УМАЊИВАЊЕ ИНСАЈДЕРСКЕ ПРЕТЊЕ СКРИПТА

Проф.др Горан Матић

САДРЖАЈ

СКРИПТА ПРЕДСТАВЉА ЛИЧНО, СТРУЧНО И НАУЧНО ВИЂЕЊЕ ПРОБЛЕМАТИКЕ ОД СТРАНЕ АУТОРА, КОЈА РАЂЕНА НА ОСНОВУ АНАЛИЗЕ ЈАВНИХ ИЗВОРА ПОДАТАКА….

- ПРОПИСА
- ПРАКСЕ
- НАУЧНИХ И СТРУЧНИХ ТЕКСТОВА
- МЕДИЈА
- ИСКУСТВА У РАДУ СА ПОДАЦИМА

УВОДНЕ НАПОМЕНЕ

Инсајдерска претња је једна од најзначајнијих тема последњих година која је у директној вези са безбедности организација и пословања и којој је посвећивано најмање пажње.....

Термин ИНСАЈДЕР се изузетно широко користи и најчешће то ствара забуну у превентивној делатности....

Танка је линија између слободе говора и мишљења, дувача у звиждаљку, мобинга, повреда радне дисциплине, инсајдерске опасности, злоупотребе положаја, шпијунаже, саботаже....

Истраживање инсајдерских претњи је у теорији и пракси критиковано.

Критичари су тврдили да је инсајдерска претња лоше дефинисан концепт.

Форензичко истраживање крађе инсајдерских података је веома тешко и захтева нове технике као што је стохастичка форензика.

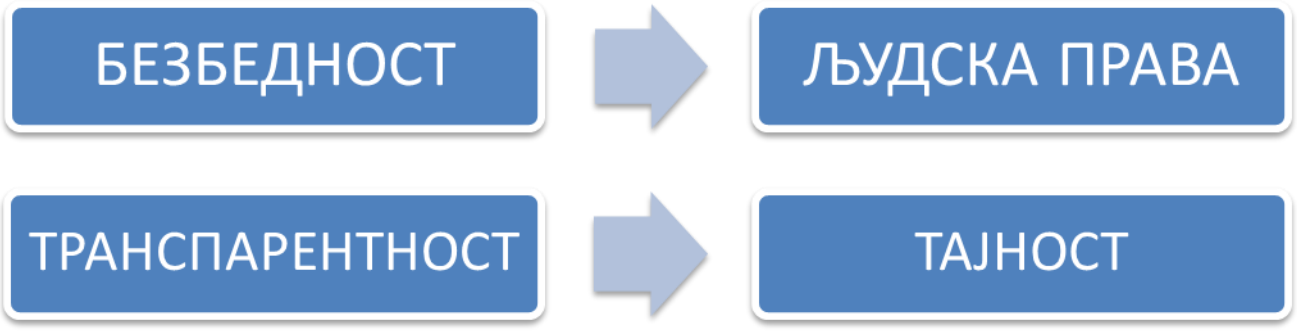
Подаци који подржавају инсајдерске претње су генерално власнички – односе се на интелектуалну својину (тј. шифровани подаци).

Теоријски/концептуални модели инсајдерске претње су често засновани на лабавим тумачењима истраживања у психолошко-бихејвиоралним и друштвеним наукама, користећи „дедуктивне принципе и интуицију стручњака за предметну материју“.

Усвајајући социотехничке приступе, истраживачи су такође заговарали потребу да се инсајдерска претња размотри из перспективе друштвених система.

Поједини аутори тврде да „надзор захтева разумевање како су уоквирени системи санкционисања, како ће запослени реаговати на надзор, које се норме на радном месту сматрају релевантним и шта 'одступање' значи, на пример, одступање од оправдане норме организације или пропуст да се у складу са организационом нормом која се коси са општим друштвеним вредностима“.

Третирајући све запослене као потенцијалне инсајдерске претње, организације могу створити услове који доводе до инсајдерских претњи.



Које су границе до којих се може ићи у успостављању система заштите?

Оданост или лојалност означава унутрашњу повезаност и изражавање те повезаности кроз:

- понашање према особи,
- групи или
- заједници

Лојалност – значење изведено преко синонима: оданост, верност, исправност, поданичка верност, честитост, часност, привржености, поверљивост, постојаност, непроменљивост, искреност,поштење.

Лојалност значи да се систем вредности са осталим дели и да се ставови заједнице бране и онда када се има различито мишљење.

Лојалност означава унутрашњу повезност. Она је увек добровољна те се показује у понашању према онима с којима се осећа повезаност, као и према трећим особама.

Мотиви лојалности могу бити интересни, идеолошки и емоционални.

Проблеми могу настати кад се оданост од друге стране тражи по потреби.

То може довести до сукоба лојалности.

На пример, ако се запослени према послодавцу мора понашати лојално, иако с њим не дели одређене циљеве и вредности.

Озбиљне последице могу настати код неизвршавања наређења у војсци.

И у питањима заштите околине, рачуноводственим, кадровским и сличним осетљивим питањима увек се очекује оданост, а понекад се такво понашање завршава и као превара.

Лојалност чине компоненте:

- **Искреност** – темељ односа и кључна компонента
- **Комуникација** – неопходна за лојалност и разумевање, може помоћи у спречавању сукоба
- **Поштовање** – вредновање ставова организције, иако се не слажете са њима. Код инсајдерске претње поштовање прво нестаје
- **Поверење** – темељ лојалности. Веровање и посвећеност циљевима у организацији
- **Поштовање граница** – постављање сопствених и поштовање граница организације, шта је прихватљиво, а шта није
- **Подршка** – организацији у успонима и падовима

КЉУЧНА НАПОМЕНА

Инсајдер је на екстреман начин растрзан између две различите лојалности

Једној страни мора да буде крајње одан, али да би био инсајдер, истовремено мора да прекрши лојалност према онима који му поклањају нарочито поверење...

Конфликт је, у најужем схватању, увек сукоб различитих по смеру деловања, супротних мотива.

То је резултат динамичких психичких збивања и зато изазива фрустрацију, посебно уколико су супротности веће а препреке за њихово испољавање теже.

У друштвеним односима, конфликт је:

- стање, неслагања и инкомпатибилности између више људи (интероргнизацијски, интерперсонални, интергрупни сукоб), група људи и нација (интернационални, социјални конфликт).

Већина конфликата (сукоба) може се описати следећим обрасцем:

- Две или више особа/лица у интеракцији доживљавају неускладиве међусобне разлике у жељи да дођу до нечега (лопте, наклоности, унапређења, новца...) или да задовоље неке потребе и остваре неке вредности
- Након те временске тачке конфликт се може повећавати или ублажавати

Конфликт међу појединцима или групама може водити физичком насиљу, а међу народима сукобима различитог интензитета.

У ранијем пероду, инсајдер и унутрашњи непријатељ – шпијунажа, саботажа су били исти концепти.

Саботажа је појам који се односи на:

- намерно ометање економског или војног деловања како би се постигли одређени (најчешће политички) циљеви.

Појам саботажа се користи за опис

- насилних оштећења и уништавања опреме, машина, инфраструктуре и сличног у сврху постизања идеолошких или политичких циљева.

Од саботаже морамо разликовати вандализам, који је уништавање јавне или приватне имовине или масовно јавно вређање, понижавање и насиље.

Саботажа може бити и дело против

- Производног процеса,
- Информационих система и база података,
- Документације и
- Других вредности, активности, имовине.

Реч „саботажа“ је вероватно настала када су француски радници током индустријске револуције убацивали своје дрвене клompе (у француским језику „сабот“) у машине за кошење и вршење са сврхом да се супротставе ширењу модерне механизације или да добију на времену за одмор док је строј био поправљан.

Из тог разлога, „сабот“ је био кориштен као симбол анархистичких радника.

ТЕРМИНОЛОШКО ОДРЕЂЕЊЕ РЕЛЕВАНТНИХ ПОЈМОВА

Инсајдерске претње представљају сложен и динамичан ризик који утиче на јавне и приватне домене свих сектора критичне инфраструктуре. Дефинисање ових претњи је критичан корак у разумевању и успостављању инсајдерског програма за ублажавање претњи.

Пример САД - Агенција за сајбер безбедност и безбедност инфраструктуре (ЦИСА) дефинише инсајдерску претњу као претњу да ће инсајдер користити свој овлашћени приступ, намерно или ненамерно, да нанесе штету мисији, ресурсима, особљу, објектима, информацијама, опреми, мрежама или системима одељења.

Инсајдерска претња је потенцијал инсајдера да искористи свој овлашћени приступ штићеним подацима или информацијама организације у намери да науди тој организацији.

Ова штета може укључивати злонамерне, самозадовољне или ненамерне радње које негативно утичу на интегритет, поверљивост и пословање (јавни имиџ) организације, њених података, особља или објеката.

У пракси се дефинише инсајдерска претња као претња да ће инсајдер користити свој овлашћени приступ, свесно или несвесно, да нанесе штету мисији, ресурсима, особљу, објектима, информацијама, штићеним подацима, опреми, мрежама или ИКТ системима органа јавне власти или компаније.

Ова претња се може манифестовати кроз следећа инсајдерска понашања:

- Шпијунажу; - Тероризам; - Неовлашћено откривање/изношење информација; - Корупцију, укључујући учешће у транснационалном организованом криминалу; - Саботажу; Насиље на радном месту; - Намеран или ненамеран губитак или деградација ресурса или способности.

