PROCES MANAŽÉRSTVA BEZPEČNOSTI I
PLÁNOVANIE BEZPEČNOSTI

Security Management Process I – Security Planning

Ľubomír BELAN
FBI UNIZA, Katedra bezpečnostného manažmentu, Ul.1.mája 32, 010 26, Žilina, SR
Lubomir.Belan@fbi.uniza.sk

Lubomír BELAN
AOS, Katedra manažmentu, Demänová 393, 031 06, Liptovský Mikuláš
Lubomir.Belan@aos.sk

Abstrakt Príspevok rieši problematiku postupnosti procesu manažérstva bezpečnosti spracovanú podľa prílohy SL a je zameraný na súvislosti organizácie a prvú časť Demingovho cyklu manažérstva bezpečnosti organizácie – Vedenie, Plánovanie a Podpora.

Abstract The contribution deals with the issue a sequence of security management process carried out according to Annex SL and are focused on the context of the organization and the first part of the PDCA cycle – Leadership, planning and support.

ÚVOD

Manažérstvo bezpečnosti predstavuje sústavný, opakujúci sa súbor navzájom previazaných aktivít organizácie na plánovanie, zavedenie, prevádzkovanie, monitorovanie, hodnotenie a trvalé zlepšovanie systému manažérstva bezpečnosti (SMB), s cieľom dosiahnuť požadovanú úroveň bezpečnosti organizácie.

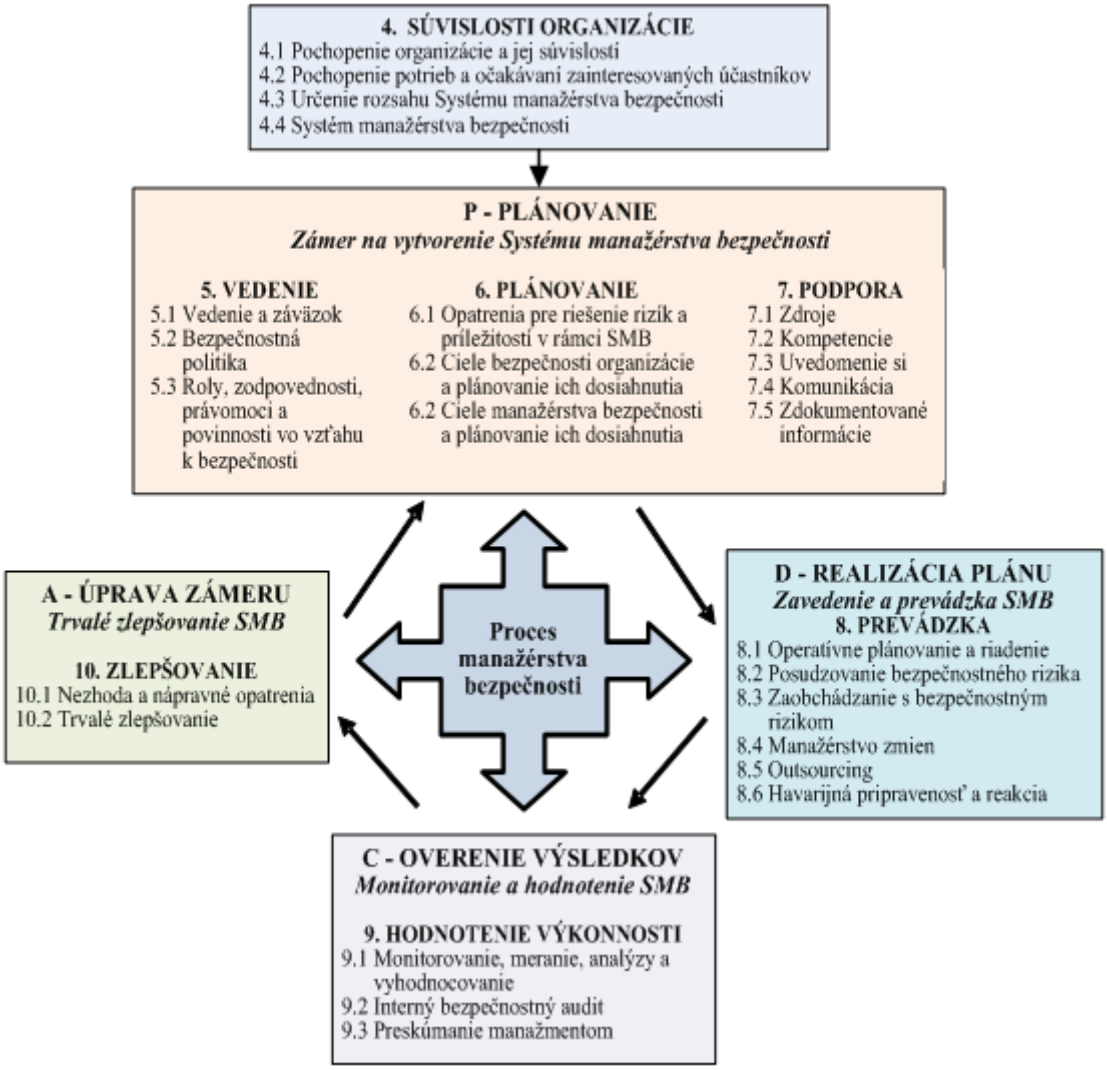
Na stanovenie postupnosti procesu manažérstva bezpečnosti je možné využiť všeobecnú normu, predpísanú pre systémy manažérstva, spracovanú podľa prílohy SL. Proces manažérstva bezpečnosti organizácie je potom možné názorne zobraziť s využitím PDCA cyklu (Demingov cyklus), ktorý je vhodným modelom pre všetky typy manažérskeho zlepšovania procesov, kvality výrobkov, služieb, aplikácií, dát, prebiehajúci formou opakovaného vykonávania štyroch základných činností, uvedených na obr. 1.

