**ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – СОФИЯ**

**ФАКУЛТЕТ КОМПЮТЪРНИ СИСТЕМИ И ТЕХНОЛОГИИ**

# КУРСОВА РАБОТА

## Научна статия

**Дисциплина: „Мениджмънт на информационни системи”**

**тема:**

# “Оценка на рисковете, породени от служители, изпълнители и други вътрешни лица (Insider Threat Vulnerabilities)”

***Изготвил:***

Божидар Николаев Захов
фак. №: 121323044, група: 222
e-mail: bzahov1998@gmail.com
LinkedIn: https://www.linkedin.com/in/bzahov98/

***Ръководител:***

доц. д-р инж. Иван Станков

**София, 2024**

## Ключови думи:

**Оценка на риска, Вътрешни заплахи, Вътрешен човек, Вътрешни заплахи от невнимание, Вътрешни заплахи от неглижиране, Умишлени вътрешни заплахи, системи EDR, Insider Threat Vulnerabilities, Vulnerabilities, Corporations, Insider, Negligent Insider Threat, Accidental Insider Threat, Malicious Insider Threat, Prevention Insider Threats, EDR Systems, The principle of least privilege (PoLP), Cost of Insider Threats, Zero-day attacks, Ways to reduce insider threats,**

## 1. Резюме:

В тази научна статия се изследва сложният проблем с **вътрешните заплахи в различните видове организации**.

В началото се дава определение на вътрешните заплахи и се изтъква нарастващото им значение в съвременния свят на информационните технологии.

В статията статията се правят задълбочени **оценки** на **различните уязвимости**, свързани със заплахите от вътрешна употреба (**insider threats**), които обхващат **човешкия фактор**, проблеми с контрола на достъпа (**access control**), **изтичане на данни**, **тайни споразумения** (договорки), **социално инженерство**, нарушаване на политиките на компаниите (**policy violations**) и рискове от трети страни (**third party risks**).

В статията е наблегнато на най-добрите практики и стратегии, които трябва да се следват, за ограничаването на пораженията от потенциалните заплахи. Те включват методи за засичане на вътрешните заплахи, мерки за контрол на достъпа, повишаване на осведомеността и подготовката на служителите, изготвяне на планове за реакция при инциденти

Целта е да се направи детайлен разбор и оценка на **рисковете, породени от служители, изпълнители и други вътрешни лица**, застрашаващи компаниите, правителствените организации и дори стартиращите компании (Start Ups).

## 2. Съдържание:

# 3. Въведение

През последните години ситуацията със заплахите за киберсигурността претърпя значителни промени, като **вътрешните заплахи все повече се признават за огромно предизвикателств**о.

**Вътрешните заплахи са сериозен проблем**, с който се **сблъскват организации от всички размери и индустрии**, включително финансови институции, правителствени агенции, здравни учреждения, корпорации и малки и големи фирми и др.

Новият Доклад за заплахите от вътрешни лица за 2024 г., публикуван от Cybersecurity Insiders и поръчан от Securonix, установява, че 53% от специалистите по киберсигурност смятат, че **откриването и предотвратяването на атаки от вътрешни лица е по-трудно, отколкото от външни кибератаки**. Това е увеличение с повече от 10% през последните пет години, което подчертава промяната във възприятието, което е изключително важно развитие в областта на киберсигурността.[15][16]

Съвременните предизвикателства, подчертават **необходимостта от по-усъвършенствани стратегии за сигурност** при вътрешни заплахи, включване на усъвършенствани решения за сигурност и възприемане на комплексен подход, за да се подобри видимостта на потребителското поведение и да се укрепи цялостната позиция на организацията по отношение на сигурността.[15]

**Вътрешните атаки** могат да бъдат причинени от **служители**, **изпълнители** или **други вътрешни лица**, които **умишлено** или **неволно нарушават правилата** за сигурност, за да навредят на организацията.

**Последиците** от вътрешните заплахи **могат да бъдат опустошителни**. Те обикновено включват[1]:

- Финансови загуби и наказания.
- Кражба на данни.
- Нарушаване на репутацията
- Правна отговорност

# 4. Какво представлява вътрешната заплаха?

Вътрешните заплахи представляват сложен и динамичен риск, който засяга публичната и частната сфера на всички сектори на критичната инфраструктура[2].

Определянето на тези заплахи е изключително важна стъпка в разбирането и създаването на програма за намаляване на вътрешните заплахи[2].

**Агенцията за киберсигурност и инфраструктурна сигурност, на Америка (CISA),** определя вътрешната заплаха като:

*"Заплаха, при която вътрешен човек ще използва умишлено или неумишлено оторизирания си достъп, за да навреди на службата, нейните ресурси, персонал, съоръжения, информация, оборудване, мрежи или системи."*[2]

Вътрешните заплахи се проявяват по различни начини: насилие, шпионаж, саботаж, кражба и кибернетични действия.

## 4.1. Какво представлява "вътрешен човек" (Insider)

**Вътрешно лице**, известен с английския термин "**Insider"**, е всяко лице, което има или е имало някога, **оторизиран достъп** или **познания** за **ресурсите** на дадена организация, включително **персонал**, **финанси**, **информация**, **предстоящи сделки**, **съоръжения**, , **оборудване**, **мрежи**, **системи** или **данни**, **недостъпни** за **обществеността**.[2]

### 4.1.1. Примери за вътрешен човек:

- Лице, **на което организацията има доверие**, включително служители, членове на организацията и лица, на които организацията **е предоставила чувствителна информация и достъп**.[2]
- Лице, на което е **предоставен бадж** или **устройство за достъп**, **идентифициращо го** като лице с **редовен** или **постоянен** достъп (напр. служител или член на организацията, изпълнител, доставчик, пазач или строително лице).[2]
- Лице, на което организацията е **предоставила достъп до служебно устройство**(компютър, мобилно или др.) и/или **вътрешна мрежа**.[2]
- Лице, което разработва продуктите и услугите на организацията. Тази група включва лицата, които знаят тайните на продуктите, които осигуряват стойност за организацията. [2]
- Лице, което е запознато с основните принципи на организацията, включително ценообразуването, разходите и силните и слабите страни на организацията. [2]
- Лице, което е запознато с **бизнес стратегията** и **целите** на **организацията**, на което са **поверени бъдещите планове** или средствата за поддържане на организацията и осигуряване на благосъстоянието на хората и. [2]
- В контекста на правителствените функции вътрешно лице може да бъде лице с **достъп до защитена информация**, която, ако бъде компрометирана, може да **причини вреди на националната сигурност и обществената безопасност**.[2]