У теорији је предложено више система класификације и онтологија за класификацију инсајдерских претњи. Традиционални модели инсајдерских претњи идентификују три широке категорије:

- **Злонамерни инсајдери**, то су људи који користе свој приступ да нанесу штету организацији;
- **Немарни инсајдери**, људи који праве грешке и занемарују политику, што доводи њихове организације у опасност;
- **Инфилтратори**, који су спољни актери који добијају легитимне акредитиве за приступ без овлашћења.

Шта се све подразумева под појмом инсајдер:

- **Незадовољан запосленик** (радник)
- **Сведок из организације у неком поступку** (сарадник полиције – информант или информатор и тужилаштва)
- **Узбуњивач, звиждач** или **дувач у пиштаљку**
- **Запосленик извршилац КД - криминалац** (крађа, утаја, корупција, злоупотреба фондова...)
- **Саботер** (идеолошка, национална, верска мотивација)
- **Шпијун** (за потребе стране државе, друге компаније...)
- **Вандал** – лице које уништава јавну или приватну својину...

Инсајдерска активност може бити:

- Законита (узбуњивач, сведок итд)
- Незаконита (злоупотреба права или криминал)
- Усмерена ка стицању личне добити или искључиво наношењу штете организацији
- Индивидуална активност појединца (усамљени вук) или организована унутрашња (спољна) активност

Лични мотиви за инсајдерску активност могу бити:

- Иделошке, верске и националне побуде
- Материјални разлози (лоше финансијско стање, дугови)
- Жеља за осветом због увреде (убрајајући ту и умишљене)
- Завист, страх, сујета, усамљеност, авантуризам
- Систематско вређање националних или религиозних осећања
- Незадовољство положајем у организацији („каријерно лудило“)
- Психо-патолошка стања (маније, депресија...)
- Проблеми у емотивном животу (неуспешан брак, веза...)

Инсајдерска активност по структури:

- Радник, запосленик на нижим дужностима
- Менаџмент средњег нивоа
- Менаџмент високог нивоа
- Бивши запосленик, радник, менаџер
- Подизвођач – контрактор
- Спољни сарадник организације
- Кртица – лице које је дошло на незаконит начин до приступа штићеним системима и подацима организације (супруг/а; љубавник/ца; пријатељ; рођак...)

Примери инсајдера могу укључивати:

- Особу којој је додељена пропусница/значка или приступни уређај.
- Особу којој је организација обезбедила приступ рачунару или мрежи.
- Особу која развија производе и услуге.
- Особу која познаје основе организације.
- Особу са приступом заштићеним информацијама.

Инсајдери укључују и:

- Кориснике са високим привилегијама као што су мрежни администратори, руководиоци, партнери и други корисници са дозволама за приступ осетљивим и штићеним подацима.
- Програмери са приступом подацима који користе развојно или сценско окружење.
- Корисници запослени који су отпуштени или дали отказ, а којима је остао омогућени профил и акредитиви.
- Менаџери набавке и запослени.
- Продавци са интерним приступом.
- Извођачи са интерним приступом.
- Партнери са интерним приступом.

Инсајдер (енг. insider - "неко унутра") је назив за особу која је припадник неке друштвене групе због чега располаже одређеним сазнањима недоступним широј јавности.

Може имати следеће конотације:

Негативне – кад је у питању особа која као члан неког тајног удружења сазнаје поверљиве пословне и друге информације које после користи за незаконито или неморално стицање богатства.

Позитивне – када је реч о особама које су вољне да тако стечене информације о неморалним и незаконитим радњама одају као сведоци, узбуњивачи јавности - звиждачи, било јавности, било органима власти.

Злонамерне инсајдерске претње

Такође се називају и преокретом, главни циљеви злонамерних инсајдерских претњи укључују шпијунажу, превару, крађу интелектуалне својине и саботажу. Они намерно злоупотребљавају свој привилеговани приступ да би украли информације или деградирали системе из финансијских, личних и/или злонамерних разлога.

Примери укључују запосленог који продаје поверљиве податке конкуренту или незадовољном бившем уговарачу који уводи слабајући малвер на мрежу организације. Злонамерне инсајдерске претње могу бити колаборационисти/сарадници или усамљени вукови.

Колаборационисти - Сарадници су овлашћени корисници штићених података који раде са трећом страном са намером да нанесу штету организацији. Трећа страна може бити конкурент, национална држава, организована криминална мрежа или појединац.

Радња сарадника би довела до цурења поверљивих информација или ометања пословања.

Вукови самотњаци делују потпуно независно и делују без спољне манипулације или утицаја. Они могу бити посебно опасни јер често имају привилегован приступ систему као што су администратори базе података.

Неопрезне/ненамерне инсајдерске претње

Неопрезне инсајдерске безбедносне претње се јављају ненамерно. Често су резултат људске грешке, лошег просуђивања, ненамерног помагања и подржавања, погодности, фишинга (и других тактика друштвеног инжењеринга), малвера и украдених акредитива.

Појединац који је укључен несвесно излаже системе организације спољним нападима.

Неопрезне инсајдерске претње могу бити пиони или корисни глупани.

Пиони су овлашћени корисници који су изманипулисани да ненамерно делују злонамерно, често кроз технике друштвеног инжењеринга као што је фишинг. Ове ненамерне радње могу укључивати преузимање малвера на њиховом рачунару или ненамерно откривање поверљивих информација преваранту.

Корисни глупани намерно предузимају потенцијално штетне радње, али немају злу намеру. Они су арогантни, неуки и/или некомпетентни корисници који не препознају потребу за поштовањем безбедносних политика и процедура. Глупост може бити корисник који чува поверљиве информације о клијентима на свом личном уређају, иако зна да је то противно смерницама организације.

Кртица је аутсајдер, изван организације, али онај који је добио инсајдерски приступ системима организације. Они се могу представљати као продавац, партнер, уговарач или запослени, чиме добијају привилеговано овлашћење за које се иначе не би квалификовали у редовној процедури.

ЗАКОН О ЗАШТИТИ УЗБУЊИВАЧА (члан 2.)

1. „узбуњивање” је откривање информације о кршењу прописа, кршењу људских права, вршењу јавног овлашћења противно сврси због које је поверено, опасности по живот, јавно здравље, безбедност, животну средину, као и ради спречавања штете великих размера;
2. „узбуњивач” је физичко лице које изврши узбуњивање у вези са својим радним ангажовањем, поступком запошљавања, коришћењем услуга државних и других органа, носилаца јавних овлашћења или јавних служби, пословном сарадњом и правом власништва на привредном друштву;

Узбуњивач, звиждач или дувач у пиштаљку (енгл. whistleblower) израз је за храброг појединца који из високо моралних разлога одлучује да, уз ризик по сопствену каријеру, јавно проговори о незаконитим или неетичким делима надређених му појединаца.

Узбуњивач - је физичко лице које узбуњује у вези са својим радним ангажовањем, поступком запошљавања, коришћењем услуга органа власти, носилаца јавних овлашћења или јавних служби, пословном сарадњом и правом власништва у привредном друштву.

Под "узбуњивањем" се сматра откривање информације о кршењу прописа, кршењу људских права, вршењу јавног овлашћења противно сврси због које је поверено, опасности по живот, јавно здравље, безбедност, као и ради спречавања штете великих размера.

Закон о заштити узбуњивача из 2014, године се односи и на оне који су повезани са узбуњивачима, који трпе штетне последице због тога, и пружа пуну заштиту онима која пријављују сумњу на корупцију или случај злоупотребе јавног интереса чиме се отклањају недостаци неадекватне и недовољне заштите појединих категорија узбуњивача.

- УНУТРАШЊЕ УЗБУЊИВАЊЕ – код послодавца
- СПОЉНО УЗБУЊИВАЊЕ – код надлежног органа
- УЗБУЊИВАЊЕ ЈАВНОСТИ – под условима и на начин предвиђен законом

У Америци постоји посебна установа која се бави заштитом појединаца које одликује таква грађанска храброст:

National Whistleblower Center

Саботер је лице које свесно и намерно онемогућава неке редовне делатности, рада или ратних припрема и деловања. Огледа се у деструкцији претпоставки неке делатности, нпр. рушење или намерно кварење машина и постројења, средстава комуникација (телекомуникацијска средства, путеви, пруге и мостови), као и избегавање обављања неких обвеза и дужности (нпр. радна обавеза) или одуговлачења послова.

У саботажу спада и пасивни отпор и намерно лоше или немарно обављање радног процеса. За разлику од диверзије, саботажа је обично потајна, замаскирана делатност.

Вандал – значење појма изведено преко синонима: хулиган, насилник, силеџија, насилник, разбијач, злотвор, напасник, мучитељ, крволок, манијак, грубијан, окрутник, сивоња, батинаш, крвник, горопадник, бичеватељ, махнитац.

Шпијун (УХОДА, ДОУШНИК, ДОСТАВЉАЧ, ПОТКАЗИВАЧ, ВРЕБАЧ, ЖБИР...)

Шпијунажа као појам означава обавештајне делатности које се састоје од одавања или саопштавања другој особи (или ратној страни, држави или организацији) прикупљених података или чињеница које представљају тајну (војну, службену, економску, индустријску...).

