Финансирано от Европейския съюз
NextGenerationEU

4.1. Защита на устройства

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

ЩЕ НАУЧИТЕ:

- Потенциалните рискове и заплахи за дигиталните устройства и софтуерни програми.
- Методи за защита на устройства и електронна информация.
- Как да приложите базова защита на електронни устройства.

НОВИ ПОНЯТИЯ:

Понятие	Описание
Защита на дигитално устройство	Защита на дигиталното устройство, чрез инсталиране и поддържане на актуализирани версии на програми, антивирусен софтуер, защитни стени и прилагане на политика за пароли.
Рискове, свързани с дигиталните устройства	Опасности и заплахи за дигиталните устройства и софтуерни програми.

Финансирано от
Европейския съюз
NextGenerationEU

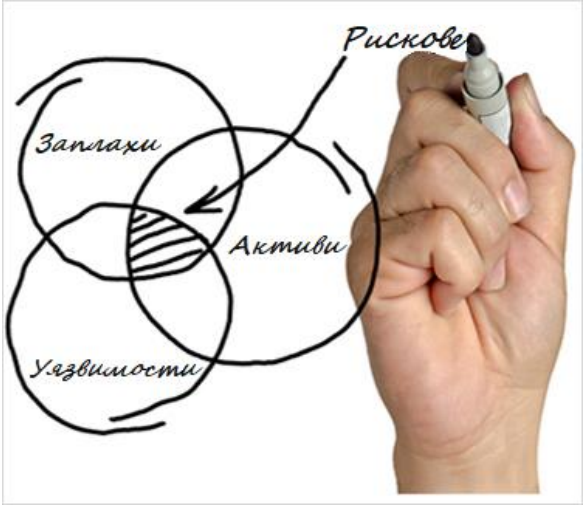
Съдържание

1 Потенциални рискове и заплахи за дигиталните устройства и софтуерни програми

Извършителите искат да получат достъп до нашите активи, като например данни и друга интелектуална собственост, сървъри, компютри, смартфони, таблети и т.н.

От една страна имаме активите (Assets), от друга уязвимостите (Vulnerability), а от трета – възможните заплахи (Threats).

За да се приложи адекватна защита за дигиталните устройства и софтуерните програми, трябва да се направи оценка какви са потенциалните рисковете и до какви последствия биха довели те. (Фигура 1)



Фигура 1. Рискове

Преди да можем да разпознаваме потенциални рискове и заплахи, трябва да знаем определени термини, свързани със сигурността.

1.1 Термини, свързани със сигурността

- Какво означава **Заплаха**? – Това е потенциалната опасност за даден актив, например данни или самата мрежа.
- Какво означава **Уязвимост**? – Това е слабост в системата или нейния дизайн, която може да бъде използвана от дадена заплаха.
- Съвкупността от уязвимостите в дадена система, които са достъпни за нападателя се нарича **Атакуваща повърхност**. Атакуващата повърхност описва различни точки, в които нападателят може да влезе в системата и откъде може да получи данни от нея.
- **Експлойт** - Механизъм, при който се използва дадена уязвимост, за да се компрометира даден актив. Експлойтите могат да бъдат отдалечени или локални.
    - Отдалечен експлойт – този, който работи по мрежата без да е имал предварителен достъп до целевата система.
    - Локален експлойт - извършителят има някакъв вид потребителски или административен достъп до крайната система. Това не означава непременно, че той има физически достъп до крайната система.

- **Риск** - Вероятността определена заплаха, да се възползва от конкретна уязвимост на даден актив и да доведе до нежелани последствия.
- **Управление на риска** - Процес, при който се изследва, анализира и проследява развитието на съществуващите рискове, с цел да се намали негативния ефект от евентуалното им настъпване или да се предостави възможност за възползване от тяхното настъпване.
- Идентифицирането на рискове е процес, при който се определят възможните източници на рискове, а самите рискове от своя страна се идентифицират и описват.
- **Контрамярка** - Действия, предприети за защита на активите, чрез смекчаване на заплахата или намаляване на риска.
- **Влияние** - Потенциалните щети за организацията, причинени от заплахата.