- **Къртица** - самозванец, който **технически е външен човек,** но **е успял да получи вътрешен достъп** до привилегирована мрежа. Това е човек извън организацията, който се представя за служител или партньор.[13]

## 4.2. Какво представлява “вътрешна заплаха”- (Insider Threat)

Вътрешна заплаха е **потенциалната възможност за използване на оторизиран достъп** на организацията от страна на вътрешен човек, за да навреди на организацията.

**Общото определение** за вътрешна заплаха според CISA е:

*“Всяка вреда, която може да включва поне едно, или повече злонамерени, самонадеяни или непреднамерени действия, които оказват отрицателно въздействие върху целостта, поверителността и наличността на организацията, нейните данни, персонал или съоръжения.”*[2]

Външните заинтересовани страни и клиенти на Агенцията за киберсигурност и инфраструктурна сигурност (CISA) могат да намерят горното по-общо определение, за по-подходящо и приспособимо за използване от тяхната организация. [2].

**CISA дефинира вътрешната заплаха**, по следния начин, като:

“*Заплахата, свързана с възможността, вътрешно лице да използва своя оторизиран достъп, съзнателно или несъзнателно, за да навреди на мисията, ресурсите, персонала, съоръженията, информацията, оборудването, мрежите и/или системите на отдела.*”[2]

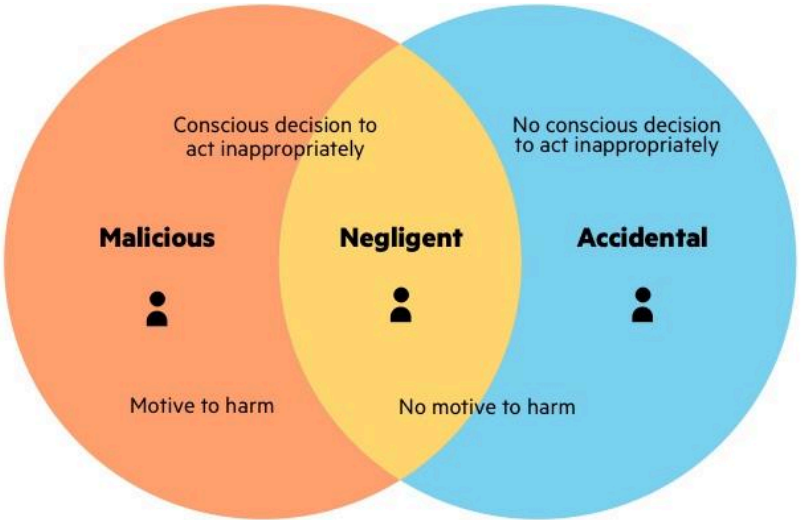
Тази заплаха може да се прояви като вреда за отдела, чрез следните действия на вътрешни лица[2]:

- **Шпионаж**
- **Тероризъм**
- **Неразрешено разкриване на информация**
- **Корупция**, включително участие в международна организирана престъпност
- **Саботаж**
- **Насилие** на работното място
- Умишлена или неумишлена **загуба** или **влошаване на ресурсите** или **възможностите на отдела**


Фиг. 1 Класификация на типовете вътрешните заплахи.[12]

## 4.3. Категоризация на вътрешните заплахи

Най-общо казано, вътрешните заплахи произтичат от два основни вида дейности: **непреднамерени**(небрежни или случайни) и **умишлени**. Графичното обяснение на трите вида дейности може да се видят на фигурата по-долу (Фиг.2).




Фиг. 2 Графично обяснение на трите вида рисково поведение.[13]

### 4.3.1. Непреднамерени

Непреднамерените действия могат да бъдат допълнително разделени на небрежни и случайни действия.

- **Действия породени от небрежност (Negligent)**

Вътрешните лица могат да изложат организацията на заплаха, чрез своята небрежност и необмислени действия.

Лицата от този тип обикновено са запознати с политиките за сигурност и/или ИТ, но избират да ги пренебрегнат, като по този начин създават риск за организацията. Примерите включват позволяване на някого да "заобиколи" през защитения вход на офиса, неправилно поставяне или загубване на преносимо устройство за съхранение, съдържащо чувствителна информация, както и игнориране на съобщения за инсталиране на нови актуализации свързани с пачове за сигурност. [12]

Небрежните вътрешни лица, обикновено са самодоволни или незаинтересовани за сигурността и проявяват умишлено пренебрегване на правилата. Това демонстрирано поведение, може да бъде установено и коригирано, преди да доведе до пробив в сигурността. [12]

- **Случайни действия (Accidental)**

**Дори и най-добрият служител може да бъде небрежен или наивен и да допусне грешка**, която да доведе до непреднамерен риск за организацията.[12]

Примерите включват грешно въвеждане на имейл адрес, случайно изпращане на чувствителен бизнес документ на конкурент, или неправилно изхвърляне на поверителни документи, без те да бъдат унищожени. Също е възможно и несъзнателно или по невнимание щракване, върху хипервръзка или отваряне на на прикачен файл, който съдържа вирус намиращи се във фишинг имейл (phishing email). [12]

Организациите **могат** успешно **да сведат до минимум потенциалните инциденти**, чрез различни подходи описани в глава **6. Начини за справяне с вътрешните атаки.** [12]

Въпреки тези усилия все пак има не малка вероятност, такива инциденти да се случат, тъй като те не могат да се премахнат напълно, а само да се редуцират до минимум. [12]