Међународно право регулише шпијунажу искључиво у области међународног хуманитарног права док шпијунажа у мирнодопским условима спада под кривично право поједине државе.

Особе које се баве шпијунажом називамо шпијунима, а средства и начини којима они долазе до података су разни (праћење, тајно мотрење кретања, рада или неке друге активности посматране стране, достављање података, потказивање или цинкарење и слично).

Тешко је подвући теоријску и практичну границу између шпијуна, саботера и инсајдера када сагледавамо нашу тему....

ИСТОРИЈАТ ОБАВЕШТАЈНЕ ДЕЛАТНОСТИ - ПРИКУПЉАЊА ИНФОРМАЦИЈА (ЈАВНИХ И ТАЈНИХ) ЗА:

- Потребе вођења ратова, освајање и продоре на друге територије...
- Очување власти круне, откривање завера, превратa, побуна, атентата...
- Потребе вођења политике према другим краљевствима
- Религиозно и идеолошко деловање....
- Потребе вођења прекоморске и друге трговине …
- Крађе технологија и патената – „индустријска шпијунажа“ …

ИНФОРМАНТ

лица која случајно и пригодно сазнају за планирана или извршена кривична дела и њихове учиниоце

ИНФОРМАТОРИ (поузданик, вигилант и агент провокатор)

Особе спремне да дуже време полицији пружају криминалистички и кривично правне релевантне информације, при чему се њихов идентитет чува у тајности

ИНСАЈДЕРСКА ПРЕТЊА

Све безбедносне службе, али и корпоративна безбедност у предузећима, се у свом раду традиционално фокусира на активности усмерене на детектовање и супротстављање **спољашњим претњама**.

- Лице са законским овлашћењем да приступи подацима које својим поступком или пропустом узрокује штету својој организацији;
- Инсајдер представља већу претњу него шпијунажа;
- Таква претња може да доведе до крађе заштићених података, неуспеха политичког процеса, физичког уништења имовине, губитка кредибилитета.

Које су врсте инсајдерских претњи?

- Ненамерна претња (немар и случајно)
- Намерне претње
- Друге претње (тајне претње и претње од трећих лица)

Немар

- Инсајдер овог типа излаже организацију претњи непажњом. Немарни инсајдери су генерално упознати са безбедносним и/или ИТ политикама, али бирају да их игноришу, стварајући ризик за организацију. Примери укључују омогућавање некоме да „поврати“ кроз безбедну улазну тачку, губљење или губљење преносивог уређаја за складиштење који садржи осетљиве информације и игнорисање порука ради инсталирања нових ажурирања и безбедносних закрпа.

Случајност

- Инсајдер овог типа грешком проузрокује ненамерни ризик за организацију. Примери укључују погрешно уписивање адресе е-поште и случајно слање осетљивог пословног документа конкуренту, несвесно или ненамерно кликање на хипервезу, отварање прилога у е-поруци за крађу идентитета која садржи вирус или непрописно одлагање осетљивих докумената.

Намерне претње

- Намерни инсајдер се често синонимно помиње као „злонамерни инсајдер“. Намерне претње су радње које се предузимају да се нашкоди организацији ради личне користи или да се поступи на основу личне притужбе. На пример, многи инсајдери су мотивисани да се „обрачунају (свете)” због уоченог недостатка признања (нпр. унапређење, бонуси, пожељно путовање) или отказа. Њихове радње могу укључивати «цурење» осетљивих информација, узнемиравање сарадника, саботирање опреме, вршење насиља или крађу власничких података или интелектуалне својине у лажној нади да ће напредовати у каријери.

Тајне претње

- Подскуп злонамерних инсајдерских претњи назива се тајним претњама, где један или више инсајдера сарађују са спољним актером претње како би компромитовали организацију. Ови инциденти често укључују сајбер криминалце

који регрутују инсајдера или неколико инсајдера да би омогућили превару, крађу интелектуалне својине, шпијунажу или комбинацију ова три.

Претње од трећих лица

- Поред тога, претње трећих страна су обично подизвођачи или ангажована физичка и правна лица који нису формални чланови организације, али којима је одобрен одређени ниво приступа штићеним подацима, објектима, системима, мрежама или људима да заврше свој посао.

Ове претње могу бити директне или индиректне претње.

Ипак, недавни случајеви који се тичу повреде безбедности штићених података показују да унутрашње или интерно откривање података може бити опасно исто тако као и њихово откривање од стране страних или спољних субјеката.

Зашто се о инсајдерским претњама не говори довољно?

Неколико кључних разлога:

- Инсајдерске инциденте је тешко открити. Малициозни инсајдер може годинама да неопажено краде податке. Када се инцидент орткрије, тешко је утврдити који су све подаци компромитовани.
- Пријављивање – обеладоњивање цурења података може лоше да утиче на репутацију организације.
- Тешко се доказује. Када се утврди да је неко изнутра износио информације, тешко је утврдити ко је кривац, чак и ако се зна ко је кривац, тешко је пронаћи доказе који би били прихватљиви на суду.

Дефиниција кључних појмова

- **Инсајдер**: Физичка лица или организациони субјекти овлашћени да физички или електронски приступе сензитивним подацима и инфраструктурним ресурсима.
- **Претња**: Способност физичких лица или организационих субјеката да прекораче или злоупотребе своје овлашћење за приступ поменутим ресурсима, како би искористили, напали и/или на други начин негативно утицали на сензитивне податке и информационе системе.

ГЛАВНИ ПОКАЗАТЕЉИ

Лични фактори:

- Опхрваност животном кризом
- Финансијске потешкоће
- Компулзивно/деструктивно понашање
- Бес
- Освета усмерена против органа власти/ауторитета

Фактори на радном месту:

- Лако уклањање заштићених материјала
- Приступ заштићеним материјалима
- Лабава безбедносна правила
- Средина коју карактеришу кадровска редукција и привремена отпуштања

Знаци који указују на активног инсајдера:

- Непотребно умножавање материјала
- Разочараност приватним животом/ радним местом (незадовољство)
- Непријављени страни контакт/пут у иностранство
- Сумњиви лични контакти

Ризичне карактеристике у понашању:

- Непријављена путовања у иностранство
- Тражење података о власништву или тајних података који нису повезани са радним местом
- Параноично понашање на помен истраге
- Изражени степен беса због разочарења у каријери

Извори/узроци проблема са инсајдером:

- Злоба (незадовољни службеник)
- Непоштовање безбедносних процедура
- Несавесно поступање (намерно избегавање процедура)
- Незнање (без намере да нашкоди)

ПРИМЕРИ ИЗ ПРАКСЕ

Инсајдери, а не хакери су највећа претња за безбедност организације (сајбер безбедност) ...“

HANNESEN	**ASSANGE**	**MANNING**
SNOWDEN	**DEVENNEY**	**DELISLESIMM**

Викиликс (енгл. WikiLeaks) је међународна непрофитна медијска организација која објављује на други начин недоступне материјале од анонимних извора. Њен веб-сајт, покренут 2006. води Саншајн прес. Од настанка сајта, Викиликс тврди да има базу података која је нарасла на више од 1,2 милиона докумената.

Интернет страница Викиликс, коју је 2006. основао Џулијан Асанж, 39. годишњи Аустралијанац са групом истомишљеника које је контактирао посредством Интернета, сакупља и објављује осетљива документа и податке које државе или концерни сматрају тајним.

Сам назив „Викиликс” је спој два појма: „Википедија”, најчитаније енциклопедију на Интернету, и „ликс” (leaks), енглеска реч за „цурење информација”, односно одавање строго чуваних тајних.

Оснивач своју веб страницу описује као „јавни сервис” за новинаре и активисте против корупције, с циљем „борбе за слободу уз помоћ информација”.

Викиликс опстаје захваљујући донацијама, а гарантује анонимност и заштиту извора информација. Од оснивања пласира осетљива документа о разним стварима - на пример, о транспорту отровног отпада у Обалу Слоноваче или смерницама америчке армије о третману у бази Гвантанамо.

Челси Елизабет Менинг, рођена као Бредли Едвард Менинг, била је амерички војник.

Ухапшен је у Ираку маја 2010. због сумње да је проследио поверљиве документе Владе САД сајту Викиликс.

Менинг је, између осталог, оптужен за достављање информација о националној одбрани неовлашћеним лицима и помагање непријатељу, дела за која је прописана смртна казна, иако су тужиоци саопштили да га неће тражити.

Осуђен је на 35 година затвора 24. августа 2013. пред војним судом. Нешто касније обратио се јавности са обавештењем о промени пола из мушког у женски, променом имена у Челси и молбом да га сви ословљавају у складу са новим околностима.

Бредли/Челзи Мининг
Лични фактори:
- идеологија
- криза идентитета

Фактори на радном месту:
- приступ заштићеном материјалу
- нерегистровани приступ

Знаци активног инсајдера:
- проблеми у радном окружењу

Цефри Дилајл (Канада) – обавештајни аналитичар у Морнаричким снагама.

После распада брака 2007. године контактирао је руску амбасаду у Отави са понудом да прода обавештајне податке руској Војној обавештајној служби (ГРУ).

Лични фактори:

- опхрваност животном кризом
- финансијске потешкоће

Фактори на радном месту:

- лако склањање заштићеног материјала

Знаци активног инсајдера:

- непотребно умножавање материјала
- непријављени страни контакт/путовање
- сумњиви лични контакти

Едвард Девени (УК) је 33-годишњи подофицир Краљевске морнарице за дужим досијеом проблема у понашању током каријере. Контактирао је руску Амбасаду телефоном 2011. године са понудом да им прода податке у вези са британском флотом нуклеарних подморница.