Когато се прави оценката на риска, трябва да се прецени дали да се вложат средства за защитата от този риск или влиянието му няма да доведе до такива щети, чието възстановяване ще струва по-малко от защитата.

1.2 Видове заплахи

Какви са най-често срещаните видове заплахи?:

- Кражба на информация – Достъп до поверителна (конфиденциална) информация, която може да се използва или продава за различни цели.
- Изтриване или манипулация на данни.
- Кражба на самоличност – Кражба на лични данни, напр. с цел финансова злоупотреба, или неоторизирани онлайн покупки.
- Отказ от услуга – Прекъсване на предоставянето на услуга за легитимните потребители на дадена услуги или системи.

1.3 Видове уязвимости

Как злонамерените лица достигат до устройствата или данните?

Освен заплахите, устройствата и системите имат уязвимости.

1.3.1 Технологични

- Слабост на протокола TCP/IP[1], на чийто концептуален модел са създадени и протоколите HTTP[2], FTP[3], ICMP, на което се дължат

[1] TCP/IP (Transmission Control Protocol / Internet Protocol) - концептуален модел на семейство от протоколи за комуникация между компютрите, който се използва в Internet и в почти всички съвременни мрежи
[2] Протокол за пренос на хипертекст (Hypertext Transfer Protocol, HTTP)
[3] File Transfer Protocol (Протокол за пренос на файлове, FTP)

техните слабости, както и на протоколите - SNMP[4], SMTP[5], базирани на TCP[6]).

- Уязвимости в операционната система на устройствата.
- Незащитени мрежови устройства – напр. такива със слаби пароли или липсата на такива, липса на автентикация (удостоверение) при вход към тях, пропуски в защитната стена.

1.3.2 Конфигурационни

- Незащитени потребителски акаунти, административни акаунти с пароли по подразбиране или лесни за откриване.
- Пропуски при конфигурацията на интернет услуги.
- Използване на настройки по подразбиране в устройствата.
- Пропуски в конфигурацията на мрежовото оборудване.

1.3.3 Уязвимости в политиката по сигурност

- Липсваща или непълна писмена политика за сигурност.
- Несъвместимост на правилата в политиката по сигурност.
- Лошо избрани, лесно пробиващи се пароли или такива по подразбиране.
- Неадекватен мониторинг и одит, което би позволило, ако има атака или неоторизирано (неупълномощено) използване, те да не бъдат открити.
- Промени в хардуера и/или софтуера, които не покриват изискванията в политиката по сигурност.
- Не съществува план за възстановяване при възникване на проблеми (Disaster recovery plan).

Политиката по сигурност е съвкупност от разписани правила, целящи защитата на дадена организация и ресурсите/услугите ѝ.

Всички служители в организацията трябва да бъдат обучени да прилагат правилно тази политика и според нея да знаят какви действия имат право да извършват по отношение на достъпа до устройства и/или ресурсите.

1.3.4 Пропуски във физическата сигурност

- По отношение на хардуера - физическа повреда на устройства, компоненти или мрежова свързаност.
- Безопасност на средата - екстремни температура или влажност.
- Електричество – промени в напрежението, прекъсвания на захранването, шум или загуба на мощност.
- Поддръжка – неправилно инсталиране на ключови електрически компоненти, липса на критични резервни части, лошо окабеляване и лошо етикетиране.

[4] Simple Network Management Protocol (SNMP) е протокол за управление на мрежи
[5] SMTP (Simple Mail Transfer Protocol) е интернет стандарт за пренос на електронна поща
[6] TCP (Transmission Control Protocol) е мрежов протокол за управление на обмена на информация

Физическа сигурност не бива да бъде подценявана. Трябва да се знае, че, ако злонамереното лице има физически достъп, то е твърде вероятно атаката да е успешна.

Съществуват специфични изискванията, които трябва да се спазват за помещенията, в които се поставят сървъри или ключови мрежови устройства.

1.4 Видове зловреден код или софтуер

Освен, че се възползват от уязвимостите, злонамерените лица могат да достигат до устройствата и данните, чрез различни инструменти и/или така наречените малуери (malware).

Малуер (malware) е зловреден код или софтуер, специално проектиран да повреди, наруши, открадне или нанесе „лоши“ или незаконни действия върху данни, устройства или мрежи.

