Тема 2

Анализ на риска

Увод

- Основната задача пред цялостната програма за сигурност на една организация е да **намали** риска.
- Рискът от заплаха за сигурността на информацията **не може** да бъде избегнат. Винаги съществува риск от пробив и атака.
- Целта е този риск да се намали до допустими граници.
- Изключително важно е да се **идентифицират** видовете заплахи.
- Тук основна роля играе **анализа на риска,** често говорим и за **управление на риска**.
- Той ще помогне да се **установи**, **какво** да се защити, **кои** са конкретните заплахи и **мерките**, които трябва да се предприемат.

Определяне на заплахите

- **Идентифицирането и оценката** на заплахите пред сигурността е основната задача на анализа на риска.
- Чрез вярната идентификация се постига **фокусиране** върху наистина най-силните заплахи и цялостната стратегия се гради **адекватно**, без риск от пропуски.
- Тъй като заплахите могат да бъдат от различни посоки и форми, за правилното формиране на стратегии, трябва да бъде направен **прецизен** анализа на риска.

Заплахи за сигурността

- За да се опази информацията на една организация трябва да сме наясно с това какво всъщност е **състоянието** в нея.
- Отнася се, както до самата информация, като тип/характер, начини за съхранение и използване, така и до персонала, който има достъп, информационните системи и процедурите за работа.
- В контекста на информационната сигурност, **заплаха** е обект, човек или друг субект, който представлява постоянна опасност за даден актив.
- Или **възможна опасност** за компютърна система, която може да доведе до прихващане, промяна, възпрепятстване или унищожаване на изчислителни ресурси или друго прекъсване на системата.
- **Събитие или състояние**, което има потенциал да причини загуба на актив и нежеланите последици или въздействие от такава загуба.

Хакер

- Преди да се запознаем с детайли относно видовете заплахи нека да отделим малко внимание и на субектите, които „**искат“ нашата информация**.
- Наричаме ги **Хакери.**
- **Хакерът е човек, който има знанията и уменията да заобиколи контролите за защита или да намери и използва уязвимости в информационни системи**.
- **Black hat hacker** - е човек, който **компрометира** компютърна система със злонамерено намерение и без разрешението на собственика на информационната система.
- **White hat или ethical hacker –** човек, който прониква в информационна система със знанието на собственика с цел да установи кои са нейните слаби места.

Видове заплахи

- Заплахите идват от **различни** места и техни обекти са различни активи на една организация или личността.
- Такива са: нарушаване на интелектуалната собственост, софтуерни атаки, човешки грешки, природни бедствия, шпионаж, саботаж, кражба, отказ от услуга, неоторизиран достъп, кражба на самоличност и др.

 Помислете и дайте конкретни примери. Не се **ограничавайте** само до дигитални активи. Скица, чертеж, разпечатка на чернова на роман от популярен автор също са ценен информационен актив.

- Тъй като в наши дни почти всичко е **дигитализирано** и се обработва от **компютри**, ще акцентираме на заплахи именно от този тип.

Видове заплахи

- Всеки компютър и потребител е **застрашен** от атака постоянно. Особено този, който е достъпен в рамките на компютърна мрежа или Интернет.
- Сигурно е, че опитите за пробив в сигурността ще се **увеличават**, както се увеличава и обема на информацията обработвана в мрежата.
- Макар и за някои категории компютри (Mobile) и операционни системи (Linux) да се смята, че са **сравнително защитени**, атаките срещу тях също се увеличават.
- Един позитивен факт днес е, че дори и обикновените потребители знаят за и използват **антивирусен софтуер**, инсталират на компютрите си **актуализации** редовно и използват **сложни** за разгадаване **пароли**.

Интернет измами (част)

- Предложения за покупка или търговия на акции с потенциална голяма печалба или различни инвестиции в някаква платформа (обикновено е пирамида) или криптовалута.

- Това е най-популярният начин, някой ви пише във Facebook, Instagram, Messenger, Telegram, Viber или на друго място и ви обещава сериозни печалби, ако последвате примера или препоръките му за инвестиция. Той предлага да Ви „помогне“ да се регистрирате и да вкарате пари в някаква платформа, от която да спечелите. Схемата обикновено е да ви помогне да купите Bitcoin или друга криптовалута и да я изпратите към сайта, където да бъде инвестирана. Измамникът иска да Ви помогне да си направите и уж ваш портфейл, в който да следите как се развива инвестицията, в действителност изпращате криптовалутата към него.

- Пример от 2023 г. Бизнесмен от столицата е измамен с над 1 милион лева. От чужд колцентър той е бил заблуден, че ще инвестира в криптовалути с много висока доходност. Измамеият е контактувал с представящия за се инвестиционен консултант през криптирани чат-канали. Парите са превеждани в различни банкови сметки в страни от Европейския съюз, Великобритания и Близкия и Средния изток.