Лични фактори:

- бес
- компулзивно/деструктивно понашање
- освета уперена против организације у којој ради

Фактори на радном месту:

- средина коју карактеришу кадровска редукција и отпуштања

Знаци активног инсајдера:

- проблеми у понашању на радном месту

Даниел Џејмс (УК) је преводилац генерала Ричардса, командата Међународних снага за безбедносну помоћ (ИСАФ) у Авганистану. Огорченост и одбачност због неуспелог унапређења и расизма навели су га да открије Ирану податке у вези са НАТО трупама.

Лични фактори:
- Похлепа
- Подељена лојалност
- Освета организацији

Фактори на радном месту:
- Лако склањање заштићеног материјала

Знаци активног инсајдера:
- Проблеми у понашању на радном месту
- Разочараност радним местом / каријером

Едвард Џозеф Сноуден, бивши је радник ЦИА, који је радио као саветник за NSA (National Security Agency USA). Сноуден је изазвао велику контроверзу када је у јавност изнео тајне документе који су показали постојање великог броја тајних пројеката надзирања, као на пример, PRISM и Baundles informant и документе који показују да су САД спроводиле хакерске нападе у рачунаре широм света, између осталог и у току састанка Г-20 у Лондону 2009. године, у Хонгконгу и Кини. Сноуден је предао документе новинарима Гардијана и Вашингтон поста, у јуну 2013.

Сноуден је након објављивања докумената ЦИА-е, пребегао најпре у Хонгконг, а касније у Москву, 23. јуна 2013. где га је дочекао дипломатски аутомобил који је вероватно припадао Еквадору. Сноуден је добио помоћ од организације Викиликс и њеног оснивача Џулијана Асанжа. Након што му је већи број држава одбио дати азил, 6. јула 2013. године Венецуела је понудила азил Сноудену. Међутим 1. августа 2013. године азил је добио од Русије, где је касније добио и држављанство.

Лични фактори:
- Незадовољан
- Комплекс више вредности
- Арогантан

Фактори на радном месту:
- Лоше урађена безбедносна провера
- Лако склањање заштићеног материјала
- Успешно заобилажење безбедносних процедура

Знаци активног инсајдера:
- Проблеми у понашању на радном месту
- Разочараност радним местом / каријером
- Подељена лојалност

Један до најпознатијих сајтова за трговину поверљивим информацијама компанија је **Kick Ass Marketplace**.

Он се налази на „пијаци“ Dark Weba, месту на коме можете продати и купити готово све – од нарокотика до алата за експлоатацију, малвера и украдених података.

Kick Ass Marketplace нуди корисницима претплату која се креће и до једног Bitcoina месечно (тренутно вреди око $1.105) како би им омогућила приступ различитим „провереним и тачнинм“ инсајдерским информацијама на сајту.

Сваком посту се додељује „рејтинг поузданости“ уз савет да ли купити или продати акције у компанији и на тај начин остварити зараду од инсајдерских информација.

Поред продаје поверљивих информација, неки запослени сарађују са хакерима у операцијама **убацивања малвера у мрежу организације**.

Откривен је и случај да је хакер у сарадњи са инсајдерима убацио малвер директно у мрежу банке. Овај приступ умањује трошкове и напоре јер хакер не мора да спроводи phishing технике, а може да заобиђе нивое одбране (npr. анти-вирус и sandbox). Откривен је и случај хакера који је био спреман да плати седмоцифрену суму недељно (у доларима) инсајдеру који би му омогућио приступ рачунару банке.

Бројни инсајдерски сајбер напади се дешавају сваке године, али огромна већина не стигне до вести. Било је, међутим, инсајдерских претњи у сајбер безбедности које су се истакле последњих година.

- У 2018. години, Фејсбук је отпустио инжењера безбедности оптуженог да је искористио привилеговане информације које му је његов положај дао за ухођење жена на на мрежи.
- У 2018. години, запослени у Тесли је наводно саботирао системе компаније и слао власничке информације трећим лицима.
- У упаду података Цапитал Оне 2019., бивши инжењер Амазона је преузео више од 100 милиона података о клијентима. Искористио је своје унутрашње знање Амазон ЕЦ2 да заобиђу погрешно конфигурисани заштитни зид на серверу у облаку Цапитал Оне.
- Године 2020., бивши извршни директор Гугла осуђен је на 18 месеци затвора због крађе пословних тајни из Гугловог одељења за самовозеће аутомобиле и предао их Уберу, свом новом послодавцу.
- На почетку пандемије ЦОВИД-19, незадовољни бивши радник компаније за медицинско паковање користио је претходно креирани администраторски налог да постави лажни нови кориснички налог, а затим променио хиљаде датотека на начин који би одложио или зауставио испоруке личних заштитну опрему болницама и здравственим радницима (веза се налази изван ибм.цом).
- У 2022. један радник Твитера је ухапшен јер је слао приватне информације корисника Твитера званичницима Краљевине Саудијске Арабије и саудијске краљевске породице у замену за мито (линк се налази изван ибм.цом). Према

америчком Министарству правде, запослени „...поступао је у тајности као агент стране владе који је циљао на гласове неслагања“.

- Кока Кола: Истражитељ је открио да је запосленик Кока Коле копирао податке о око 8000 запослених на лични екстерни чврсти диск. Након што је Кок Кола сазнала за кршење безбедности података, организација је обавестила запослене и понудила бесплатно праћење стања њихових кредита на годину дана.
- СунТруст Банка: Бивши запосленик СунТруста украо је 1,5 милиона имена, адреса, бројева телефона и стања рачуна за клијенте банке. Другим осетљивим подацима није се приступало, али су представљали ризик за банку и њене клијенте.

ИНСАЈДЕРСКИ ПОКАЗАТЕЉИ

Већина безбедносних алата за праћење претњи фокусира се на анализу података о мрежи, рачунару и апликацијама, а придаје мало пажње акцијама овлашћених особа које би могле да злоупотребе свој привилеговани приступ.

За поуздану сајбер одбрану од инсајдерских претњи, морате да пазите на понашање запослених и њихове дигиталне активности.

Инсајдерске претње се манифестују на различите начине:

- насиље,
- шпијунажа,
- саботажа,
- крађа и
- сајбер напади

Насиље – Ова радња укључује претњу насиљем, као и друга претећа понашања која стварају застрашујуће, непријатељско или увредљиво окружење.

- **Насиље на радном месту/организационо насиље** је свака радња или претња физичким насиљем, узнемиравањем, сексуалним узнемиравањем, застрашивањем, малтретирањем, увредљивим шалама или другим претећим понашањем од стране сарадника или сарадника које се дешава у радном месту или док особа ради.
- **Тероризам** као инсајдерска претња је незаконита употреба или претња насиљем од стране запослених, чланова или других блиско повезаних са организацијом, против те организације. Циљ тероризма је промовисање политичког или друштвеног циља.

Шпијунажа – је прикривена или недозвољена пракса шпијунирања за потребе стране владе, организације, ентитета или особе ради добијања поверљивих информација ради војне, политичке, стратешке или финансијске користи.

- **Економска шпијунажа** је тајна пракса прибављања пословних тајни од стране страних компанија или друге државе (нпр., сви облици и врсте финансијских, пословних, научних, техничких, економских или инжењерских информација и метода, техника, процеса, процедура, програма или кодова за производњу).
- **Државна шпијунажа** је тајна активност прикупљања обавештајних података једне владе против друге ради добијања политичке или војне предности. То такође може укључити шпијунирање владе(а) корпоративних ентитета као што су аеронаутичке фирме, консултантске фирме, истраживачки центри или компаније за производњу муниције. Државна шпијунажа се такође назива прикупљањем обавештајних података.

Саботажа – описује намерне радње којима се наноси штета физичкој или виртуелној инфраструктури организације, укључујући непоштовање процедура одржавања или ИТ, контаминирање чистих простора, физичко оштећење објеката или брисање кода ради спречавања редовних операција.

- **Физичка саботажа** је предузимање намерних радњи које имају за циљ наношење штете физичкој инфраструктури организације (нпр. објектима или опреми).
- **Виртуелна саботажа** је предузимање злонамерних радњи помоћу техничких средстава да поремети или заустави нормално пословање организације.

Крађа – је чин противправног присвајања имовине, било покретних ствари, новца или интелектуалне својине.

- **Финансијски криминал** је неовлашћено узимање или незаконито коришћење новца или имовине неке особе, предузећа или организације са намером да се од тога извуче корист.
- **Крађа интелектуалне својине** је крађа или незаконита употреба идеја, изума или креативних израза појединца или организације, укључујући пословне тајне и власничке производе (патенте, лиценце, робне ознаке...), чак и ако концепти или предмети који се краду потичу од лопова.

Сајбер претња укључује крађу, шпијунажу, насиље и саботажу свега што је повезано са технологијом, виртуелном стварношћу, рачунарима, уређајима или интернетом.