- Вирус – Злонамерен код, прикачен към изпълним файл на устройство и се разпространява чрез вмъкване на свое копие в програмата или става част от нея. Изисква се потребителя да го изпълни, за да се активира.
- Червей – самостоятелен софтуер, който възпроизвежда свои функционални копия, без да има нужда от допълнителна намеса.
- Троянски кон – Софтуер, който изглежда легитимен и след зареждане от потребителя, извършва атаки срещу устройството/компютъра. Често създава т.нар. дупка в сигурността (back door), като осигурява достъп на злонамерени потребители до системата.
- Спайуер (Spyware) – Шпионски софтуер, който следи Вашата онлайн активност и натискането на клавиши, като улавя данните Ви, включително чувствителна лична информация (пр. данни за вход, за онлайн банкиране и кредитни карти, история на електронната поща и браузъра). Може да редактира настройките за сигурност на Вашите устройства и може да влоши производителността им. Често се съчетава с легитимен софтуер или троянски коне.
- Рансъмуерът (Ransomware) - Злонамерен софтуер предназначен да държи заключена компютърната система или данните, докато не бъде платен откуп. Обикновено се възползва от системни уязвимости и криптира данни Ви, така че да нямате достъп до тях. Често се разпространява чрез фишинг имейли.

1.5 Видове атаки

Какви са видовете атаки, които използват злонамерените лица?

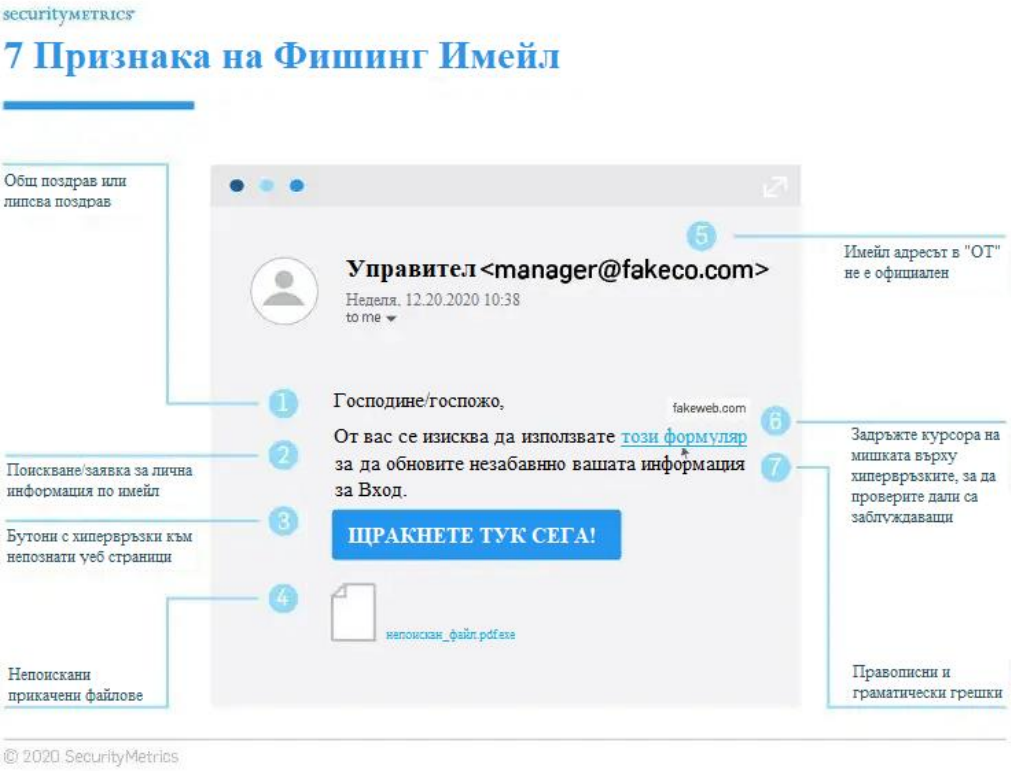
- Разузнавателни – Цели се опознаване и описание на целевите системи, услуги или уязвимости, като се събират данни за имена, IP адреси, включени услуги (отворени портове).
- Атаки за достъп – Не оторизирана манипулация на данни, достъп до системата/устройствата или използване привилегии на потребителя.
- Отказ от услуга (Denial-of-Service) - предоставени услуги, да спрат или частично да се забавят и да станат недостъпни за легитимните им потребители. Атаката може да бъде проведена чрез изчерпване на ресурса или чрез възползване от грешка в софтуера. Най-често биват атакувани популярни уеб сървъри, като целта е те да не могат да изпълняват заявки от интернет.
- Фишинг (phishing) – това, реално е атака, посредством, която злонамереното лице получава достъп до данни или устройства от самата жертвата. Обикновено целта е финансова или други облаги за злонамереното лице, което Ви измамва, за да Ви накара да разкриете лична информация, като например номера на кредитни карти, банкова информация или пароли. Киберпрестъпниците обикновено се представят за реномирани фирми, приятели или познати във фалшиво съобщение по имейла или чрез фалшив уеб сайт, които изглежда легитимен.

