**Bezpečnostné riziká**

Fyzická bezpečnosť objektu či organizácie sa odvíja od bezpečnostných rizík (rizík bezpečnosti). Keby žiadne bezpečnostné riziká neboli, nemusela by sa bezpečnosť vôbec riešiť. Ideálnym cieľom bezpečnostnej politiky by mala byť snaha o modifikáciu všetkých bezpečnostných rizík. To však v praxi nie je možné, pretože modifikovať všetky riziká by stálo nekonečné množstvo opatrení a organizácia má vždy iba obmedzený limit prostriedkov, ktoré môže do svojej bezpečnosti vložiť.

Táto veľkosť prostriedkov záleží na rozhodnutí vrcholového manažmentu a je v každej organizácii iná. S nimi je možné modifikovať najzávažnejšie bezpečnostné riziká, avšak nikdy sa nepodarí pokryť všetky. Ak má organizácia nulové výdavky na bezpečnosť, nemodifikuje žiadne riziká, teda aj tie najväčšie bezpečnostné riziká pretrvávajú.

Efektívna je len taká bezpečnosť, kde sa na bezpečnosť nevydáva viac, ani menej prostriedkov, než je suma hodnôt neriadených rizík.

Bezpečnostné riziká (čisté riziká) tvoria špecifickú kategóriu rizík, ktoré majú svoj zdroj v určitom nebezpečenstve. Nebezpečenstvo predstavuje zdroj možného poškodenia, môže byť zdrojom rizika.

Nebezpečenstvo, ako zdroj rizika, je vlastnosť alebo schopnosť objektu (systému, stroja, materiálu, výrobnej technológie a pracovnej činnosti, prípadne ich komponentov) spôsobovať nebezpečné udalosti, ktoré môžu narušiť bezpečnosť, ohroziť stabilitu a fungovanie príslušného systému, prípadne aj jeho okolia.

Pravdepodobnosť výskytu a možný následok úmyselnej alebo náhodnej nebezpečnej udalosti predstavuje konkrétne riziko, že dôjde kujme na zdraví zamestnancov, zákazníkov a ostatných osôb, hmotných a nehmotných aktívach organizácie, životnom prostredí alebo ohroziť činnosti a ciele organizácie.

Bezpečnostné riziká vo všetkých prípadoch vyjadrujú len mieru ohrozenia, nikdy nepredstavujú príležitosti. Bezpečnostné riziko je preto kombináciou pravdepodobnosti výskytu určitej nebezpečnej udalosti a jej potenciálnych následkov (škody).

Rozdelenie bezpečnostných rizík

V závislosti od druhu nebezpečenstva ako zdroja, a spôsobov jeho prejavu možno bezpečnostné riziká deliť na:

a) Riziká úmyselného napadnutia (riziká úmyselného ohrozenia bezpečnosti) – Security risks,

b) Náhodné bezpečnostné riziká (riziká náhodného ohrozenia bezpečnosti) – Hazard risks.

**RIZIKÁ ÚMYSELNÉHO NAPADNUTIA**

Riziká úmyselného napadnutia môžu spôsobiť ujmu úmyselným konaním. Znamenajú pravdepodobnosť, že dôjde k ohrozeniu chráneného záujmu (hodnoty) kriminálnym činom iných ľudí a veľkosť možných následkov takejto udalosti (napr. pravdepodobnosť a následky vlámania).

Podrobnejšia definícia podľa Talbota a Jakemana je: *„riziko úmyselného napadnutia je udalosť, ktorá by mohla viesť k ohrozeniu aktív organizácie, t. j. neoprávnené použitie, strata, poškodenie, prezradenie alebo upravenie aktív organizácie pre zisk, osobný záujem alebo politické záujmy jednotlivcov, skupín alebo iných entít, ktoré predstavujú ohrozenie aktív a zahŕňajú riziko zranenia ľudí. Ohrozenie aktív môže negatívne ovplyvniť organizáciu, jej prevádzkové jednotky a klientov. Z toho dôvodu je posúdenie bezpečnostných rizík dôležitou súčasťou riadenia rizík“(Talbot, Jakeman, 2009).*

Zdrojom úmyselného napadnutia je teda cieľavedome konajúca fyzická osoba, pričom motív takéhoto konania môže byť:

• politický, alebo politicko-vojenský, vyplývajúci z politických, vojenských alebo ekonomických záujmov štátov (napr. spravodajské služby),

• ideologický, viažuci sa na určitý politický a/alebo ideologický systém (napr. politický terorizmus, extrémizmus, náboženský fundamentalizmus, ekologický radikalizmus a pod.),

• ekonomický, založený na snahe o bezprácny zisk (kriminálni jedinci a zločinecké skupiny), alebo poškodenie konkurencie (odporcovia, konkurenti, komerčné spravodajské služby),

• osobný, vyvolaný napr. pocitom nenávisti, krivdy, vydieraním vlastnej osoby alebo ohrozovaním rodinného príslušníka, povahovými črtami osoby a pod.

