Финансирано от Европейския съюз
NextGenerationEU

4.1. Защита на устройства

МУЛТИМЕДИЕН ТЕКСТ (ПОМАГАЛО) ТИП ЛЕКЦИЯ (УЧЕБНИК)/
БЕЗОПАСТНОСТ – СРЕДНО НИВО

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.
- Да използвате рутинни методи за защита на устройства и програми.
- Да умеете да работите с антивирусен софтуер на компютърна система и защитна стена.
- Да използвате стратегии за защитени пароли.
- Да поддържате актуализирани версии на софтуерните програми.

НОВИ ПОНЯТИЯ:

Понятие	Описание
Правила за защита на дигиталните устройства	Система от предписания, които трябва да се изпълнят по определен начин, за да се защитят дигиталните устройства.

Финансирано от
Европейския съюз
NextGenerationEU

Съдържание

1 РИСКОВЕ И ЗАПЛАХИ ЗА ДИГИТАЛНИТЕ УСТРОЙСТВА И ПРОГРАМИ

Преди да можем да защитим нашата мрежа и устройствата ни, трябва да знаем кой може да ни атакува и защо?

Обикновено, ако става въпрос за организация, 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, които обикновено наричаме с общо название „хостове“.

В личен план, злонамерените лица искат достъп до устройствата ни, за да получат информация за личните ни данни.

1.1 ВИДОВЕ ХАКЕРИ

Какво всъщност се има предвид под „хакер“?

Често срещан термин, използван за описание на заплаха и злонамерено лице. (Фигура 1)

Фигура 1. Изображение на 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 (неправомерен) достъп до устройства в интернет.
- Човек, който изпълнява програми за предотвратяване или забавяне на мрежовия достъп до голям брой потребители или поврежда, или изтрива данни на сървъри.

Видове хакери, според целта: (Фигура 2)

- 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.

Фигура 2. Видове хакери, според целта

1.2 Видове атаки

Злонамерените лица използват различни инструменти за сигурност и злонамерен софтуер, за да извършат съответните атаки.

Видове злонамерен софтуер са: вирус, червей, троянски кон, спайуер, рансъмуер и др.

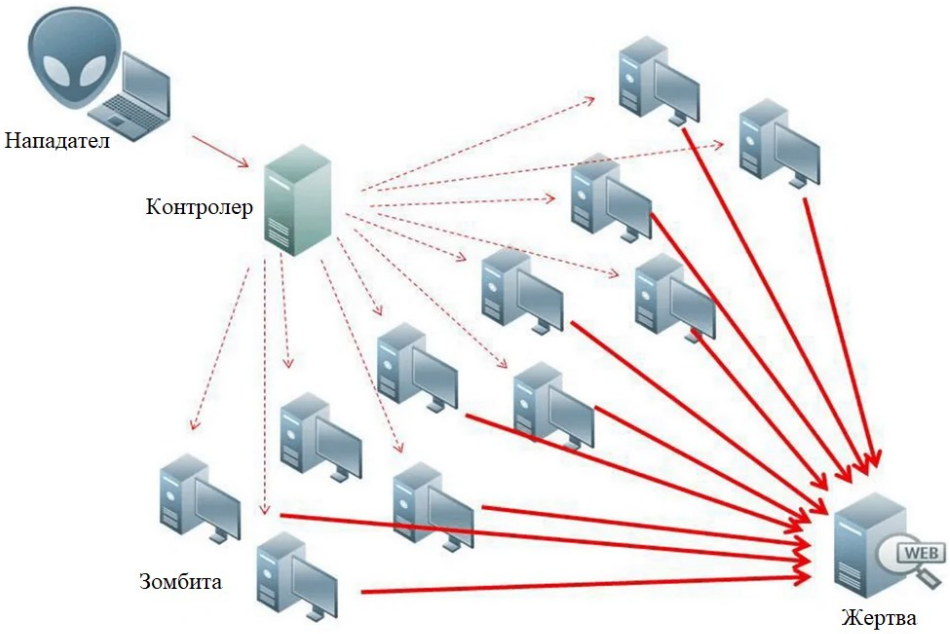
Често срещани видове атаки:

- Атаки за подслушване (шпиониране) – улавя се и прослушва дадена система 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.
  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 от тях или за да се представи за едното устройство.*
- Атака отказ от услуга (DoS[1]) – 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).
- Разпределена атака отказ от услуга (DDoS[2]) - 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 контролера и ботнет мрежата от зомбита извършва DDoS атаката. Зомбитата могат още да*

[1] DoS (Denial-of-Service)
[2] DDoS (Distributed denial of service)

разпространяват злонамерен софтуер, нежелани имейли (спам) или да извършват атака с парола - груба сила. (Фигура 3)

- 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.



Фигура 3. Разпределена атака отказ от услуга DDoS

2 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.

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.

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.

3 РУТИННИ МЕТОДИ ЗА ЗАЩИТА НА УСТРОЙСТВА И ПРОГРАМИ

За защитата на устройствата и програмите, се използват 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.

1. **Антивирусен (Антималуер) софтуер** предоставя 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.*

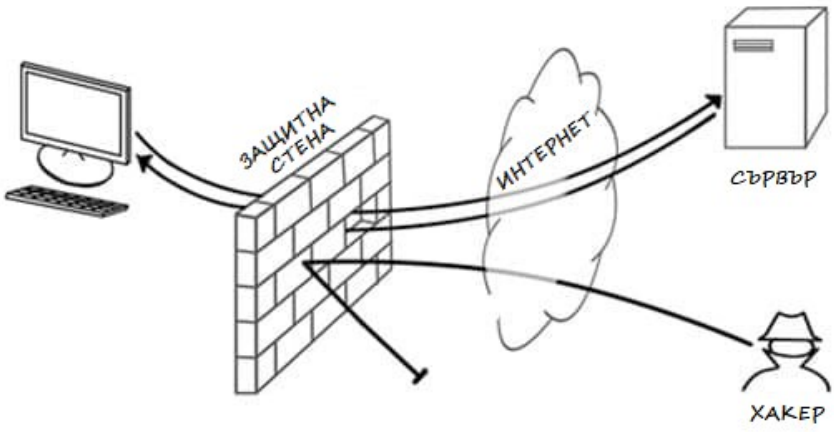
Препоръчително е системата да се сканира периодично, инициирано от потребителя, за да проверява за зловреден код.

2. **Защитна стена** (Firewall) е 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, като 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. (Фигура 4)



Фигура 4. Защитна стена (Firewall)

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:

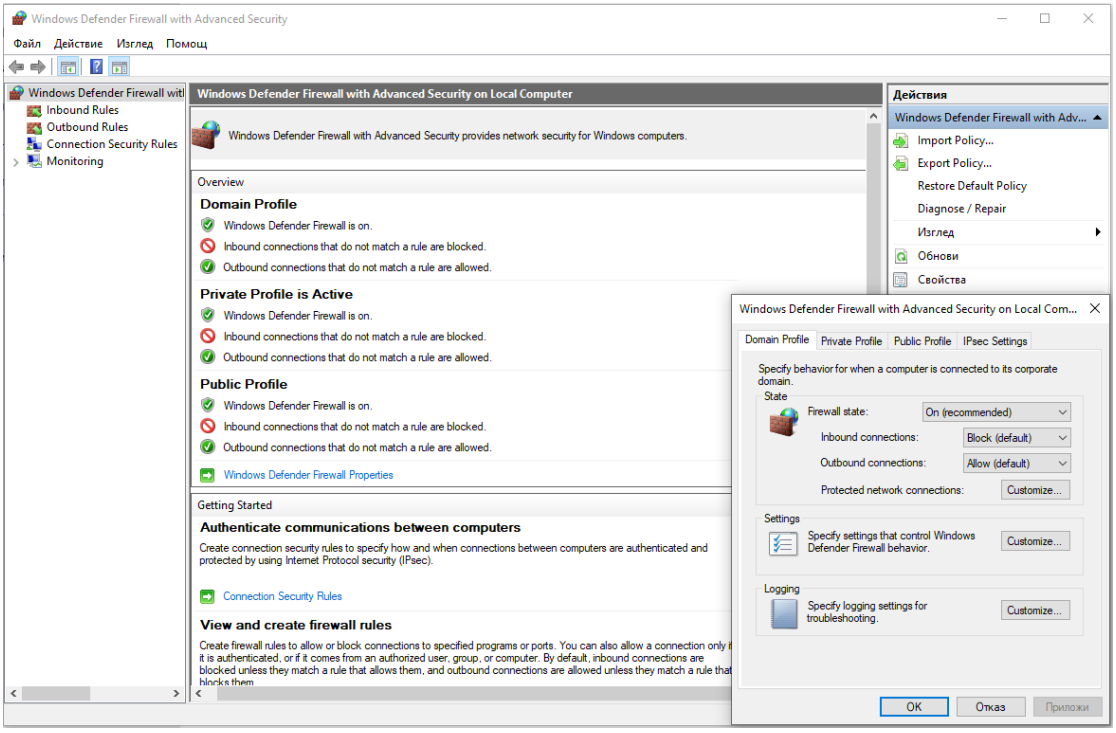
- Филтриране на пакети - Предотвратява или позволява достъп въз основа на IP[3] (логически) или MAC [4](физически) адреси.
- Филтриране на приложения - Предотвратява или позволява достъп от определени типове приложения, въз основа на номера на портове.
- Филтриране на URL адреси - предотвратява или позволява достъп до уебсайтове въз основа на конкретни URL адреси или ключови думи.
- Динамична инспекция на пакети (SPI[5]) - 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).

3. **Персонална защитна стена** е защитна стена, инсталирана на крайно устройство (компютър, лаптоп, мобилен телефон и др.) Тя е самостоятелна софтуерна програма, която контролира трафика, влизащ или напускащ устройството, а също може да попречи на устройството да се зарази и да разпространява зловреден софтуер към други устройства. Тази функция е включена в някои операционни системи.

[3] Internet Protocol (IP) адрес– Уникален адрес на устройство, свързано и комуникиращо в мрежа, използвайки интернет протокол (IP).
[4] Media Access Control (MAC) адрес – Уникален адрес на всеки мрежов адаптер (мрежова карта).
[5] Stateful packet inspection (SPI)

Персоналните защитни стени могат също да сигнализират на потребителите при откриване на подозрително поведение.

Windows включва защитна стена Windows Defender с разширена защита. (Фигура 5)



Фигура 5. Защитна стена Windows Defender - правила за контрол на трафика

4. **Система за предотвратяване на проникванията (IPS[6]), 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.

   Системата е 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.

5. **Стратегии за използване за защитени пароли** – за да бъдат защитени потребителските акаунти, е необходимо да бъдат създадени/използвани сигурни пароли. За да бъдат такива, паролите трябва да отговарят на следните изисквания:
   - 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.

[6] Intrusion Prevention System (IPS)

6. **Двуфакторно удостоверяване** - друг защитен метод за вход е 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).
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).
   - Подобрява се производителността на софтуера или устройството.
   - Адаптиране на продукта към друга или нова среда.

Поддръжката на софтуера е важна, защото в противен случай, може да спре работата на даден софтуер или да блокират някои негови функции. Също така, може да започне забавяне на работата му и се нуждае от оптимизация. *Напр. При нарастване на обем на данни в него.*
При обновяването обикновено се отстраняват операторски грешки или бъгове, а също и могат да се добавят нови функционалности.

4 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/
- Hacker Types: Black Hat, White Hat, and Gray Hat Hackers - https://www.avast.com/c-hacker-types
- Какво е DDoS атака и как да се предотврати през 2023 г. - https://bg.safetydetectives.com/blog/%D0%BA%D0%B0%D0%BA%D0%B2%D0%BE-%D0%B5-ddos-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0/

- What is a Firewall? - https://www.hotspotshield.com/resources/what-is-a-computer-firewall/