НОВ БЪЛГАРСКИ УНИВЕРСИТЕТ

## МАГИСТЪРСКИ ФАКУЛТЕТ

# ДЕПАРТАМЕНТ "ИНФОРМАТИКА"

**ПРОГРАМА „Софтуерни технологии в Интернет”**



### ЗАДАЧА ЗА ТЕКУЩА ОЦЕНКА

**КУРС: INFM102 Компютърна сигурност в Интернет**

**ТЕМА: Въпроси по задача 1**

**НА СТУДЕНТА** : Георги Иванов Георгиев

**Фак. №:** f88683

**Дата:** 06/01/2018 г.

**Преподавател:**

/ доц. В.Къдрев / …………………

София

**ВЪПРОС 1**

* 1. ***Какво е киберзащита, решава ли проблема „сигурност” на мрежата и на предаваната информация***.

Отговор: Киберзащитата представлява всеобхватно понятие описващо прилагането на различен набор от мерки и практики за осигуряване на ИТ сигурност в публичното и частното интернет пространство. Осигуряването на пълна защита, обаче, е на практика невъзможно, поради динамичния характер на сектора и непрекъсващо нарастващите киберзаплахи. Точно поради тази причина едни от основните изисквания за ефективна киберзащита са доброто планиране на предпазните мерки и непрекъснатото адекватно адаптиране на дигиталната среда, в която се намираме. Един пример за осигуряване на киберзащита в една бизнес единица е прилагането и периодичното адаптиране на политика за сигурност, таргетираща инфраструктурните компоненти и информационните системи осигуряващи информационната ѝ обезпеченост. Но дори това да е факт, целостта на мрежите и инфраструктурата е са до известна степен уязвими. Добре организираната съвкупност от мерки за осигуряване на киберсигурност увеличава защитата, но не би могла да пребори изцяло проблема с непрекъснато нарастващия брой и видове кибератаки.

* 1. Какви са аспектите на осигуряването на сигурност на информацията.

Отговор: Съществуват множество аспекти, всеки от които предоставя различно ниво на сигурност. Типичен пример са цифровите сертификати използвани с цел доказване на идентичността на участниците в дадено дигитално взаимоотношение. Те също така предоставят конфиденциалност на информацията и осигуряват нейната цялостност. Друг много важен аспект са така наречените частни виртуални мрежи (VPN).Тяхното предимство е създаването на защитен изолиран канал за предаване на информация между различните участници във виртуалната мрежа.

Интерес представляват различните видове контрол на достъп извън мрежата. Поддържането на политики за сигурност осигурява т.нар. административен контрол. Контролирането и изолирането на мрежовите устройства пък осигурява т.нар. физически контрол, а чрез използването на различните криптографски техники осигуряваме т.нар. логически контрол.

В рамките на дадена бизнес единица бихме могли да осъществим контрол чрез оторизиране и автентикиране. Първоначалният достъп до информация е защитен чрез създаването на потребителски групи и акаунти към тях. Последващият контрол се осъществява чрез периодичното водене на отчети по отношение на състоянието на системата и нейните ресурси.

* 1. Какво е уязвимост и какво е заплаха за конфиденциалността на информацията в Интернет и какви накратко са техните особености.

Отговор: Уязвимостта е наличие на слабо място или недостатък в защитата на информацията, с което може да се злоупотреби. Заплахата за конфиденциалността на информацията представлява възможността за използването или фактическото използване на някаква уязвимост със злонамерена цел. Като основни причини за създаването на уязвимости в защитата на една система бихме могли да посочим естественото ѝ развитие и разширяване в следствие, на което се увеличава достъпът на потребителите до различни нейни модули и се увеличава размерът на данните с които тя разполага. Необновяването на остарели защитни протоколи и механизми, както и неправилното конфигуриране на защитите също биха довели до нови уязвимости.

Заплахите могат да бъдат разделени според своето въздействие върху сигурността на информацията:

* Заплахи за обектите
* Заплахи за процесите
* Заплахи за процедурите
* Заплахи за информацията

* 1. Какви накратко са обобщените характеристики на заплахите за конфиденциалността на информацията.

Отговор: Заплахите за конфиденциалността на информацията обобщават неправомерното присвояване или премахване на пароли или кодове за достъп; прихващане или кражба на информация или най-общо злоупотреба с правомощия.

**ВЪПРОС 2**

2.1. Как дадена техника за нападение е свързана със "заплаха" и "уязвимост".