1.6 Рисково поведение с лични данни

Индикатори за рисково поведение с лични данни, чрез използване на фишинг (phishing) измама/атака са:

- За Електронна поща: (Фигура 2)
  - Неофициални имейл адреси на организации или непознат изпращач.
  - Общи поздрави или липса на такива, т.е. не е лично обръщение към Вас.
  - Правописни/пунктуационни грешки, лош език.
  - Приканване за изпращане на лична информация и заплахи, в случай, че не го направите.
  - Подвеждащи хипервръзки към непознати уеб страници или чрез изображения.
- Фалшиви уеб сайтове
  - Най-често URL адресът на сайта, не отговаря на името му.
  - Логото прилича, но има различия в детайлите или е поставено на не обичайно място.
  - Обикновено Ви предлагат да подобрят нещо за Вас, ако изпратите определени данни и присъства предупреждение какво ще се случаи, ако не го направите.
- Нежелана поща (спам, spam) – получаване на прекомерно количество съобщения с рекламно съдържание.

За нарушение на правата Ви, свързани с лични данни, се грижи Комисията за защита на личните данни (КЗЛД).



Фигура 2. Пример за фишинг имейл

2 МЕТОДИ ЗА ЗАЩИТА НА УСТРОЙСТВА И ЕЛЕКТРОННА ИНФОРМАЦИЯ

За защита на мрежата, потребителите и активите си, организациите използват модели/подходи за сигурност, включващи комбинация от мрежови устройства и услуги.

2.1 ОБЩИ МЕРКИ ЗА СМЕКЧАВАНЕ/ПРЕДОТВРАТЯВАНЕ МРЕЖОВИТЕ АТАКИ

- Защита на мрежата от вън, чрез използване на защитни стени и/или системи против проникванията, осигуряване на защитен криптиран (шифрован) достъп на потребителите отвън.
- Във вътрешната мрежа – защитата на всички устройствата, чрез сигурни силни пароли, промяна на всички настройки/пароли по подразбиране, актуализация на софтуера и операционните системи, поддръжка на хардуера.
- Защита на достъпа и данните на потребителите, чрез осигуряване на удостоверяване, упълномощаване и отчетност.
- Уеб и имейл защита – за филтрация подозрителни/зловредни сайтове и спам поща.
- Поддържка на архивни копия на конфигурациите на устройства, както и на данните, като се вземат предвид и:
    - Честотата на архивиране - на определени периоди, според важността и както е указано в политиката по сигурност.
    - Валидирането на резервните копия, както и на процедурата за възстановяване на файловете, чрез което се осигурява целостта на данните.
    - Съхранение на архивите – на различни места и на ротационен принцип, според политиката по сигурност.
    - Сигурност на архивните файлове – защита на архивите и възстановяването им.
- Надстройка, актуализация и корекция (upgrade, update, patch):
    - Актуализация на всички приложения с най-новите им разработки (антивирус, анти-спайуер) – предпазване от зловреден софтуер.
    - Актуализация на сигурността (security update) на операционната система и корекция (patch) на всички уязвими системи – защита от червеи.
    - Актуализиране на всички крайни системи без намеса на потребителя.

