Финансирано от Европейския съюз
NextGenerationEU

4.1 Защита на устройства

БЕЗОПАСНОСТ - СРЕДНО НИВО

ЕВРОПЕЙСКА РАМКА НА ДИГИТАЛНИТЕ КОМПЕТЕНТНОСТИ С ПЕТТЕ ОБЛАСТИ НА ДИГИТАЛНА КОМПЕТЕНТНОСТ И 21 ДИГИТАЛНИ УМЕНИЯ/ КОМПЕТЕНТНОСТИ (DIGCOMP 2.1)

Какво ще научите

- Да познавате рисковете и заплахите за дигиталните устройства и програми и да умеете да ги разграничавате.
- Да познавате начини за защита на своите устройства и дигитално съдържание.
- Как да приложите рутинни методи за защита на устройства и програми:
  - Антивирусен софтуер на компютърна система.
  - Защитна стена.
  - Стратегии за използване за защитени пароли.
  - Поддръжка на актуализирани версии на софтуерните програми.

Рискове и заплахи за дигиталните устройства и програми

- Кой атакува нашата мрежа и защо?
  - Нападателите искат достъп до нашите активи.
  - Активите са всичко, което има стойност за една организация като данни и друга интелектуална собственост, сървъри, компютри, смарт телефони, таблети и др.
  - В личен план – лични данни.

Рискове и заплахи за дигиталните устройства и програми - 2

- Какво всъщност се има предвид под „хакер“?
  - Често срещан термин, използван за описание на заплаха, злонамерено лице.
  - Всъщност терминът има различни значения, напр.:
    - Умен програмист, способен да разработва нови програми и да кодира промени в съществуващи програми, за да ги направи по-ефективни.
    - Мрежов професионалист, който използва сложни умения за програмиране, за да гарантира, че мрежите и устройствата не са уязвими за атаки.
    - Лице, което се опитва да получи неоторизиран достъп до устройства в интернет.
    - Човек, който изпълнява програми за предотвратяване или забавяне на мрежовия достъп до голям брой потребители или повреждa, или изтрива данни на сървъри.

Рискове и заплахи за дигиталните устройства и програми - 3

- Какво всъщност се има предвид под „хакер“? (продължение)
  - Видове хакери, според целта:
    - Хакери с бяла шапка - Етични хакери, които използват уменията си за програмиране за добри, етични и законни цели. *Напр. Откриват уязвимости, с цел подобряване на защитата и с предварително позволение.*
    - Хакери със сива шапка - Такива, които извършват престъпления и неетични действия, но не с цел лична изгода или нанасяне на щети. *Напр. Откриват уязвимости, но без позволение и могат да ги докладват или публикуват.*
    - Хакери с черна шапка - неетични престъпници, които се възползват от всяка уязвимост, като нарушават компютърната и мрежовата сигурност с цел лична, финансова или политическа изгода.
    - За злонамерените лица се има предвид, хакери със сива и черна шапка.

Рискове и заплахи за дигиталните устройства и програми - 4

- Злонамерените лица използват различни инструменти за сигурност и злонамерен софтуер, за да извършат съответните атаки.
- Злонамерен софтуер: вирус, червей, троянски кон, спайуер, рансъмуер и др.
- Често срещани видове атаки:
  - Атаки за подслушване (шпиониране) – улавя се и прослушва дадена системи или мрежовия трафик (потока от данни), с цел събиране на информация.
  - Атаки за модифициране на данни – улава се трафикът и се променят данните в пакетите, без знанието на изпращача или получателя.
  - Атаки, базирани на парола – използват се привилегии на валиден за системата потребител, за да се получат данни за потребителите или информация. Могат да бъдат променени конфигурации или изтрити данни.

