Прегледни рад
UDK 005.334:334.72
DOI 10.7251/BLCZB0219205S
COBISS.RS-ID 7634200

ПОСЛОВИ У НАДЛЕЖНОСТИ ФУНКЦИЈЕ КОРПОРАТИВНЕ БЕЗБЕДНОСТИ

Слободан Симовић[1], Михајло Манић[2]

АПСТРАКТ

Основни задатак менаџера безбедности, као одговорног лица за ниво безбедности у компанији и за дешавања у оквиру своје функције је, да организује службу безбедности као и радне функције запослених. Мора да буде рационалан, што подразумева да не сме да дозволи да корпоративна безбедност као функција постане гломазна и скупа по компанију. Сходно овоме, његов приоритетан задатак је идентификовање кључних вредности компаније којима треба посветити највише пажње. Предмет овакве анализе су материјалне и нематеријалне вредности, облици имовине и личности руководиоца који су од великог значаја, те би се њихов губитак одразио погубно за компанију.[3]

Кључне речи: *кључне вредности компаније, професионалност и рационалност, менаџер безбедности, ризик и претња..*

ABSTRAKT

Grundaufgabe des Sichercheitmanagers als der Verantwotlicher für die Sicherheitsstufe im Unternehmen und für die Vorgänge im Bereich seiner Funktion ist: sowie Sicherheitsdienst als auch Arbeitsfunktionen zu organisieren. Er muss vernünftig sein d. h. er darf nicht erlauben dass die Untenehmenssicherheit als eine Funktion schwerfällig und teuer für den Untenehmen wird. Deswegen ist seine erste Aufgabe die Schlüsselwerte des Unternehmens, auf die er achten sollte, zu erkennen. Der Gegenstand solcher Analyse sind die materielle und unmaterielle Werte, die Gestalten des Vermögens und die Persöhnlichkeiten des Leiters die vom Bedeutung sind und welcher Verlösung könnte schwierige Folgen für den Unternehmen verbringen.

Die Schlüsselwörter: *die Schlüsselwerte des Unternehmens, Professionalität und Vernünftigkeit, der Sicherheitsmanager, das Risiko und die Bedrohung*

1 Ванредни професор на Факултету за дипломатију и безбедност у Београду
2 Ванредни професор на Факултету за дипломатију и безбедност у Београду
3 Примери закључне вредности:
1.Компанија је у својој истраживачкој лабораторији развила нов производ. Потрошила је неколико година рада , своја и позајмљена средства. Резултати истраживања су још увек пословна тајна компаније. Кључни задатак корпоративне безбедности је, у овом случају, заштита пословне тајне од индустријске шпијунаже.
2.Водећи инжењер компаније је кључна личност за даљи напреда компаније, њену доминантну улогу на тржишту. Многа битна питања развоја зависе искључиво од њега. Анализом прикупљених информација установљено је постојање ризика од нарушавања личне безбедности инжењера., нпр.отмица. Кључни задатак корпоративне безбедности је заштита кључних вредности компаније, а у овом случају то је главни инжењер.

УВОД

Појава корпоративне безбедности везује се за настанак својине и корпопрације као заједнице људи о чијој заштити су бринули чланови корпорације. Стога се за корпоративну безбедност везује способност прилагођавања корпорације безбедносним изазовима, ризицима и претњама из окружења, али и одређеном социјалном идеалу и вредностима својине које је ваљало штитити, укључујући ту човека, породицу, нацију и друштво.[4]

Своју функцију корпоративна безбедност мора да остварује рационално и ефикасно, а надасве професионално и стручно.

Ово значи, да су радно време запослених у служби и финансијска средства усмерена у правом смеру и да је тиме максимизирана корисност функције кроз одржавање високог нивоа сигурности компаније. Да су професионалним методама и средствима, стручно идентификоване кључне вредности компаније, на основу чега се избегава непотребно расипање ресурса, како финансијских тако и људских, а самим тим може да се поклони адекватна безбедносна пажња кључним вредностима компаније.

Рационалност и ефикасност корпоративне безбедности огледа се и у редоследу поступања. Прво се врши прецизно дефинисање ризика у окружењу и претњи по сигурност компаније, па се тек онда приступа успостављању система заштите.

Савремени концепт корпоративне безбедности предвиђа системе заштите који могу успешно одговорити на савремене претње које угрожавају компаније, имовину и лица, а то су *:*

- анализа ризика и претњи (дефинисање анализе ризика је одређивање детаљног прегледа који укључује испитивање ризика, оцену ризика и управљање алтернативама ризика, које се изводе да би се разумела природа нежељених, негативних последица по људски живот здравље, имовину или животну средину. То је аналитички процес који омогућава информације за сагледавање непожељних догађаја. То је процес квантификације вероватноће и очекиваних последица идентификованог ризика).[5]
- Дефинисање ризика и претњи и њихова анализа спроводи се у циљу добијања што више прецизних информација од којих се саставља база података са свим релевантним догађајима из поља безбедности. Анализа ризика је један од основних задатака специјализованих служби корпоративне безбедности, чиме оне пружају основну помоћ менаџеру безбедности у доношењу најоптималнијих одлука.
- Анализа ризика у безбедности је сложен процес, захтева систематичност и поступност у предузимању одређених радњи, а то су:
- идентификација ризика,
- утврђивање нивоа ризика,
- праћење ризика, и
- утврђивање нивоа прихватљивости.

4 Кековић З;"Корпоративна безбедност."У:Кековић,З;Димитртијевић,И; „Системи безбедности са системом безбедности Републике Србије, Београд, Факултет безбедности,2017, стр.233.

5 General Security risk assessment, ASIS international , 2003, str..5

Јасно је да се одређени ризици у пословању, а тако и у безбедности, не могу у потпуности неутрализовати, с тога се заједно са директорима осталих пословних функција мора дискутовати о прихватљивом нивоу ризика. То је онај ниво који компанија свесно преузима на себе. Мора се напоменути да одређени ризици немају ниво прихватљивости, односно толеранције.

Као мере редукције јављају се:

- смањење ризика, а односи се на утицање и деловање од стране компаније на извор ризика, релевантне чиниоце на тржишту, органе безбедности, како би се интензитет претњи редуковао;
- трансфер се примењује уколико није могуће смањити ниво ризика. Осигурање се јавља као метод трансфера ризика улагањем финансијских средстава као вида заједничког сношења ризика. Послове осигурања обавља специјализована финансијска институција.[6]

Прихватање ризика је крајња солуција уколико су све друге могућности исцрпљене. Функција корпоративне безбедности се у том случају посебно припрема за могуће негативне последице са намером да издржи опасност када претња испољи своје деловање.

Прихватање ризика као крајња солуција је релативно прихватљиво решење за компанију, али само у изузетним ситуацијама. Функција корпоративне безбедности је да предупреди све врсте ризика који могу настати деловањем конкуренције или, нпр; индустријских шпијуна, а не да се "носи" са последицама свог неуспеха.

Ипак, неспорна је чињеница, да потпуно заштићено пословно окружење не постоји. У пословању по тржишним законима сваки независни економски субјект, у већој или мањој мери, трпи последице ризика (политички, правни, економски, безбедносни). Међутим, као олакшавајућа околност узима се чињеница, да не прерастају сви ризици у претње, а потом у опасност која се испољава негативним утицајем на пословање компаније. Одређени број ризика се угаси, или напорима корпоративне безбедности неутрализује, смањи, трансферише. На основу изнетог може се закључити: „Да свака претња јесте и ризик, док није сваки ризик претња".[7]

Када се једном претња идентификује и препозна поклања се много већа пажња анализи која је по својствима идентична анализи ризика уз битну разлику да претња реално поседује могућност негативног утицаја по пословање компаније. Кораци у анализи претње су такође: идентификација, утврђивање нивоа претње, праћење или мониторинг, утврђивање нивоа прихватљивости (уколико постоји ниво прихватљивости за такав вид претње). Посебан значај има аналитичка функција у правовременом извештавању о променама и тренутном статусу идентификованих ризика и претњи.[8]

6 Наши привредници сматрају да су заштитили своју имовину, ако су исту осигурали. Погрешан прилаз, јер се уговарањем осигурања имовина не штити, већ се само надокнађује настала штета од насталих последица неким деловањем на осигурану имовину. И на Западу се имовина осигурава, али се премија осигурања одређује у зависности од предузетих мера заштите објекта и имовине која се осигурава. Заштита већа – обавеза осигурања мања.

7 Анђелковић Слободан, Специјалистички рад „Савремени концепт корпоративне безбедности", Факултет политичких наука, Београд, јуни 2005,стр.12.