Отговор: Атаките по своята същност са комбинации от целенасочени действия за възползване от дадена уязвимост в една система. Целта е да се реализира определена заплаха за нея и да се постигне срив в сигурността и компрометиране на информационната и цялост. Успехът на атаката е пряко свързан с нанесената щета, в следствие на намерената уязвимост.

2.2. Какво е защита на информацията в Интернет и какво е противодействие на атака.

Отговор: Защитата на информацията в Интернет по своята същност е противодействие на всякакви атакуващи действия върху мрежата. По-конкретно прилагането на различните техники за защита на компютърна система или мрежа водят до успешното отблъскване на инвазивни въздействия. Те биват:

* Компютърни – реализират се чрез софтуер за контрол на достъп и съхранение на данни;
* Комуникационни – реализират се чрез мрежов достъп до системата
* Физически – реализират се чрез мерки срещу природни бедствия и злоумишленици

2.3. Какви са особеностите на злонамерения софтуер.

Отговор: Злонамерения софтуер представлява софтуер инсталиран и работещ на потребителска машина против волята и знанието на потребителя. Основната причина в наши дни е чисто финансова. Например чрез кражба на финансова и банкова информация на даден потребител, се получава достъп до авоари на жертвата. Създаването на бот нет мрежи от своя страна позволява използването на „зомби“ компютри ръководени от централно място, за лично облагодетелстване или за продажба като ресурс на трета страна.

2.4. Какво е условието за незаразяване със злонамерен софтуер.

Отговор: Възможно най-простия и надежден начин, за да не се зарази дадена система със злонамерен софтуер е неговото не инсталиране. На втор място е неговото не стартиране. На практика обаче това не е толкова лесно, тъй като този тип софтуери се маскират умело. Също така съществува зловреден софтуер, който не изисква намесата на потребител, за да зарази системата. Типичен пример от последните дни е използването на открита хардуерна слабост в процесорите на Intel, която позволява изпълнение на код с цел достъпване на паметта на различни приложения.

2.5. Какви са особеностите на зловредния код (вирус, червей, троянски кон, задна врата).

Отговор:

* Вирус – това е зловреден код, който не може да съществува самостоятелно, а се прикрепя към даден изпълним файл. След своето стартиране остава зареден в паметта на машината и започва да заразява таргетирани файлове – еднократно (нерезидентен) или при всяко тяхно отваряне (резидентен). Най-безобидни са вирусите, които просто се репликират. Най-опасни, макар и по редки, са полиморфните вируси, които се пренаписват отначало при всяко заразяване.
* Червей – мрежови зловреден софтуер, който се възползва от мрежовите слабости или други уязвимости в операционната система. След активацията си, червеят се държи като вирус и се разпространява чрез електронната поща на заразения. Често се използва с цел да имитира потребителско поведение. Позволява изпълнението да става на отдалечена машина.
* Троянски кон – зловреден софтуер с най-универсално приложение. Маскира се като полезна програма и има възможността да изтрива, променя, запазва или изпраща характеристиките на потребителски файлове към трета страна. Типичен таргет на троянски кон са потребителски пароли и сензитивна информация, като банкови смети.
* Задна врата – предоставя достъп до дадена програма или машина на външен участник. Инсталира се чрез троянски кон или червей и се състои от клиент и сървър.

**ВЪПРОС 3**

3.1. Какви са потенциалните заплахи от рекламен софтуер (adware) и от фалшив софтуер (rogueware).

Отговор: Главната заплаха от рекламният софтуер е наличието на модул за запис на клавишите на машината и изпращането им на отдалечен сървър. Освен това рекламният софтуер по-скоро предизвиква досада в потребителя отколкото заплаха.

Фалшивият софтуер, по своята същност е пълна противоположност на рекламния. Той е изключително скрит и най-често се представя за легитимен софтуер за премахване на измислени вируси и иска пари за тази си дейност.

3.2. Какви са заплахите от шпионския софтуер (spyware).

Отговор: Шпионският софтуер представлява софтуер, който събира и изпраща към своя създател определена информация от заразената машина. Типични приложения на този софтуер са следенето на активността на потребителя в интернет, записване на клавишите чрез keylogger модул, конфигуриране на мрежовата карта на машината с цел вкарването ѝ в режим на пропускане на всички пакети и др. И тук целта е достъп до пароли пренасяни от мрежовите приложения.

3.3. Какво е експлойт (exploit) и какви са заплахите от него.