Obsah normy pre systémy manažérstva spracovanej podľa prílohy SL je možné rozdeliť na časti:

A. Všeobecná časť, body:
0. Úvod,
1. Rozsah,
2. Citované normatívne dokumenty,
3. Termíny a definície.

B. Vstupy do procesu manažérstva – bod 4. Súvislosti organizácie.

C. Cyklický proces manažérstva podľa modelu P (5, 6, 7), **D** (8), **C** (9), **A** (10).



Obr. 1 PDCA cyklus manažérstva bezpečnosti organizácie

SÚVISLOSTI ORGANIZÁCIE

Organizácia má túto časť vykonať ešte pred zvážením zavedenia systému manažérstva bezpečnosti. Predstavuje základ pre systém manažérstva bezpečnosti – ide o určenie, prečo vlastne je pre organizáciu potrebný systém manažérstva bezpečnosti. Organizácia potrebuje určiť:

- svoje závažné ***vnútorné a vonkajšie súvislosti***, ktoré môžu mať vplyv na jej bezpečnosť a dosiahnutie cieľov organizácie,
- všetkých ***zainteresovaných účastníkov a ich požiadavky*** vo vzťahu k bezpečnosti,
- ***rozsah a rozhranie systému manažérstva bezpečnosti*** – čo je vo vnútri a čo je mimo neho.

Toto poskytne **súhrnný významný vnútorný pohľad na organizáciu.** Nemalo by ísť iba o prostý zoznam, ale o ***úplný zoznam***, ktorý poskytne ***súhrnný významný vnútorný pohľad na organizáciu, ktorý by bol jasný a zrozumiteľný.*** Uvedené skutočnosti sú potrebné na určenie cieľov organizácie. Identifikované problémy a požiadavky sa budú riešiť v časti 6. Plánovanie. Nakoniec organizácia potrebuje **vytvoriť a prevádzkovať svoj systém manažérstva**.

Etapa súvislosti organizácie obsahuje:

1. **Pochopenie organizácie a jej súvislostí (*ciele organizácie a plánované výsledky, vnútorné a vonkajšie problémy v bezpečnosti),***
2. **Pochopenie potrieb a očakávaní zainteresovaných účastníkov.**
3. **Určenie rozsahu Systému manažérstva bezpečnosti.**
4. **Systém manažérstva bezpečnosti** (SMB).

Pochopenie organizácie a jej súvislostí

Základom pre pochopenie organizácie a jej súvislostí je **zistenie aktuálneho stavu bezpečnosti v organizácii**, ***kladov a nedostatkov*.** Aktuálny stav bezpečnosti v organizácii je možné zistiť vykonaním **analýzy stavu bezpečnosti organizácie**. Postup pri riešení **súvislostí organizácie** sa má vykonať v súlade s bodom **4.3.1 Chápanie organizácie a jej súvislostí normy STN ISO 31000:2011 Manažérstvo rizika. Zásady a návod,** kde je uvedený obsah hodnotenia externých i vnútorných súvislostí organizácie.

Analýza stavu bezpečnosti organizácie môže potom obsahovať:

1. **Ujasnenie základných údajov o organizácii:**
   - účel, vízia, ciele, stratégia, umiestnenie, organizačná schéma, činnosti, funkcie, služby, produkty, partnerstvo, dodávateľské reťazce, vzťahy si zainteresovanými účastníkmi a potenciálny dopad spojený s rušivým incidentom,
   - väzby medzi uplatňovanou politikou bezpečnosti a cieľmi organizácie a ďalšími politikami, vrátane stratégie manažérstva rizika,
   - ochota organizácie prijímať riziká.
2. **Posúdenie a pochopenie externých súvislostí** (podľa STN ISO 31000):
   a) **Faktory prostredia na medzinárodnej, národnej, regionálnej alebo miestnej úrovni:** sociálne, politické, právne, kultúrne, ekonomické a finančné, technické, prírodné, ekologické a konkurenčné faktory.
   b) **Kľúčové motívy a trendy, ktoré ovplyvňujú ciele organizácie:**
   c) **Vzťahy, vnímanie a hodnoty externých zainteresovaných účastníkov,**
   d) **Faktory, ktoré majú vplyv na bezpečnosť:**
      - ***geografické faktory okolia,***
      - ***zdroje mimoriadnych udalostí,***
      - ***kriminalisticko-bezpečnostné faktory.***
3. **Posúdenie a pochopenie interných súvislostí** (podľa STN ISO 31000):
   - riadenie, organizačná štruktúra, úlohy a zodpovednosti,
   - politika, ciele a stratégie, ktoré sa využívajú na ich dosiahnutie,
   - spôsobilosť organizácie v zmysle zdrojov a znalostí (napr. kapitál, čas, ľudia, procesy, systémy a technológie),
   - informačné systémy, tok informácií a procesy prijímania rozhodnutí (oficiálnych i neoficiálnych),
   - vzťahy s internými zainteresovanými účastníkmi, ich vnímanie a hodnoty,
   - vnímanie hodnôt a kultúry organizácie,
   - normy, návody, a modely prijaté organizáciou,
   - formu a rozsah zmluvných vzťahov, ale aj iné skutočnosti.
4. **Analýzu aktuálnej úrovne bezpečnosti** v jednotlivých podsektoroch a oblastiach bezpečnostného sektora:
   - zistenie stavu manažérstva bezpečnosti a manažérstva rizika, klady a nedostatky,

- posúdenie stavu ochrany osôb a majetku – plášťová a obvodová ochrana, priestorová ochrana, kontrola vstupov, predmetová ochrana, režimové opatrenia ochrany, fyzická ochrana, protipožiarna ochrana, ochrana pred účinkami priemyselných havárií a pod.,
- posúdenie stavu informačnej bezpečnosti – personálna, administratívna, fyzická a objektová, OUS, ochrana osobných údajov, ochrana bankového a iného tajomstva atď.,
- posúdenie stavu bezpečnosti infraštruktúry organizácie atď.

Metódami na zistenie (meranie) súčasného stavu bezpečnosti môžu byť napr.:

a) **prieskum medzi zamestnancami** – zameriava sa na parametre, ktoré určujú ***stav bezpečnostnej kultúry***, najmä ako ju vnímajú zamestnanci a poznajú jej hodnoty.
b) **analýza bezpečnostnej politiky –** poskytuje informácie o oficiálnych hodnotách organizácie a požadovaných štandardoch na jej vykonávanie, toto meranie by sa malo opakovať v pravidelných intervaloch.**,**
c) **pohovory s manažérmi, zodpovednými za bezpečnosť** a pod.