8 Исто, стр.12

Након прецизног дефинисања ризика у окружењу и претњи по сигурност компаније, идентификовања кључних вредности, приступа се успостављању система заштите. Савремени концепт корпоративне безбедности предвиђа системе заштите који могу успешно одговорити на савремене претње које угрожавају виталне интересе компанија, имовину и лица.

ЗАШТИТА ИМОВИНЕ

Појавни облици имовине компаније, које се међусобно разликују према својим специфичностима, трпе и различите облике угрожавања по основу безбедности. Облици и начини угрожавања, поред облика имовине, су ти на основу којих се пројектују механизми заштите. **Тако разликујемо следеће облике имовине:**[9]

- **непокретности** које су у власништву компаније и представљају стална материјална средства (пословне зграде, фабричка постројења, магацини, системи за производњу, итд;)
- **материјална средства**, као што су новчана средства у готовини, хартије од вредности, племенити метали, уметничка дела и друге драгоцености;
- **интелектуалну својину,** (за нас је битна заштита поверљивих информација-пословне тајне) и
- **информациони системи.**

ЗАШТИТА ЛИЦА

Заштита лица у савременом концепту корпоративне безбедности обухвата мере и радње за повећање нивоа сигурности лица, како запослених у компанији тако и оних који се тренутно налазе у кругу компаније.

Заштита лица обухвата више различитих облика протекције, и то су:

- **општа заштита,** је заштита која свим учесницима и посетиоцима (запосленима и незапосленима) пружа основни ниво сигурности за безбедан боравак и обављање пословања;
- **VIP (very important person) заштита**[10] се примењује када се анализом ризика и претњи установи реална потреба за личном заштитом руководећег кадра компаније. Тада се приступа изради елабората о личном обезбеђењу и организује служба за личну, односно телесну заштиту.

Лична заштита као подсистем службе обезбеђења је по много чему специфичан и различит од других подгрупа функције безбедности. Да би један вид заштитног механизма могао да се сматра подсистемом у оквиру постојећег система безбедности, мора да се одликује особеностима као што су:

- организационо издвојен део службе са посебном структуром, опремом, обуком, кадровима;
- посебни видови претње који остварују свој утицај на посебне делове компаније;

9 Исто,. стр.12

10 У домаћој пракси личне заштите, познати су термини заштите: ВДФ (високих државних функционера), ВВФ (високих војних функционера и ВИП (веома важна личност).

- постојање посебних облика угрожавања који захтевају адекватне одговоре у виду специфичних мера заштите.

У оквиру рада службе за личну заштиту неопходна је одређена самосталност у доношењу оперативних одлука и избора средстава за рад, као што су возила, лично наоружање, средства заштите (панцири, панцирни плаштови) и техника. Друга специфичност огледа се у чињеници да потпуно лична заштита подразумева заштиту штићене личности дан и ноћ. Без обзира да ли је на радном месту, одмору, кући и ван ње. Све ово захтева, поред високог степена стручности, и дискрецију кадрова из службе личне заштите, како социјални живот штићене особе не би био поремећен и угрожен.

Један од специфичних проблема са којима се још сусреће корпоративна безбедност су: **Асоцијални видови понашања на радном месту,** а из разлога што својом манифестацијом у великој мери наносе штету пословању компаније. Штетни утицају су многобројни и комплексни, претећи да ескалирају у још веће, са елементима кризе. Понашање које је најчешће повезано са безбедносним ризиком је злоупотреба алкохола и дрога, емотивни и ментални проблеми, финансијски проблеми.[11]

Када се ови проблеми испољавају на радном месту, последице за компанију су: пад рејтинга, губитак угледа код пословних партнера, клијената, добављача, целокупног пословног окружења.

Проблем може бити још већи, а последице несагледиве ако се ови видови асоцијалног понашања манифестују и у средини где носиоц таквог понашања живи. Посебно ако се ради о лицима високо рангираним у компанији, носиоцима и корисницима поверљивих информација. Нпр; један од приоритетних задатака индустријских шпијуна је идентификација носиоца поверљивих информација у компанији која је предмет обавештајног интересовања. Такво лице, по откривању, оперативно се покрива, сагледавају му се особине, навике, породични и друштвени живот, пријатељи и непријатељи, а посебно асоцијална понашања. За "индустријског шпијуна" који је типовао директора, нпр; развоја неке компаније, идеално је сазнање да се ради о лицу које употребљава опијате, или пак о страсном коцкару који дугује велике суме новца "зеленашима". Овим сазнањем ствара се идеална ситуација за приступ типованом лицу, а у зависности од умећа и до куповине пословних тајни, или регрутовања "кртице". Мотиви и подстицаји су лако препознатљиви.

За корпоративну безбедност изазов је и **заштита запослених на путовању.**[12]Посматрајући и анализирајући ризике и појаву претње, путовања, због већег броја променљивих и непознатих чиниоца, готово увек представљају већи ризик по безбедност запослених, него када су у месту пребивалишта и одлазе на посао где постоји устројена безбедносна служба. У зависности од процене ризика, задатак корпоративне безбедности је да контра-обавештајно припреми лице, што подразумева предочавање свих ризика којима може бити изложен на путу и боравку у другом месту, те контактима са пословним и другим лицима. Такво лице мора да се упозори на поштовање безбедносних норми понашања. Предочавање одређених

11 АнђелковићС., оп.цит. стр.20
12 Исто, стр.23

безбедносних ситуација мора бити у функцији упозорења, али и препознавања могућих ризика.

Уколико постоји основана потреба личне заштите, нпр; генералног директора (или других битних личности по компанију), организација безбедносних аспекта путовања представља задатак корпоративне безбедности.

БЕЗБЕДНОСТ ПОВЕРЉИВИХ ИНФОРМАЦИЈА

Под термином, безбедност поверљивих информација, подразумева се заштита информација и поверљивих података од њиховог откривања, модификације или преправљања.[13]

Систем безбедности информација обухвата људе, процесе, организацију и технологију, односно то је систем који се састоји из уравнотеженог скупа мера заштите:

- безбедносне провере особља,
- физичко - техничке безбедности,
- безбедности података,
- безбедности информационих система, и
- координираног увођења формалних процедура као што су процена ризика, сертификација особља и опреме, као и акредитација техничких система за примену у одређеном сегменту пословног процеса.

Уравнотеженост и координација битних мера и поступака постиже се организацијом и управљањем безбедношћу информација.[14]

Да би се у потпуности схватио термин безбедност пословних тајни (поверљивих информација) морају се претходно дефинисати појмови као што су: податак, информација, информациони систем, итд.

Податак је скуп препознатљивих симбола који су записани на одређеном носиоцу.

Информација је податак с одређеним значењем, односно сазнање које се може пренети у било ком облику (писаном, визуелном, аудио, електронском или неком другом).

Информациони систем је сваки систем уз помоћ којег се прикупљају, уносе и чувају, обрађују, приказују, узимају и шаљу информације тако да буду доступне и употребљиве свакоме ко има право да их користи.

Информациона опрема су сви физички уређаји и/или средства који чине информациони систем.

Најједноставнија дефиниција безбедности информација је дефиниција која безбедност информација означава као очување (заштиту),[15]поверљивости– обезбеђивање да је информација доступна само оним лицима која имају овлашћени приступ, **интегритета** – заштита постојања, тачности и комплетности информације као и методе за њихову обраду, **расположивости** – обезбеђивање да ауторизовани

13 Првуловић Владимир, „Економска дипломатија“, ПС“Грмеч“-„Привредни преглед“, Београд, 2001. стр. 59

14 Стандард ИСО 17799, Информационе технологије – Правила праксе за управљање безбедношћу информација, ИСО/ИЕС, 2000.

15 Исто

корисници имају могућност приступа информацији и припадајућим средствима кад код је то потребно.

Заштиту можемо дефинисати ***као скуп мера за очување безбедности.*** Самим тим да би неки систем заштите функционисао морају да постоје одређена правила. У случају заштите то је скуп правила, а где постоје прописана правила мора да постоји и надзор, одговорност и овлашћење.

- **Надзор** је проверавање функционисања система заштите.
- **Одговорност** је понашање према унапред утврђеном скупу правила.
- **Овлашћење** је право поступања у утврђеним оквирима.

Постоје унутрашњи и спољашњи аспекти безбедности поверљивих информација.

Унутрашња безбедност поверљивих информација, подразумева њихову заштиту од:

- Функционера запослених у компанији, неовлашћених да дођу у контакт са дотичним информацијама;
- коментарисање садржаја информација у кругу њених овлашћених корисника:
- коришћење поверљиве информације у личне сврхе;
- проваљивање информација преко подмићених радника;
- дотурање дотичне информације конкурентским снагама или страним ДКП;
- од запослених службеника-компјутерских сурфера и хакера и радозналих посетилаца сајта компаније, и
- осталог непрофесионалног и неодговорног понашања унутар компаније према поверљивим информацијама које компанија поседује.