- Интернет аукциони и магазини – различни измами от невярна информация през не получаване на стоката изобщо, фалшиви наддаващи, препратка към друг сайт чрез реклама на същия продукт

- Тормоз, изнудване и заплахи по различни Интернет канали за комуникация

- Романтични (Romance Scams) – по различни канали или платформи за запознанства. Може да е свързано и с кражба на самоличност.

- **Дискусия за други видове**

Кражба на самоличност (Identity Theft)

- Това е престъпление при което някой се представя за друг във виртуалното пространство
- Осъществява се чрез кражба на лична информация, потребителски имена, пароли и др.
- Тази кражба може да бъде осъществена по няколко начина:

❑ Инсталиране на спайуеър на компютъра на жертвата

❑ Кражба на информация от сайтове, БД и информационни системи след пробив

❑ Фишинг

- След кражбата на лична информация жертвата може да претърпи финансови загуби, да бъде проследяван, да пострада неговото добро име, да бъде изнудван и т.н.

Предпазване от кражба на самоличност

- Най-важно – **да не се предоставя никаква лична информация** на лица, които не познаваме лично или не е доказано необходима
- Ако се настоява за предоставяне на лична информация по телефон, имейл или друг канал **да се поиска алтернатива**, например на място в офис
- Чрез търсене в Интернет да се проверява дали телефоните, имейлите, имената и др. не са **докладвани за подозрителни или направо за измама**
- **Да се унищожават** всички документи на хартия или дигитални, които съдържат лична информация и вече не са необходими
- **Да не се използват публични компютри или безжични мрежи**, когато трябва да се подават лични данни

Социален инженеринг

- **Social Engineering -** използва се като обобщаващ термин за множество зловредни дейности при комуникация. Основава се на доверие, страх или други психологични фактори.
- Обикновено се отнася до това да се убеди потребител да разкрие чувствителна информация с помощта на която хакерът да получи достъп до мрежа или система.
- Може да се осъществи по много начини, например:

➢ Baiting – „забравен“ в асансьор диск с етикет Клиенти-сметки или флашка с лого на известна банка, но всъщност съдържащ зловреден софтуер;

➢ Phishing и Vishing – създава се дубликат на съществуваща уеб страница, например на голяма банка или държавна организация или се получава обаждане, за да се разкрие информация;

➢ Email/SMS haking – съобщение от приятел/колега/ началник – съдържащ линк или файл за сваляне или съобщение за заразена система и молба за инсталиране на софтуер.

Дискусия за начините на защита …

Софтуерни атаки - зловреден код

- Освен описаните до тук атаките днес се изразяват **предимно** в програмен код написан от хакер, който се разпространява по КМ или друг носител.
- Този код наричаме **зловреден.**
- Целта на кода е да открие начин да пробие защитата на компютъра/информационната система и да изпълни определена задача, като продължи да се **разпространява** по нататък в КМ, ако е възможно.
- Макар и **по-малко** приложим начин за атака, остава и възможността човек да атакува компютърна система и **локално** без достъп по мрежа.

Зловреден код

- Съществуват четири основни категории зловреден код:
  1. Вирус
  2. Т.нар. червей
  3. Троянски кон
  4. Задна врата
- В допълнение, много от атаките днес се осъществяват, чрез злонамерени програми, които **комбинират** два или повече вида.
- **Жизнения цикъл** на такава програма (код) се заключава в: търсене, пробив, инфектиране и повторение на цикъла.

Компютърни вируси

- Компютърният вирус е програма, която се възпроизвежда, като използва компютърен **файл за приемник**.
- Повечето вируси заразяват файлове и когато заразеният файл се отвори или изпълни се изпълнява и зловредния код на вируса.
- Вирусите могат за **заразят**: изпълними файлове, зареждащите сектори, файлове с данни, оперативната памет и др.
- Разпространяват се чрез КМ, носители на данни, имейл или други форми за пренос на данни.

Компютърни вируси

- Компютърният вирус се характеризира с това, че в повечето случаи „**окупира**“ ресурсите на компютъра, за да се разпространява и изпълнява задачите за които е създаден: промяна и изтриване на системни и програмни файлове, извличане на важна лична информация – пароли, номера на кредитни и дебитни карти и много други.
- Тази окупация води до **забавяне** на КС или до **спиране** на работа.
- Много често вирусите **деактивират** програмите за сигурност, като позволяват на друг зловреден софтуер да атакува същата КС.

Видове КВ

Вирусите се делят на няколко вида:

1. **Boot секторен вирус** – Този тип вируси инфектира boot записа на хард диска; Най-често заразяването става от USB памет или друг носител. При следващото рестартиране на компютъра записа в буут сектора е променен и при зареждането зловредния код ще се изпълни незабавно.