Pochopenie potrieb a očakávaní zainteresovaných účastníkov

Pri vytváraní SMB musí organizácia určiť:

- ***zainteresovaných účastníkov***, ktorí majú vzťah k SMB,
- ***požiadavky*** týchto zainteresovaných účastníkov (ich potreby a očakávania, či už boli vyhlásené všeobecne alebo sa predpokladajú, či sú záväzné),
- postupy pre identifikáciu, zaistenie prístupu a posudzovanie príslušných ***požiadaviek zákonov a predpisov***, ku ktorým sa zaviazala, tieto použiteľné požiadavky zákonov a predpisov zohľadňovať, dokumentovať a udržiavať ich aktuálne, nové požiadavky alebo zmeny požiadaviek zákonov a predpisov oznamovať dotyčným zamestnancom a zainteresovaným účastníkom.

Určenie rozsahu systému manažérstva bezpečnosti.

Pri stanovení rozsahu a hraníc SMB sa berú do úvahy: strategické ciele organizácie, hlavné produkty a služby, kritériá rizika, a všetky usmernenia, zmluvy alebo záväzky so zainteresovanými účastníkmi.

Organizácia v tomto kroku musí stanoviť **hranice a aplikovateľnosť SMB** pre ustanovenie rozsahu pôsobnosti, pričom musí zvážiť vonkajšie a vnútorné súvislosti organizácie a požiadavky zainteresovaných účastníkov.

Okrem toho organizácia musí:

a) určiť časti organizácie, ktoré majú byť zaradené do SMB,
b) určiť požiadavky SMB, ktoré zohľadňujú poslanie organizácie, jej dlhodobé zámery, vnútorné a vonkajšie záväzky a zodpovednosti vyplývajúce zo zákonov a predpisov,
c) identifikovať produkty a služby a všetky s nimi spojené činnosti v rámci SMB,
d) do úvahy vziať aj potreby a záujmy zainteresovaných účastníkov, ako sú zákazníci, investori, akcionári, dodávateľský reťazec, vstupy od verejnosti alebo spoločenstiev a ich potreby, očakávania a záujmy,
e) definovať rozsah SMB v podobe vhodnej pre veľkosť, povahu a komplexnosť organizácie.

Organizácia musí **vytvoriť, zaviesť, udržiavať a trvale zlepšovať SMB**, vrátane potrebných procesov a ich vzájomných väzieb, podľa požiadaviek noriem.

PLÁNOVANIE

Prvú časť Demingovho cyklu tvorí **Plánovanie (Plan),** v ktorom sú zaradené etapy:

- **Vedenie.**
- **Plánovanie.**
- **Podpora**.

VEDENIE

Etapa vedenia obsahuje:

1. **Vedenie a záväzok.**
2. **Politika bezpečnosti.**
3. **Roly, zodpovednosti a právomoci v organizácii.**

Vedenie a záväzok

Nové ustanovenia pre najvyššiu úroveň vedenia kladú ***osobitný dôraz na vedenie, nielen riadenie,*** to znamená, že vrcholový manažment má teraz väčšiu zodpovednosť a zapojenie do systému manažérstva bezpečnosti.

To znamená, že **vrcholový manažment musí mať zodpovednosť a byť zapojený do SMB**. Je potrebné začleniť ***požiadavky SMB do hlavných procesov organizácie***, zabezpečiť, aby dosiahol svoje plánované výsledky a prideliť mu potrebné zdroje.

Vrcholový manažment je tiež zodpovedný za ***komunikáciu*** o systéme manažérstva bezpečnosti a ***zvýšenie povedomia*** o jeho dôležitosti a za ***zapojenie zamestnancov***. Navyše musí dať najavo svoj ***záväzok na uistenie, že systém manažérstva vytvorí***. Zapojenie vrcholového manažmentu do systému manažérstva je potom jednoznačné a aktívne.

Manažérstvo bezpečnosti nie je jednorazový projekt, ale ide o trvalú a neprerušovanú aktivitu a ako taká, si vyžaduje jasný a trvalý **záväzok**. Záväzok predstavuje povinnosť, vyplývajúcu zo záväzného sľubu, zmluvy a pod.

Aby bol záväzok trvalý, musí byť iniciovaný **mandátom** zo strany vedenia organizácie, implementovaný vyšším manažmentom a podporovaný na všetkých úrovniach organizácie. Mandát znamená ***splnomocnenie (poverenie, oprávnenie) funkcionára*** mať zodpovednosť za riadenie určitej oblasti bezpečnosti v organizácii.

Vrcholový manažment musí **demonštrovať svoju vodcovskú rolu a záväzok** vzhľadom **na SMB:**

a) zaistením:
   - že sú vytvorené bezpečnostné politiky a ciele SMB a že sú v súlade so strategickým smerovaním organizácie,
   - integrácie požiadaviek SMB do hlavných podnikateľských procesov organizácie,
   - pridelenia zdrojov potrebných pre SMB,
   - že SMB dosiahne svoje plánované výsledky,
   - vykonávania interných bezpečnostných auditov,
b) ustanovením rolí, zodpovedností a právomocí pre manažérstvo bezpečnosti,
c) komunikovaním o význame a potrebe efektívneho SMB,
d) nasmerovaním a podporovaním osôb na prispievanie k efektívnosti SMB,
e) aktívnym zapojením do nácvikov a testovania,
f) podporovaním trvalého zlepšovania SMB a bezpečnosti organizácie,
g) podporovaním ďalších manažérskych rolí na preukázanie ich vodcovskej roly a záväzkov, ktoré sa vzťahujú k ich oblastiam zodpovednosti za bezpečnosť.

Politika bezpečnosti

Politika bezpečnosti, niekedy aj Bezpečnostná politika (stratégia bezpečnosti) je základný a východiskový dokument, ktorým organizácia deklaruje svoj záujem na implementáciu bezpečnosti do všetkých sfér činnosti. Predstavuje súhrn najvýznamnejších rozhodnutí, zameraných na zabezpečenie prijateľnej úrovne bezpečnosti organizácie. Je to prvý dôležitý míľnik implementácie SMB, ktorý definuje hodnotu bezpečnosti v celkovej činnosti organizácie a spôsob dosiahnutia bezpečnosti v rámci organizácie.

Bezpečnostná politika hovorí o význame bezpečnosti, kto je zodpovedný za bezpečnostné funkcie a aká úroveň bezpečnosti sa má dosiahnuť. Musí zahŕňať ***záväzok*** na splnenie platných požiadaviek a trvalé zlepšovanie systému manažérstva. Má potvrdiť zodpovednosť organizácie za oblasť bezpečnosti a jednoznačne ukázať, že ***zaistenie bezpečnosti je najvyššou prioritou v poskytovaní služieb***. Predstavuje deklaráciu zodpovednosti subjektu bezpečnosti (organizácie, podniku a pod.) za bezpečnosť osôb, ochranu majetku, informácií a životného prostredia. Definuje chránené záujmy subjektu a systémové zásady, ako tieto záujmy chrániť.