## 4.3.2. Умишлени (Malicious)

Злонамерен вътрешен човек - известен също като изменник (Turncloak), това е някой който злонамерено и умишлено злоупотребява със законно предоставени му правомощия, обикновено с цел кражба на информация за финансови или лични стимули. [13]

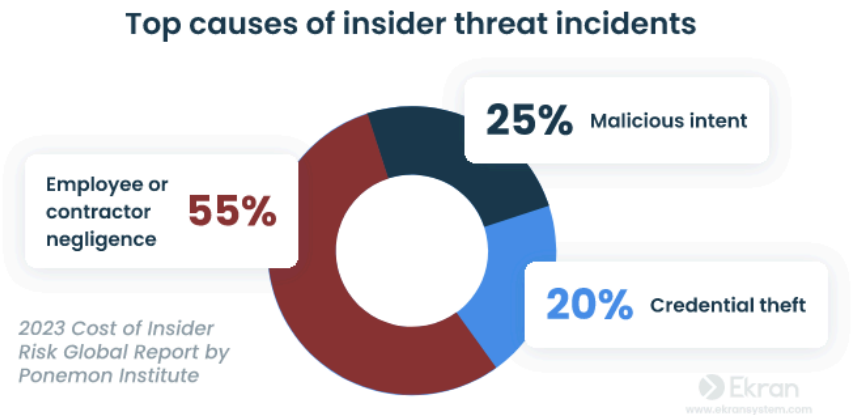
Например, лице, което изпитва неприязън към бивш работодател, Някои умишлени вътрешни лица са мотивирани от недоволство и/или неприязън свързано с възприета обида, амбиция или финансов натиск. Други може да

имат желание за признание и да търсят внимание, като създават опасност или разкриване на чувствителна информация. Те дори може да смятат, че действат в името на общественото благо. Например, неудовлетворени очаквания поради липса на някаква форма на признание (напр. повишение, бонуси, желано пътуване) или дори уволнение, са мотивирали много вътрешни лица да си "отмъстят" чрез изтичане на поверителна информация, тормоз на сътрудници, саботиране на оборудване или насилие. Други пък крадат патентовани данни или интелектуална собственост, за да напреднат в кариерата си. [12]

Изменниците (Turncloack) имат предимство пред другите нападатели, защото са запознати с политиките и процедурите за сигурност на дадена организация, както и с нейните уязвимости.[13]

### 4.3.3. Анализ на количеството инциденти, по категории.

- **Основните причини за вътрешни инциденти**




Фиг. 3 Основните причини за вътрешни инциденти.[4]

Графиката по-горе (Фиг.3) показва основните причини за инциденти, свързани с вътрешни заплахи, за 2023 година. Данните са според проучването "**Cost of Insider Risk Global Report 2023** година"[3] и са част от статията[4]:

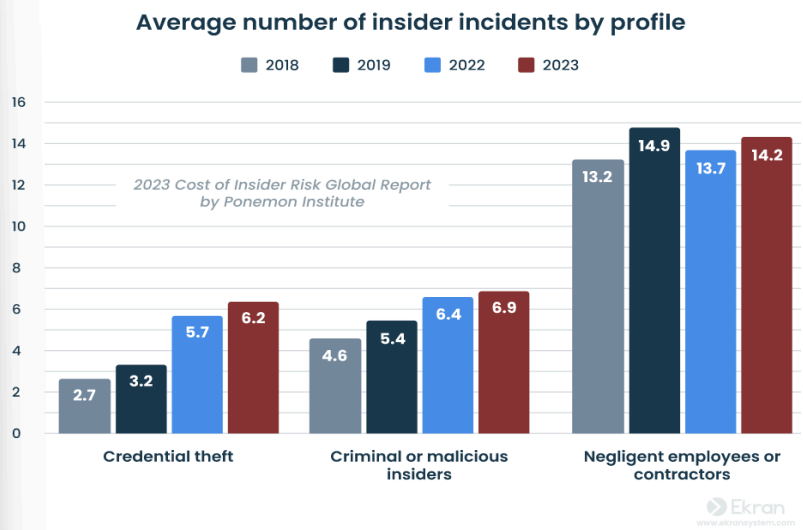
**Най-голямото звено** от кръговата диаграма, съставляващо **55%**, е "**Небрежност от страна на служители**". Това означава, че най-често срещаната причина за инциденти, свързани с вътрешни заплахи, е **небрежност** от страна на служители или наемници.

Второто по големина звено на диаграмата, съставляващо **25%**, е "**Злоумишлени действия**". Това свидетелства, че **една четвърт от инцидентите с вътрешни заплахи са причинени от хора,** които **умишлено искат да навредят** на **организацията**.

Най-малката част от графиката, съставляваща **20%**, е "**Кражба на удостоверен достъп**". Това показва, че **една пета** от инцидентите, свързани с вътрешни заплахи, **са причинени от някой, който е откраднал идентификационните данни за вход,** на служители или наемници.

- **Среден брой инциденти, по категории.**

На фигурата, по-долу (Фиг. 4), може да видите средния брой инциденти с вътрешна информация за годините от 2018 до 2023, разбити на категории. Данните са според проучването "**Cost of Insider Risk Global Report 2023**"[3] и са част от статията[4]:




Фиг. 4 Среден брой инциденти с вътрешна информация, по категории.[4]

Първата категория най-вляво е за "**Кражба на идентичност**". Както може да видите стойностите от 2.7 през 2018 г., са **скочили повече от двойно** до 6.2 през 2023 година, което подсказва за притеснителната тенденция и нуждата от превантивни мерки относно тази заплаха. Това е и **категорията с най-малък дял**, като през 2018 е разликата е доста голяма спрямо другите, докато през 2023 разликата с втората по големина категория е само 0.7.

Втората категория по средата е за "**Криминални деяния или умишлени вътрешни заплахи**". Както може да видите стойностите от 4.6 през 2018 г., са **скочили почти двойно** до 6.9 през 2023 година.