- Тъй като този вирус може да направи системата абсолютно неизползваема последните разработки на OS включват защитни механизми за промяна на boot записа на хард диска.
- Отстраняването на такъв вирус е трудно и в редица случаи изисква **преформатиране** на хард диска.
- Днес се срещат рядко, но могат да заразят стари компютри. Пример: Barrotes (aka Boot-347) (засечен първо 1997)
- Bootkits (Rootkit) е съвременният вариант, не заразява removable устройства, но може да се разпространи по други начини. Преодолява се на ниво хардуер чрез технологии като UFEI и Secure Boot.

Видове КВ

2. Файлов вирус – Това е един от най-разпространените видове вируси. Тези вируси търсят файлове с определено разширение (например изпълними Windows файлове като *.com и *.exe) и ги инфектират, като се „залепят“ за тях.

- Оригиналният код на файла не се променя, а само входната точка - кое да се изпълни първо.
- Когато програмата бъде стартирана, вирусът се стартира първи и инфектира още файлове или извършва операциите, които са зададени в кода му.

Видове КВ

3. **Полиморфни вируси** - Тези вируси променят своя код с всяка инфекция, което ги прави трудни за засичане;

- Вирусът е способен да редактира или пренапише своя код с всяко заразяване.
- Той е един от най-опасните, тъй като дори и антивирусната програма може да го засече трудно.
- Според публикация 97% от вирусите днес имат такива характеристики (https://www.kaspersky.com/resource-center/definitions/what-is-a-polymorphic-virus)
- Тъй като антивирусните програми идентифицират вирусите по тяхната сигнатура (уникален низ от битове - отпечатък) а тези вируси с промяната на кода си фактически променят своята сигнатура, то ако не бъде засечен много бързо може и изобщо да не се засече в бъдеще и да остане заразена системата без потребителя да подозира.
- Пример **VirLock**

Видове КВ

4. Стелт вируси - Лесно избягват сканиранията на антивирусните програми (чрез криптиране на програмния си код или се «крият» в паметта) и им пречат да открият промените в заразените от тях файлове, като им предоставят стари данни за същите файлове;

5. Резидентни - те остават резидентни в паметта, така както остава някой драйвер (до изключването или рестартирането на компютъра). Така могат да заразят всеки файл, който се зарежда в паметта. Така дори и антивирусната програма да сканира и намери заразен файл, ако не се сканира и паметта заразата ще остане.

6. E - Mail вируси - особено актуална категория вируси разпространява се чрез електронна поща и използва адресната книга, за да атакува нови пощенски кутии.

7. **Ransomware** (криптовирус) – също много актуални в последните години. Причинява криптиране на потребителските файлове или заключва системата и я прави неизползваема и изисква заплащане на откуп(биткойни) за отварянето им. Примери: Cryptolocker и WannaCry.

Кратка история на КВ

- **През 1983 г.** Фред Коен като студент провежда поредица от експерименти, свързани с компютърната сигурност, в резултат на което създава официално признатата дефиниция за компютърен вирус. Написва код, който е скрит в програма заредена чрез флопи, който може да се разпространява на други компютри.

- **През 1986 г.** се създава Brain - първият вирус за PC с MS-DOS, с което започва и новата съвременна история на компютърните вируси. Заразява буут сектора. Създаден е от двама братя от Пакистан.

- **През 1988 г.** се създава Internet Worm – първият вирус (червей) за Internet. Чрез него съвременната цивилизация за първи път се сблъсква с мащабите на това явление и осъзнава доколко е незащитена от злонамереното мислене. Създава го студента от MIT Robert Morris, за да изследва пропуски в сигурността на UNIX, но той заразява около 6000 сървъра и някои спират работа за до два дни. Morris е осъден на 4 години условно и 10 000 долара глоба.

- **През 1991 г.** се появяват първите полиморфни (самопроменящи се) компютърни вируси, които рязко променят изискванията към защитните системи. Тъй като този тип вируси позволяват всяко следващо поколение от даден вирус да се различава значително от всички предходни и от всички следващи екземпляри, то създадените вирусни сигнатури не могат да откриват абсолютно всички вирусни екземпляри. Това изисква нови методи и средства за създаване на антивирусни програми.

• • •

През 1992 г. се появява WinVir – първият вирус за операционната система MS Windows, с което се слага началото на една основна линия в развитието на компютърните вируси. Създаден е в Холандия и заразява exe файлове, но успешно само в Windows директорията.

През 1995 г. се появява Concept – първият макровирус за MS Word. С него се слага началото на създаване на компютърни вируси, които манипулират документни файлове.

През 1999 г започва създаването на принципно нови компютърни вируси с ярко подчертани злонамерени цели, за чието постигане се разчита на Internet среда и WEB – базирани ресурси.

През 2000 г. започва интегрирането на технологиите за създаване на различните разновидности на компютърните вируси с финансови насоченост, като електронно банкиране, електронна търговия, електронни борсови операции и т.н.