Спољашња[16]заштита поверљивих информација подразумева заштиту од нежељеног откривања информације или утицаја на њу, коју могу вршити:

- конкурентске снаге-економски противници или партнери,
- случајни "посетиоци",
- органи државне администрације или контроле,
- стране економске дипломате или сакупљачи економских информација,
- компјутерски сурфери, хакери, нежељени посетиоци сајта и др. (када је у питању електронска информација у бази података или на сајту власника поверљиве информације),
- убачени електронски вируси, и
- други спољашњи фактори утицаја на поверљиву информацију.

За безбедност информација одговорни су власници података и њихова одговорност везана је за сва поступања с подацима који су у њиховој надлежности, током животног циклуса података. Ова одговорност их приморава на организовање система корпоративне безбедности који ће максимално бити у функцији заштите информација.

16 Исто

Информација је, видели смо то, драгоцена роба коју није лако добити, употребити и што је још важније – сачувати. Због тога је веома важно на прави начин и одговарајућим средствима заштитити информацију у било ком облику.[17]

Заштићеност пословних тајни од злоупотреба максимално повећава пословне могућности компанија. С тим у вези, основни задатак корпоративне безбедности је да пронађе најоптималније начине заштите пословне тајне.

Један начин заштите пословних тајни је **безбедносно- организациони** и он у себи садржи познавање и поштовање правила културе пословне заштите, правну регулативу свега тога и адекватну организацију и систематизацију радних места.

Други начин заштите пословних тајни се остварује правилним избором и коришћењем техничких и електронских средстава за обезбеђење, контролу приступа и надзор објеката компаније, као и ефикасном употребом запослених који раде послове физичке заштите.Оптимални резултати заштите се постижу јединственим коришћењем техничке и електронске заштите са оспособљеним радницима физичког обезбеђења. Овим се постиже јединствен систем заштите, контроле приступа и надзора просторија и објеката компаније. Овако конципиран облик заштите има двојну функцију, поред заштите пословних тајни, служи и за заштиту основних средстава, робе и производа компаније од инкриминисаних радњи.

Безбедност поверљивих података се остварује на основу закона, систематском применом прописаних безбедносних и заштитних мера и поступака за овлашћено прикупљање, обраду, употребу и чување, спречавање и опоравак од губитка, или неовлашћено објављивање поверљивих података. Пошто су методе које користе индустријски шпијуни исте онима које користе традиционални („државни") шпијуни, против мере које се користе у спречавању традиционалне шпијунаже могу се применити и на заштиту пословне тајне од индустријске шпијунаже.

Први, и један од најважнијих корака у остваривању безбедности података, је **класификација података** у односу на степен ризика и потребне мере за њихову заштиту.[18]

КЛАСИФИКАЦИЈА ПОДАТАКА[19]

Класификација података прописана је законима и пратећим извршним прописима који заједно омогућавају јединствено одређивање назива класе или разреда података, одговарајућих обавезних ознака и њима одговарајућих поступака, метода, средстава и извршитеља, али и правне санкције за свако одступање од прописаног поступка унутар класе и унутар одређеног правног простора. Класификација треба да буде истог степена којег је највиши поверљиви део, али треба избегавати и претерану и преоскудну класификацију у интересу ефикасне безбедности. **Класификација сама по себи није заштита**, већ смерница која указује на потребу за посебним мерама за руковање и заштиту. Класификована информација мора да се заштити кроз свој циклус трајања до нивоа који је у складу с њеним нивоом класификације. С њом је потребно руковати на начин да је одговарајуће означена, јасно одређена као класификована и да остаје класификована само онолико дуго колико је то

17 Милошевић М;Заштита пословних података и докумената, Правни информатор, www.Informator.co.yu.
18 Исто
19 Mitnick D. Kevin, »Уметност обмане«, Микро књига, Београд, 2003.,стр.269

потребно. Одговорност за доделу класификације и њено периодично ревидирање треба да остане у оквиру одређеног власника информације. По истеку потребе за класификацијом потребно је извршити декласификацију. Ознака некласификовано или непостојање било какве класификационе ознаке не подразумева поимање тог податка као јавног и не представља одобрење за његово објављивање. Објављивање некласификованих података мора да се изврши путем посебно прописаних формалних процедура.

Класификација података је неопходна за заштиту корпоративних информација. То је поступак прављења категорија за контролу објављивања осетљивих информација. Свим запосленима се ставља до знања колико је свака појединa информација осетљива.

Ако се подаци не класификују, доношење одлуке се препушта појединцима. Класификацијом података, вредне информације се смештају у једну од више категорија. Сваки радник мора да научи класификацију корпоративних података, укључујући и раднике који обично не користе рачунаре, нити комуникационе системе фирме. С обзиром на то да сваки радник, укључујући чистаче, чуваре, особе које фотокопирају документе, као и саветнике, привремене раднике, па чак и стажисте, може имати приступ осетљивијим информацијама, свако од њих може бити мета напада.

Податке треба одвојити у различите нивое у зависности од њихове осетљивости. Промена класификационог система после успостављања је скупа и дуготрајна. Постоје четири нивоа класификације који се могу применити на већину средњих и већих компанија и то:

ПОВЕРЉИВО.Ова категорија информација је најосетљивија. Поверљиве информације се користе само у оквиру организације. У већини случајева, само ограничен број људи зна за њих. Природа поверљивих података је таква, да би свако неовлашћено обелодањивање проузроковало озбиљну штету фирми, њеним деоничарима, пословним партнерима и/или клијентима. Поверљиве информације углавном спадају у једну од следећих категорија:[20]

- Пословне тајне, изворни кодови програма, техничке или функционалне спецификације или информације о производу које би могле користити конкуренцији.
- Информације маркентишке и финансијске природе које нису намењене јавности.
- Све друге информације које су суштински значајне за рад фирме, као што су будуће пословне стратегије.

ПРИВАТНО. У ову категорију спадају приватни подаци намењени интерној употреби у оквиру организације. Свако неовлашћено откривање приватних података (нарочито обмањивачима) могло би озбиљно оштетити запослене или фирму. У приватне податке могу се сврстати здравствени подаци запослених, подаци о њиховим банковним рачунима, историјат о плати, као и све друге сличне информације које нису за јавност.

20 Исто, стр .269

ИНТЕРНО. Ови подаци се могу слободно давати свим запосленима у организацији. Обично се не очекује да ће неовлашћено објављивање интерних информација нанети озбиљну штету фирми. Међутим, вешти обмањивачи могу да употребе такве информације да би се представили као запослени, привремени радници , или добављачи, и на тај начин измамили осетљивије податке од неприпремљеног особља и тако неовлашћено приступили рачунарским системима фирме. Пре него што се интерне информације саопште трећим лицима (као што су особље добављача, привремени радници, пословни партнери итд) мора се потписати уговор о поверљивости података. Интерним информацијама углавном припада све што се свакодневно користи у пословању, а што се не сме саопштавати трећим лицима, као што су организациона структура фирме, позивни бројеви за прикључење на мрежу, интерни називи система, поступци за даљински приступ, контни бројеви и тако даље[21].

ЈАВНО. То су подаци посебно намењени јавности. Они се слободно могу давати свима, у изјавама за штампу, у контакту са корисницима или у брошурама о производима[22].

Сама информација би требала да буде раздвојена у неколико делова саме зграде. Само особе које имају потребу да познају поверљиву информацију би требало да имају приступ релевантним областима и да дођу у додир са тим областима. Примера ради, сама финансијска књига би требало да буде закључана у посебној просторији. Само особе које имају потребу за овим информацијама би требало да имају кључ. Сам натпис би требало да стоји "само запослени", или "ауторизовано особље" или "забрањен приступ", или пак нека од сличних фраза ће помоћи у обесхрабривању људи да уђу у ове просторије у којима је приступ ограничен. Различите процедуре се могу користити у заштити информације које долазе споља. Неретко компаније дискретно деле поверљиве информације између многих ималаца. Наиме, ни једном од запослених се не даје довољно информације, тако да би он дошао у могућност да спозна или користи поверљиву информацију. Данас се користе неколико метода по којима поверљиве информације могу бити ограничене само на она лица која имају потребу да знају информацију. Шифре су један од метода. Одвојени компјутерски системи су други. Такође компјутерски систем може да избаци упозорење када неко покуша да "провали" шифру, идентификујући истовремено и проблем, као и који се терминал користи. Саме поверљиве информације би требало да буду одложене када се не користе. Машину треба покрити када се она не користи. Просторија би требало да буде закључана и затворена. Компанија може захтевати да столови буду потпуно чисти на крају сваког дана. Треба имати у виду да и само смеће у оквиру саме компаније може бити предмет прегледа од стране људи који траже туђе поверљиве информације. Машина за сецкање би требало да буде коришћена када се ради о поверљивим информацијама. Други степен заштите, исто тако важан као и први је, да се код запослених, а нарочито код руководства елиминише " урођена " жеља да се свима прича о пословним успесима и неуспесима[23]. Знати коме ће те поверити поверљиву информацију на коришћење је основ успешности