Рискове и заплахи за дигиталните устройства и програми - 5

- Често срещани видове атаки: (продължение)
  - Примери за атака с парола:
    - Атака с груба сила (Brute-force) - метод за откриване на целева парола чрез систематично пробване на всички комбинации от букви, цифри и символи.
    - Речник атака (Dictionary) – пробване на всяка дума в речник или списък с често използвани думи.
  - Човек в средата (Man-in-the-Middle) - атакуващият е разположен между изпращача и получателя, за да чете или променя данните, които преминават между тях. *Напр. между уеб браузър и уеб сървър или да събира информация или за да се представи за едното.*
  - Атака отказ от услуга (DoS) – спира се или забавя нормалното използване на компютър, мрежа или услуга от потребителите, имащи такова право. Може да доведе до срив, чрез претоварване на ресурс или система, или да блокира достъпа до ресурсите от легитимните потребители (тези, които имат право на ползване).

Рискове и заплахи за дигиталните устройства и програми - 6

- Често срещани видове атаки: (продължение)
  - Разпределена атака отказ от услуга (DDoS) - подобна на DoS атака, но произхожда от множество координирани източници и цели да изчерпи ресурсите. *Напр.: Нападателят изгражда мрежа, наречена ботнет, от заразени устройства (зомбита), които се контролират от целева система (контролер). Компютрите-зомбита непрекъснато сканират и заразяват повече устройства, създавайки все повече и повече зомбита. Когато е готов, хакерът инструктира контролер и ботнет мрежата от зомбита извършва DDoS атаката. Зомбитата могат още да разпространяват злонамерен софтуер, нежелани имейли (спам) или да извършват атака с парола - груба сила.*
  - Социално инженерство - манипулиране на хората да извършват действия или да разкриват поверителна информация. Злонамереното лице разчита на тяхната добронамереност и готовност за помощ или се възползва от техни слабости. *Напр.: Хакер се обажда на упълномощен служител със спешен проблем, който изисква незабавен достъп до мрежата и споменава име на човек с ръководна длъжност, за да получи този достъп.*

    Често тези заблуди са посредством фалшиви имейли (фишинг) или телефонни обаждания.

Начини за защита на устройства и дигитално съдържание

- Всяка атака има уникални разпознаваеми атрибути - функции, които идентифицират файлове със зловреден софтуер, IP адреси на сървъри, които се използват при атаки, имена на файлове и характерни промени, направени в потребителския системен софтуер.
- Много атаки могат да бъдат предотвратени чрез споделяне на информация за т. нар. индикатори за компрометиране - доказателството, че е извършена атака, които веднага се споделя с общността, за да ѝ помогне да защити мрежите и устройствата си от конкретната заплаха.
- Индикаторите помагат да се изясни какво се е случило при атаката и да се разработи защити срещу нея.

Начини за защита на устройства и дигитално съдържание - 2

- Важно е да могат да се разпознават често срещани симптоми на заразена система, като:
  - Увеличаване използването на централния процесор, което забавя устройство.
  - Компютърът често замръзва или се срива.
  - Намаляване на скоростта на сърфиране в мрежата.
  - Необясними мрежови проблеми или проблеми с мрежови връзки.
  - Променени или изтрити файлове, както й наличието на непознати файлове, програми или икони на работния плот.
  - Изпълняване се неизвестни процеси, самоизключване или преконфигуриране на програми.
  - Изключване на антивирусния софтуер или защитната стена.
  - Изпращане на имейли без Ваше знание или съгласие.

Начини за защита на устройства и дигитално съдържание - 3

- Познавайки различните типове атаки и как се разпространяват, е от ключово значение за ограничаването и премахването им.
- Организациите трябва да предприемат действия, за да защитят своите активи, потребители и клиенти. Те трябва да разработят и практикуват задачи по киберсигурност, като например следните:
  - Да бъде инсталиран софтуер по сигурността – антивирусен софтуер, защитна стена, антиспайуер софтуер.
  - Да бъде поддържана и актуализирана редовно операционната система със съответните обновления, както и софтуерът.
  - Да се използват силни пароли, защитни политики за пароли, дву- или много-факторно удостоверяване.
  - Периодично да бъде архивирана информацията и съхранявана на различни места.
  - Да бъде създадена политика по сигурност, като служителите са обучени да я използват коректно.