През 2001 г. се забелязва ярка тенденция компютърните вируси и техните разновидности да се използват за шпиониране. Това включва извличане на всякаква информация от атакувания компютър. Създават се напълно автоматични системи, чрез технологиите на компютърните вируси и техните разновидности, които мигрирайки в WEB – базираните ресурси на Internet средата, извличат конфиденциална информация.

Какво следва?

- С бързото разпространение на мобилните устройства днес се наблюдава и засилване на атаките към тях.
- Според Kaspersky Lab за 2020 г. са засечени:
- 5,683,694 malicious installation packages
- 156,710 new mobile banking Trojans
- 20,708 new mobile ransomware Trojans

Примери:

- **Triada** -позволява добиване на super-user права и от там контрол над цялото устройство чрез задна врата- може да краде информация(например от МП на Фейсбук) или да криптира устройството.
- **DroidSnake** – инсталира се през игра и инсталира други приложения за кражба на информация
- **ExoBot –** кражба на информация за банкови приложения (логин)
- **Android Police Virus** - криптовирус
- Интересно е да се отбележи, че в пандемичния период много зловреден код се разпространява в пакети за инсталиране с име включващи думата „covid “ (covid.apk, covidMapv8.1.7.apk, tousanticovid.apk, covidMappia_v1.0.3.apk and coviddetect.apk) или “corona” - https://securelist.com/mobile-malware-evolution-2020/101029/

. . .

Статистиката показва, че атаките към мобилните устройства са в следните *направления*:

1. Около 32% от атаките са свързани с кражба на информация;
2. 25% са традиционни заплахи, като изтриване на информация, отказ от работа и др.;
3. 15% касаят проследяване на потребителя;
4. 13% касаят изпращане на съдържание от устройството;
5. 8% преконфигуриране на устройството;
6. и 8% нежелани реклами.

IoT – рутери, смарт ТВ, камери, автомобили, др.

- Разпространението на този вид устройства води и до насочване на интереса на хакерите към създаване на злонамерн код и за тях.
- С помощта на такива заразени устройства лесно хакерите изграждат т.нар. Botnets(пример Mirai) за разпространение на злонамерн код или копаят криптовалута.
- Например през 2023 г. официално се продават устройства за CTV boxes ТВ управлявани от Андроид заразени с Triada.
- Към момента най-атакувани са охранителни камери и рутери.
- Любопитен факт е, че в Интернет пространството се намират множество страници за хакване на модерни вендинг автомати позволяващи плащане със смартфон и приложение.
- Повече в темата Мобилна сигурност.

Компютърни червеи

- Компютърният червей (computer worm) е самовъзпроизвеждаща се компютърна програма.
- Той използва компютърната мрежа, за да разпраща свои копия до крайните устройства – други компютри.
- За разлика от компютърния вирус, компютърният червей не се нуждае от прикачване към вече съществуваща програма. Също така не е необходимо потребител да активира по някакъв начин червея.
- Червеите почти винаги причиняват вреда на самата мрежа, тъй като намаляват нейната пропусквателна способност.
- В наши дни те често се използват да «пренесат» и инсталират друг зловреден код, напр. spyware или ransomware
- Може да задръсти мрежата, да изтрива файлове, да отвори задна врата, да стартира distributed denial of service (DDoS) атака и др.
- Съществуват Интернет, имейл, Peer-to-peer (P2P) и Instant messaging (IM) червеи.

Троянски кон

- Троянски кон – Троянският кон е зловредна програма, която е **скрита** в безобидна такава (например игра).
- Когато тази програма бъде стартирана, се стартира и троянският кон, за да изпълни определена задача.
- Троянските коне могат да откраднат лична информация (пароли, потребителски имена), да изтрият файлове, да форматират твърдия диск, да отвори задна врата и др.
- Не е в състояние да се самовъзпроизвежда или копира и обикновенно се предават от друг потребител, по пощата или чрез сваляне на файлове от интернет.
- Не може да се самостартира.

Троянски кон

- Троянският кон може да се държи по такъв начин, че потребителя много дълго време (седмици, месеци и дори години) да не разбере за съществуването му.
- Съществува и една категория триянски коне, които са известни като **троянски коне с отдалечен достъп**.
- След като са инсталирани те служат за заден вход за хакера, който поучава достъп до компютъра. Могат да изтриват и манипулират файлове да преконфигурират системата и да прихващат клавиатурата и снимат екрана.
- Такъв вид троянски кон може да записва звук и видео например от смартфон.

Отказ от услуга (DoS) атаки

- **Атака за отказ на услуга** бива два основни вида:

1. Buffer overflow - Принуждаване на атакуваната система да се рестартира или да потреби всичките си ресурси(дисково пространство, оперативна памет, CPU), така че вече да не може да предоставя целевата услуга;

2. Flood - Възпрепятстване на комуникацията между атакуваната система и потребители на услугата, така че те вече да не могат да я достъпват адекватно в следствие на прекалено много заявки.