21 Исто, стр. 270
22 Исто, стр. 270
23 Исто, стр.271

унутрашње безбедности поверљивих информација. За постизање овог циља важне су безбедносне провере запослених

БЕЗБЕДНОСНЕ ПРОВЕРЕ

Безбедносна провера запослених, осим примарних мера којима се процењује могућност додељивања овлашћења, подразумева и активну бригу око усмеравања, едукације и контроле исправног поступања сваког појединца.[24]

Безбедносна провера особља пре свега обухвата процену да ли се за неког појединца у погледу лојалности, поверљивости, поузданости и веродостојности може дати овлашћење за приступ поверљивим информацијама, а да то не представља неприхватљив ризик за безбедност информације. Процена проистиче као резултат обављене безбедносне провере (провере поузданости) оних лица чије запошљавање или напредовање подразумева приступ поверљивим информацијама. Безбедносну проверу је потребно спроводити и за уговорне стране и за лица која су само привремено у контакту с поверљивим информацијама. Безбедносне провере спроводе се у опсегу који је прописан за доступан ниво поверљивости, као и уз знање и пристанак особе која се проверава.

Безбедносна провера особља подразумева и правовремену безбедносну информисаност, образовање и обуку. Особље треба да буде упознато са својим безбедносним обавезама и прописаним поступцима, и мора да буде редовно информисано о безбедносној политици. Мора такође да буде упознато и са службеном процедуром извештавања за случај безбедносних инцидената или неправилности, али и са санкцијама за безбедносне прекршаје.

Путем програма безбедносног образовања потребно је развити свест о безбедносним претњама и бризи за информацију, као и способност пружања подршке безбедносној политици током обављања свог редовног посла.[25]

Ово су уопштени примери понашања према поверљивим информацијама. Заштитити своје поверљиве информације је озбиљан процес који захтева организованост, дисциплину и професионалност. Зато ћемо теми која следи поклонити пуну пажњу.

ФИЗИЧКО - ТЕХНИЧКА БЕЗБЕДНОСТ (ЗАШТИТА)

Физичка безбедност обухвата примену физичких и техничких мера заштите на местима, у зградама и просторијама које захтевају заштиту од губитака или компромитације поверљивих информација. Улога ових мера је спречавање недопуштеног и насилног уласка неовлашћених лица, затим одвраћање, откривање и реаговање на деловање неовлашћеног лица.

Дефинисање обима физичких и техничких мера заштите треба да буде усклађено са степеном тајности података, вероватноћом претње и количином информација којима је потребна заштита. У просторијама у којима се рукује поверљивим подацима утврђују се начела класификације простора на безбедносне зоне и административне зоне. Физичка безбедност спроводи се уградњом баријера, система

24 Исто, стр..271.
25 Исто, стр 272

за детекцију неовлашћеног приступа, као и система за контролу уласка и изласка. Физичка безбедност спроводи се даље ангажовањем службе обезбеђења и вршењем претреса, пратње и надзора посетилаца.

ПОЈАМ ФИЗИЧКО-ТЕХНИЧКОГ ОБЕЗБЕЂЕЊА

Физичко-техничко обезбеђење*"представља специјализовану безбедносну делатност која се обавља углавном у привреди од стране специјализованих предузећа, специјализованих делова неких привредних субјеката (агенција, компанија и сл;) и обучених појединаца-радника, ради заштите имовине и лица од неовлашћених спољних утицаја (индустријске шпијунаже), криминалитета – класичног, привредног и другог"*[26].

На основу напред изнетог, основ за одређивање обима и организације физичко-техничке заштите у некој компанији мора бити **безбедносна процена**, и она је**, сигурни смо у то, основ постављања система заштите,** и исту, због тога морају урадити стручна и едукована лица за процену ризика и претњи које могу настати и угрозити дату компанију. Зато у тиму корпоративне безбедности морају бити стручњаци (инжењери, правници, организатори, технолози итд;) свих профила, док доминантну улогу морају имати стручњаци за безбедност.

Проценом се још оцењују и процењују критичне фазе времена у којем се врше највећа угрожавања, облици угрожавања, мотиви за угрожавање, структуре и организације које врше угрожавање. Код овог начина заштите акценат се ставља и на **процену критичности свих објеката предузећа, те лица која су у контакту са поверљивим информацијама.** Са аспекта нашег истраживања, посебна пажња се мора усмерити на одговорност према поверљивим документима, начин чувања истих, касе , закључавање просторија, број улаза итд. Процењује се и сарадња са полицијом и другим органима, могући ризици из политичких мотива, могући ризици из криминалних мотива и многи други ризици и претње. Након адекватне процене угрожености и ризика, врши се процена и предлог мера безбедности и заштите, као одговор на сваку угрожавајућу ставку предупређену за ризик.[27]

Да поједноставимо: Мере безбедности се постављају сразмерно исказаном ризику, а то значи да из овога произилази и организација службе обезбеђења и њихова конкретна делатност.

ОРГАНИЗАЦИЈА СЛУЖБЕ ФИЗИЧКО-ТЕХНИЧКОГ ОБЕЗБЕЂЕЊА (ФТО)

Један од задатака и дужности корпоративне безбедности је и организација и управљање службом физичко-техничког обезбеђења, која потом чини део организационе структуре функције безбедности. Интерес за професионалном и функционалном службом обезбеђења, у ужем смислу посматрано, се јавља код управе корпоративне безбедности која је за функционисање својих служби одговорна топ менаџменту компаније. С другог аспекта руководство саме компаније дужно је и одговорно пред запосленима, клијентима пословним партнерима, окружењу, али и

26 Пејановић Љ., Лаковић В., Стојановић С., Угрожавање и физичко-техничка заштита, Београд, 2007.,стр..93-182.
27 Исто, стр.160

сопственој држави која брине о својој националној безбедности, да створи услове за безбедно и несметано обављање свих пословних функција.

Да би се оформила и уклопила у организациону целину једна професионална служба физичко-техничког обезбеђења потребно је створити услове и обезбедити средства за такву имплементацију.Ефикасност и професионалност службе физичко – техничког обезбеђења се огледа у:

- нивоу оспособљености запослених, што подразумева обученост, образовање и искуство;
- техничкој опремљености савременим техничким средствима;
- мотивисаност је један од кључних проблема у функционисању свих видова обезбеђења. Професионалац од свог конкретног рада прибавља средства за живот за себе и своју породицу. Ако је задовољан својим примањима, мотивациони фактор, као процес усмеравања људске енергије ка остварењу задатих циљева, утиче на његове резултате, побољшава исте. Мотивација може да буде материјална и нематеријална. Битно је да она постоји и да је у функцији побољшања квалитета рада;
- стручној управи, односно одговарајућем руководећем кадру. Руководилац поред високог стручног знања из области безбедности и заштите мора да поседује знања и умећа за управљање људима. Управљање као процес се свакодневно учи, али кадрови који поседују одговарајуће личне особине успешнији су у овој области од других. Пошто у овој области заштите, праћење техничких иновација, захтева свакодневно усавршавање свих, обавезан је континуирани процес учења и обуке на савременим системима заштите.

Једно од веома битних питања, на које одговор треба да да онај ко је у функцији корпоративне безбедности компаније,је избор између организовања сопствене службе или ангажовања спољње службе физичко-техничког обезбеђења.[28]

Оба решења су у пракси исказала низ недостатака, али и повољности:

Позитивне стране организовања сопствене службе обезбеђења огледају се у следећем:

- на основу постављених критеријума, високих стандарда, сами бирамо раднике обезбеђења. Сами их опремамо опремом, униформама и адекватним средствима за коју сматрамо да је одговарајућа и да је у функцији успешности рада. Има се непосредни утицај на службу, користи се формални ауторитет.
- Свакодневна непосредна контрола на свим нивоима;
- успостављање идентификације са компанијским циљевима, итд.

Негативне стране, огледају се у следећем:

- зближавању радника обезбеђења са другим радницима компаније што се посебно запажа у деликтним ситуацијама. Пошто су радници исте компаније, имају истог власника, директора, исте проблеме што утиче на социјализацију међу запосленима и то неминовно доводи до негативног утицаја на пословне и безбедносне процесе. Стварају се пријатељски односи са радницима обезбеђења што доводи до непоштовања безбедносних процедура. Као

28 Исто, стр.165

последица злоупотреба оваквих односа јавља се немогућност детекције појединих кривичних дела, првенствено ситних крађа.
- Проблем ауторитета је такође битан фактор где се не поштује безбедносна процедура. Страх да, ако савесно и професионално раде свој посао, неће од виших руководиоца навући на себе негативну пажњу и изгубити посао.
- У већини случајева сопствена служба је предимензионирана што непотребно повећава трошкове обезбеђења.