Рутинни методи за защита на устройства и програми

- Използване на пакети за сигурност, които включват:
  - Пакет продукти за сигурност в домашни и бизнес мрежи, за осигуряване на многослойна защита срещу най-често срещаните заплахи.
  - Антивирусни (антималуер) продукти, антифишинг, безопасно сърфиране, система за предотвратяване на проникванията в хост и възможности за защитна стена.
- Антивирусен (Антималуер) софтуер – защита в реално време.
  - Това е софтуер, който е инсталиран на устройството за откриване и смекчаване на вируси и зловреден софтуер (малуер). *Например Windows Defender Virus & Threat Protection, Norton Security, McAfee, Trend Micro, AVG, Avast и други.*
  - Препоръчително е системата да се сканира периодично, инициирано от потребителя, за да проверява за зловреден код.

Рутинни методи за защита на устройства и програми - 2

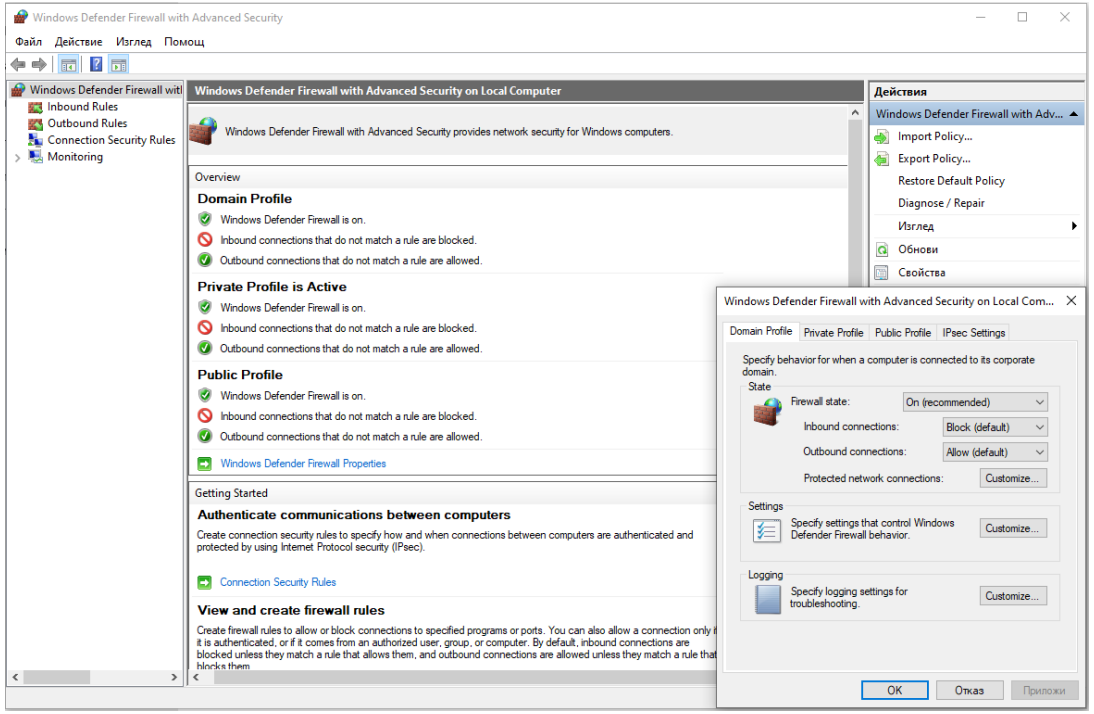
- Защитна стена (Firewall):
  - Един от най-ефективните налични инструменти за защита на потребителите от заплахи отвън.
  - Защитава компютрите и мрежите, като предотвратява навлизането на нежелан трафик във вътрешната мрежа.
  - Намира се между две или повече мрежи, контролира трафика между тях и помага за предотвратяване на неоторизиран достъп.
  - Прилага политика за контрол на достъпа между мрежите - Най-често трафикът инициран от вътрешната мрежа (отвътре-навън и обратно) е позволен, а този от външната (отвън-навътре) – забранен.