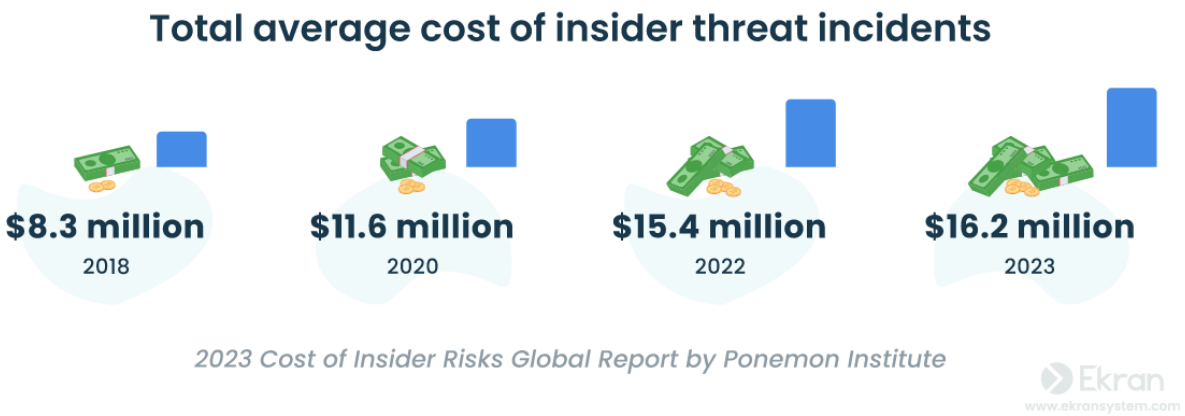
Третата категория най-вдясно е за "**Действия породени от небрежност**". Както може да видите стойностите от 13.2 през 2018 г., са **макар и с малко, са се повишили** до 14.2 през 2023 година. Това е и **категорията с няколко пъти по-голям дял от другите**, както през 2018 така и през 2023.

## 4.4. Каква е значимостта на вътрешните заплахи?

Вътрешните опасности не се ограничават само до неосъзнати действия на служители; според мнозина специалисти, коренът на опасността може да бъде открит в злонамерени действия, а тенденцията за кражба на идентификационни данни се очаква да нарасне и да стане значителен бизнес през следващите години.[1]

Те са причина за значителни щети върху репутацията, финансовата стабилност, надеждността и интелектуалната собственост на организацията. Има няколко причини за техния растеж в последно време. [1]

Тенденциите свързани с вътрешните заплахи са плашещи, **в рамките на 5 години щетите от инциденти са скочили двойно** - от малко над 8 милиона долара, през 2018 година, до над 16 милиона долара през 2023 година. Виж фигурата по-долу (Фиг. 5) [4] Поради тази причина е от особена значимост, борбата с причинителите на вътрешни заплахи.

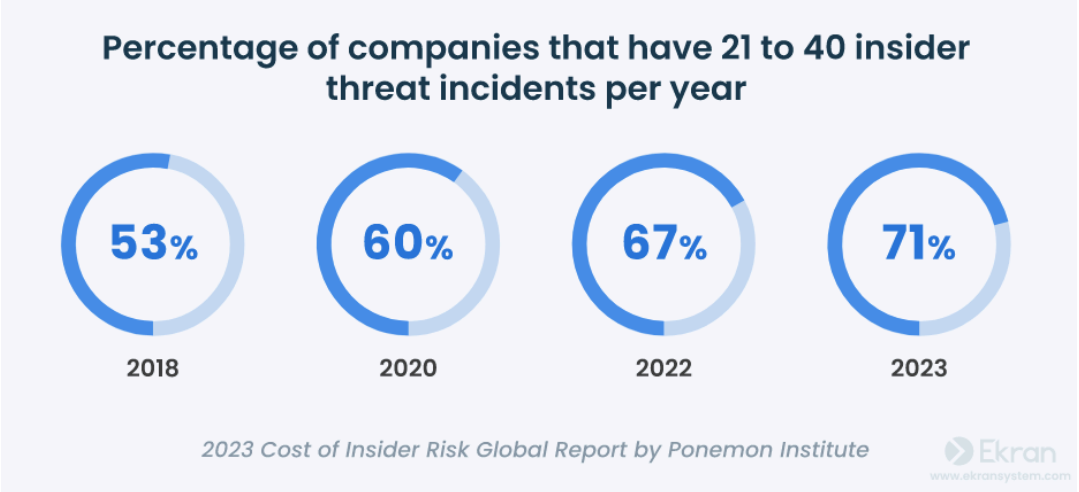



Фиг. 5 Двойният ръст на разходи свързани със вътрешни заплахи.[4]

# 5. Защо вътрешните заплахи стават все по-чести?

## 5.1. Случаите с вътрешни заплахи са в подем

**Процентът на вътрешните заплахи непрекъснато нараства**. Глобалният доклад на института Ponemon "Цената на вътрешния риск за 2023 г." (The 2023 Cost of Insider Risk Global Report) показва, че делът на организациите, които се сблъскват с 21 до 40 инцидента, свързани със заплахи от вътрешни лица, е нараснал през последните години.[3][4]




Фиг. 6 Компаниите, с 21 до 40 инцидента годишно.[4]

## 5.2. Нарастваща зависимост от технологиите

С нарастващото използване на технологиите и интернет в бизнес-дейностите организациите стават все по-уязвими към вътрешни заплахи. **Компаниите съхраняват повече данни в цифров вид. Следователно става по-лесно за вътрешните лица да имат достъп до чувствителна информация**, да крадат или злоупотребяват с нея. Тези особи могат да използват технологиите, за да прикрият следите си, което на свой ред затруднява организациите да откриват и предотвратяват заплахи. [1]