Ангажованаслужба физичко-техничког обезбеђења је економски исплатива.[29]

Рационална је у организовању функционисања службе обезбеђења. Ово, под условом, да је ангажовано специјализовано предузеће чији је искључиви посао обезбеђење, што иницира професионализам и упућеност у нове трендове заштите објеката, имовине и лица. Овакво предузеће располаже са већим бројем стручних кадрова и других средстава за рад, као и могућност тренутног ангажовања већег броја радника на пословима обезбеђења ако то изискују одређене ситуације.

Проблем је што код нас, још увек не постоје стандарди о квалитету услуга које треба да пружи ангажована служба ФТО. Постојећа конкуренција уместо да повећава квалитет услуга, снизује цену ангажовања, што доводи до запошљавања нестручних кадрова, без мотивације за сопствено напредовање.[30]

Оваква ситуација на тржишту услуга обезбеђења, иницира да је, бар за сада, најоптималније решење комбинација услуга ангажоване службе физичко-техничког обезбеђења са руководећим или контролним фактором интерне службе безбедности, чиме ће се добити добре перформансе, користећи предности обе врсте служби обезбеђења и неутрализацијом недостатака.

Да би физичко-техничка заштита у потпуности била у функцији заштите од спољног и унутрашњег угрожавања, неопходно је, за заштиту изнутра, али и запослених, прописати интерним актом**начине понашања,потребе, обавезе и дужности сваког радника на радном месту, од задњег радника до директора**. Нпр; начин коришћења докумената са ознаком „поверљиво," начин идентификације уласка у просторију са документима, регистровање времена уласка, изласка, време враћаја документа. Регистровање фотокопирања, посебно броја примерака и коме се исти достављају, итд. Ово подразумева, да је интерним актом, који је такође поверљив документ, прописано која лица могу доћи у додир са поверљивом документацијом.

За разлику од начина како се прописује обавезно понашање свих запослених у једној компанији, **процедуре послова безбедности и заштите**, а у циљу побољшања квалитета услуга обезбеђења и стандардизације послова у свим предузећима на нивоу Републике Србије, прописују државни органи.[31]

Процедуром се прописују мере, радње и задаци, у следећем:
- Евиденција запослених
- евиденција уласка запослених у предузеће,
- евиденција изласка запослених из предузећа,

29 Анђелковић С., оп.цит. стр.25
30 Пејановић Љ., Лаковић В., Стојановић С., оп.цит., стр.167.
31 Исто, стр.170

- евиденција доласка и одласка са задатка радника FTO.
- Евиденција посета
- евиденција уласка-изласка странки и пословних сарадника,
- евиденција времена одржавања састанака у предузећу и присутних лица,
- евиденција уласка и изласка страних држављана, регистровање остварених контаката,
- евиденција унете и изнете робе и других материјалних средстава,
- евиденција насталих инцидената у предузећу,
- евиденција контраобавештајних активности у предузећу,
- евиденција контроле државних органа у предузећу,
- **евиденција пословних тајни,** и друге евиденције.

Ако је компанија, на основу процена и предлога стручних лица корпоративне безбедности добро проценила и одредила мере обезбеђења улазака у круг компаније или зграде истих, послови обезбеђења на улазима објекта, зграде су следећи:

према запосленима:

- свако изношење ствари, докумената, средстава и др; обавезно се прилаже прописана излазница која мора бити прописно, од овлашћеног лица оверена,
- при сваком уласку обавезно је показивање идентификационе картице, оверене дозволе или другог идентификационо приступног документа,
- за време продуженог радног времена доставља се прописна дозвола,
- обавезна је контрола личних торби или пакета који се уносе и износе,
- и друге обавезе које се пропишу.

посета странака:

- мора бити видно означено да је странка у обавези да раднику обезбеђења да на увид лична документа и да је по добијању беџа или идентификационе картице за посетиоце, странка дужна исти носити на видном месту, вратити исте по одјављивању, односно изласку из зграде, круга компаније,
- ако било шта износи мора да поседује дозволу за изношење, а пожељно је да радник обезбеђења буде непосредно обавештен шта странка износи и да писмено региструје ко је из компаније дао дозволу за изношење, упутио позив,
- радник обезбеђења треба од странке да тражи код кога иде, по ком основу и да ли је са тим лицем остварила контакт. По пријему ових обавештења да позове то лице из компаније и да провери наводе странке, најави посету. Пожељно је да запослени странку прихвати при самом уласку и да, кад странка одлази исту испрати до изласка. Ово мора бити обавеза када су у питању страни држављани, уз још једну обавезу да запослени, без обзира ког је ранга о посети састави писани извештај, у коме ће акценат ставити на исказаним интересовањима страног држављанина, и исти достави менаџеру безбедности. На овај начин запослени је у непосредно у функцији обезбеђења присуства странке у објекту.[32]

32 Исто, стр..170

У функцији обезбеђења је и **паркирање возила,** процедура и то, како запослених, тако и посетилаца, странки. И једни и други то морају радити на за то предвиђеним местима. Ако не постоје за то одређени паркинзи који су под контролом радника обезбеђења не треба дозвољавати улазак возила у круг компаније, близини објеката, или њихово задржавање. Возила запослених морају бити адекватно обележена и запослени одговарају за злоупотребе идентификационих ознака. Такође и возила странака морају бити обележена, регистрован њихов улазак и излазак, контролисана како при уласку тако и изласку. Свако неправилно паркирање мора бити регистровано и према таквом возилу, лицу које га је увезло у круг, морају се применити мере контроле. Самим тим што је такво лице упозорено на процедуре са возилом, местом паркирања, одступања морају бити третирана са појачаном безбедносном пажњом.

У овом делу, где говоримо о физичкој заштити, изложићемо још један, од многих других послова и задатака које предузимају радници обезбеђења кроз овај вид заштите, а то је: **унутрашња контрола објекта**.[33]

Иста мора да буде свеобухватна, константна, одрађена у различитим временским интервалима, ненајављена. Када је у питању заштита поверљивих информација, циљ контроле је да свакодневно проверава да ли се поштује процедура заштите овако означених докумената. Какав је однос носиоца поверљивих информација према истима? Однос запослених према било каквим информацијама до којих долазе у току радног времена? Да ли су им на столовима роковници, шта уписују, нпр. календарима, папирићима, да ли их уништавају или бацају у канте за отпатке? Да ли су просторије у којима се одлаже поверљива документација прописно обезбеђене, касе закључане, итд. Свакодневном контролом, регистровањем пропуста, спречава се понављање истих, утиче се на запослене да безбедносну пажњу држе на високом нивоу и да буду у функцији безбедности своје компаније. Уочени пропусти морају да се јавно искажу, изврши упозорење, а по потреби изрекну и одређене казне.

Унутрашња контрола објекта, посебно по завршетку радног времена је важна и због евентуалног откривања, нпр; крадљивца поверљивих докумената који је искористио легалну могућност уласка у објект, сакрио се, чекао да запослени оду, када би кренуо у акцију. Потенцијални крадљивци пословних тајни сигурно нису случајни лопови, већ за то припремљена лица која ће сигурно добро проучити систем обезбеђења објекта који „нападају". Сазнање да се врши свакодневна, у различито време свеобухватна унутрашња контрола објекта, врло је важан фактор одбијања оваквих лица. Код овог облика заштите битне су и **унутрашње препреке.** Потенцијални крадљивци, бар то раде професионалци, прво сагледавају објект споља, због начина и могућности уласка и изласка из објекта, а онда и изнутра користећи за то разне начине, нпр; преко "кртице" из компаније. Интересоваће га, пре свега, да ли су врата ојачана, има ли решетки на прозорима, који је тип касе, сензори, аларми, камере и др. Добро осмишљене унутрашње препреке веома су ефикасне у функцији безбедности. Нпр; светла која се активирају на основу покрета, такође су добра и ван и унутар просторија.