Отговор: Експлойтът представлява софтуер, който търси у язвимости от общ вид – на ниво операционна система, браузър, приложение и др. Разновидност са т.нар. пакети екслпойти – готови пакети за автоматизиране на атака на дадена уязвимост.

3.4. Какво е руткит (rootkit) и какви са заплахите от него.

Отговор: Руткит е сравнително нов вид софтуер, който се използва за превръщане на машината в „зомби“. По своята същност това не е зловреден софтуер. Антивирусните програми например го използват, за да се защитят от вируси.

**ВЪПРОС 4**

4.1. Какво е препълване на ресурс (Flood, Floods, Flooder).

Отговор: Препълването на ресурс има за цел да натовари максимално отсрещната страна. Типичен пример е MAC flooding – препълване на кеша на мрежови суитч (комутатор). Комутатора преминава в режим хъб, опитвайки се да изчисти кеша, като в този режим комутирането на пакети се прекратява и те достигат всички портове. Така атакуващия има възможността да следи трафика.

Друга атака е Ping of Death. Тя се получава когато отсрещната машина не е настроена да отхвърля fragmented ICMP пакети с големина над 64 KB и в резултат на това е принудена да ги сглобява препълвайки буфера си.

4.2. Какво е значението на подправянето (Spoofing).

Отговор: Подправянето се прави с цел да проникне в системата и да следи нейния трафик. Има различни начини за реализация. Един вариант е подправянето на поредния номер на мрежовите пакети. Всеки пакет е номериран уникално от OS. Разкодирайки алгоритъма за това номериране, атакуващия може да автентикира подправени пакети при установяване на връзка с машината. Друг вариант за фалшифициране е лъжлив MAC адрес с цел получаване на пакети предназначени за друг. Ако хакерът успее да подмени MAC адресите в ARP таблицата на машината, която служи за бързо разпознаване на вече търсени релации IP адрес към MAC адрес. По този начин пакетите ще бъдат изпращани към новото „хакнато“ IP.

4.3. Какво е значението на мрежите от подчинени компютри (botnet).

Отговор: Основната цел е кражба на лични данни, обикновено чрез инсталиране на троянски кон в дадена машина. Най-често машината работи в автономен режим с още „отровени“ машини и съставя голям ресурс за извършване на кибератаки.

4.4. Какво е отказ от обслужване (услуга) - DoS (Denial of Service) и DDoS (Distributed Denial of Service).

Отговор: На пръв поглед целта е да се блокира обслужването на ресурса от неговите целеви потребители (например даден сайт или платформа да бъде блокирана и да не може да обработи заявки от потребители). Това обаче не е единственото приложение на тези атаки. След като бъде свален ресурсът, хакерите може да получат достъп до него, да запишат свои данни в системата и да инсталират свои програми. Примери за DoS:

* TCP SYN претоварващи атаки (изпращане на голям брой пакети симулиращи валидни заявки за връзки)
* Land.c атаки (изпращане на множество подправени SYN пакети, с еднакви адреси и портове на подател и получател)
* SMURF наводняващи атаки (изпращане на безполезен трафик към машината)

DDoS атаките са доста по-сложни от DoS атаките, тъй като изискват координация на множество машини извършващи атаката към ресурса.

4.5. Какво е зарибяване (phishing).

Отговор: Зарибяването представлява атака, при която се изпраща съобщение, което се представя за някоя финансова институция с цел получаване на пароли и акаунти за достъп до финансовите ресурси на жертвата. Би могло да се постигнат и нефинансови цели с тази атака – spear phishing, който цели получаване на неоторизиран достъп до информация, подвеждайки потребителя да въведе акаунт и парола в неистински сайт.

4.6. Какво е заключване на данни.

Отговор: И тук основната цел е финансова облага, като тази атака си има доста голяма популярност в наши дни. В най-общ случай атаката криптира файловете на потребителската машина и атакуващият иска пари, за да се предостави декриптиращия ключ.

**ДИСКУСИЯ**

Как, по ваше мнение, могат да се обобщят видовете техники за нападение (атаки) в Интернет.

Отговор: Според мен най-общо бихме могли да групираме атаките в две големи групи:

* Инвазивни и нескрити от потребителя – основната цел е блокиране достъпа до даден ресурс
* Неинвазивни и скрити – подслушване на трафика или подпъхване на зловреден код с цел придобиване на пароли, конфиденциална информация или организационна информация за системата.

Всяка една от тези атаки има за цел да се нанесе щета на даден потребител или организация и да донесе лична облага за атакуващия, която по разбираеми причини почти винаги е финансова.