Prijatie zodpovednosti a záväzku vrcholovým manažmentom za dodržiavanie a zavedenie všetkých noriem bezpečnosti v politike bezpečnosti veľkej i malej organizácie je významným krokom, ktorý vylepší ich hodnotu a povesť, získa dôveru investorov a klientov, zvýši motiváciu a oddanosť zamestnancov a produktivitu práce a zníži náklady na úrazy, choroby a poistenie.

Manažment sa týmto zaväzuje, že bude podporovať zavádzanie SMB, čo v praxi znamená, že to spoločnosť bude stáť v najlepšom prípade ľudské zdroje a financie. V prípade certifikácie SMB, bude toto prvý dokument, ktorý vyžadujú audítori. Organizácia preto musí zdokumentovanú informáciu o bezpečnostnej politike uchovávať.

Ide o vyhlásenie záväzku vrcholového manažmentu organizácie, že zabezpečí, aby všetky oblasti činností a poskytovaných služieb splnili ciele bezpečnosti v súlade so všeobecne záväznými medzinárodnými a národnými právnymi normami, vnútornými normami organizácie a jej zmluvnými záväzkami.

Ciele bezpečnosti sa dosahujú prostredníctvom ďalšieho záväzku organizácie poskytnúť potrebné **zdroje** pre efektívne riadenie bezpečnosti. Prijatie záväzku v bezpečnostnej politike obsahuje:

a) **vyhlásenie manažmentu** o podpore politiky bezpečnosti organizácie,
b) stanovenie **úloh manažmentu organizácie** pri zaisťovaní bezpečnosti a integrity,
c) zabezpečenie **zhody noriem bezpečnosti organizácie** so všeobecne záväznými právnymi predpismi, vnútornými predpismi organizácie a jej zmluvnými záväzkami,
d) vytvorenie **základného a východiskového dokumentu**, ktorým organizácia deklaruje svoj ***záujem na implementáciu bezpečnosti do všetkých sfér činnosti organizácie*** v súlade s medzinárodnými a národnými požiadavkami, ktorý musí byť podpísaný zodpovednými vedúcimi organizácie, s názvom **Politika bezpečnosti.**
e) vytvorenie **systémových politík bezpečnosti** (v jednotlivých oblastiach bezpečnosti).

Politika bezpečnosti musí byť **oznámená vo vnútri organizácie a byť k dispozícii pre zainteresovaných účastníkov.**

Roly, zodpovednosti a právomoci vo vzťahu k bezpečnosti organizácie

Osoby vo vrcholovom manažmente a ďalších podobných manažérskych funkciách v celej organizácii musia demonštrovať svoju **vodcovskú rolu** vo vzťahu k SMB. Táto

vodcovská rola a záväzok sa môžu preukázať motiváciou a zmocnením osôb prispievať k efektívnosti SMB.

Vrcholový manažment musí zaistiť, že v rámci organizácie sú ***pridelené a oznámené zodpovednosti a právomoci pre príslušné roly***. Zodpovednosť a právomoc musí byť pridelená pre:

- zaistenie, že systém manažmentu zodpovedá požiadavkám noriem bezpečnosti,
- podávanie správ vrcholovému manažmentu o plnení úloh SMB v rámci organizácie.

Obsahom tohto kroku je najmä:

a) určenie zodpovedného vedúceho pracovníka alebo pracovníkov, ktorí musia, bez ohľadu na ďalšie úlohy, mať konečnú zodpovednosť za zavedenie a udržiavanie SMB,

b) vytvorenie riadiaceho orgánu bezpečnosti (výbor alebo rada bezpečnosti) za účelom vyhodnocovania výkonnosti bezpečnosti,

c) určenie zodpovednosti všetkých členov manažmentu, bez ohľadu na ďalšie úlohy a zodpovednosti, vzhľadom na výkonnosť systému manažérstva bezpečnosti v otázkach bezpečnosti,

d) zdokumentovanie zodpovednosti a právomoci za bezpečnosť a **zoznámenie** celej organizácie (musí obsahovať stanovenie úrovní manažmentu s právomocou prijímať rozhodnutia vzťahujúce sa na prijateľnosť bezpečnostného rizika),

e) menovanie kľúčových bezpečnostných pracovníkov, najmä:

- ***bezpečnostného manažéra*** ako zodpovednú samostatnú a hlavnú osobu pri zavádzaní a udržiavaní účinného systému manažérstva bezpečnosti,
- ***manažéra rizík*** a ***tím manažérstva rizika*** na čo najskoršie začatie procesu manažérstva rizík v celej organizácii,

f) vymedzenie pomeru zodpovednosti za bezpečnosť medzi manažmentom organizácie a vonkajšími spoločnosťami (bezpečnostnými službami),

g) menovaním jednej alebo viac osôb zodpovedných za SMB s primeranou právomocou a kompetenciami pre prijatie zodpovednosti za zavedenie a udržiavanie SMB (tieto osoby môžu mať i iné zodpovednosti v organizácii), obvykle sa vytvára tím pre implementáciu SMB a zabezpečuje sa jeho príprava a školenie.

PLÁNOVANIE

Táto etapa zdôrazňuje vysokú dôležitosť **manažérstva rizika**. Keď organizácia takto zvýrazní ***riziká a príležitosti***, je potrebné stanoviť, ako sa budú riešiť. Fázy plánovania musia ukázať, ***aké, koho, ako a kedy riziká*** musia byť riešené. Tento proaktívny prístup nahrádza preventívne kroky a neskôr znižuje potrebu nápravných opatrení. Je potrebné sa tiež zamerať na pozitívne aspekty – príležitosti pre podnikanie a jej optimalizovanie. Identifikované riziká a príležitosti umožňujú vytvoriť ciele a politiky.