Известен пример за такава атака е от февруари 2020 г., когато сървърите на Amazon Web Services (AWS) са атакувани от заявки със скорост 2.3 terabits per second (Tbps)

През 2023 г. Microsoft съобщава за DDoS атака срещу услугите M365 и Azure. Атаката е осъществена през множество cloud услуги и open proxy инфраструктури.

Задна врата (backdoor)

- Задната врата е зловреден софтуер, който се инсталира и предлага възможност за **контрол** над дадената програма или целия компютър на трето лице.
- Задните врати не са винаги зловредни и има случаи, в които се използват за легитимни цели от оторизирани системни администратори.
- Обикновено се инсталират от червеи или троянски коне. Една задна врата се състои от два компонента: **сървър и клиент**. Сървърът е компонентът, който се инсталира на компютъра, който ще трябва да бъде контролиран, а клиентът е компонентът, който се използва от недоброжелателната личност.

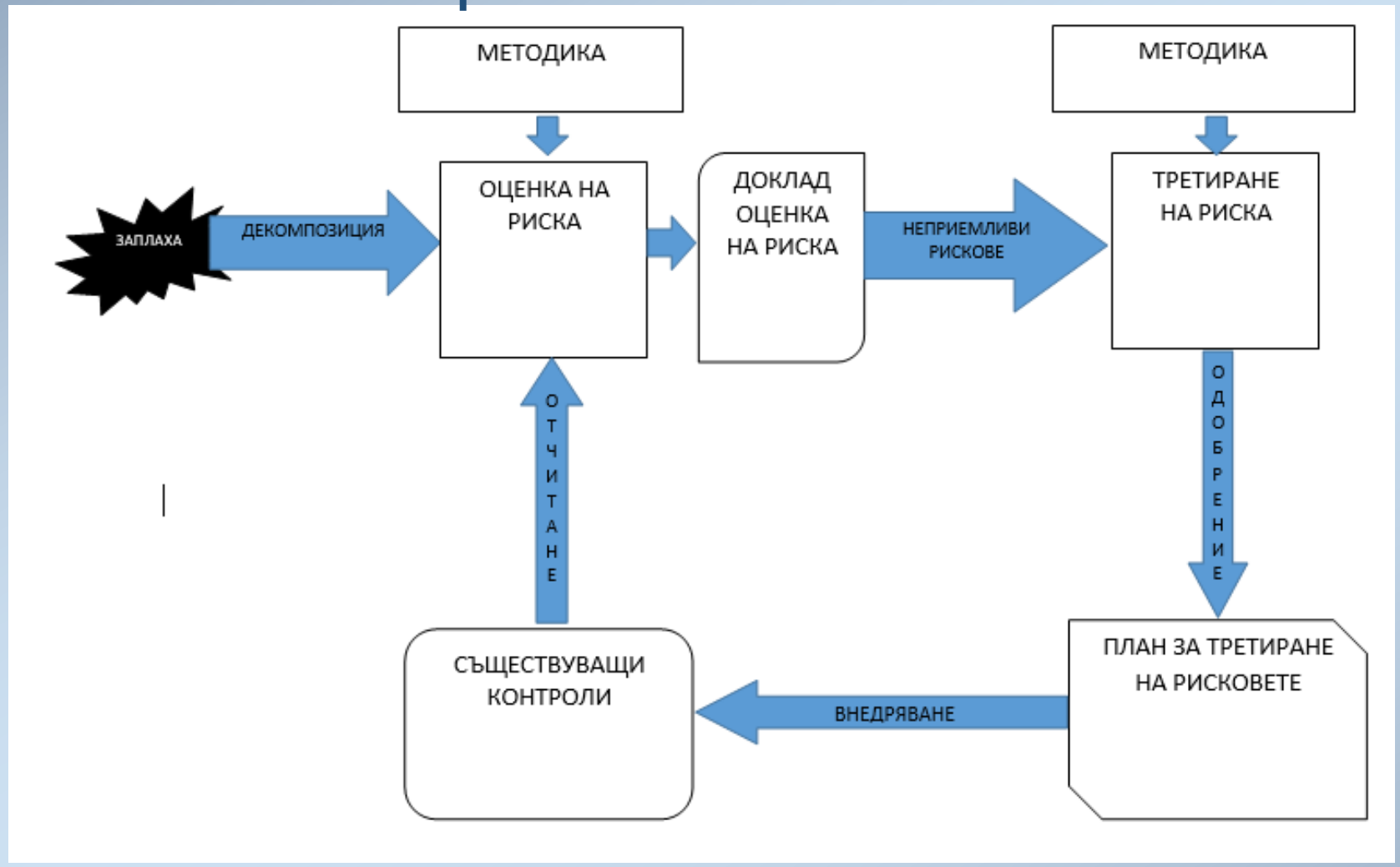
Източници на информация за текущи атаки

- https://www.malwarebytes.com/blog/category/news
- https://www.securityweek.com/
- https://www.infosecurity-magazine.com/malware/
- https://cyware.com/category/malware-and-vulnerabilities-news