До сада презентирани начини физичко-техничке заштите, аспект је више стављен на физичку заштиту, у функцији су физичког спречавања крађа, па и крађа

33 Исто, стр.172

информација. Предочили смо (кроз методе и средства индустријске шпијунаже), да данас „индустријски шпијуни" користе софистициране методе и средства долажења до „наших" поверљивих информација. Један од тих начина је и прислушкивање. Један од задатака, професионалних, добро организованих и опремљених служби физичко-техничког обезбеђења је и да **„бубицама" не дају никакву шансу.**[34]

ЗАШТИТА ОД ПРИСЛУШКИВАЊА

Добро организовано обезбеђење подразумева, да им је један од основних задатака осигурање безбедности поверљивих информација којима располаже компанија коју штите. Ово, без обзира да ли је физичко-техничко обезбеђење ангажовано или формирано, као специфична служба компаније. Осим информација које циркулишу посредством средстава комуникације и у компјутерској мрежи, објекат заштите требало би да буду и усмена саопштења, за време пословних преговора, у телефонским разговорима, у говорима на седницама и једноставно у свакодневним разговорима у установи, из којих конкуренција или противници могу извући корисне информације за себе. За "пресретање", односно крађу, такве информације користе се активна средства тајног преузимања акустичне информације (АСТПАИ), оспособљени за њено преношење заинтересованим лицима преко радиоканала. Због тога, задатак спречавања отицања информација преко канала (АСТПАИ), традиционално је један од најактуелнијих за јединице и службе безбедности приватних и државних установа и институција. Овај задатак се решава помоћу техничких средстава аутоматизоване радиоконтроле (АРК), која су у могућности да открију постојање прислушних уређаја и лоцирају их у границама контролисане просторије или објекта.

Највећи проблем за корисника технике аутоматизоване радиоконтроле је у избору апаратуре, способне да обезбеди извршење наведених функција у складу с адекватним начинима решења сваког од задатака радиоконтроле. Управо спој квалитетне апаратуре и успешних начина обраде омогућава најефикаснију аутоматизацију радиоконтроле, минимализовање за то потребног времена и поједностављење задатка оператера. Проблем избора решава се једноставно, ангажовањем за ту област стручног лица, који ће бити у функцији корпоративне безбедности компаније.

У овом делу биће изложена средства и начини проналажења и локализације прислушних уређаја у просторијама, као и могућности за повећање њихове ефикасности. При том, узимајући у обзир специфичност менталитета наших привредника, потенцијалних корисника, највећа пажња биће посвећена средствима која обезбеђују највећи степен аутоматизације и најмање учешће оператера, а самим тим у каснијој експлоатацији изискује и најмање средстава. Ово из разлога, што "наш власник капитала, директор", прво пита-колико ће то да кошта?

34 Извор: APIS Security Consulting „Odbrana od krađe informacija«, file://F.ISH 4.html,21.03.2006, str.1-7.

ИЗВОРИ РАДИОЕМИТОВАЊА У РАДНОМ ДИЈАПАЗОНУ ФРЕКВЕНЦИЈА[35]

Радни дијапазон фреквенција које користе прислушни уређаји за пренос информација преко радиоканала је између 30 и 2000 мегахерца. На нижим фреквенцијама потребне су антене много већих димензија, што отежава њихово маскирање, док на вишим долази до релативно брзог пригушења радиосигнала и ширење радиоталаса се у већој мери потчињава законима геометријске оптике. Све то отежава рад прислушних уређаја.

Проналажење радиоканала, преко којих долази до отицања информација, бива све теже због интензивног раста оптерећености радиодијапазона, који је условљен следећим чиниоцима:

1. увођењем нових система преносне радиовезе службене и опште намене с динамичком расподелом фреквенција;
2. повећањем броја стационираних и мобилних радиостаница и предајника с фиксираном расподелом фреквенција;
3. хотимичним и нехотимичним коришћењем радиотелефона и радиостаница за чију употребу не постоје одговарајуће лиценце;
4. мењањем задатих техничких параметара радиостанице, и
5. порастом броја извора сметњи индустријског порекла.

Сви наведени чиниоци довели су до тога да је у већини крупних индустријских центара слободни етер постао презасићен.

Сваким даном се све више проширује асортиман специјалних средстава преузимања информација и побољшавају се њихове тактичко-техничке карактеристике (ТТК). Усавршавају се и методе коришћења прислушних уређаја: њих производе и уграђују узимајући у обзир реалне електромагнетске услове на месту претпостављеног коришћења, камуфлирају их у предмете свакодневне намене, што практично искључује њихово откривање једноставним средствима; све су заступљенији и прислушни уређаји с дистанциним (даљинским) управљањем.

Све то отежава рад на откривању и блокирању канала отицања акустичке информације и диктира неопходност коришћења најновијих средстава контрашпијунаже.

АПАРАТУРА ЗА ПРОНАЛАЖЕЊЕ РАДИОМИКРОФОНА[36]

Паралелно с развојем АСТПАИ усавршава се и апаратура за откривање радиоканала отицања акустичне (говорне) информације. При избору средстава која ће мо представити у овом прегледу, предност је дата апаратури, заснованој на коришћењу висококвалитетних ускоопсежних канала фреквенцијске селекције, јер широкопојасни пријемници непосредног појачања, индикатори поља, нумерички мериоци фреквенције и други слични уређаји не решавају задатак у пуном обиму, као и апаратури за аутоматско проналажење и идентификацију емитовања, која захтева минимално учешће оператера у процесу откривања.

35 Исто
36 Исто

Од аутоматизованих индустријских радиопријемних уређаја с добром вредношћу показатеља „ефикасност-цена," распрострањени су уређаји **AP- 3000A јапанске фирме "AOR Ltd".** Још више показатеља и добру перспективу има радиопријемник **AP-5000** исте фирме, који је на тржишту од почетка 2001. године.[37]

ПРАВЦИ УСАВРШАВАЊА АПАРАТУРЕ ЗА ПРОНАЛАЖЕЊЕ ПРИСЛУШНИХ УРЕЂАЈА[38]

Основна сврха апаратуре за проналажење прислушних уређаја је доношење поузданог решења за информациону безбедност у границама контролисане просторије или објекта за што је могуће краће време уз минимално учешће оператера, те је брзина рада веома пожељна. Задатак одређивања места пронађеног прислушног уређаја у границама конкретне просторије има помоћни значај и може се у интересу даље организације ове контраигре решавати на каснијим нивоима. (Нпр; за неутрализацију могуће штете од откривеног прислушног уређаја за време састанка може бити укључена апаратура за стварање сметњи, које отежавају пријем сигнала).

Задатак откривања прислушних уређаја треба решавати како за посебне просторије, станове, аутомобиле, тако и за установу у целини, што иницира неопходност развоја разноврсних преносних средстава и комплекса, као и стационираних комплекса.

КОНТРОЛА НЕКОЛИКО ПРОСТОРИЈА У ЈЕДНОЈ УСТАНОВИ[39]

Даље повећање функционалних могућности апаратуре за откривање радиоканала несанкционисаног прислушкивања могуће је уз обезбеђење контроле неколико просторија у једној установи. Слични задаци могу се решавати при опремању уређаја за проналажење таквим допунским апаратурним и програмским блоковима као што су пулт сакупљања информација с вишеканалним антенским и нискофреквенцијским комутаторима, као и антене, акустички ступци и блокови за спој с пултом сакупљања информација према броју контролисаних просторија. На пример, апаратура АРК-Д3, са коришћењем детаљне опреме, која обезбеђује истовремену контролу неколико (до 12) просторија, удаљених од пулта сакупљања информација до 100 м, при минималном учешћу оператера, може извршити анализу радног дијапазона фреквенција за откривање у контролисаним просторијама разних прислушних уређаја (између осталог и простим скрембловањем) и (по команди оператера) одредити њихове координате.

БЕЗБЕДНОСТ ИНФОРМАЦИОНИХ СИСТЕМА

Безбедност информационих система (**INFOSEC**) подразумева безбедност података на електронским медијима и рачунарима (**COMPUSEC**), безбедност података у системима за пренос података (**COMSEC**) и обезбеђење информационе

37 Исто
38 Исто
39 Исто

инфраструктуре у посебним категоријама простора од различитих врста пасивног или активног прислушкивања (**TECSEC**).

Пре обраде ове теме изнећемо неке податке о спроведеним истраживањима која ће допринети разумевању значаја безбедности информационих система.Терористички напади на САД од стране Ал-каиде, 11.09.2001. године, иницирали су компанију „КПМГ" да спроведе истраживање у области информационих система у свету. Током истраживања, спонзорисаног од више познатих фирми (CheckPoint, Symantec, Info-Security Magazine итд.), обављен је 641 телефонски разговор са одговорним лицима за безбедност информационих система у различитим организацијама из различитих економских области са седиштима у скоро свим крајевима света. Контактиране су махом велике фирме, од којих је 31% имало од 1.000 до 5.000 запослених. Све анкетиране фирме су имале преко 50 милиона долара годишњег обрта.