Medzi riziká úmyselného napadnutia možno zaradiť:

**1. Sociálnopolitické riziká:**

• vzbury, pouličné nepokoje a teroristické incidenty (Alexander, 2000),

• rabovanie – nekontrolované branie cudzích vecí a tovaru počas katastrofickej udalosti, či občianskych nepokojov vrátane vojny v období anarchie, kedy štátne zložky dozerajúce na poriadok nie sú schopné alebo ochotné zasiahnuť, poprípade majú rozkaz nezasahovať,

**2. Sociálne riziká – podľa Alexandra (2000) sem patria vzbury, pouličné nepokoje a teroristické incidenty.**

**3. Riziká úmyselného násilia proti osobám:**

a) fyzické násilie – úmyselné použitie sily proti inej osobe, bez zákonného oprávnenia, čo môže mať za následok fyzické zranenie alebo osobnú ujmu, napr.:

• útok na zamestnanca,

• násilie voči skupine,

• nebezpečné vyhrážanie

b) sexuálne násilie – forma diskriminácie na základe pohlavia, ktoré má svoje osobité prejavy, príčiny a vyžaduje si preto špecifické spôsoby eliminácie a prevencie. Ide o verbálne, neverbálne alebo fyzické správanie sexuálnej povahy, ktorého úmyslom alebo následkom je alebo môže byť narušenie dôstojnosti osoby a ktoré vytvára zastrašujúce, ponižujúce, zneucťujúce, nepriateľské alebo urážlivé prostredie,

c) nefyzické násilie – správanie, ktoré priamo narúša slobodnú vôľu a sebaúctu iného človeka. Nezanecháva síce žiadne viditeľné poranenia, napriek tomu môže byť najhoršou formou násilia, často sa spája s fyzickým násilím. Znamená použitie nevhodných slov alebo správanie, ktoré spôsobuje strach a / alebo predstavuje obťažovanie (narušenie medziľudských vzťahov). Používa sa v osobnom styku, telefonicky, listami, emailom alebo inou formou komunikácie, napr. graffiti

(zneužitie právomoci, • diskriminácia, • korupcia, úplatkárstvo, úžera,)

d) psychické násilie:

• psychické násilie, psychický teror, vyhrážky, vulgárna a dotieravá konverzácia; nežiaduce alebo hanlivé poznámky; ohováranie,

• šikanovanie – opakované a zámerné správanie, ktorého cieľom je vysmievať sa, ubližovať niekomu, ponižovať ho, agresor zneužíva svoju moc nad obeťou,

• kyberšikanovanie (elektronické šikanovanie, kyberbullying, kybermobbing) – forma šikanovania, pri ktorej sa používajú nové technológie, ako je počíňtač, internet, mobilný telefón.

• kybernetické prenasledovanie (online prenasledovanie, kyberstalking) – neustále sledovanie niekoho vo virtuálnom prostredí, často spojené s obťažovaním, vyhrážaním a zastrašovaním.

• happy slapping – násilné alebo sexuálne útoky na obete (často aj náhodne vybrané), ktoré sú natáčané na mobilný telefón, útočníci videá ďalej rozposielajú alebo zverejňujú na internete.

• mobbing, čiže psychický teror – trvalé, systematické a intenzívne útoky, intrigy a šikanovanie väčšieho počtu pracovníkov alebo nadriadeného voči jednotlivcovi alebo menšej skupine

**4. Riziko úmyselného spôsobenia majetkovej ujmy – úmyselné narušenie bezpečnosti majetku a infraštruktúry organizácie, čo môže spôsobiť majetkové škody, napr.:**

a) krádež – prisvojenie si cudzej veci či hodnoty zmocnením sa tejto veci či hodnoty:

• krádež vlámaním

• prostá krádež

• krádeže zamestnancami (insider),

b) lúpež (lúpež so zbraňou) – použitie násilia alebo hrozba bezprostredného násilia v úmysle zmocniť sa cudzej veci bez alebo s použitím zbrane,

c) vandalizmus – úmyselné poškodenie alebo úmyselné zničenie veci, zlomyseľné konanie, napr. páchateľ porozbíja okná na budove alebo poleje kyselinou motorové vozidlo atď.,

d) sabotáž – obvykle utajené a často násilné, úmyselné a plánované narušenie funkčnosti či výkonnosti (dôležitého) zariadenia prostredníctvom jeho poškodenia alebo zničenia,

e) podvod – obohatenie uvedením niekoho do omylu alebo využitím omylu niekoho a spôsobenie škody na cudzom majetku,

f) sprenevera – prisvojenie cudzej veci, ktorá bola zverená zamestnancovi, a spôsobenie škody na cudzom majetku,

g) špionáž – ohrozenie utajovanej skutočnosti,

h) úmyselné porušenie tajomstva – listového, bankového, tajomstva informácie, tajomstvo neverejného prenosu počítačových dát,

i) ďalšie spôsoby poškodzovania cudzej veci: (• záškodníctvo, podpaľačstvo,

• zničenie, poškodenie cudzej veci a spôsobenie škody na cudzom majetku, • fyzické poškodenie informačných a komunikačných technológií, • poškodenie technických zariadení – kanalizácia, vodovod, plynovod, vykurovanie, • úmyselný výbuch plynu, • použitie výbušniny, • poškodenie alebo ohrozenie prevádzky, k. neoprávnené používanie cudzej veci, či motorového vozidla.)

**4. Riziká úmyselného narušenia všeobecnej bezpečnosti:**

a) útok na verejného činiteľa v organizácii v štádiu prípravy alebo pokusu,

b) všeobecné ohrozenie.

**5. Riziká úmyselného poškodenia životného prostredia** – nezákonné nakladanie s odpadkami, vypúšťanie znečisťujúcich látok, znečisťovanie vôd a ovzdušia