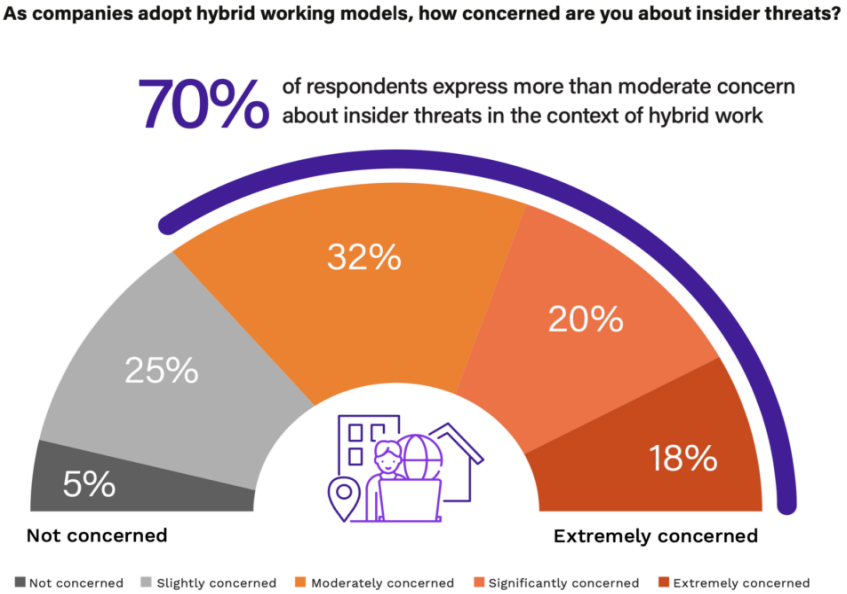
## 5.3. Дистанционна работа

Докато ИТ компаниите се радват на ускорена дигитализация, предизвикана от пандемията, бързо приетите политики за дистанционна работа водят до значителен риск от разнообразни вътрешни заплахи, включително кражба на данни, саботаж, разпространение на злонамерен софтуер, шпиониране и други[1].

Пандемията, спомогна за повече стрес и несигурност, породени от прибързаност, може да е допълнителен фактор за увеличаване на тези заплахи.

Важно е да се отбележи, че не всички служители, работещи дистанционно, представляват заплаха. [1]

За да се минимизират рисковете, е необходимо да се прилагат строги политики за сигурност, да се обучават служителите за потенциалните заплахи и да се насърчава култура на доверие и отворена комуникация. [1]




Фиг. 7 Проучване за това, колко компании се притесняват от вътрешни атаки[15]

## 5.4. Подценяване на опасностите

Въпреки че бизнесът често съсредоточава усилията си за сигурност върху **външни заплахи**, **подценяването на риска**, породен от вътрешни източници, може да улесни злонамерени служители, с легитимен достъп, да извършват престъпни деяния. [1]

Проучването "2023 Data Breach Investigations Report" на Verizon за разследванията на нарушения на сигурността на данните през 2023 г. се казва, че 89% от всички случаи на злоупотреба с привилегии са финансово мотивирани.[4]

## 5.5. Недоволни служители

Служителите, които не са доволни от работодателя си, са по-склонни да участват във вътрешни атаки. Тези работници могат да откраднат информация, да увредят активи на компанията или да участват в други злонамерени дейности като отмъщение или кражба в полза на конкурент. [1]

Докладът на Ponemon Institute разкрива тревожна тенденция, почти половината от служителите са обмисляли да напуснат работодателя си през последната година, а немалка част от тях са признали, че са обмисляли да извършат действия, които биха могли да навредят на компанията.[10]

Недоволните служители представляват сериозна вътрешна заплаха за организациите в условията на пост пандемична реалност. Работодателите, които не се справят с проблемите, свързани с недоволството на служителите, рискуват да понесат значителни финансови и репутационни загуби. [1]

### 5.5.1. Фактори, допринасящи за недоволството на служителите:

- **Претоварване и стрес:**

Пандемията доведе до безпрецедентно ниво на стрес и претоварване за много служители, които работеха от дома си, често при липса на ясни граници между работа и личен живот.[1][6]

- **Липса на признание и недостатъчно възнаграждение:**

Много служители се чувстват недооценени и невъзнаградени за труда си, което може да доведе до чувство на негодувание и гняв, което да се превърне в перфектната среда за развитие на вътрешни заплахи.[1]

- **Лошо управление:**

Неефективното управление, липсата на комуникация и несправедливото отношение могат да демотивират служителите и да ги накарат да се чувстват незачетени.[1]

- **Липса на възможности за развитие:**

Служителите, които не виждат възможности за кариерно развитие в рамките на организацията, са по-склонни да търсят работа другаде.[1]

### 5.5.2. Последици от недоволството на служителите:

- **Финансови загуби**:

Злонамерените действия на недоволни служители могат да доведат до значителни финансови загуби, включително разходи за възстановяване на данни, поправяне на системи и правни такси.[1]

- **Повреден имидж:**

Разкриването на вътрешни заплахи може да навреди на репутацията на компанията и да затрудни привличането и задържането на талантливи служители.[1]

- **Нарушена продуктивност**:

Страхът и недоверието сред служителите, могат да доведат до намалена продуктивност и неефективност.[1]

### 5.5.3. Какво могат да направят работодателите?

- **Създаване на култура на доверие и уважение:**

Важно е работодателите да изградят култура на доверие и уважение, в която служителите да се чувстват ценени и чути.[1]

- **Подобряване на комуникацията:**

Редовната и прозрачна комуникация между ръководството и служителите, е от съществено значение за избягване на недоразумения и недоволство.[1]

- **Предлагане на конкурентни заплати и обезщетения:**

Работодателите трябва да предлагат конкурентни заплати и обезщетения, за да привличат и задържат талантливи служители.[1]

- **Осигуряване на възможности за развитие:**

Инвестирането в обучение и развитие на служителите, е от съществено значение за тяхното мотивиране и ангажираност.[1]

- **Борба с претоварването и стреса:**

Работодателите трябва да предприемат стъпки за намаляване на претоварването и стреса сред служителите, като например предлагане на гъвкави условия на работа и програми за подпомагане на психичното здраве.[1]