Након обављених разговора, извршених анализа добијени су резултати који су се односили на извршене нападе на информационе системе анкетираних фирми.[40]

Ови напади рангирани су по следећем:

- Инциденти са рачунарским вирусима.....22%
- Напади од стране хакера.....21%
- Губљење даљинске контроле.....17%
- Нарушавање безбедности у раду на Интернету…….....10%
- Рушење тајности личне информације.....5%
- Недостатак нивоа обучености корисника.....5%
- Нарушавање безбедности система Б2Б.....5%
- Преваре од стране запослених.....4%
- Крађе или кварење података информација.....4%
- Остало.....7%

Истраживање КПМГ-а, али пре свега (Ernest & Young-а) и ФБИ-а, извршена почетком овог века, недвосмислено указују на следећи закључак: "**Сигурност података – проблем људског понашања".**

Ernst & Young овакав закључак базирају на следећим показатељима[41]:

- 66% компанија кажу да имају проблем са заштитом података;
- 65% компанија су нападане од својих запослених;
- 51% компанија виде безбедност информација као приоритет, а
- 40% не истражује безбедносне инциденте.

Ово су подаци добијени од компанија. За разлику од ових сазнања, **ФБИ износи своја истраживања о компанијама.** Према истима, подаци су следећи[42]:

- 70% указују да је Интернет најчешће тачка напада;
- 64% компанија претрпеле су финансијске губитке;
- 49% су детектовале неауторизован приступ од стране инсајдера (ово је тзв; **унутрашњи напад** и представља коришћење система легитимног корисника на недозвољен начин. Ово је један од најопаснијих напада на систем. Спречава

40 KPMG, Global information Security Survey, www.kpmg.ru 2002.
41 EY, information Security Survey 2001-2002.
42 FBI, Computer Crime and Security Survey, 2001.

се ригорозном провером особља, праћењем коришћења система (откривање покушаја напада), пажљивом провером конфигурације система, уређаја и програма, те спровођењем безбедносних механизама како би се омогућио исправан рад система.[43]
- 40% су детектовале спољне упаде, и
- 36% компанија су детектовале безбедносне инциденте.

Анализом напада на информационе системе бавио се и **John Howard.** Према његовим истраживањима, садржана су у његовој докторској дисертацији из 1997. године, већина компјутерских злоупотреба остане неоткривено, па чак и намерно сакривено. Посебно банке прикривају компјутерске злоупотребе јер би се откривањем крађа банке лоше котирале на банкарском тржишту. За идентификоване крађе, средња вредност штете кретала се око 500.000 америчких долара.[44]

На основу свега досад реченог о информационим системима намеће се закључак да је човечанство ушло у критичну фазу зависности од информационих технологија (ИЦТ). Ову констатацију потврђујемо тиме, што се данас скоро ни један посао не може иницирати и реализовати без употребе ИЦТ. Још важнија констатација садржана је у чињеници да је велики број података, сложена опрема велики узрок рањивости ИЦТ-а. Због ових чињеница, посебно због пресудно животног значаја информација, питање заштите ИЦТ се изузетно заоштрава на свим нивоима.

Безбедност информационих система обухвата примену мера за заштиту података који су у обради или су унесени, или је у току њихов пренос, од губитка поверљивости, интегритета и расположивости, као и због спречавања губитка интегритета или расположивости самих система.

Безбедносне мере укључују механизме и процедуре који треба да буду спроведени у сврху одвраћања, превенције, детекције и опоравка од утицаја инцидената који делују на поверљивост, интегритет и расположивост података и пратећих системских услуга и ресурса, укључујући и извештавање о безбедносним инцидентима.

Безбедност информационих система, да би била у функцији намене, мора бити систематизована и као[45]:
- **административна** (управна) безбедност (подразумева прописивање организационих мера ради безбедности);
- **безбедност особља** (којом се детерминише понашање особља);
- **физичка безбедност** (могућност планирања **backup** процедура у случају прекида сервиса и заштита опреме ради спречавања неауторизованог увида у информације, уништавања или мењања информација, и
- **процедурална безбедност** (подразумева одговор у случају инцидента, а менаџмент ризика бави се проценом баланса безбедносног система у односу на идентификовану претњу и рањивост система).

43 Брачик Н., Живадиновић Ј., Пословни и финансијски информациони системи, друго издање, Чачак 2006, стр.109.
44 Howard D. John, An Analysis of Security incidents on the Internet 1989 – 1995,THESIS-SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY, Carnegie Mellon University-Cornegie Institute of Techology, 1997.
45 Родић Бошко и Костић Мирољуб, Идентификација фактора информационе безбедности у амбијенту примене информационо-комуникационе технологије (у Републици Србији), Међународни научно-стручни скуп-ИНФОРМАЦИОНА БЕЗБЕДНОСТ 2009, Академија за дипломатију и безбедност, Београд, стр.63.

Према напред изнетом, безбедност информационих система је динамичан процес током целог животног циклуса система, па је потребно, да упростимо, размотрити га од фазе његовог планирања, развоја, спровођења, оперативности и раста до расходовања и уништавања према потреби. То је заправо процес управљања ризиком који се користи за процену, надгледање, укидање, избегавање или прихватање ризика. Управљање ризиком је вештина која ставља у равнотежу трошкове примене додатних безбедносних противмера због користи која из тога проистиче. Сврха процеса управљања ризиком је осигурање трајне функционалности безбедносних циљева поверљивости, интегритета и расположивости података.

ОПЕРАЦИОНА ЗАШТИТА

Операциона заштита се односи на пословне процесе у компанији који могу прикупити информације на нетехничким путем. Политика забране коришћења отворених комуникационих линија, као што су интернет и телефонски системи, смањују могућност прикупљања информација од стране индустријских шпијуна. Друге врсте операционе безбедности се односе на компанијине клијенте, купце и продавце.

Операциона заштита је комплексна и захтева детаљну студију како компанија послује. Компаније морају проучити целокупно истраживање, развој, производњу и продајне процесе као потенцијалне путеве прикупљања информација. Мора постојати јасно разумевање коме поверити информације и под којим условима. Људи морају знати које информације морају заштитити и начин на који да их заштити. **Сваки запослени, да би био у функцији безбедности, мора бити охрабрен да пријави сумњиве појаве.**

ЗАШТИТА ЗАПОСЛЕНИХ

Сви запослени који имају приступ поверљивим информацијама морају бити, већ смо то истакли, подвргнути темељној провери.

Термин запосленисе односи на све оне који имају физички приступ објектима или информацијама. Објекти су сви, нпр; компјутерски терминали којима се приступа до компанијиних информација.Многе компаније не обраћају пажњу на запослене на најнижем нивоу као што су, нпр; домари, нижи службеници и обезбеђење.

Колико је важна безбедносна заштита запослених показаћемо на следећем случају: власник једне компаније-ималац пословне тајне, дозволио је својим запосленима, пушачима, да пуше у једној за то одвојеној просторији. По изласку службеника, листа корисника коју је он понео са собом је остала без надзора на столу просторије за пушаче. Посетиоцима компаније је такође било дозвољено да седну унутар ове просторије и у овом случају, „и да имају слободан приступ важном документу компаније, њиховој пословној тајни-листи конзумената без икаквог надзора". Овај пример показује недостатак безбедносне културе код запослених, недостатак једне пословне заштите, јер је очигледно да је једна пословна тајна могла да дође у додир са непозваним лицима.

Да би се овакви пропусти спречили, неопходно је предузети одређене мере и то према свим запосленима, од њиховог запослења у одређену компанију.

РАЗГОВОРИ СА ЗАПОСЛЕНИМА

Минимално, разговоре са запосленима би требало водити на почетку радног односа, периодично током радног односа (годишње), када се појави проблем и коначно након окончавања радног односа. Сваки разговор би требало да укључује потписану изјаву да им је процедура поверљивости јасно објашњена, (**изложили смо шта су „нотес мере", које су процедуре обавештавања и њихов значај***)* да ће следити све процедуре и да ће вратити све информације компанији онда када им више не буде потребна за пословање, као и да уколико икада буду желели да користе информацију (или открију) која може бити поверљива – да ће тражити најпре дозволу од компаније за то.

Свим запосленима, а посебно оним која су у контакту са поверљивим информацијама, **мора бити објашњен начин обележавања докумената,** посебно поверљивих. Већина компјутерских система ће аутоматски штампати поверљивост на свакој страници онда када су адекватно програмирани. **Гумена значка која носи ознаку „поверљиво"** може бити смештена на сто сваке особе која често гледа поверљиве материјале. Такође, често се користи и **црвено мастило** на таквим ознакама. Јасна ознака „поверљиво" на тим документима представља и изузетно добар начин обавештења, а и психолошки делује на онога ко је у додиру са поверљивом информацијом. Ако је добро обавештен, припремљен за рад са поверљивим информацијама, зна значај тајне за компанију, страх од губљења исте изазива повећање пажње, а самим тим и безбедност такве поверљиве информације-пословне тајне.