Etapa plánovania obsahuje:

1. **Opatrenia pre riešenie rizík a príležitostí v rámci SMB:**
   a) všeobecne,
   b) posudzovanie rizík,
   c) zaobchádzanie s rizikami.
2. **Ciele bezpečnosti organizácie a plánovanie ich dosiahnutia.**
3. **Ciele manažérstva bezpečnosti a plánovanie ich dosiahnutia.**

Opatrenia pre riešenie rizík a príležitostí v rámci SMB

Pri plánovaní činnosti SMB musí organizácia zvážiť závery z pochopenia svojich vonkajších a vnútorných súvislostí a zainteresovaných účastníkov a určiť riziká a príležitosti, na ktoré je potrebné sa zamerať pre:

- zaistenie, že SMB môže dosiahnuť svoje zamýšľané výstupy,
- zabránenie alebo zníženie nežiaducich účinkov,
- dosiahnutie neustáleho zlepšovania.

Organizácia musí plánovať:

- činnosti, ktoré sa zaoberajú rizikami a príležitosťami (posudzovanie rizika, zaobchádzanie s rizikom),
- ako integrovať a zaviesť tieto činnosti do procesov SMB,
- ako vyhodnocovať efektívnosť týchto činností.

Posudzovanie rizika

Organizácia musí definovať a použiť **proces posudzovania rizika** ktorý:

a) stanoví a udržiava **kritériá rizika**, ktoré zahŕňajú:
- kritériá pre špekulatívne (podnikateľské) riziká;
- kritériá pre bezpečnostné riziká;

b) zaručuje, že **opakované posudzovanie bezpečnostného rizika** vytvorí zodpovedajúce, platné a porovnateľné výsledky.

c) identifikuje riziká:
- používa metódy a techniky posudzovania rizík na identifikáciu rizík podľa STN EN 31010:2011,
- identifikuje vlastníkov rizík.

d) analyzuje riziká:
- posúdi potenciálne následky, ktoré by nastali v prípade realizovania identifikovaných rizík,
- posúdi reálnu pravdepodobnosť výskytu identifikovaných rizík,
- zistí úroveň každého rizika;

e) vyhodnocuje riziká:
- porovná výsledky analýzy rizík s kritériami rizík,
- rozhodne a vydá rozhodnutie o rizikách, ktoré vyžadujú zaobchádzanie a zoradí ich podľa dôležitosti pre zaobchádzanie.

Organizácia musí uchovávať ***zdokumentované informácie*** o procese posudzovania rizík informačnej bezpečnosti.

Zaobchádzanie s rizikom

Organizácia musí definovať a aplikovať **proces zaobchádzania s rizikami** na:

a) výber vhodného spôsobu zaobchádzania s rizikom, vzhľadom na výsledky posudzovania rizika,
b) určenie všetkých opatrení, ktoré sú nevyhnutné na zavedenie vybraného spôsobu zaobchádzania s rizikom (organizácia môže navrhnúť opatrenia podľa požiadaviek, alebo ich môže identifikovať z ľubovoľného zdroja).
c) formulovanie **Plánu zaobchádzania s rizikami**,
d) získanie súhlasu vlastníkov rizika s Plánom zaobchádzania s rizikami a prijatím zvyškových (reziduálnych) rizík.

Organizácia musí uchovávať zdokumentované informácie o procese zaobchádzania s rizikami.

Manažérstvo rizika

Proces manažérstva rizika sa musí vykonávať nepretržite, pretože z neho vyplýva návrh opatrení, ktoré by mali modifikovať zistené riziká, aby sa na jednej strane mohol dosiahnuť zisk alebo, na druhej strane, znížili možnosti strát, zabránilo zraneniam ľudí alebo stratám na životoch a škodám na majetku a životnom prostredí.

Manažéri i bezpečnostní pracovníci organizácie využívajú systematický a logický proces manažérstva rizika tak, že najprv **vyhodnotia chránené záujmy** a **určia kritériá rizika**. Chráneným záujmom je život, zdravie, majetok, infraštruktúra alebo iné hodnoty, ktoré chránime pred zničením, poškodením, odcudzením alebo inou ujmou, sú to teda **aktíva** organizácie.

V priebehu **posúdenia rizika** identifikujú, analyzujú a vyhodnotia každé riziko, a rozhodnú, či sa ním budú zaoberať, aby vyhovovalo vopred určeným kritériám. Počas tohto procesu organizácia komunikuje a konzultuje so zainteresovanými účastníkmi, monitoruje a preskúmava riziko a vyberá **spôsoby zaobchádzania** s ním, ktoré ho modifikujú, s cieľom dosiahnuť, že sa nebude vyžadovať jeho ďalšie riadenie.

Manažérstvo rizika sa má **začleniť do všetkých postupov a procesov organizácie,** nesmie sa oddeľovať. Osobitne sa má zahrnúť do politiky vývoja, podnikania, strategického plánovania a preskúmavania, ako aj do procesov manažérskych zmien. V priebehu tohto procesu majú dôležitú úlohu vrcholoví manažéri i bezpečnostní pracovníci.

Vrcholový manažment v riadiacom orgáne bezpečnosti organizácie v priebehu procesu manažérstva rizika:

a) **identifikuje všetky aktíva organizácie** (hmotné a nehmotné aktíva a významné činnosti) a určí zodpovednosť za ne,
b) **určí chránené objekty a chránené priestory** v nich a hodnoty chráneného záujmu v jednotlivých priestoroch (**aktíva**),
c) **vytvorí Politiku manažérstva rizika,**
d) **určí zodpovednosti za manažérstvo rizika**, **vytvorí štruktúry na riešenie rizík** podriadené manažérovi rizík alebo priamo bezpečnostnému manažérovi,
e) **spracuje Plán manažérstva rizika,**
f) **definuje kritériá rizík** vzhľadom na veľkosť aktív organizácie**,** v porovnaní s ktorými sa bude hodnotiť každé riziko na určenie jeho prijateľnosti, prípustnosti alebo neprijateľnosti.