Рутинни методи за защита на устройства и програми - 3

- Защитните стени използват различни техники за определяне на това, на което ще бъде разрешен или отказан достъп до мрежа.
  - В зависимост от вида на филтрирането, съществуват следните видове:
    - Филтриране на пакети - Предотвратява или позволява достъп въз основа на IP (логически) или MAC (физически) адреси.
    - Филтриране на приложения - Предотвратява или позволява достъп от определени типове приложения, въз основа на номера на портове.
    - Филтриране на URL адреси - предотвратява или позволява достъп до уебсайтове въз основа на конкретни URL адреси или ключови думи.
    - Динамична инспекция на пакети (SPI) - Входящите пакети трябва да бъдат легитимен отговор на заявки от вътрешни хостове. Нежеланите пакети се блокират, освен ако не е изрично разрешено. SPI може също да включва способността да разпознава и филтрира специфични видове атаки, като отказ на услуга (DoS).

Рутинни методи за защита на устройства и програми - 4

- Персонална защитна стена (Защитна стена, инсталирана на компютър)
  - Самостоятелна софтуерна програма, която контролира трафика, влизащ или напускащ компютъра.
  - Може да попречи на компютъра да се зарази и да разпространява зловреден софтуер към други компютри. Тази функция е включена в някои операционни системи.
  - Могат да сигнализират на потребителите при откриване на подозрително поведение.



Windows включва защитна стена Windows Defender с разширена защита.

Рутинни методи за защита на устройства и програми - 5

- Системи за предотвратяване на прониквания (IPS), базирана на хост – за крайна система, напр. компютър.
  - Защитава компютърът, на който е инсталирана, срещу известен и неизвестен зловреден софтуер.
  - Може да извършва подробен мониторинг (наблюдение) и отчитане на системната конфигурация и дейността на приложението.
  - Цялостно приложение за сигурност, което съчетава функционалностите на анти-зловреден софтуер, с функционалност на защитната стена.
  - Открива аномалии и може да идентифицира заразени компютри в мрежата, които сканират за други уязвими компютри.

Рутинни методи за защита на устройства и програми - 6

- Стратегии за използване за защитени пароли.
  - Създаване и използване на сигурни пароли – за защита на акаунти.
    - Изисквания за силна парола:
      - По-голям брой символи, поне 12.
      - Комбинация от главни букви, малки букви, цифри и символи.
      - Да не е дума, която може да бъде намерена в речник или името на човек, знак, продукт или организация.
      - Значително да се различава от предишните Ви пароли.
      - Лесно Ви е да запомните, но е трудно за другите да я познаят.
      - Може да се използва фраза или последователност от думи и след това съкратено изписване.
  - Използване на двуфакторно удостоверяване – настройка, която освен потребителско име и парола, изисква втори фактор, за да докажете кой сте (съобщение, изпратено на мобилен номер, ПИН, пръстов отпечатък).

Рутинни методи за защита на устройства и програми - 7

- Поддръжка на актуализирани версии на софтуерните програми.
  - Поддръжка на софтуера е необходима, за да се гарантира безпроблемната му употреба в дългосрочен план.
  - Софтуерният продукт се нуждае от поправки, за да се гарантира оптимална му работа (Коригиране на неизправности, след първоначалното му инсталиране).
  - Подобряване на производителността.
  - Адаптиране на продукта към друга или нова среда.
- Защо поддръжката на софтуер е толкова важна?
  - Може да спре работата на даден софтуер или да блокират на някои негови функции.
  - Може да започне забавяне на работата му и се нуждае от оптимизация. Напр. При нарастване на обем на данни в него.
  - Отстраняване на операторски грешки или бъгове.
  - Форсмажорни обстоятелства или добавяне на нови функционалности.