- **Ненамерне претње** су незлонамерно (често случајно или ненамерно) излагање ИТ инфраструктуре, система и података организације које наноси ненамерну штету организацији. Примери укључују фишинг е-поруке, лажни софтвер и „злонамерно оглашавање“ (уграђивање злонамерног садржаја у легитимно онлајн оглашавање).
- **Намерне претње** су злонамерне радње које изводе злонамерни инсајдери који користе техничка средства да поремете или зауставе редовне пословне операције организације, идентификују ИТ слабости, добију заштићене информације или на други начин унапреде план напада путем приступа ИТ системима. Ова радња може укључивати промену података или уметање злонамерног софтвера или других делова увредљивог софтвера да би се пореметили системи и мреже.

Дигитални индикатори

- Пријављивање у пословне апликације и мреже у неуобичајеним временима. На пример, запослени који се, без упита, пријављује на мрежу у 3 сата ујутро може бити разлог за забринутост.
- Пораст обима мрежног саобраћаја. Ако неко покушава да копира велике количине података широм мреже, видећете необичне скокове у мрежном саобраћају.
- Приступ ресурсима које обично немају или им није дозвољено.
- Приступ подацима који нису релевантни за њихову радну функцију.
- Поновљени захтеви за приступ системским ресурсима који нису релевантни за њихову радну функцију.
- Коришћење неовлашћених уређаја као што су USB уређаји и CD дискови.
- Прикривено коришћење мреже и намерна претрага осетљивих информација.
- Слање осетљивих информација е-поштом ван организације.

Индикатори понашања запослених

Постоји неколико различитих индикатора инсајдерске претње на које треба обратити пажњу, укључујући:

- Незадовољан запосленик, извођач радова, подуговарач или партнер.
- Константни покушаји заобилажења безбедносних процедура.
- Редован рад ван радног времена.
- Показивање огорченост према другим запосленим и сарадницима.
- Рутинско кршење организационих политика.
- Размишљање о оставци или разговарање о новим пословниим приликама.

СТРЕС НА РАДНОМ МЕСТУ

Стрес је скуп неспецифичних реакција човековог организма на штетне факторе из радног окружења:

- превише прековремених сати рада,
- кратки рокови извршења радних задатака,
- лоше понашања руководиоца - шефа,
- напет однос са колегама,
- лоша радна атмосфера,
- стални притисак или превише посла,
- несигурности радног места.

Код неких ће ове и сличне ситуације изазвати више или мање стреса.

Потенцијалне понашајно психолошке манифестације:

- Фрустрација
- Бес (пасивни и агресивни)
- Трач
- Злоупотреба права
- Повреде радне обавезе

Фрустрација или **осујећеност** је стање лишености човека да задовољи неки, у довољној мери активан мотив који је било по субјективној, било по објективној оцени за једну личност веома важан.

Људи на различите начине реагују када не могу да задовоље своје мотиве што све зависи од њихове фрустрационе толеранције. Што је човек фрустрационо толерантнији он лакше подноси неуспехе у задовољавању својих мотива, а ако је мање фрустрационо толерантан он се тешко мири и са најмањим неуспехом.

Уколико наступи стање фрустрираности човек може реаговати:

- **Реалистички**, тако што ће да тражи рационално решење проблема или променом понашања или променом циља и

- **Нереалистички**, када проблем решава пребацујући узроке немоћи на друге људе или агресивним понашањем.

Дуготрајно стање фрустрираности има за последицу дезорганизовано понашање и најчешће, анксиозност тј. осећање неспокојства, несигурности, тескобе и неодређеног страха. На тај начин се угрожава човеково ментално здравље.

Трач је реч немачког порекла и означава:

- Оговарање,
- Олајавање,
- Клеветење, па и
- Брбљање.

Користе се и термини трачарење (трачање) и „трач партија“. Трачарење је уобичајен начин разговора и тешко га је избећи у свакодневном животу, али је у већини случајева безопасан. Чак, може бити и забаван, а и погодан да се научи понешто о себи и другима. Такође, циљ трача може да буде и повећање угледа, да одређеној особи да на значају и привуче пажњу.

Ипак, постоје и негативне последице. Уколико се трач користи као освета или претња, има сврху да омаловажи, заплаши или подстакне на насиље на националној, верској, родној, сексуалној или некој другој основи. Истраживања су показала да су трачу склоније особе женског пола и то се објашњава тиме што трач представља посредан облик агресивности (мушке особе, наиме, радије посежу за директнијим облицима агресије). Такође, женске особе су усмерениje на пријатеље, емоционално су им важнији, па користе такве облике насиља који могу да доведу до раскидања пријатељства и избацивање из социјалних група.

Нпр. родитељима чија су деца жртве трачева се препоручује да разговарају са децом о томе, помогну им саветима како да се поставе и да им буду подршка.

Бес је емоција проистекла из нечије психолошке интерпретације услед вређања, повређивања или пак одбијања те особе. Увек га прати и снажна жеља за осветом и исправљањем туђих поступака на једнако офанзиван начин.

Појавни облици **пасивног беса**:

- **равнодушност** - употреба лажних и апатичних гестова и фраза, лажни осмеси, слегање раменима, став „нек одлуче други“. Причање о својим фрустрацијама без показаних емоција;
- **Избегавање** - не улажење у расправе и конфликте, окретање леђа приликом кризних ситуација, изражена фобија;
- **Безвредност** - дефитизам, ослањање на непоуздане особе, сексуална импотенција, истицање мање битних ствари и исказивање фрустрације око њих али зато занемаривање оних битнијих.
- **Манипулисање** - изазивање беса у другима а онда давање савета и утеха тим истим особама, „закувавање“ агресије а онда избегавање учешћа у истим,

емотивно уцењивање, лажни изливи туге, уништавање веза, гомилање пара или ресурса;

- **Тајновитост у радњама** - оговарање, нагомилавање озлојеђености и пражњење исте људима иза леђа, избегавање контакта очима, остављање других на „цедилу“, било која форма анонимне критике.
- **Опсесивно понашање** - стална провера стања ствари около, опсесија за чистоћом или перфекцијом, опседнутост дијетама или пак преједање;
- **Кривљење себе** - претерано извињавање за своје понашање, претерана самокритика, усмеравање разговора тако да те други критикују;
- **Саможртвовање** - бити увек од помоћи (преко мере), задовољавање са подређеном позицијом, тихо одавање знакова да патиш али и одбијање помоћи, велика захвалност за обичне ствари.

Појавни облици активног беса:

- **Малтретирање** - насилно понашање, гурање, викање, користећи моћ зарад угњетавања, играјући се са слабостима других;
- **Деструктивност** - уништавање објеката, наношење бола животињама, уништавање односа, агресивна вожња, злоупотреба супстанци;
- **Грандиозност** - хвалисавост, изражавање неповерења, не делегирање, жеља да се буде у центру пажње стално, не слушање других кад причају, очекивање да ће сама помпезност наступа решити све проблеме;
- **Повређивање** – физичко насиље, вербално злостављање, пристрасне двосмислене и вулгарне шале на нечији рачун, рушење поверења, псовање, игнорисање осећања других, намерна дискриминација, неправедно окривљавање и кажњавање других, олако давање етикета;
- **Манично понашање** – пребрзо причање, пребрза вожња, пребрзо ходање, претеривање у раду, и очекивање од других да прате овај темпо;
- **Себичност** – игнорисање туђих потреба, одбијање захтева за помоћ.
- **Претње** – отворено застрашивање људи и показивање на примерима на који начин им можете нанети штету или повреде, упирање прстом, „ломљење“ руку приликом разговора (гест), ношење одеће и симбола који се доводе у везу са насилним понашањем, честа употреба сирене у колима, лупање вратима;
- **Неправедно окривљавање других** – оптуживање других за своје грешке, кривити околину за своја осећања, често изношење оптужби;
- **Непредвидљивост** – експлозивност особе услед малих фрустрација, напада на друге неселективно, издавање неправедних казни и наношење штете другима због тога, коришћење алкохола и психоактивних супстанци, излагање нелогичних аргумената;
- **Осветољубивост** – бити веома прек у кажњивању, одбијање да се опрости и заборави некоме ко нам је нанео зло и често преувеличавање размера тог дела, стално понављање и навођење болних сећања из прошлости.

Злоупотреба права је санкционисана у домаћој судској пракси, односно сви видови злоупотребе (који нису стриктно уређени законом) обухваћени су општим правним

начелом забране злоупотребе права, као непружање правне заштите злоупотреби права, које код нас важи као неписано правно начело, прихваћено у судској пракси и литератури.

ДА ЛИ ЈЕ ТО БАШ ТАКО?

Шиканозно понашање:

- У ужем смислу подразумева специфично понашање особе само да би другом нашкодило или првенствено зато;
- У ширем смислу, лице има још неки допуштени мотив за вршење радње али је мање важан од намере шкођења, а ова намера није ограничена на намеру нанети штету имовинску или неимовинску, него обухвата и намеру сметње (циљ шкођења приоритет).

Бескорисно понашање – ако лице нема никаквог оправданог интереса или иоле значајног интереса за понашање шкодљиво другоме.

Услови за постојање овог вида злоупотребе су:

- помањкање или
- безначајност интереса.

Несразмерно понашање – служи задовољењу интереса чија је важност минимална када се пореди са шкођењем другом, односно, вредност интереса који се понашањем остварује несразмерно је мања од вредности интереса којим се шкоди.