Анализ на риска

- Той трябва да бъде основен **приоритет**.
- Установява и категоризира информацията, която трябва да бъде защитена, рисковете, които да бъдат избегнати.
- Резултата са поредица от **мерки и препоръки**.
- Обхвата и дълбочината на анализа зависи от конкретната организация, като там където се събира и обработва най-голям обем и важна информация този анализ съответно е най-детайлен и изисква най-много ресурси.

Анализ на риска - обща схема



За примерна методика за оценка на риска вижте Наредба … (https://www.mtc.government.bg/sites/default/files/nar_minimalnite_iziskvaniq_mrejova_info_sigurnost-072019.pdf)

Процеси

Основните процеси за оценка на риска са:

- **Дефиниране** на критерии за приемливост на рисковете и преоценка;
- **Идентифициране** на рисковете свързани с поверителност, наличност и цялостност на информацията и източниците на риска;
- **Анализиране** на нивото на риска, чрез определяне на вероятността и въздействието;
- **Оценяване** на рисковете, съобразно критериите за приемливост.

Критерии за приемливост на риска

- Отрасъл
- Законодателство
- Работна атмосфера
- Конкуренция
- Визия и стратегия
- Собственици
- Концепция
- Традиции
- Ценности
- Хора

Класификация на активите (информацията/данните)

- За оценка на активите е необходимо данните да се класифицират в съответствие с последствията от нарушаване на цялостта или конфиденциалността им.
- **Критични данни**. Това са данни, изискващи специални мерки за сигурност, които гарантират цялостността на данните и защитата им от неоторизирана модификация и изтриване. Неоторизиран достъп до тези данни може да доведе до фатални последствия за организацията.
- **Служебни данни**. Това са данни, предназначени за използване само вътре в организацията. Неоторизиран достъп до тези данни може да доведе до сериозни последствия за организацията и нейните делови партньори.
- **Лични данни**. Това са данни, отнасящи се до персонала, които могат да се използват само вътре в организацията от ограничен кръг. Неоторизиран достъп до тези данни може да доведе до сериозни последствия за организацията тъй като са защитени със закон.
- **Данни за вътрешно ползване**. Това ниво се използва за данни, който не попадат в по-горните нива. Неоторизиран достъп до тези данни не може да навреди сериозно на организацията.

**** Внимание, по Наредба за минималните изисквания за мрежова и информационна сигурност класификацията е друга.***

Как може да оценим риска?

- Една формална дефиниция е

Риск = вероятност от атака * цената на увреден актив

- ***Количествен подход -*** към анализ на риска ще се вземат предвид действителните стойности на вероятността от проблем, заедно с действителната стойност на загубата или компрометиране на въпросните активи.
- Един често използван подход за определяне на разходите за рискове е очакваната годишна загуба. Това е цената на нежеланото събитие и единичната загуба умножена по броя пъти, които се очакват това събитие да се случи за една година.

Очакваната годишна загуба = единичната загуба * брой

Как може да оценим риска?

- Този начин на оценка не е много точен, докато всяка отделна загуба може да се оцени то броя на случвания за годината не може да се определи (например колко пъти за една година даден сървър ще спре да работи).
- Съществува и ***качествен подход*** за анализ на риска, който може да е достатъчен в по-малки организации или тези, с ограничени ресурси, който може да бъде също толкова ефективен.
- Може да се идентифицират важни активи (например, уеб сървър, база данни, съдържаща поверителна информация, работни станции, компютри и т.н.). Може да се идентифицират заплахите за тези активи (зловреден софтуер, хакерски атаки, грешки и бъгове, прекъсване на електрозахранването, и т.н.). Така може да се приоритизира процеса на възстановяване след атака.

Нормативна рамка - управление на риска

- Както и останалите аспекти на ИС, така и управлението на риска е предмет на регулации, стандартизация и добри практики.
- Например ISO/IEC 27001/27005. Information security risk management. Процес включващ 5 стъпки:

1. Establish a risk management framework
2. Identify risks
3. Analyze risks
4. Evaluate risks
5. Select risk treatment options (‘Avoid’ the risk by eliminating it entirely ‘Modify’ the risk by applying security controls ‘Share’ the risk to a third party (through insurance or outsourced)‘Retain’ the risk (if the risk falls within established risk acceptance criteria))

NIST Special Publication 800-39

- Risk management is a comprehensive process that requires organizations to: (i) frame risk (i.e., establish the context for risk-based decisions); (ii) assess risk; (iii) respond to risk once determined; and (iv) monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations.
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View