2.2 ОСНОВНА РАМКА ЗА КОНТРОЛА НА ДОСТЪПА ДО МРЕЖОВИТЕ УСТРОЙСТВА (ТРИТЕ А)

- Удостоверяване (Authentication) – на кого е позволен достъпа.
- Упълномощаване (Authorization) – какви действия се извършват при достъпа.
- Отчетност (Accounting) – запис и отчет на извършеното по време на достъпа.

2.3 Защитна стени

Един от най-ефективните налични инструменти за защита на потребителите от външни заплахи са защитните стени (firewall).

Съществуват хардуерни и софтуерни защитни стени, а също такива свързани с мрежата и за крайните потребители – персонални защитни стени.

Обикновено защитните стени се намират между две или повече мрежи, контролират трафика (потока на данни) между тях и помагат за предотвратяване на неоторизиран (неудостоверен) достъп.

Най-често трафикът иницииран от вътрешната мрежа (отвътре-навън и обратно) е позволен, а този от външната мрежа (отвън-навътре) – забранен.

Съществува и специална мрежа – демилитаризирана зона (DMZ), в която е възможно да бъде осигурен контролиран достъп до определени услуги за външни потребители. Например. Сървъри, до които трябва да се стигне от външната мрежа.

Персоналните защитни стени обикновено са част (пакет) от защитата на крайни потребителски устройства/компютри и имат предефинирани правила, но потребителите могат да създават и активират нови или спират/изтриват други.

2.4 Защита на крайни устройства

Защитата на крайните устройства (компютри, сървъри, лаптопи, смартфони и таблети) е една от най-трудните задачи, т.к. се разчита основно на потребителите – техните знания и действия.

Всяка организация трябва да има добре документирани политики по сигурността и служителите трябва да са наясно с тези правила.

Политиките често включват използването на антивирусен софтуер и предотвратяване на проникване в устройствата.

Цялостните решения за сигурност на крайните устройства разчитат на контрол на достъпа до мрежата.

Служителите трябва да бъдат обучени за правилно използване на мрежата.

3 Базова защита на електронни устройства

3.1 Базови препоръки за подобряване на сигурността на устройствата в мрежата

- Потребителските имена и пароли по подразбиране да бъдат променени.
- Паролите да бъдат комплексни и/или криптирани.
- Достъпът до системните ресурси трябва да бъде ограничен само за лицата, които имат право да използват тези ресурси.
- Отдаленият достъп до устройствата трябва да бъде защитен.
- Всички ненужни услуги и приложения трябва да бъдат изключени и деинсталирани, когато е възможно.

- Софтуерът на устройствата трябва да бъде най-актуалният и да бъдат инсталирани всички корекции за сигурност преди внедряването.

3.2 Изисквания за пароли

- Въвеждане на високи изисквания за пароли. Изискване за дължина и ползване на големи и малки букви, цифри и символи. Изискване за периодична смяна на паролата (през 60-90 дни). (Фигура 4)
- Въвеждане на двуфакторна (мултифакторна) идентификация. Изисква се въвеждането на допълнителна информация от потребителя, например ПИН код, отговор на „таен въпрос", еднократна парола (автоматично генерирана парола след всеки опит за влизане в потребителския профил, получавана обикновено чрез имейл или СМС), и т.н. (Фигура 3)
- Въвеждане на ограничение за грешно въведени пароли. При този метод се ограничава броя на грешно въведени пароли, за да се намали значително риска от атака с груба сила „brute force" (между 3 и 5 грешни опита за влизане). (Фигура 4)