О пословним плановима компаније, програмима развоја, губицима и профиту, кадровским и другим решењима, добављачима и купцима, **разговара се на стручним састанцима,** колегијуму, управним одборима, састанцима акционара итд. На овим састанцима износе се поверљиве информације, дефинишу се пословне тајне компаније, одређују лица која имају право располагања истима, одређују процедуре заштите. Самим тим неопходно је увести, да сви присутни учесници оваквих поверљивих састанака о томе буду обавештени на почетку састанка и да ће сви морати да потпишу **изјаву о поверљивости** у циљу обавезивања чувања поверљивих информација изнетих на састанку. Ово је посао менаџера безбедности или саветника за безбедност чија управљачка функција на оваквим састанцима треба да дође до правог изражаја.Посебан аспект безбедности запослених даје и **озбиљност санкционисања пропуста**у заштити поверљивих информација. Ако неко у компанији не поштује, следи процедуре поверљивости, мора за то да сноси санкције. Санкције морају бити еквивалент насталим последицама за компанију. Изречене казне, нпр; опомена, смањење примања за одређени период, премештај на ниже радно место, губљење годишњег бонуса, добијање отказа, морају се јавно презентирати у циљу општег упозорења, сталног притиска на запослене да је поштовање процедура поверљивости неопходна.

Колико је овај аспект код заштите запослених битан, можда је још битнији **аспект награђивања.** Награде би требало користити када су одређене последице озбиљније и исте би требало дати онима који су открили или иницирали актуелна и потенцијална места где информације „цуре". Такође, награде могу бити прописане и за оне запослене који указују на лица која не следе процедуру поверљивости. Често запослени имају више разумевања (говорећи појединачно) о томе, како се поједине поверљиве информације третирају у компанији, него сами менаџери.

Награде делују стимулативно на запослене, утичу да они више пажње посвећују развијању своје опште безбедносне културе, односа према компанији у којој раде.

Једна од најбитнијих компоненти опште заштите било ког привредног ентитета је успети у томе, да сви запослени буду у функцији безбедности. По нашем мишљењу ово треба да буде и основни параметар вредности и успешности функције корпоративне безбедности у једној компанији.Ако се некада, бивша СФРЈ поносила својим системом ОНО и ДС, крилатицом: „сви смо ми војска", онда би крилатица запослених у сваком привредном ентитету (компанији) требала да буде: „сви смо ми заштитари своје компаније."Ово су уопштени примери понашања према поверљивим информацијама. Заштитити своје поверљиве информације је озбиљан процес који захтева организованост, дисциплину и професионалност.[46]

Већ смо навели три основна начина нарушавања информационе безбедности у савременом свету. Заједничко им је да сви ови облици угрожавања националне безбедности имају значајне међународно-правне импликације, али ћемо ми, због значаја, највећу пажњу посветити могућностима међународног јавног права да санкционише покушаје угрожавања информационе безбедности у савременој међународној заједници.

ЗАКЉУЧАК

Анализирани правци развоја уређаја за прислушкивање не исцрпљују њихову разноликост, а апаратура за откривање радиоканала отицања говорне информације нема граница за усавршавање, исто као и супротна њој техника прислушкивања акустичне информације. Уједно, ако је пренос добијене акустичне информације везан њеним емитовањем преко радиоканала, што у блиској зони (тј; у границама контролисане просторије) није могуће потпуно сакрити, приказани правци развоја технике спречавања шпијунаже, који се састоје у повећању брзине рада, ширењу функционалних могућности и побољшању техничких параметара, актуелни су за откривање било каквих техничких средстава, предвиђених за задовољавање професионалне радозналости индустријских шпијуна.Овде је приказан начин и средства за откривање прислушних средстава. Ако је ФТО компаније дошло у ту фазу, сумња да су индустријски шпијуни пробили њен систем заштите, уградили прислушно средство, морају анализом констатовати да су им затајиле превентивне мере.**Превентивне мере,** усмерене на затварање могућих канала отицања информација пожељно је вршити при усељењу фирме у нове просторије, приликом закупа опреме, куповини намештаја, као и за време извођења грађевинско-ремонтних радова. Ово су идеалне ситуације које се користе за уградњу прислушних

46 Симовић С; Индустријска шпијунажа и заштита пословне тајне, Графостил, Крагујевац, 2012, стр.243.

средстава. Превентивно постављање се огледа и у затварању канала којима могу отицати информације. Ових "канала" има пет, и то:[47]

1. **Акустички канали** (тавани, рупе, цеви кроз које струји ваздух, итд.)
2. **Виброакустички канали** (батерије, чврста средина носећих конструкција зграде, постављених цеви).
3. **Проводни канали** у које спадају и проводне линије које излазе из конкретне просторије (телефонске, енергетске итд.).
4. **Електрична и магнетна поља** изнад 30 мегахерца, електромагнетна поља и радио етар, и
5. **Оптички канал,** којим долази до отицања информација преко модулације јачине осветљавања или инфрацрвених извора зрачења.

Ови канали морају се редовно проверавати, а пре почетка рада компаније на одређеној локацији, новом простору, просторији потребна је потпуна провера свих канала. За то су потребна адекватна техничка средства, а пре свега добро обучени кадрови корпоративне безбедности.Генерални закључак, када су у питању мере физичке-техничке заштите поверљивих информација био би: мере физичке заштите треба бирати у складу са самим послом компаније која се штити. Где год се то чини разумним поставити мере физичке заштите. Као што је раније поменуто, до једног броја поверљивих информација се долази путем "обичних" провала и крађа, због тога физички приступ објектима мора бити пажљиво регулисан и контролисан. Овде се подразумева не само ограничен приступ посетиоцима у рестриктивни простор, већ и самим запосленима.Сви у штићеном објекту морају носити идентификационе беџеве којима се потврђује њихов статус, као што је посетилац, запослени итд. Наравно, неопходно је имати обезбеђење које ће ова лица идентификовати. Што рестриктивније мере обезбеђења неко користи, мања је опасност да ће мере обезбеђења бити нарушене. Уколико се и појаве безбедносни проблеми, код добре организације физичке заштите брзо се неутралишу.Техничка заштита смањује рањивост која је присутна у електронском систему. Ту се подразумева тајност, интегритет и доступност компјутерских система и мрежа. Добра техничка безбедност такође чува друге електронске системе као што је говорна пошта. Електронска безбедност је најчешћа и присутна у свим већим компанијама. Данас је само једно сигурно: " да је више физичко-техничке заштите далеко боље него мања заштита, и да је превентивно постављање основ успешности ФТО, односно укупне заштите компаније".

У том циљу, заштите компаније у свим сегментима безбедности, а посебно заштите пословне тајне је и безбедност информационих система, операциона заштита и заштита запослених.

ЛИТЕРАТУРА:

1. **Анђелковић** Слободан, Специјалистички рад „Савремени концепт корпоративне безбедности", Факултет политичких наука, Београд, јуни 2005.

47 APIS Security Consulting, Индустријскашпијунажаиодбранаодње,оп.цит.

2. **Брачик** Н., Живадиновић Ј., Пословни и финансијски информациони системи, друго издање, Чачак 2006.
3. **Mitnick** D. Kevin, "Уметност обмане", Микрокњига, Београд, 2003.
4. **Пејановић** Љ., Лаковић В., Стојановић С., Угрожавање и физичко-техничка заштита, Београд, 2007.
5. **Првуловић** Владимир, „Економска дипломатија", ПС"Грмеч"-„Привредни преглед", Београд, 2001.
6. **Симовић** С; Индустријска шпијунажа и заштита пословне тајне, Графостил, Крагујевац, 2012
7. **Родић** Бошко и Костић Мирољуб, Идентификација фактора информационе безбедности у амбијенту примене информационо-комуникационе технологије (у Републици Србији), Међународни научно-стручни скуп-ИНФОРМАЦИОНА БЕЗБЕДНОСТ 2009, Академија за дипломатију и безбедност, Београд.
8. **Милошевић** М; Заштита пословних података и докумената, Правни информатор, www.Informator.co.yu.
9. **Кековић Зоран „**Корпоративна безбедност." У: Кековић, З; Димитртијевић, И; „Системи безбедности са системом безбедности Републике Србије", Београд, Факултет безбедности, 2017
10. **Howard** D. John, An Analysis of Security incidents on the Internet 1989 – 1995,THE SIS-SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY, Carnegie Mellon University-Cornegie Institute of Techology, 1997.
11. Стандард ИСО 17799, Информационе технологије – Правила праксе за управљање безбедношћу информација, ИСО/ИЕС, 2000.
12. General Security risk assessment, ASIS international , 2003.
13. Извор: APIS Security Consulting "Odbrana od krađe informacija", file://F.ISH 4.html,21.03.2006..
14. KPMG, Global information Security Survey, www.kpmg.ru 2002.
15. EY, information Security Survey 2001-2002.
16. FBI, Computer Crime and Security Survey, 2001.