Създаването на положителна работна среда, основана на доверие, уважение, отворена комуникация и възможности за развитие, е ключов фактор за предотвратяване на вътрешни заплахи и за гарантиране на успеха на организацията в дългосрочен план. [1]

## 5.6. Липса на информираност и обучение

Вътрешни заплахи могат да възникнат и от неволни действия от служители, които не са наясно с рисковете за сигурността или не разбират политиките и процедурите на компанията. Например, това може да се случи, когато служителите по невнимание споделят чувствителна информация или отварят писма с подозрително съдържание, при което стават жертва на фишинг-измами. Организациите трябва да осигурят редовно обучение и да изграждат информираност относно сигурността у своите служители, за да предотвратят неволни пробиви в сигурността.[1]

# 6. Начини за справяне с вътрешните атаки

За да откриват ефективно вътрешните заплахи, организациите трябва да възприемат превантивен подход към установяването на подозрителни дейности и признаци за наличие на вътрешни заплахи. Това включва използването на усъвършенствани техники за анализ, разузнаване на заплахите и поведенчески анализ за разпознаване на необичайно поведение и потенциални вътрешни заплахи. В тази глава ще бъдат разгледани ключовите стратегии за превенция от вътрешни заплахи. [5]


Фиг. 8 Идентифициране на потенциалните рискове[14]

## 6.1. Проследяване на дейностите на служителите

Ефективното наблюдение на дейностите на потребителите е от решаващо значение за идентифицирането на потенциални вътрешни заплахи. Това включва проследяване на моделите на достъп, използването на чувствителни файлове и необичайно поведение, което може да бъде признак за риск в сигурността. Внедряването на усъвършенствани инструменти за откриване на

заплахи и установяването на цялостни практики за регистриране помагат на организациите да изпреварят потенциалните заплахи, породени както от дистанционно работещите, така и от нормалните служители. [6]

## 6.2. Поведенчески анализ на служителите

Внедряване на специализирани инструменти за анализ на поведението на служителите на организацията.[1]

**Целта е да се откриват отклонения от обичайните модели на поведение**, като например необичайно време на влизане в системата, нетипичен достъп до файлове или подозрителни дейности по прехвърляне на данни.[5]

## 6.3. Сигурност за крайните устройства (Системи EDR)

Множеството устройства, използвани при работа, създават предизвикателства при осигуряването на постоянна сигурност на крайните точки. Ненадежден софтуер, остарели операционни системи или липса на мерки за сигурност, могат да бъдат използвани, както от неволни, така и от злонамерени вътрешни лица.

### 6.3.1. Системите EDR

Екипите трябва да бъдат снабдени с **ясни протоколи за сигурност**, осигуряващи поддържане на **надеждността на техните устройства**.[6]

Това става, чрез **Системите EDR (Endpoint Detection and Response)** или още познати като **EPP (EndPoint Protection)**. Те представляват надграждане на познатите Антивирусни решения, като **добавят проактивен елемент** в тяхната работа. Атаките от неизвестни заплахи (**zero-day атаки**) представляват критични рискове за бизнеса и са най-трудни за предотвратяване.[7]

Благодарение на усъвършенстваните технологии, базирани на **задълбоченото обучение (deep learning)** и **машинно обучение (machine learning)**, системите за защита на крайните устройства успяват да идентифицират поведение, подсказващо, че има атака в ход и да спрат както познати, така и zero-day атаки. [7]

### 6.3.2. Какво представляват Zero-Day атаките?

Това са заплахи, които се възползват от откритите уязвимости на машината на жертвата. [9]

С други думи, много бърза и непозната (нова) атака, която се стартира от кибер-престъпниците, преди експертите по сигурността и антивирусните програми да могат да направят, каквото и да е по въпроса. Всяка атака от този

тип е мечтата на хакера, предвид факта, че той става незабавно „известен“ с поразяването на много машини. Понякога тези уязвимости вземат жертви по целия свят и биват много разрушителни. Те също така са полезен ресурс и за някои правителства, които имат за цел да саботират чужди системи или бизнес интереси.[9]

## 6.4. Обучение и повишаване на чувствителността на служителите

Обучение на служителите за рисковете от вътрешни заплахи и насърчаване на културата на информираност за сигурността в организацията. Това включва провеждане на обучение за разпознаване на тактиките на социалното инженерство, опазване на чувствителна информация и своевременно докладване на подозрително поведение. [5]

Служителите трябва редовно да бъдат обучавани за най-добрите практики в областта на киберсигурността, за последиците от небрежни действия и за ролята, която играят в поддържането на сигурна работна среда. Като насърчават чувството за споделена отговорност, организациите могат да дадат възможност на служителите да допринасят активно за собствената си сигурност и тази на компанията.[6]

## 6.5. Контрол на достъпа до данни и принципа на най-малкото, но достатъчни права (PoLP)

Въвеждането на строг контрол на достъпа, основан на най-малкото но достатъчни права (привилегии), е основна стъпка в намаляването на заплахите, свързани с вътрешни лица. [6]. Терминът на английски е **The principle of least privilege (PoLP)**, може да се научи повече в точка 5.5.1**.**

Служителите, работещи от разстояние, трябва да имат достъп само до информацията, необходима за изпълнение на конкретните им функции. Редовното преразглеждане и актуализиране на разрешенията за достъп гарантира, че лицата имат минималното ниво на достъп, необходимо за техните задачи. [6]

### 6.5.1. The principle of least privilege (PoLP)

**The principle of least privilege (PoLP)** е концепция за информационна сигурност, според която даден потребител или субект трябва да има достъп само до специфичните данни, ресурси и приложения, необходими за изпълнението на дадена задача. Организациите, които следват принципа на най-малките привилегии, могат да подобрят своята позиция по отношение на сигурността, като значително намаляват повърхността на атака и риска от разпространение на зловреден софтуер.[11]

## 6.6. Създаване на надеждна политика за сигурност

Служителите, които умишлено или неволно нарушават политиките за сигурност, могат да причинят сериозни щети, включително кражба на данни, финансови загуби и уронване на репутацията. Създаването на стриктна политика за сигурност е от съществено значение за минимизиране на тези рискове и защита на ценните активи на организацията.[17]