Bezpečnostný manažér s manažérom rizík, tímom manažérstva rizika a odborníkmi na manažérstvo rizika v ďalšom priebehu procesu manažérstva rizika:

a) **analyzuje vonkajšie a vnútorné bezpečnostné prostredie** (vonkajšie a vnútorné súvislosti),
b) **identifikuje vonkajšie a vnútorné riziká,** ktorým sú alebo môžu byť aktíva vystavené (udalosti a ich príčiny a potenciálne následky, proces hľadania, spoznávania a opísania rizika),
c) **spracuje Zoznam rizík,** v ktorom uvedie slovný popis jednotlivých rizík, ich pravdepodobnosť a následky a iné dôležité údaje o riziku,
d) **analyzuje každé riziko** uvedené v zozname rizík, **zistí jeho úroveň** podľa vzťahu pravdepodobnosti výskytu udalosti a jej následku,

e) **vyhodnotí každé riziko** porovnaním úrovne rizika zistenej v analýze rizika s kritériami rizika určenými manažmentom organizácie pri hľadaní súvislostí a zaradí riziko do príslušnej kategórie (prijateľné, prípustné znesiteľné, prípustné nežiaduce, neprijateľné),
f) **rozhodne o rizikách, ktoré vyžadujú zaobchádzanie a ich prioritách pre zaobchádzanie,**
g) **v procese zaobchádzania s rizikami, ktoré vyžadujú zaobchádzanie** rozhodne o výbere jedného alebo viacerých spôsobov zaobchádzania s rizikom a spôsobe ich zavedenia,
h) **spracuje Plán zaobchádzania s rizikami,**
i) **v priebehu monitorovania a preskúmavania** vykonáva pravidelné kontroly a merania efektívnosti a účinnosti zmiernenia dopadov rizík po ich modifikovaní (zvyškových rizík) a vyhľadáva novo vzniknuté riziká,
j) **spracuje Záznam procesu manažérstva rizika** o celej činnosti v procese manažérstva rizika.

Ciele bezpečnosti organizácie a plánovanie ich dosiahnutia

Dôležitým predpokladom pre aktívnu implementáciu SMB je **plánovanie bezpečnosti**. V jeho priebehu sa formulujú ***ciele*** pre bezpečný výkon organizácie, určujú ***stratégie (postupy na ich dosiahnutie)*** a spracovávajú konkrétne ***plány*** na dosiahnutie prijateľnej úrovne bezpečnosti.

Podkladmi pre stanovenie cieľov bezpečnosti sú:
- ***analýza stavu bezpečnosti organizácie***,
- výsledky ***manažérstva rizika***,
- ***možnosti*** každej organizácie a ***predstavy o fungujúcom systéme manažérstva bezpečnosti*** v organizácii.
- ***zákonné bezpečnostné normy***.

Stanovenie cieľov bezpečnosti je **vecou vrcholového manažmentu** každej organizácie. Organizácia stanovuje **ciele bezpečnosti** konkrétne pre svoje potreby, no vychádza zo všeobecného rámca, podľa ktorého možno definovať niektoré ciele, napr.:
- definovať infraštruktúru a najdôležitejšie aktíva organizácie, ktoré je potrebné chrániť,
- identifikovať, analyzovať a vyhodnotiť bezpečnostné riziká a modifikovať neprijateľné a prípustné riziká na požadovanú úroveň,
- vytvoriť bezpečnostné prostredie na ochranu zdravia a života príslušníkov manažmentu, všetkých ďalších zamestnancov a všetkých zainteresovaných účastníkov,
- vytvoriť SMB organizácie s vymedzením zodpovednosti pre riadiacu zložku, výkonnú zložku a kontrolnú zložku,
- vybudovať vonkajšiu ochranu objektov ako komplex opatrení na vymedzenie hraníc objektov, kontrolu vstupov do objektu a výstupov z objektu,
- zabezpečiť monitorovanie možného narušenia stanovených hraníc objektov organizácie,
- zaviesť potrebné mechanické zábranné prostriedky a technické zabezpečovacie prostriedky na ochranu a monitorovanie hraníc objektu, vstupov do objektu a ochranu chránených priestorov,
- vytvoriť vnútornú ochranu dôležitých objektov s dôrazom na ochranu chránených priestorov,
- zaviesť komplexné režimové opatrenia na vonkajšiu a vnútornú ochranu organizácie,
- vypracovať komplexnú, havarijnú a iné bezpečnostné dokumenty organizácie,
- vytvoriť podmienky pre ochranu utajovaných skutočností, citlivých informácií, ochranu osobných údajov a vytvoriť systém manažérstva informačnej bezpečnosti,
- zabezpečiť ochranu obchodného, výrobného a iných tajomstiev,

- vytvoriť systém manažérstva BOZP, systém manažérstva životného prostredia organizácie (EMS), systém manažérstva informačnej bezpečnosti a systém manažérstva plynulosti podnikania (BCMS),
- vytvoriť systém vyšetrovania incidentov a podvodov,
- zabezpečiť monitorovanie, kontroly, audit a vyhodnocovanie výkonnosti SMB a úrovne bezpečnosti organizácie.

Ciele bezpečnosti je vhodné ***vymedziť vo vertikálnej a horizontálnej úrovni, určiť konkrétnu zodpovednosť, v ich funkčnej, obsahovej, ekonomickej rovine a hlavne v právnej a finančnej rovine.***

V priebehu stanovenia cieľov bezpečnosti organizácie a plánovania ich dosiahnutia sa najmä:

1. **stanovujú konkrétne ciele bezpečnosti** organizácie, **spôsoby a kritériá ich vyhodnocovania** a **spôsoby kontroly ich dosahovania**,
2. **určujú normy bezpečnosti** v jednotlivých sektoroch a oblastiach bezpečnosti,
3. **plánuje implementácia SMB** do procesov organizácie – ***Plán implementácie SMB,***
4. **plánujú postupy na dosiahnutie cieľov bezpečnosti v podsektoroch sektora bezpečnosti** v jednotlivých plánoch, napr.:
   - **BOZP** – ***Plán bezpečnosti a ochrany zdravia pri práci na stavenisku***.
   - **ochrana objektov** s využitím už spracovaného Plánu zaobchádzania s rizikami – ***Bezpečnostný plán ochrany objektu*** (OUS), ***Bezpečnostný plán*** (kritická infraštruktúra), pre iné objekty ***Bezpečnostný plán ochrany objektu*** alebo ***Projekt ochrany objektu,***
   - **informačná bezpečnosť,**
   - **ochrana osobných údajov** – ***Bezpečnostný projekt (smernica) na ochranu osobných údajov v informačnom systéme,***
5. **koordinuje plánovanie reakcie na núdzové situácie,**
6. **plánujú postupy na riešenie incidentov** – ***Plán manažérstva incidentov,***
7. **stanovuje program environmentálneho manažérstva** – ***Akčný plán (programy) environmentálneho manažérstva.***

Ciele systému manažérstva bezpečnosti a plánovanie ich dosiahnutia

Osobitný dôraz sa tiež kladie na ***ciele SMB***, ktoré by mali byť ***merateľné, monitorované, oznamované*** a ***zladené*** s politikou SMB a v prípade potreby ***aktualizované***. Ciele musia byť stanovené pre ***dôležité funkcie a úrovne***.