Практическа задача 1. Проверка на сигурността на системата

Проверете сигурността на системата си, чрез Windows Security (Старт -> Настройки -> Актуализиране & защита -> Защита в Windows).

- Кои са инструментите, които можете да управлявате и които защитават вашето устройство и вашите данни. Какъв статус имат?
- Влезте във „Защита от вируси & заплахи“. Каква антивирусна програма е включена и какви са резултатите от предишните сканирания на вируси?
- От „Текущи заплахи“, започнете ново бързо сканиране. Какви са резултатите?

Ако е необходимо, за ръководство използвайте връзка - https://support.microsoft.com/bg-bg/windows/защита-от-вируси-и-заплахи-в-защита-в-windows-1362f4cd-d71a-b52a-0b66-c2820032b65e

- Изтеглете и инсталирайте антивирусна програма AVG (https://www.avg.com/en-eu/homepage#pc), разгледайте я. Какви разлики се получиха в Windows Security - „Защита от вируси & заплахи“.

Практическа задача 2. Актуализация на програми

- Проверете сигурността на системата си, чрез Windows Security (Старт -> Настройки -> Актуализиране & защита -> Защита в Windows).
- Изберете „Защита от вируси и заплахи“ -> „Актуализации на защитата от вируси и заплахи“ , изберете „Проверка за актуализации“, за да сканирате за най-новата аналитична информация за защитата.
- Изберете „Производителност и изправност на устройството“, за да прегледате отчета за изправност.
- След последното сканиране ще видите състоянието на ключовите области, които се наблюдават от изправността на устройството. Какъв е отчетът за изправност?
- Вижте от „Приложения и софтуер“ дали софтуерът ви дава грешки или се нуждае от актуализация? Ако се нуждае, обновете го.
- За ръководство използвайте връзките: https://support.microsoft.com/bg-bg/windows/проверете-производителността-и-изправността-на-устройството-в-защита-в-windows-59d8499d-b6fd-6930-7667-ebf8ae10e08d и https://support.microsoft.com/bg-bg/windows/ защита-от-вируси-и-заплахи-в-защита-в-windows-1362f4cd-d71a-b52a-0b66-c2820032b65e

Практическа задача 3. Защитна стена

- Прегледайте състоянието на Microsoft Defender защитна стена, вижте към кои мрежи е свързано вашето устройство и за кои от тях е включена защитната стена?
- Изберете „Разрешаване на приложение през защитната стена“ и разгледайте какви приложения са позволени/забранени. Какъв е статуса за: “Google Gmail” и “File and Printer Sharing”?
- Върнете се към “Настройки на мрежата” и влезе в “Разширени настройки” -инструмент за защитна стена на Windows Defender, който ви позволява да създавате входящи или изходящи правила. Вляво изберете „Входящи правила“, след което вдясно изберете филтриране за частния профил. Направете и филтриране за активните услуги/приложения и проверете има ли такива, които са блокирани. Изчистете филтрите и затворете. *Заб. Неправилното добавяне, промяна или изтриване на правила може да доведе до по-голяма уязвимост на вашата система или може да доведе до това някои приложения да не работят.*

За ръководство използвайте връзка - https://support.microsoft.com/bg-bg/windows/защитна-стена-и-мрежова-защита-в-защита-в-windows-aef9838b-d081-fd75-3b1b-e5fa794c003b

Практическа задача 4. Разграничаване различни видове зловреден софтуер

Открийте кой от отговорите съответства на описанието:

- Adware (Адуер)
- Ransomware (Рансъмуер)
- Spyware (Спайуер)
- Virus (Вирус)
- Worm (Червей)

Зловреден софтуер	Описание
	Зловреден софтуер, предназначен да проследява вашата онлайн активност и да улавя вашите данни.
	Софтуер, който автоматично добавя реклами.
	Злонамерен софтуер, който държи компютърна система в плен, докато не бъде извършено плащане на нападателя.
	Злонамерен код, който се прикрепя към законни програми и обикновено се разпространява чрез USB устройства, оптични носители, мрежови споделяния или имейл.
	Злонамерен код, който се репликира независимо, като използва уязвимости в мрежовия.