ПРИМЕРЕН МОДЕЛ ЗА АНАЛИЗ НА РИСКА(извадка от курсова работа)

Анализиране на основните бизнес услуги на организация

1. Анализират се основните бизнес услуги на дадена организация;

2. Идентифицират се информационните компоненти в тях;

3. Определя се физическото или логическото им нахождение;

4. Идентифицира се управлението на IT компонентите;

5. Определя се тяхното влияние за бизнес процеса по скалата:

Анализ на бизнес услуга предоставена от брокерска фирма и нейните активи, които подлежат на влияние от риск

№	Информация	Разположение	Управление	Влияние
1.	Лични данни на клиенти	Офис	Брокери	Високо
2.	Финансова и-ция. на клиенти	Офис	Брокери	Високо
№	Хардуер	Разположение	Управление	Влияние
1.	Сървър	Офис	SysAdmin	Високо
2.	Офис	София	Управител	Ниско
№	Информационни системи	Разположение	Управление	Влияние
1.	Софтуер използван от брокери	Офис	SysAdmin	Високо
№	Документи и външни носители	Разположение	Управление	Влияние
1.	Общи условия на фирмата	Офис	Управител	Ниско
2.	Договори	Офис	Управител	Средно
№	Персонал	Разположение	Управление	Влияние
1.	SysAdmin	Офис	Управител	Високо
2.	Служители	Офис	Управител	Средно
№	Услуги	Разположение	Управление	Влияние
1.	Интернет	Офис	SysAdmin	Високо

Скала на влияние

ВИСОКО	Отсъствието на компонента, грешка в него или загуба на поверителност би довела до срив на работата, масиран отлив на клиенти, сериозни глоби, влошаване на имиджа, възможност за изгубване на лицензи и щети над 10% (оборот или печалба).
СРЕДНО	Отсъствието на компонента, грешка в него или загуба на поверителност би създала неудобства в работата, би влошила качеството и би довела до глоби, отлив на лоялни клиенти и щети до 10% (оборот или печалба).
НИСКО	Отсъствието на компонента, грешка в него или загуба на поверителност би създала съвсем леки смущения в дейността и няма да доведе до щети.

ВЪЗДЕЙСТВИЕТО ВЪРХУ БИЗНЕСА

НИВО	НАИМЕНОВАНИЕ	ФУНКЦИОНАЛНОСТ	КЛИЕНТИ	НОРМАТИВНИ АСПЕКТИ	ШЕТИ	КОМУНИКАЦИЯ
5	Критично	Услугата не се предоставя	Масиран отлив на клиенти чрез прекратяване на договорите	Отнемане на лицензa или принудително затваряне на обект	>15%	Пълно отпадане на свързаност за дълъг период от време
4	Високо	Липсват ключови компоненти на услугата	Случай на лоялни клиенти да отиват при конкуренцията	Спиране на дейността за определен период и подвеждане под съдебна отговорност	10%-15%	Сериозно намаляне на скоростта и чести прекъсвания
3	Средно	Липсват работни компоненти на услугата	Сериозни оплаквания от лоялни клиенти	Съществени глоби	05%-10%	Намаляне на скоростта и редки прекъсвания
2	Ниско	Намаляване на качеството на услугата	Леко недоволство при някой клиенти	Актове и налагане на несъществени глоби	<05%	Леко намаляване на скоростта
1	Несъществено	Няма влияние	Няма влияние	Забележки и предписания	Липсват	Леки смущения

Оценка на въздействието на брокерска фирма

КОМПОНЕНТ	ЗАПЛАХА	ВЪЗДЕЙСТВИЕ
1.СЪРВЪР	Техническа повреда	5
	Нерегламентиран достъп (hack)	4
	Неразрешен достъп (вътрешен)	4
	Загуба на данни	5
2.ИНТЕРНЕТ	Срив	5
	Забавяне	2
3. ОФИС	Наводнение	4
	Пожар	4
	Терористичен акт	5
	Невъзможност за ползване	2
4.БРОКЕРИ	Епидемия	4
	Самоотлъчка	4
	Злоумишлени действия	3
	Разкриване на информация	4

Внедрени контроли

- Контролите са защитни механизми, който имат за цел да опишат по-точно съществуващото въздействие за даден бизнес процес.

