.06-0008 „Подпомагане израстването на научните кадри в инженерните науки и информационните технологии".

ЛИТЕРАТУРА

[1] Salomon, D. Foundations of Computer Security, Springer-Verlag London Limited, 2006, 389p.

[2] Easttom, Ch. Computer Security Fundamentals. Copyright Pearson, 2012, 350p.

[3] General Internet Security, https://www.us-cert.gov/security-publications, използван през юли 2014г.

За контакти:

Доц. д-р Валентина Войноховска, Катедра *Информатика и информационни технологии*, Русенски университет *Ангел Кънчев*, тел.: 082-888 645, e-mail: voinohovska@ami-uni.ru.acad.bg

Гл. ас. д-р Светлозар Цанков, Катедра *Информатика и информационни технологии*, Русенски университет *Ангел Кънчев*, тел.: 082-888 645, e-mail: stzancov@ami.uni-ruse.bg