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 3**

**НА СТУДЕНТА** : Георги Иванов Георгиев

**Фак. №:** f88683

**Дата:** 08/01/2018 г.

**Преподавател:**

/ доц. В.Къдрев / …………………

София

**ВЪПРОС 1**

* 1. ***Какви са методите и средствата за защита от кибератаки.***

Отговор: Пред всяка една организация стои въпросът кои методи и средства за защита да избере, тъй като съществуват множество различни такива. Този избор се прави в зависимост от оценката ѝ на риска за нейните информационни системи и, разбира се, от финансовия ресурс, с който разполага.

Един от основните методи е изграждането на стабилна и адекватна политика за сигурност. Тя трябва да бъде строго специфична за дадена организация, както и прилагането ѝ трябва да бъде съблюдавано. Тя следва да се обновява и да ограничава информационната експозиция на компанията. Тъй като сами по себе си политиките за сигурност не са достатъчен предпазен механизъм за една компания, взаимовръзката между различните компании е от изключително значение. Друг метод е повишаването на знанията и квалификацията на потребителите по отношение на заплахите за информационната сигурност и начините за тяхното отстраняване. Това е възможно посредством най-различни уеб платформи, брошури, статии и др.

* 1. ***Какви са основните принципи на методите за осигуряване на информационна сигурност.***

Отговор:

* CIA – идва от конфиденциалност (C), интегритет (I) и достъпност (А). Конфиденциалността се отнася до това само оторизирани лица да имат достъп до сензитивната информация за дадена компания. Итегритета засяга неизменността на информацията по време на нейното съхранение. Достъпността се отнася до това оторизираните лица да имат достъп до информацията при поискване и навреме.
* Принципът на шест елементният модел на Паркър – представлява своеобразно разширение на CIA. Добавя още три елемента – владение(да не се изпуса контрол над сензитивната информация), автентичност(правилното обозначаване на информацията) и полезност.
* Седемте принципа на ISO модела – включва конфиденциалност, интегритет, достъпност, невъзможност за отричане, проследимост, автентичност и надеждност.
  1. ***Какво е политика за сигурност***.

Отговор: Политиката за сигурност представлява съвкупност от формални правила, които служителите в дадена компания прилагат с цел опазване на чувствителните за нея технологии и информация. Тя включва принципи за опазване на информацията и насоки за рутинните действия спрямо установените формални правила. Добрата политика за сигурност гарантира интегритет, съхранение и лесен достъп до данните. Качествената политика за сигурност неминуемо води до оптимизиране на разходите по нейното приложение.

* 1. ***Какви са основните видове политики за информационна сигурност.***

Отговор:

* Корпоративна – описва основната рамка по отношение на всички политики в компанията
* Политика по администриране – свързана с административните дейности на фирмата
* Мрежова политика – свързана с мрежовата инфраструктура и обезпеченост на фирмата

и др.

* 1. ***Какво е процедура за реализиране на политика за информационна сигурност.***

Отговор: Това представлява изпълнение на предварително зададен сценарий по отстраняване на проблеми в сигурността. В нея подробно се описват действията, които трябва да се предприемат в дадена ситуация.

**ВЪПРОС 2**

***2.1. Какви са основните видове криптографски техники и какви накратко са техните особености.***

Отговор: Криптографията сама по себе си се занимава със създаване и декодиране на шифри. Съществуват три основни вида криптографски техники:

* Кодиране със симетричен ключ – при тази техника двете страни разполагат с ключа и след като едната е успяла да разкодира съобщението може успешно да установи връзка с другата. Много е важно ключът да е известен само на двете страни участващи в комуникацията. Типични примери за алгоритми използващи тази техника са Data Encryption Standard и Tripple DES. Размерът на ключа определя силата на защитата.
* Криптиране с несиметричен ключ – единият ключ е математическа функция на другия, но без двата заедно е невъзможно да се изчисли, който и да било. Единият се използва за криптиране и се пази в тайна, а другият е публично достъпен и служи за декриптиране. Пример е техниката RSA. Тези алгоритми са по-бавно и се използват главно за автентикация.
* Използване на хеш функции – превръщат съобщение в код с фиксирана дължина. Представляват контролна криптографска сума, от която не може да се възпроизведе оригиналното съобщение. Примери: MD5, SHA.

***2.2. Какви са характеристиките на една силна криптографска система.***

Отговор: Тя трябва да се базира на петте постулата разработени на базата на основните криптографски принципи, а именно опазване на криптографския ключ, наличие на голямо пространство на криптографските ключове, генерирания шифриран текст не подлежи на статистически анализ, тоест символите в него са със случайно статистическо разпределение, усилията да се разбие алгоритъма да са по-големи от наградата да се получи информацията и времето за разбиване да е по-дълго от актуалността на информацията, която е защитавана.