Непримерено понашање – је оно којим се остварује интерес (који нити је неоправдан, ни безначајан, ни несразмерно мање вредан од интереса коме се шкоди, ни такав да неко одређено субјективно право не би могло да му служи), ако би интерес могао да се оствари другачијим понашањем, а да се другом не нашкоди или да се нашкоди мање.

Противциљно понашање – када се лице шкодећи другоме позива на неко субјективно право мада је његово дотично понашање неспојиво са циљем тог права.

Ако неко шкодећи другоме остварује интересе који се не могу протумачити као циљеви чијем је остварењу намењено одређено право, тада то понашање не може ни да се оправда тим правом јер је право само средство за циљ, па ако то није циљ коме право служи неумесно је и позивање на то право.

Кверулантско понашање – злоупотреба права на подношење притужби, поднесака и слично. Када се лице у намери да нашкоди другоме позива на неко право у писменој форми, односно када констатно подноси притужбе на рад неких лица, тражење права на увећање плате позивајући се на конкретан случај и слично. Кверулант је тужибаба, онај који пати од тога да стално неког тужака, односно у правном смислу предавалац тужбе суду.

Злоупотребу права на заштиту од злостављања, у смислу Закона о спречавању злостављања на раду, чини запослени који је свестан или је морао бити свестан да не постоје основани разлози за покретање поступка за заштиту од злостављања, а покрене

или иницира покретање тог поступка са циљем да за себе или другог прибави материјалну или нематеријалну корист или да нанесе штету другом лицу (чл 11 ст 3 овог закона)

Члан 13. Закона о слободном приступу информацијама од јавног значаја каже:

...Орган власти неће тражиоцу омогућити остваривање права на приступ информацијама од јавног значаја ако тражилац злоупотребљава права на приступ информацијама од јавног значаја, нарочито, ако је тражење неразумно, често, када се понавља захтев за истим или већ добијеним информацијама или када се тражи превелики број информација.

Члан 83. Закона о јавном информисању и медијима (право на одговор)

... Лице на које се односи информација, која може да повреди његово право или интерес, може од одговорног уредника захтевати да, без накнаде, објави одговор у коме оно тврди да је информација неистинита, непотпуна или нетачно пренета.

Ако одговорни уредник не објави одговор, а за то не постоји неки од разлога за необјављивање одређен овим законом, као и ако одговор објави на непрописан начин, ималац права на одговор може против одговорног уредника поднети тужбу за објављивање одговора. У парници ради објављивања одговора расправља се само о чињеницама, одређеним овим законом, од којих зависи обавеза одговорног уредника да објави одговор.

Правилник о раду као и уговор о раду треба да дефинишу све могуће ситуације у вези са овом повредом јер Закон о раду не дефинише све могуће ситуације већ само неке опште случајеве, који треба да буду разрађени и прецизно дефинисани од стране свих организација засебно. Неки од примера повреде радне обавезе су:

- одавање важних информација компаније,
- напуштање радног места неовлашћено,
- непоступање по упутствима послодавца и претпостављених,
- немарно и несавесно извршавање радних обавеза,
- неоправдано одсуство...

Индикатори у контексту – критични пут

ЛИЧНЕ ПРЕДИСПОЗИЦИЈЕ	СТРЕСОРИ	ПРОБЛЕМАТИЧНО ПОНАШАЊЕ	НЕОДГОВАРАЈУЋИ ИЛИ НЕПОСТОЈЕЋИ ОРГАНИЗАЦИЈСКИ ОДГОВОРИ
• Здравствене/психијатријске • Поремећаји личности • Личност и друштвене вештине • Претходна кршења правила • Ризици друштвених мрежа	• Лични/породични • Професионални • Финансијски	• Интерперсонално • Технолошко • Безбедносно • Финансијско • Друштвене мреже • Путовања • Лично	• Нормативни • Персонални • Руководећи • Заштита података

НЕПРИЈАТЕЉСКИ АКТ И ПОНАШАЊЕ
- шпијунажа; саботажа; тероризам; криминал; сајбер...

ЦИЉЕВИ ИНСАЈДЕРСКИХ НАПАДА

Инсајдерска опасност је својим деловањем углавном усмерена ка:

- Неовлашћеном коришћењу штићених података којима располаже организација (ТАЈНИ ПОДАЦИ, ИНТЕЛЕКТУАЛНА СВОЈИНА, ПОСЛОВНЕ ТАЈНЕ, ПРОФЕСИОНАЛНЕ ТАЈНЕ, ЛИЧНИ ПОДАЦИ, ПОДАЦИ О СУДСКИМ И ДРУГИМ ПОСТУПЦИМА);
- Наношењу материјалне и нематеријалне штете организацији (намерно и ненамерно);
- Стварању лоше радне атмосфере и незадовољства, хоризонталног мобинга, генерално лоше слике о организацији....

Под појмом заштићени подаци подразумевају се следеће категорије:

- **тајни подаци** (национални, ЕУ, НАТО, добијени на основу билатералних споразума...)
- **интелектуална својина** - проналасци, патенти, пословне тајне
- **лични подаци** (нарочито осетљиви подаци о личности, подаци о руководиоцима, кадровски подаци, здравствено стање...)
- **подаци о набавкама** и пословима
- **професионалне тајне** – однос клијент експерт
- **подаци о поступцима** (дисциплинским, пореским судским и осталим поступцима)...
- **информације о организацији**, ИКТ системима, кадровско-персоналној проблематици...

Посебно питање представља тзв. “ИНСАЈДЕРСКА ТРГОВИНА” (insider trading), односно асиметричност доступности информацијама када је у питању трговина са хартијама од вредности.... Инсајдерску информацију чине све информације које нису обелодањене а односе се на тржиште хартија од вредности.

Ова појава је у банкарском и финансијском пословању строго санкционисана!

Амерички државни тужиоци подигли су оптужнице против бивђег радника компаније "Фајзер" (Pfizer), шефа полиције савезне државе Масачусетс, бившег директора једне фармацеутске комапније, као и инвеститора у медијску компанију Доналда Трампа у више одвојених случајева инсајдерског трговања, односно, због злоупотребе поверљивих информација за трговину на берзи, у склопу широке акције против наводне корупције на јавним тржиштима.

Канцеларија државног тужиоца на Менхетну оптужила је 10 особа за превару са хартијама од вредности и друга кривична дела, у којима је, како се наводи, трговањем поверљивим информацијама украдено укупно 30 милиона долара.

Под термином наношење штете подразумевају се следеће активности:

- физичко уништавање алата, возила, просторија, опреме, технике, ИКТ система, канцеларијског материјала;
- компромитација штићених података и неовлашћена употреба

- блокирање рада информационо-телекомуникационих система и других система везе;
- изношење информација у средствима јавног информисања којима се може нанети штета угледу и пословању организације;
- оговарање, трачарење и преношење неистинитих гласина лицима од утицаја која нису у саставу организације....
- **Шпијунажа** – за стране државе или компаније
- **Имовински криминалитет** (крађе, утаје, преваре, проневере средстава....)
- **Криминалитет "белог оковратника"** (корупција, замена редоследа услуга, чињење услуга одређеним људима, злоупотреба службеног положаја....)
- **Привредни криминалитет** (кривична дела против привреде – оштећење повериоца, злоупотреба монополистичког положаја, недозвољена производња и трговина....)
- **Сајбер криминал** (engl. Cyber crime) представља облик криминалног понашања, код кога се коришћење компјутерске технологије и информационих система испољава као начин извршења кривичног дела, где се компјутер или рачунарска мрежа употребљавају као средство или циљ извршења.

Конвенција о високотехнолошком криминалу Савета Европе прави разлику између четири различите врсте кривичних дела:

- Дела против поверљивости, интегритета и доступности компјутерских података и система – њих чине незаконити приступ, пресретање, уплитање у податке или системе, коришћење уређаја (производња, продаја, увоз, дистрибуција), програма, лозинке;
- Дела везана за компјутере – код којих су фалсификовање и крађе најтипичнији облици напада;
- Дела везана за садржаје – дечја порнографија је најчешћи садржај који се појављује у овој групи обухватајући поседовање, дистрибуцију, трансмисију, чување или чињење доступним и расположивим ових материјала, њихова производња ради дистрибуције и обрада у компјутерском систему или на носиоцу података;
- Дела везана за кршење ауторских и сродних права обухватају репродуковање и дистрибуцију неауторизованих примерака дела компјутерским системима

Појавни облици инсајдерског понашања:

- константно испољавање личног незадовољства због радног статуса, положаја, плате, паркинг места, понашања осталих запослених....
- дволичност у комуникацији према руководству и према колегама....
- константно писање службених белешки (кверуланстко понашање), извештаја и дописа унутар организације и ка другим органима јавне власти....
- не прихватање одговорности за пропусте у раду и константно окривљавање других за своје грешке

- константно исказивање незадовољства условима рада, просторијама, намештајем, нормативом организације
- пружање отвореног отпора руководству, ометање радног процеса, незаинтересованост....

Помињање термина мобинг је све чешће у радним окружењима, при чему је поред **вертикалног мобинга** на који се позива већина запослених који су поднели тужбу за мобинг, за једну организацију изузетно опасно, ако не и опасније постојање **хоризонталног мобинга**.

Хоризонтални мобинг најчешће је присутан као појава шиканирања између радника на једнаком положају у хијерархијској организацији. Осећај угрожености једног или групе радника, љубомора и завист могу да подстакну жељу да се елиминише неки сарадник из колектива (доскорашњи пријатељ) поготову ако постоји услов да његова елиминација води напретку у каријери. Жртва ове врсте мобинга често може бити радник који се истиче по квалитету и привржености послу и радним задацима, већој плати и бројним наградама и похвалама.