Vrcholový manažment musí zaistiť, aby ciele manažérstva bezpečnosti boli prijaté a oznamované podľa príslušnej úrovne a funkcie v rámci organizácie. **Ciele manažérstva bezpečnosti musia:**

- byť zladené s bezpečnostnou politikou,
- zohľadniť minimálnu úroveň produktov a služieb, ktorá je prijateľná pre organizáciu, aby dosiahla svoje ciele,
- byť merateľné,
- zohľadniť použiteľné požiadavky,
- byť monitorované a aktualizované, pokiaľ je to vhodné.

Organizácia musí udržiavať **zdokumentované informácie o cieľoch manažérstva bezpečnosti**. Na dosiahnutie týchto cieľov musí organizácia určiť:

- *kto bude zodpovedný,*
- *čo sa má vykonať,*
- *aké zdroje budú požadované,*

- *kedy to musí byť dokončené,*
- *ako budú vyhodnocované výsledky.*

Určenie noriem bezpečnosti

Normy bezpečnosti musia dodržať súlad s platnými požiadavkami bezpečnostných predpisov a zabezpečiť snahu organizácie prijať medzinárodne uznávané bezpečnostné normy a osvedčené postupy v oblasti manažérstva bezpečnosti. Organizácia v prvom rade musí **dodržiavať normy stanovené v zákonoch a smerniciach,** ktoré môže doplniť svojimi štandardmi.

Je potrebné:

a) určiť, aké **normy bezpečnosti** zaviesť v organizácii,
b) definovať **prijateľnú úroveň bezpečnosti** (minimálny stupeň/úroveň bezpečnosti, ktorú musí SMB dosiahnuť v praxi,
c) stanoviť **výkonnostné ciele bezpečnosti a ich hodnoty –** kvantifikované ciele, ktoré zabezpečia požadovanú úroveň bezpečnosti organizácie,
d) nastaviť **ukazovatele výkonnosti v oblasti bezpečnosti (indikátory bezpečnosti**) a ich **hodnoty** – parametre na určenie, či sa dosiahla požadovaná úroveň bezpečnosti, napr.: rast, frekvencia, počet nehôd; rast, frekvencia, počet incidentov; úroveň zhody s právnymi normami atď.,
e) dodržiavať existujúce, nové a zmenené technické a prevádzkové normy alebo iné podmienky určené v technických špecifikáciách interoperability, národných bezpečnostných predpisoch, iných predpisoch a v rozhodnutiach bezpečnostného orgánu.

Plánovanie implementácie SMB

Plán implementácie SMB organizácie má zaistiť konzistentný, cielený a komplexný prístup k rozvoju potrebnej organizačné štruktúry SMB, procesov a postupov manažérstva bezpečnosti. Plán implementácie SMB organizácie:

- **stanovuje prístup organizácie** k riadeniu bezpečnosti spôsobom, ktorý zodpovedá cieľom bezpečnosti pre organizáciu,
- **identifikuje náklady** na školenie a plánovanie, navrhne rozpočet pre realizáciu SMB,
- **vytvorí a udržiava dokumenty SMB**, ktorá popisuje politiku a ciele bezpečnosti, požiadavky na SMB, procesy a postupy SMB, zodpovednosti a právomoci pri procesoch a postupoch a výstupy SMB,
- **schvaľuje vrcholový manažment organizácie.**

Ako súčasť dokumentácie SMB sa obvykle vytvorí a udržiava **Príručka systémov manažérstva bezpečnosti** *(Safety Management Systems Manual)* schválená právne zodpovedným manažérom, aby bola celá organizácia zoznámená s prístupom k manažérstvu bezpečnosti.

Koordinácia plánovania reakcie na núdzové situácie

Koordinácia plánovania odozvy na núdzové situácie znamená vhodnú koordináciu plánov, ktoré riešia reakciu organizácie na núdzové situácie, s plánmi tých organizácií, s ktorými musí byť v spojení počas poskytovania svojich služieb:

a) v rámci **prevencie závažným priemyselným haváriám** je prevádzkovateľ podľa Zákona č. 261/2002 Z. z. o prevencii závažných priemyselných havárií a Vyhlášky ministerstva životného prostredia SR č. 490/2002 Z. z. o bezpečnostnej správe a o havarijnom pláne povinný vypracovať: ***Bezpečnostnú správu*** (prevádzkovateľ organizácie kategórie B), ***Havarijný plán*** a spolupracovať na vypracúvaní ***Plánu ochrany obyvateľstva*** podľa zákona NR SR č.42/1994 Z. z. o civilnej ochrane obyvateľstva.

b) v **systéme manažérstva plynulosti podnikania** sa spracováva ***Plán plynulosti podnikania*** (*Business Continuity Plan*), okrem toho sa používajú aj ***Plán obnovy činností*** (*Business Recovery Plan)* alebo ***Plán obnovy po havárii*** (*Disaster Recovery Plan).*

c) podľa Zákona č. 541/2004 Z. z.**o mierovom využívaní jadrovej energie (atómový zákon)** sa spracovávajú: ***Predbežný vnútorný havarijný plán, Vnútorný havarijný plán, Plán ochrany obyvateľstva, Havarijný dopravný poriadok.***

d) podľa Zákona č. 364/2004 Z. z. **o vodách** v znení neskorších predpisov ***Havarijný plán*** predstavuje plán preventívnych opatrení na zamedzenie vzniku neovládateľného úniku škodlivých látok a obzvlášť škodlivých látok do životného prostredia a na postup v prípade ich úniku.

e) podľa Zákona č. 24/2006 Z. z. o **posudzovaní vplyvov na životné prostredie** v znení neskorších predpisov sa spracováva ***Havarijný plán,*** ktorý tvorí súčasť prevádzkového poriadku skládky odpadov.

f) na riešenie incidentov sa spracováva ***Plán manažérstva incidentov*** *(Incident Management Plan).*

Pri vypracúvaní havarijného plánu sa vychádza z konkrétnej situácie v organizácii a jej okolí s osobitným zreteľom na výsledky manažérstva rizika.