***2.3. Как може да се направи сравнение на различните методи на шифриране.***

Отговор: При сравняване на различните методи на шифриране трябва да се има предвид ситуацията, в която ще се прилагат. Например шифрите с алгоритми ползващи симетричен ключ са бързодействащи при работа с големи по размер данни, но пък е налице необходимостта от копия на ключа. От друга страна шифрите използващи открит ключ в своите алгоритми са гъвкави откъм разпространение на публичния ключ и възможността клиент да се подписва цифрово. Техен недостатък е изискването от по-голяма изчислителна мощност сравнение с горепосочения метод, което прави работата с тях малко по-сложна при наличието на големи по обем данни.

**ВЪПРОС 3**

***3.1. Каква е причината за създаването на спецификацията Secure IP (IPSec).***

Отговор: Основната цел за създаването на тази спецификация е подсигуряване на безопасност на информацията обменяна в обществените мрежи, чрез известните протоколи. Спецификацията е базирана на общи методи на безопасност на IP, автентикационни заглавие и енкапсулация на данните. Чрез IPSec се подсигурява сигурността на предаваната информация по интернет в пъти по-добре, от който и да е друг метод.

***3.2. Каква е архитектурата на Internet Protocol Security (IPSес).***

Отговор: Архитектурата на IPSec има три основни елемента:

* Автентикационно заглавие – позволява удостоверяване, че предаваната информация между двете страни не е била променена
* Енкапсулация на данните – криптиращ формат предпазващ данните от подслушване при тяхното пренасяне
* Общи методи за безопасност на IP

***3.3. Какви накратко са параметрите на Internet Protocol Security (IPSес).***

Отговор: Това са адресът на получателя, идентификатор, посочващ протокола за защита и броя на защитните параметри. Те могат да се допълнят от отделен брояч на поредните номера, прозорец за защита от копиране, определяне на времето на защитената връзка и др.

***3.4. За какво служи протоколът IP Authentication Header (AH).***

Отговор: В своята същност IP Authentication Header протоколът има за цел да осигури целостта и автентичността на IP пакетите. По този начин е гарантирано невъзможността за тайна промяна на съдържанието в пакетите. Чрез тази технология се избягват атаки свързани с подмяна на мрежовите адреси и повторно получаване от получателя на вече регистрирани пакети. Autherntication header-а съдържа осем байтово поле за дължина на заглавието, пореден номер, алгоритми и ключове използвани за създаване на връзката, данни за автентикация и служебно (резервирано) поле за бъдеща употреба.

***3.5. За какво служи протоколът IP Encapsulating Security Payload (ESP).***

Отговор: Негова основна цел е гарантиране на конфиденциалността и защитата на предаваното съобщение. Самият протокол се състои от 6 елемента: индекс на параметрите за безопасност, пореден номер, предаваните данни, допълнение използвано от криптиращите алгоритми, дължина на допълнението, следващо заглавие и използваните протоколи.

**ВЪПРОС 4**

***4.1. Какви са особеностите на транспортния режим на AH и ESP.***

Отговор: Режимът се използва за защита на протоколите и осигуряване на сигурна връзка между комуникиращите машини. Този режим се базира на полезния товар на IP. AH съдържа IP заглавието, заглавието на AH и самите данни, а ESP шифрира ако е необходимо. ESP включва отново IP заглавието и самите данни, заглавието на ESP и ESP трейлер за аутентикатора на ESP.

***4.2. Какви са особеностите на тунелния режим на AH и ESP.***

Отговор: Използва се за комплексна защита на IP пакет и осигурява предпазване от атаки на мрежовия трафик. Самата защита става посредством добавяне на AH и ESP към данните. След това съвкупността се разглежда като данни и се енкапсулира в нов пакет. Така се маскира оригиналното IP и местоназначението на пакета. При този режим AH и ESP се поставят между изходното и новото IP заглавие.

***4.3. Какво е предназначението на протоколите: ISAKMP (Internet Security Association and Key Management Protocol), Oakley (Oakley Key Determination Protocol) и IKE (Internet Key Exchange).***

Отговор: Протоколът служи за управлението на ключовете в IPSec, както и за процедурите за тяхното генериране и разпределение. Свързан е и с полезния товар на данните за обмен и тяхната автентичност. Протоколът Oakley от своя страна се занимава с подсигуряването на обмена на ключовете като се базира на алгоритъма на Дифи-Хелман за допълнителна защита. Най-голямата полза от ползването на този протокол е осигуряването на автентични ключове. IKE протоколът е разположен на върха на ISKAMP и отговаря за осигуряването на ISAKMP SA И IPSec SA.

**ДИСКУСИЯ**

**Кои протоколи от различните нива на OSI модела се използват за изграждане на VPN мрежи.**

Отговор: Когато изграждаме VPN мрежи обикновено се използват протоколите от мрежовото, транспортното и каналното ниво. Протоколите от мрежовото ниво имат цел да криптират данните, както и да автентикират потребителите. Протоколите от каналното ниво тунелират данните и се занимават с тяхната ауторизация и автентикация. Протоколите от транспортния слой използват криптиращи функции за транспортния слой между участниците в комуникацията. Те могат да защитават както TCP така и UDP трафик.