### 6.6.1. Разработване на ясни и прости политики

Ефективната политика за сигурност трябва да бъде ясна, проста и лесна за разбиране от всички служители. Сложните политики могат да доведат до объркване, безразличие или неспазване. Препоръчително е да се използват кратки изречения, прости езикови конструкции и да се избягват ненужни технически термини.[17]

Имплементацията на стриктни и ясни политики за сигурност е ключов елемент за предотвратяване на вътрешни заплахи и защита на данните в съвременните организации. Адаптирането и прилагането на предложените по-долу съвети **(Виж 6.6.3),** може значително да подобри сигурността на информационните системи.[17]

### 6.6.2. Практически пример (Политика за пароли)

Една ясна политика за паролите може да определи изисквания като:

*"Паролите трябва да са дълги най-малко 12 символа, да включват както главни, така и малки букви и да се сменят на всеки 90 дни."* [17]

Тази ясна насока не оставя място за погрешно тълкуване.

### 6.6.3. Съвети за изготвяне на ефективна политика за сигурност

- **Включване на засегнатите отдели:**

При разработването на политиката е важно да се включат представители от всички отдели, които ще бъдат засегнати от нейното прилагане. Това ще гарантира, че политиката е съобразена с нуждите и разпоредбите на отделните екипи.[17]

- **Редовно усъвършенстване на политиката:**

Политиката за сигурност трябва да се преразглежда и актуализира редовно, за да отразява развиващите се заплахи и технологии.[17]

- **Използване на ясен език:**

Политиката трябва да бъде написана на ясен и разбираем език, достъпен за всички служители, независимо от тяхното техническо ниво.[17]

- **Адаптиране на съдържанието:**

Може да се разработят отделни раздели от политиката, съобразени с различните работни роли и отговорности.[17]

- **Използване на реални примери:**

Включването на реални сценарии, може да помогне на служителите да разберат по-добре принципите на политиката и как тя се прилага в практиката.[17]

- **Определяне на ясни стъпки за реагиране при инциденти:**

Политиката трябва да описва ясни стъпки за докладване и реагиране на инциденти, свързани със сигурността.[17]

- **Комуникация относно промените:**

Важно е да се информират служителите за всички актуализации и промени в политиката.[17]

- **Ясни последици от неспазването:**

Политиката трябва да дефинира ясни последици, за нарушаване на нейните правила.[17]

- **Достъпност:**

Трябва да бъде осигурен лесен достъп, за всички служители, до политиката за сигурност.[17]

- **Обучение:**

Провеждането на редовни обучения по сигурността е от съществено значение за гарантиране, че служителите са запознати с политиката и знаят как да я прилагат в своята работа.[17]

# 7. Вътрешните заплахи в цифри

Въпреки че е трудно да се измерят количествено, вътрешните заплахи представляват сложен и бързо изменящ се набор от проблеми, които организациите не могат да си позволят да игнорират.[12]

Точното отчитане на годишните загуби, дължащи се на вътрешни заплахи във всички индустрии е трудно постижимо поради начина, по който се изчисляват тези разходи, както и непълната информация, която остава недокладвана, относно причинените щети.[12]

Националната работна група за вътрешни заплахи на Съединените Щати (NITTF) съобщава, че честотата на случаите на вътрешни заплахи непрекъснато се увеличава, особено при технологичните кражби. Загубите могат да са резултат от физически щети върху инфраструктурата, нарушаване на производителността, кражба на интелектуална собственост, случайно изтичане на чувствителни данни или увреждане на репутацията на

организацията. Всяко от тези неща може да допринесе за загуба на конкурентно предимство на пазара. [12]

## 7.1. Разпространението на инциденти в представителни сектори

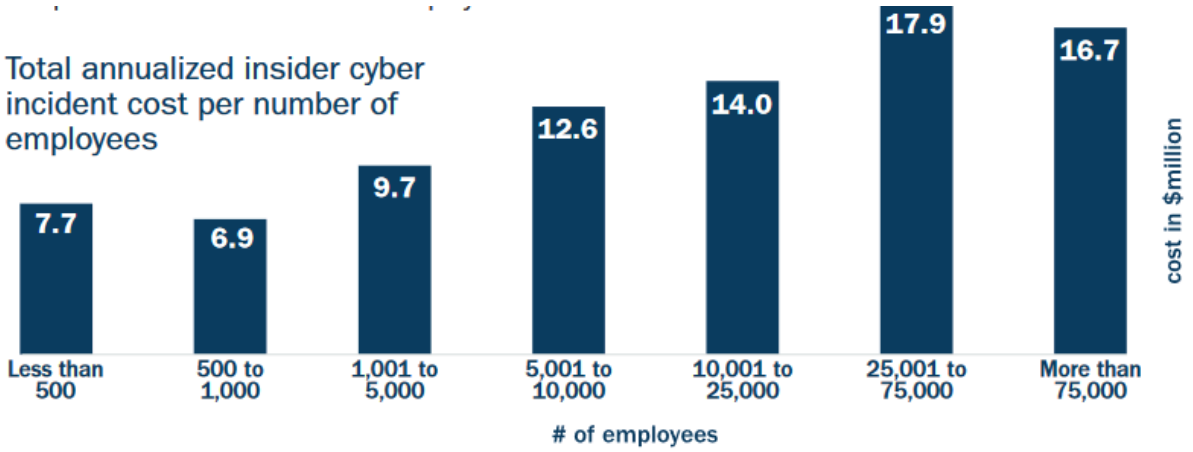
На фигурата, по-долу (Фиг. 9), представя тенденциите свързани с разпространението на вътрешни инциденти в избрани сектори..


Фиг. 9 Тенденциите свързани с разпространението на вътрешни инциденти.[12]

Според допълни, пробивите за 2019 г. са се увеличили количествено с 47% и са стрували на организациите 31% повече отколкото през предходната година.