Въпроси за самопроверка

Въпрос 1. Банкомат е хакнах без разрешението на производителя и са открити няколко уязвимости. След това извършителят се свързва с производителя на банкомата, за да сподели откритите уязвимости. Изберете кой вид е хакера от описаната ситуация.

A. С бяла шапка.
B. Със сива шапка.
C. С черна шапка.
D. С червена шапка.

Въпрос 2: Каква е основната цел на атаката отказ от услуга (DoS атака)?

A. За улесняване на достъпа до външни мрежи.
B. За да попречи на целевия сървър да предоставя услуги на легитимните си потребители.
C. За получаване на всички адреси в адресната книга в сървъра.
D. За сканиране на данните на целевия сървър.

Въпроси за самопроверка

- Въпрос 3. Кои от изброените са често срещани симптоми на заразена система? (Изберете три верни).
  - A. Забавяне на работата на устройство.
  - B. Увеличаване на скоростта на сърфиране в мрежата.
  - C. Проблеми с мрежовите настройки на устройството.
  - D. Променени или изтрити файлове
  - E. Изпращане на имейли без Ваше знание или съгласие.

Тестови въпроси

Въпрос 1. В банкомат тайно е монтирано устройство за копиране на карти. Няколко дни по-късно устройството се премахва и са копирани номерата на сметки и ПИН-кодовете на над 1000 души. След това извършителят прехвърля пари от техните сметки към офшорната си банкова сметка. Изберете кой вид е хакера от описаната ситуация.

A. С бяла шапка.
B. Със сива шапка.
C. С черна шапка.
D. С червена шапка.

Въпрос 2. Какъв тип атака позволява на нападателя да използва подход с груба сила?

A. Социално инженерство
B. Разбиване на пароли
C. Отказ на услуга
D. Наблюдаване на пакети данни, преминаващи през мрежата.

Тестови въпроси

Въпрос 3: Потребител забелязва, че антивирусната програма на компютъра му е изключена. След като ръчно я включва, антивирусната програма отново се изключва. Какво заключение може да си направи потребителя?

A. Антивирусната програма се нуждае от обновяване.
B. Защитната стена на компютъра му е спряна.
C. Компютърът му е заразен с малуер.
D. Системата за предотвратяване на проникванията е включена.

Използвани източници

- Останете защитени със "Защита в Windows“- https://support.microsoft.com/bg-bg/windows/останете-защитени-със-защита-в-windows-2ae0363d-0ada-c064-8b56-6a39afb6a963
- Какво е: Удостоверяване с многофакторни данни - https://support.microsoft.com/bg-bg/topic/какво-е-удостоверяване-с-многофакторни-данни-e5e39437-121c-be60-d123-eda06bddf661
- Създаване и използване на сигурни пароли - https://support.microsoft.com/bg-bg/windows/създаване-и-използване-на-сигурни-пароли-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb
- Система за предотвратяване на проникванията в хоста (HIPS) - https://help.eset.com/ees/9/bg-BG/idh_hips_main.html
- Що е социално инженерство и с какво ни заплашва в 2023? - https://bg.safetydetectives.com/blog/какво-е-социално-инженерство/
- Най-добрите антивирус и антималуер инструменти за сканиране под Windows - https://pcguide.bg/nai-dobrite-antivirus-antimalware-instrumenti-za-scanirane-pod-windows/
- ПОДДРЪЖКА НА СОФТУЕР - https://cyclamsoft.com/поддръжка-на-софтуер/
- Email is Hacked!: 7 Immediate Steps To Follow - https://blog.loginradius.com/identity/what-to-do-when-email-hacked/
- „Free online tech courses backed by Cisco's expertise and connected to real career paths. Discover your future today.“ - https://skillsforall.com/