Фигура 3. Двуфакторна идентификация

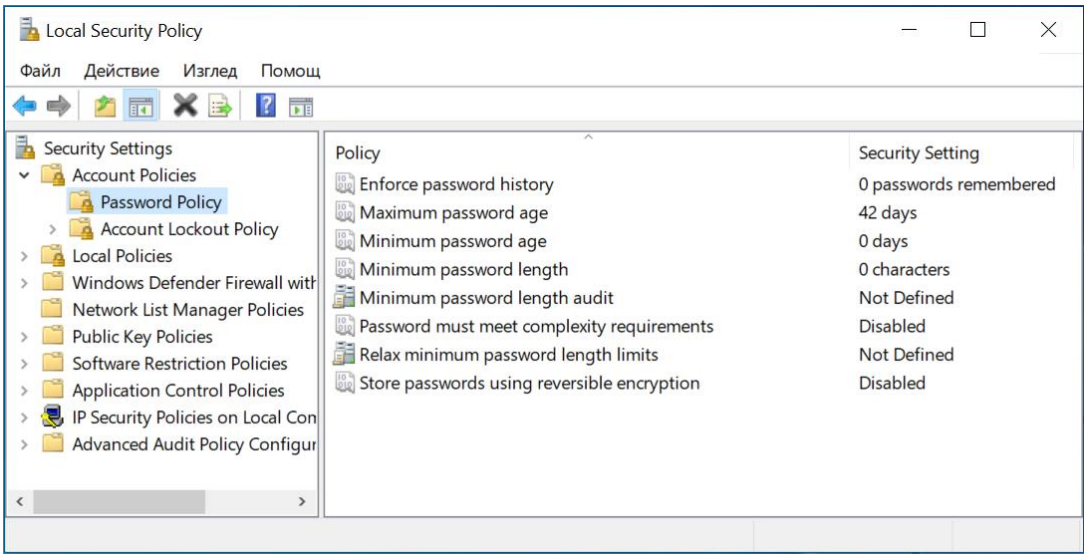
- Подобрение на защитата на пароли на компютър с Windows

  Примери за параметри, които можете да конфигурирате: (Фигура 4)

  - Прилагане на историята на паролите – брой уникални нови пароли, преди старата да бъде използвана.
  - Максимална възраст на паролата – задава времето в дни, след което се налага промяна на паролите.
  - Минимална възраст на паролата – минималното време, за което може да се използва паролата, преди да се промени.
  - Минимална дължина на паролата – брой знаци на паролата, което помага при опити за хакване.
  - Паролата трябва да отговаря на изискванията за сложност – зададени са изискванията за паролите.

  Могат да се конфигурират и правила за блокиране на профили, като за допълнително засилване на правилата за паролите, могат да бъдат зададени

прагове, до които, ако се достигне, да се блокира потребителският акаунт. Това би отказало потенциалните хакери след определен брой неуспешни опити.



Фигура 4. Подобрение на защитата на компютъра с Windows, чрез Местна политика за сигурност (Local Security Policy) – Политика за пароли

4 Използвани източници

- Останете защитени със Останете защитени със "Защита в Windows" - https://support.microsoft.com/bg-bg/windows/останете-защитени-със-защита-в-windows-2ae0363d-0ada-c064-8b56-6a39afb6a963
- Опции за влизане в Windows и защита на акаунта - https://support.microsoft.com/bg-bg/windows/опции-за-влизане-в-windows-и-защита-на-акаунта-7b34d4cf-794f-f6bd-ddcc-e73cdf1a6fbf
- Включване и изключване на Защитната стена на Microsoft Defender - https://support.microsoft.com/bg-bg/windows/включване-и-изключване-на-защитната-стена-на-microsoft-defender-ec0844f7-aebd-0583-67fe-601ecf5d774f
- Какво е спайуер? Ръководство за сигурна защита - https://bg.safetydetectives.com/blogкакво-представлява-спайуерът/
- Какво е рансъмуер? Как да предотвратим атаките в 2023 - https://bg.safetydetectives.com/blog/какво-е-рансъмуер/
- Съвети към администраторите и обработващите лични данни за защита на данните в киберпространството – КЗЛД - https://www.cpdp.bg/?p=element&aid=1316
- Хардър Windows Вход парола политика в Windows 10/8/7 - https://bg.begin-it.com/6497-windows-login-password-policy
- Изтеглете безплатен антивирус от Avast - avast! на Български - https://avast.softvisia.com/index.php/download-avast-free-pro-is
- „Free online tech courses backed by Cisco's expertise and connected to real career paths. Discover your future today.“ - https://skillsforall.com/
- Достатъчно надеждна ли е Вашата парола? - https://www.geletron.com/dostatachno-nadezhdna-li-e-vashata-parola/
- 7 Ways to Recognize a Phishing Email: Email Phishing Examples - https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email