## 7.2. Потенциалните разходи, в зависимост от размера на компанията

Разходите за вътрешни заплахи зависят от големината на организацията. Ще изследваме съотношението на потенциалните разходи, които организацията може да понесе в зависимост от размера на компанията.




Фиг. 10 Финансовото въздействие на вътрешните заплахи, върху организации с различен размер.[12]

На фигура (Фиг.10), финансовото въздействие на вътрешните заплахи, върху организации с различен размер, е представено по следният начин:

*На оста Y представлява общите годишни разходи за вътрешни инциденти в милиони долари, а на оста X - броя на служителите в съответната категория от организации.[12]*

Графиката показва, че разходите за вътрешни заплахи се увеличават с нарастването на броя на служителите, но това не пропорционално. Организациите **от 500 до 1000 служители имат най-ниски общи годишни разходи** - около 6.9 млн. долара. Важно е да се отбележи, че **най-малките организации имат малко по-големи общи годишни разходи** (около 7.7млн.), от споменатите по-горе компании. След това **разходите се увеличават постоянно** докато достигнат 17,9 млн. долара за организации с размерите от 25 001 до 75 000 служители. Важно е да се отбележи, че **най-големите организации имат малко по-малки общи годишни разходи** (около 16.7млн.), от компаниите с до 75 хил. служителя. [12]

## 7.3. Други интересни статистически данни

- 39% от организациите са създали организация за борба с вътрешните заплахи, а 46% възнамеряват да го направят в бъдеще. Тези организации, най-често се наблюдават от CISO и мениджърите по ИТ сигурност.

Според Lirex:

- 24% от случаите на загуба на данни са поради човешка грешка[8]

- Небрежност на служител или подизпълнител е причината за два от три случая (66%) на вътрешен инцидент с киберсигурността на организацията[8]
- В **92.4%** от malware атаките са по имейл[8]
- **48%** от злонамерените имейл атаки са от Microsoft (MS Office) файлове[8]

# 8. Заключение

Вътрешните заплахи са сериозен проблем за организации от всякакъв размер. Тези заплахи могат да имат опустошителни последици, включително финансови загуби, кражба на данни и уронване на репутацията.

За да се предпазят от вътрешни заплахи, организациите трябва да предприемат превантивен подход, съчетаващ технологични решения, обучение на служителите и култура на киберсигурност.

Тъй като дистанционната (хибридната) работна среда се превръща в трайна част от съвременното работно място, справянето със заплахата от вътрешни заплахи е наложително за поддържане на стабилна киберсигурност. Ориентирайки се в предизвикателствата, породени от отдалечените служители, фирмите могат да укрепят защитата си и да се предпазят от заплахите в един развиващ се цифров свят.

В заключение, вътрешните заплахи пораждат проблеми, които не могат да се подценяват и е необходимо да бъдат управлявани с правилните инструменти. Необходимо е организациите да се фокусират върху технологичните решения, обучението на служителите и превантивната култура на сигурност, като така те могат да засилят своята киберсигурност и да се предпазят от нарастващия риск от вътрешни атаки.

# 9. Използвана Литература

[1] 5 съвета за предпазване от вътрешни кибер-заплахи - от: TechNews.bg https://technews.bg/article-150289.html
[2] Defining Insider Threats - CISA.gov (An official website of the U.S. Department of Homeland Security)
https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats
[3] Cost of Insider Risk Global Report 2023 - https://www.cybersecurity-insiders.com/portfolio/2023-insider-threat-report-gurucul/
[4] Insider Threat Statistics for 2024: Reports, Facts, Actors, and Costs Origin: https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures - © Ekran System
[5] Insider Threat Tactics, Techniques, and Procedures (TTPs): Strategies for Detection and Prevention – Paritosh
https://medium.com/@paritoshblogs/insider-threat-tactics-techniques-and-procedures-ttps-strategies-for-detection-and-prevention-238d27f27f12
[6] The Insider Threat Navigating Security Risks Posed by Remote Employe https://medium.com/@Land2Cyber/the-insider-threat-navigating-security-risks-posed-by-remote-employees-5806b164f6a0
[7] Системи EDR
https://lirex.com/bg/integrirana-sigurnost/sigurnost-na-potrebiteli/endpoint-detection-and-response/
[8] Security-awareness - https://lirex.com/bg/obucheniya-za-security-awareness/
[9] Zero-Day атаките? - https://antivirus.bg/news/zero-day-attack/
[10] 2022 Cost of insider threads, global report – Ponemon Institute - https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-the-cost-of-insider-threats-ponemon-report.pdf
[11] The principle of least privilege (PoLP) - https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege
[12] Insider Threat, Mitigation Guide, NOVEMBER 2020, Cybersecurity and Infrastructure Security Agency: https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf
[13] Insider Threat - https://www.imperva.com/learn/application-security/insider-threats/
[14] Insider Threats and Mosaic Theory: Safeguarding Organizations - https://fastercapital.com/content/Insider-Threats-and-Mosaic-Theory--Safeguarding-Organizations.html
[15] Understanding the Shifting Perceptions of Insider Threats Over External Cyber Attacks - By Findlay Whitelaw, Field CTO, Securonix https://www.securonix.com/blog/shifting-perceptions-of-insider-threats-vs-external-cyber-attacks/

[16] 2024 Insider Threat Report - Securonix
https://www.securonix.com/resources/2024-insider-threat-report/

[17] Spotting Insider Threats: 10 Best Practices to Prevent Data Leaks in Your Organization - https://www.safetica.com/blog/what-is-an-insider-threat-definition-examples-and-solution

[18] Insider Threat Awareness: What Is It, Why Does It Matter, and How Can You Improve It? - Origin: https://www.ekransystem.com/en/blog/insider-threat-awareness © Ekran System

[19] Insider Threat Statistics for 2024: Reports, Facts, Actors, and Costs - Origin: https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures - © Ekran System

[20] Brute Force Attacks: How to Detect and Prevent Them, Origin: https://www.ekransystem.com/en/blog/brute-force-attacks, © Ekran System