Хоризонтални мобинг је и кад читава група радника због унутрашњих проблема, напетости и љубоморе, изабере једног радника, жртву, на којој желе да докажу да су снажнији и способнији.

КАРАКТЕРИСТИКЕ ИНСАЈДЕРА

Иако су понашања сваког инсајдера појединачно специфична, ипак се могу издвојити поједине карактеристике које су заједничке за сва инсајдерска понашања:

- увек теже да се ствари раде онако како они мисле да треба и једино им је њихова "победа" на памети;
- амбициозни су кад се ради о стицању моћи и доминацији над другима;
- увек теже да буду они који су горе и да контролишу друге;
- користе цео један арсенал суптилних и ефикасних стратегија како би задобили предност у међуљудским односима;
- могу да буду веома културни, шармантни и заводљиви;
- знају како да добро изгледају и како да побеђују, "отапајући" нашу одбрану;
- знају шта ће вам рећи како бисте заборавили на онај свој "осећај у стомаку" који вам говори да им нипошто не верујете, а онда им дали све оно што они желе.
- могу да буду бескрупулозни, подмукли и осветољубиви борци;
- знају како да капитализирају на свакој човековој слабости а појачаће своју агресивност уколико примете да сте посрнули;
- знају како да ухвате човека у моменту кад је он несвестан и неприпремљен;
- уколико сматрају да сте их у нечему надмашили или да сте добили више од њих, они ће то покушати да преокрену у своју корист или да вам се освете;
- битку не сматрају завршеном све док они не победе;
- ако се одлуче на освету према организацији, не постоји ништа што може да их кочи;
- знају да разликују исправно од погрешног, али не допуштају ничему да им стоји на путу до онога што желе;
- према њима, циљ увек оправдава средство;
- склони су да варају друге у вези онога што стварно раде.

Уколико се открију инсајдерске активности, често прибегавају обраћању јавности директно, приказујући себе као:

- жртве руководства,мобинга, сексуалних и других разлика
- борце против криминала,
- заштитнике људских права и демократије
- сараднике Викиликса

Понекад објављују и своја инсајдерска искуства у форми мемоара и филмова

„ЛИСТА ЗА ПРОВЕРУ“

Инсајдери су често добри стратези, али ипак на основу неких случајева у пракси и конкретних догађаја описаних у медијима, направљена је листа описаних карактеристика које су својствене инсајдерима, тзв. Инсајдерска чек-листа за проверу, уз напомену да је ипак сваки човек особен за себе и да се сваком случају мора прићи појединачно....

- **Слаткоречивост и површински шарм** – тенденција ка милозвучности и углађености; привлачност, шармантност; глаткост и течност говора.
- **Грандиозна самовредност** – један увелико „надуван“ поглед на своје способности са претераним самопоуздањем, јака тврдоглавост, самоувереност и хвалисање.
- **Неосетљивост и недостатак емпатије** – недостатак осећања према људима уопште; хладни, презриви, безобразни, безобзирни и нетактични.
- **Патолошко лагање** – може бити умерено или претерано; у умереној форми они ће бити лукави, препредени, превејани, тајанствени и бистри; у екстеремној форми, они ће бити варалице, лажови, подмукли, бескрупулозни, манипулативни и непоштени.
- **Варање и манипулација** – користе се обманама, склони су свакој врсти преваре или обмањивања других како би стекли неку личну корист.
- **Паразитски животни стил** – једна намерна, манипулативна, себична и експлоататорска финансијска зависност од других која се одражава недостатаком њихове мотивисаности, ниском самодисциплином и неспособношћу да започну или испуне своје обавезе.
- **Слаба контрола понашања** – изражавање иритације, досаде, нестрпљивости, претње, агресивности или вербално вређање других; недовољна контрола љутње и темперамента; понашају се пренагљено.
- **Недостатак реалних дугорочних циљева** – неспособност или стални неуспех код доношења и извођења дугорочних планова и циљева; номадска егзистенција, бесциљност, недостатак животног смера.
- **Неспособност за преузимање одговорности за властите поступке** – неспособност преузимања одговорности за властите поступке, као резултат недостатка савести; недостатак преданости на послу, антагонистичка манипулација, негирање своје личне одговорности и покушавање манипулације других.
- **Импулсивност** – испољавање поступака без предумишљаја и недостатак рефлекције и планирања; неспособност одолевања искушењима, контролисања нагона и фрустрације; недостатак промишљености и узимања у обзир могућих последица својих поступака; лудо одважни, непредвидљиви, нестални и несмотрени.
- **Неодговорност** – нису у стању да испуњавају или испоштују своје обавезе, као нпр. код плаћања рачуна и враћања дугова; аљкави су на послу, често одсуствују с посла; не испуњавају на време уговорене послове.

- ЛОША ФИНАСИЈСКА СИТУАЦИЈА (ПРЕЗАДУЖЕНОСТ)
- НЕЗАДОВОЉСТВО ЛИЧНИМ И ПОРОДИЧНИМ ЖИВОТОМ
- ПОСТОЈАЊЕ ОЗБИЉНИХ ЗДРАВСТВЕНИХ ПРОБЛЕМА У ПОРОДИЦИ
- НЕЗАДОВОЉСТВО ПОЛОЖАЈЕМ У ОРГАНИЗАЦИЈИ
- ПРОБЛЕМИ У КОМУНИКАЦИЈИ СА РУКОВОДСТВОМ И СА КОЛЕГАМА
- БЕЗБЕДНОСНО ИНТЕРЕСАНТНИ КОНТАКТИ

„ПРЕВЕНЦИЈА“

Потребно је идентификовати највредније информације:

- Штићене податке - Информације постоје у форми докумената (физичких или виртуелних, класификоване у складу са прописима), као изворни код, у мејловима, код људи (да, људи су ти који поседују кључне информације које нису садржане у документима)...

Потребно је поставити једноставно питање:

- Ако се нешто догоди са одређеном информацијом – штићеним податком, да ли се пословање може несметано наставити?
- Ако је одговор да, онда тај ресурс није критичан. Потребно је применти најјачу заштиту на највредније – критичне податке и за њих применити најфрекветнији мониторинг.

Превентивно и проактивно, а не репресивно и реакционо, деловање би требало да буде сврха сваког менаџмента у супротстављању инсајдерских активности.

На жалост, за сада су репресивно и реакционо деловање стандард у пракси!

Проактивно управљање инсајдерским претњама може зауставити путању или променити ток догађаја од штетног исхода до ефикасног ублажавања. Организације управљају инсајдерским претњама путем интервенција које имају за циљ да смање ризик који представља забрињавајућа особа. Организација мора имати на уму да су превенција инцидента инсајдерске претње и заштита организације и њених људи крајњи циљеви.

На том плану треба предвидети и обухватити следеће елементе:

- Напори на откривању и спречавању
- Мере и радње за спречавање неовлашћених активности
- Чињенице
- Стратегија
- Култура безбедности информација
- Изазови и тешкоће.

Напори на **откривању и спречавању** подразумевају:

- праћење недозвољених сајбер активности
- пажљиво праћење/посматрање запослених укључујући и циљане опсервације
- идентификовање показатеља незадовољства запосленог/их

Радње за **спречавање неовлашћених активности** су:

- дефинисање и примена ограничења за приступ заштићеним подацима
- откривање
- одвраћање/застрашивање
- ублажавање/смањивање
- одговор/реакција на неовлашћену активност

Елементи добре **Стратегије** су:

- успоставити ниво критичности (одговарајући степен заштите/тајности);
- успоставити поверење/поузданост (кроз процес провере, инспекције...);
- оснажити праксу у вези са персоналном безбедношћу и управљањем;
- заштити информациона средства;
- открити проблеме;
- реаговати/правовремено одговорити на изазове и претње.

Чињенице:

- потребно је развити културу безбедности информација
- политике и праксе су, у најмању руку, исто тако важне као технички механизми
- садашњи степен свести није у сразмери са озбиљношћу претње
- безбедносна обука у вези са инсајдерском претњом још увек није добила пажњу коју заслужује
- **59% запослених када напушта организацију је признало да носи са собом и власничке информације – интелектуалну својину (САД – ФБИ)**
- потребно је развити пословни морал и етику у мери којој је то могуће и радити констатно на подизању опште радне атмосфере (“рад са осмехом”)
- радити констатно на развоју и имплементацији етичког кодекса иако је он најчешће још један од норматива на “дугачкој” листи
- потребно је радити на подизању ефикасности дисциплинских и других поступака у организацији

Култура безбедности информација предвиђа:

- поштовање законски прописаних минималних стандарда за безбедносне едукације, информисање и програме обуке у вези са инсајдерском претњом;
- кадровско управљање и персоналну безбедност;
- обједињавање основних материјала за обуку из информационе безбедности у јединствени електронски извор који би третирао инсајдерску претњу и био доступан свим овлашћеним корисницима;
- спровођење истраживања о средствима за реаговање у случају сумње на злонамерну инсајдерску активност;
- процену расположивих технологија за бављење инсајдерском претњом;
- израду базе података у вези са инсајдерским инцидентима, карактеристикама, поукама из претходног искуства и статистикама

Пракса САД, када су у питању тајни подаци Владе и поверљиви уговори, је показала да су инсајдери који се баве шпијунском делатношћу за друге државе откривени на основу:

1. Рутинске контраобавештјне контроле и мониторинга;
2. Пријава од стране пријатеља, породице и пословних сарадника;
3. Грешака у шпијунској делатности;

4. Добијањем информација преко обавештајне мреже САД и од страних обавештајних служби.