№	ОПИСАНИЕ	ПРИЛОЖЕНИЕ
K-01.01	Symantec antivirus клиент	Всички компютри във фирмата
K-02.01	Symantec antivirus сървър	Сървърна инсталация
K-03.01	UPS MGE 2600VA	Сървър
K-04.01	Пожарогасител	Сървърно помещение
K-05.01	CISCO Firewall	Локална мрежа
K-06.01	Мрежови кабели Cat. 7e (до 10Gbit)	Локална мрежа
K-07.01	Видеонаблюдение	Целия офис
K-08.01	Пожарогасителна система	Целия офис
K-09.01	Декларация за конфиденциалност	Цялата фирма
K-10.01	Политика за контрол на достъп	Цялата фирма

КОМПОНЕНТ	ЗАПЛАХА	ВЪЗДЕЙСТВИЕ	СЪЩЕСТВУВАЩИ КОНТРОЛИ
1.СЪРВЪР	Техническа повреда	5	К-03.01, К-06.01
	Нерегламентиран достъп (hack)	4	К-01.01, К-02.01, К-05.01
	Неразрешен достъп (вътрешен)	4	К-07.01, К-10.01
	Загуба на данни	5	К-07.01, К-10.01
2.ИНТЕРНЕТ	Срив	5	К-05.01, К-06.01
	Забавяне	2	К-05.01, К-06.01
3. ОФИС	Наводнение	4	К-07.01
	Пожар	4	К-04.01, К-07.01, К-08.01
	Терористичен акт	5	К-07.01
	Невъзможност за ползване	2	К-07.01
4.БРОКЕРИ	Епидемия	4	К-07.01
	Самоотлъчка	4	К-07.01, К-09.01
	Злоумишлени действия	3	К-07.01, К-09.01, К-10.01
	Разкриване на информация	4	К-07.01, К-09.01

Степени на вероятност

НИВО	НАИМЕНОВАНИЕ	ЧЕСТОТА	ПРИМЕР
5	ПОЧТИ СИГУРНО	ЕЖЕДНЕВНО	ВИРУСНА АТАКА ПО ИНТЕРНЕТ
4	ВИСОКА	ЕЖЕСЕДМИЧНО	ГРЕШКА ПРИ ОСЧЕТОВОДЯВАНЕ
3	СРЕДНА	ЕЖЕМЕСЕЧНО	ПОГРЕШНО ИЗТРИВАНЕ НА ВАЖЕН ФАЙЛ
2	НИСКА	ЕЖЕГОДНО	ДЕФЕКТИРАНЕ НА ХАРДУЕР
1	НЕВЕРОЯТНО	ВЕДНЪЖ НА 10 ГОДИНИ	ПОЖАР

КОМПОНЕНТ	ЗАПЛАХА	ВЪЗДЕЙСТВИЕ	ВЕРОЯТНОСТ
1.СЪРВЪР	Техническа повреда	5	2
	Нерегламентиран достъп (hack)	4	2
	Неразрешен достъп (вътрешен)	4	2
	Загуба на данни	5	2
2.ИНТЕРНЕТ	Срив	5	3
	Забавяне	2	3
3. ОФИС	Наводнение	4	1
	Пожар	4	1
	Терористичен акт	5	1
	Невъзможност за ползване	2	2
4.БРОКЕРИ	Епидемия	4	1
	Самоотлъчка	4	2
	Злоумишлени действия	3	2
	Разкриване на информация	4	3

КОМПОНЕНТ	ЗАПЛАХА	ВЪЗДЕЙСТВИЕ	СЪЩЕСТВУВАЩИ КОНТРОЛИ	ВЕРОЯТНОСТ	РИСК
1.СЪРВЪР	Техническа повреда	5	К-03.01, К-06.01	2	10
	Нерегламентиран достъп (hack)	4	К-01.01, К-02.01, К-05.01	2	8
	Неразрешен достъп (вътрешен)	4	К-07.01, К-10.01	2	8
	Загуба на данни	5	К-07.01, К-10.01	2	10
2.ИНТЕРНЕТ	Срив	5	К-05.01, К-06.01	3	15
	Забавяне	2	К-05.01, К-06.01	3	6
3. ОФИС	Наводнение	4	К-07.01	1	4
	Пожар	4	К-04.01, К-07.01, К-08.01	1	4
	Терористичен акт	5	К-07.01	1	5
	Невъзможност за ползване	2	К-07.01	2	4
4.БРОКЕРИ	Епидемия	4	К-07.01	1	4
	Самоотлъчка	4	К-07.01, К-09.01	2	8
	Злоумишлени действия	3	К-07.01, К-09.01, К-10.01	2	6
	Разкриване на информация	4	К-07.01, К-09.01	3	12

Практически упражнения

- В рамките на един учебен час потърсете в Интернет пространството информация за разглежданите в темата видове заплахи. Търсенето може да направите и на чужди езици, които владеете.
- Анализирайте намерената информация и я сравнете с поднесената тук.
- Напишете на един лист каква „чувствителна“ информация съхранявате на различни устройства(смартфон, флашка, лаптоп, PC), които използвате и евентуалните щети, които може да претърпите, ако я изгубите, ви я откраднат или изтриете погрешка.
- Ако сте били жертва на атака може да опишете Вашият опит.