Изазови и тешкоће:

- ко је одговоран за инсајдерску претњу?
- стална процена претње;
- умањивање осетљивости критично важних средстава;
- проналажење нових контрамера;
- унапређивање функционисања дисциплинских и других структура;
- систем едукација.

Успешни програми за сузбијање инсајдерских претњи проактивно користе приступ ублажавања откривања и идентификовања, процене и управљања ризицима а заштите своје организације. Основа успеха програма је рано откривање и опсервација и посматрање стања запослених, у вези са понашањем или активностима.

Откривање и идентификација претњи је процес којим особе које би могле представљати ризик од инсајдерске претње због свог уочљивог понашања у вези са понашањем привлаче пажњу организације или тима за инсајдерске претње. Откривање и идентификовање потенцијалних инсајдерских претњи захтева и људске и ехнолошке елементе. Особље организације је непроцењив ресурс за посматрање понашања које изазива забринутост.

Док ће практично свака особа доживети стресне догађаје, већина то чини без прибегавања ометајућим или деструктивним радњама. За оне инсајдере који се окрећу злонамерним активностима, истраживачи су открили да су дела ретко спонтана; уместо тога, обично су резултат намерне одлуке да се делује.

Процена претње за инсајдерску претњу је процес прикупљања и анализе информација о особи од интереса која може имати интерес, мотив, намеру и способност да нанесе штету организацији или лицима.

Процена претњи за умањење инсајдерске претње је јединствена дисциплина која захтева тим посебно образованих и обучених појединаца да процени особу од интереса и одреди обим, интензитет и последице потенцијалне претње.

Ове процене се заснивају на понашању, а не на профилима, а понашања су променљиве природе. Циљ процене је спречавање инсајдерског инцидента, било намерног или ненамерног. Не постоји јединствени приступ процени. Свака процена треба да буде прецизна, темељна и спроведена у складу са организационим смерницама и важећим законима. Стратегије интервенције треба да буду усмерене на помоћ особи која је забринута, док истовремено раде на ублажавању потенцијалних ефеката непријатељског чина. Када процена сугерише да особа у питању има интерес, мотив и могућност да покуша реметилачки или деструктивни чин, тим за управљање претњама треба да препоручи и координира одобрене мере за континуирано праћење, управљање и ублажавање ризика од штетних радњи потенцијалног инсајдера.

Процена ризика:

- идентификација опасности,
- одређивање критичних контролних тачака за контролу било које опасности,
- успостављање система надгледања.

Процена ризика:

- **висок** – настанак неотклоњиве тешке штете
- **средњи** – настанак тешке штете
- **низак** – настанак штете за рад, обављање делатности

ПАРАНОЈА. САМО ЈЕДНОМ МОРАТЕ БИТИ У ПРАВУ ДА БИ СВЕ ТО БИЛО ВРЕДНО ТРУДА

СТУДИЈА СЛУЧАЈА СРБИЈА

ГОРАН МИЛОШЕВИЋ

- Радник ЈП «Путеви Србије»
- Открио малверзације у наплати путарине, којима је држава оштећена за 6,5 милиона евра...

Последице:

- 41 особа осуђена на казне затвора у тајању од 141 годину,
- Милошевић је након тога остао без посла, да би после био враћен на посао...

МОМЧИЛО ПЕРИШИЋ

Године 1991, када су избили ратови у бившој СФРЈ, Перишић је био на дужности команданта Артиљеријског школског центра у Задру.

За начелника Генералштаба ВЈ именован је 29. августа 1993. године. На тој дужности био је до 24. новембра 1998. године. Активна војна служба му се завршила 17. марта 1999. године.

Био је један од лидера Демократске опозиције Србије.

Након промена 2000. године, и избора нове Владе Србије, јануара 2001. године, Перишић је изабран за једног од потпредседника Владе коју је предводио Зоран Ђинђић.

Марта 2002. године, Перишић је ухапшен у једном мотелу на Ибарској магистрали под оптужбом за шпијунажу у корист САД. Убрзо је поднео оставку на дужност потпредседника Владе.

Марта 2005. године, након што је Хашки трибунал подигао оптужницу против њега којом га терети за ратне злочине почињене у Хрватској и Босни и Херцеговини, Перишић се добровољно предао том трибуналу. Суђење је почело октобра 2008. године.

Дана 6. септембра 2011. године, Хашки трибунал осудио је Перишића на 27 година затвора због злочина који су почињени над Муслиманима у БиХ 1993—1995. и над Хрватима у Хрватској.

Дана 28. фебруара 2013. Жалбено веће Хашког трибунала је ослободило Момчила Перишића по свим тачкама оптужнице

Пред Вишим судом у Београду је у Фебруару 2021. осуђен на три године затворске казне за шпијунажу односно одавање државних тајни званичнику САД током 2002.

Дана 2. фебруара 2022. казна му је повећана на четири године затвора због шпијунаже.

Осуђен је на казну затвора, заједно са Владаном Влајковићем и Миодрагом Секулићем, јер је утврђено да је 14. марта 2002. предао тајне војне податке службенику амбасаде САД Џону Нејбору, који су код њега касније нађени. У ТОКУ ПОСТУПАК ПО ВАНРЕДНИМ ПРАВНИМ ЛЕКОВИМА...

ТАЈНИ ПОДАЦИ

- Реч је о записнику са колегијума Генералштаба, 11. октобра 2001. са ознаком „војна тајна – строго поверљиво" и садржи војне податке. Тај записник је, како је суд утврдио, нађен код Нејбора.

АЛЕКСАНДАР ОБРАДОВИЋ

О случају Александра Обрадовића се скоро већ све зна. Узбуњивач из ваљевске фабрике оружја „Крушик“.

ОДГОВАРА за одавање тајних докумената страној новинарки, за шта је према тврдњама тужилаштва добио материјалну корист.

ИМАО У ПРИВАТНОМ НЕОВЛАШЋЕНОМ ПОСЕДУ ВИШЕ ДЕСЕТИНА ХИЉАДА ДОКУМЕНАТА «КРУШИКА» У ЕЛЕКТРОНСКОМ ОБЛИКУ...

Питање: узбуњивач или инсајдер?

ВЛАДАН ВЛАЈКОВИЋ ВИРАГА

Бивши припадник Војске Југославије, који је крајем деведесетих година XX века достављао црногорским властима достављао обавештајне податке Војске Југославије, а уз помоћ запослених у Генералштабу Војске Југославије...

Ове податке је достављао Вукашину Марашу, тадашњем шефу тајне полиције Црне Горе. После пада Слободана Милошевића, 2003. године, објавио је књигу «Војна тајна», која је тада заплењена а против Влајковића покренут кривични поступак... Књига Војна тајна учињена доступном јавности на основу одлуке Повереника....

ДОСТАВЉАО ЈЕ И ТАЈНЕ ПОДАТКЕ МОМЧИЛУ ПЕРИШИЋУ, ЗБОГ ЧЕГА ЈЕ И ПРАВОСНАЖНО ОСУЂЕН...

У ТОКУ ПОСТУПАК ПО ВАНРЕДНИМ ПРАВНИМ ЛЕКОВИМА

УМЕСТО ЗАКЉУЧКА

Танка је линија између хероја и издајника, шпијуна и патриоте, саботера и борца за демократију, слободе говора и мишљења, дувача у звиждаљку, мобинга, повреда радне дисциплине, инсајдерске опасности, злоупотребе положаја....

Инсајдерској претњи се не придаје одговарајући значај у пракси....

Унутрашње претње нису ништа мање опасне од спољашних претњи....

У пракси је још увек више питања него одговора....

Реаговање после догађаја је правило!!!

Инсајдер је термин који се изузетно широко користи у пракси и то ствара забуну....

Није свака инсајдерска активност криминал (дувач у звиждаљку?)

Потребно је претходно дефинисати шта је:

- Инсајдерска опасност по сваку организацију?
- Коју штету она може нанети?
- Како реаговати у случају појаве инсајдерске опасности?

ПРЕПОРУКЕ - Како реаговати у случају појаве инсајдерске опасности?

- Документовати одређена понашања запослених и дигиталне активности
- Обавити одговарајуће процене могуће штете
- Упутити запосленог на психолошку евалуацију
- Формирати комисију или радни тим
- Предузети мере – дисциплински поступак, прекид радног и уговорног односа, кривична пријава или тужба за накнаду штете...

Проблем инсајдерске претње повезан је са:

- Лојалношћу
- Професионалним и етичким кодексом
- Личним стањима лица потенцијалног инсајдера

У досадашњој светској пракси, имајући у виду штићене податке и информације којима располажу, утврђено је неколико уобичајених структура са високим ризиком од инсајдерских претњи:

- Финансијске услуге
- Телекомуникације
- Техничке услуге
- Здравствена заштита
- Влада и органи јавне власти

ЧОВЕК ЈЕ УВЕК НАЈСЛАБИЈА КАРИКА СВАКОГ СИСТЕМА