PODPORA

Po vyriešení súvislostí, záväzku a plánovania bezpečnosti sa bude musieť organizácia zamerať na podporu, potrebnú pre dosiahnutie svojich zámerov a cieľov. Toto zahŕňa zdroje, zameranie internej a externej komunikácie, ako aj zdokumentované informácie, čím sa nahrádzajú skôr používané pojmy ako dokumenty, dokumentácia a záznamy. Etapa podpory obsahuje:

1. **Zdroje –** organizácia musí určiť a poskytnúť zdroje potrebné pre vytvorenie, zavedenie, udržiavanie a trvalé zlepšovanie SMB a zaistenie bezpečnosti vo všetkých oblastiach činnosti.

2. **Kompetencie –** organizácia musí:
   - stanoviť konkrétne kompetencie osôb vykonávajúcich bezpečnostné činnosti, ktoré majú vplyv na výkonnosť bezpečnosti,
   - zaistiť, aby tieto osoby boli kompetentné na základe vhodného vzdelania, výcviku a skúseností,
   - tam, kde je to vhodné prijať opatrenia na získanie potrebnej kompetencie a vyhodnotiť účinnosť prijatých opatrení,
   - udržiavať vhodnú zdokumentovanú informáciu ako dôkaz o kompetencii (prístup k nim znamená možnosť povolenia nazerať do nich alebo právomoc meniť ich).

3. **Uvedomenie si –** osoby, ktoré vykonávajú práce v rámci organizácie si musia uvedomiť:
   - politiku bezpečnosti,
   - svoj príspevok k bezpečnosti a účinnosti SMB, vrátane výhod zlepšenia výkonnosti SMB,
   - následky neplnenia požiadaviek SMB,
   - svoje vlastné úlohy pri výskyte incidentov.

4. **Komunikácia –** organizácia musí určiť potrebu ***vnútornej a vonkajšej komunikácie***, ktorá sa vzťahuje na SMB a obsahuje:
   - o čom sa bude komunikovať,
   - kedy sa bude komunikovať
   - s kým sa bude komunikovať.

Organizácia musí ustanoviť, zaviesť a udržiavať **postupy:**

- vnútornej komunikácie medzi zainteresovanými účastníkmi a zamestnancami organizácie,
- vonkajšej komunikácie so zákazníkmi, partnerskými entitami, miestnymi komunitami a ďalšími zainteresovanými účastníkmi, vrátane médií,
- na prijímanie, dokumentovanie a reagovanie na komunikáciu zainteresovaných účastníkov,
- na prevzatie a integrovanie národného alebo regionálneho systému informovania o hrozbách alebo obdobného systému do plánovania a používania, pokiaľ je to vhodné,
- na zaistenie dostupnosti prostriedkov komunikácie počas rušivého incidentu,
- na uľahčenie štruktúrovanej komunikácie s príslušnými orgánmi a zaistenie vzájomnej spolupráce niekoľkých reagujúcich organizácií alebo pracovníkov, kde je to vhodné,
- prevádzku a testovanie komunikačných prostriedkov určených na použitie pri narušení normálnych komunikácií.

5. **Zdokumentované informácie –** Finálna požiadavka podpory je **zdokumentovanie informácií** (doteraz používané pojmy ako *dokumenty, dokumentácia a záznamy* sa nepoužívajú). Rozsah zdokumentovaných informácií pre SMB sa môže v rôznych organizáciách líšiť, podľa veľkosti organizácie a druhu jej činností, procesov, produktov a služieb, komplexnosti procesov a ich vzájomných väzieb a kompetencie osôb. Zdokumentované informácie SMB organizácie musia obsahovať:
    - zdokumentované informácie požadované v normách bezpečnosti,
    - zdokumentované dokumentácie, ktoré organizácia určí ako nevyhnutné pre efektívnosť SMB.

Rozsah zdokumentovaných informácií

Pri stanovení rozsahu zdokumentovaných bezpečnostných informácií musí organizácia vychádzať z platných zákonov a ďalších právnych noriem, v ktorých sú tieto dokumenty stanovené. Zdokumentované bezpečnostné informácie predstavujú okrem uvedených plánov množstvo ďalších dokumentov SMB, manažérstva rizika a jednotlivé bezpečnostné smernice, metodiky a nariadenia vo všetkých podsektoroch a oblastiach bezpečnostného sektora.

Vytváranie a aktualizovanie zdokumentovaných informácií

V tejto etape sa určujú **spracovatelia a termíny na spracovanie potrebných zdokumentovaných informácií**. Pri vytváraní a aktualizovaní zdokumentovaných informácií musí organizácia zaistiť:

- vhodnú identifikáciu a popis (napr. názov, dátum, autora alebo číslo odkazu),
- vhodný formát (napr. jazyk, verziu softvéru, grafiku) a média (napr. papierová alebo elektronická), preskúmanie a schválenie z hľadiska vhodnosti a primeranosti

Riadenie (správa) zdokumentovaných informácií

Zdokumentované informácie požadované v SMB a v medzinárodných normách bezpečnosti musia byť spravované pre zaistenie:

- ich dostupnosti a vhodnosti pre požitie tam, kde je to potrebné,
- primeranej ochrany (napr. proti strate dôvernosti, nevhodnému použitiu alebo strate integrity).

Na uloženie zdokumentovaných informácií sa musí vytvoriť **samostatné pracovisko.** Pri ich spravovaní musí organizácia, pokiaľ je to akceptovateľné, zohľadniť nasledujúce činnosti:

- rozosielanie, prístup, vyhľadávanie a použitie,
- skladovanie a ochranu vrátane ochrany čitateľnosti,
- riadenie zmien (napr. riadenie verzií),
- uschovávanie a zaobchádzanie,
- vyhľadávanie a použitie,
- ochranu čitateľnosti (či je zdokumentovaná informácia dostatočne rozpoznateľná, aby sa dala prečítať),
- ochranu nezamýšľaného použitia zastaraných informácií.

Zdokumentované **informácie externého pôvodu**, ktoré organizácia určila ako nevyhnutné pre plánovanie a prevádzku SMB, musia byť podľa potreby identifikované a spravované.

Prístupom sa rozumie rozhodnutie týkajúce sa povolenia na zobrazenie iba zdokumentovanej informácie, alebo povolenie a oprávnenie zobraziť a zmeniť zdokumentované informácie a pod.

ZÁVER

Špecifická medzinárodná norma pre manažérstvo bezpečnosti nie je zatiaľ spracovaná, pre jednotlivé druhy bezpečnosti v organizácii sú už podľa prílohy SL spracované nasledujúce samostatné normy:

- ISO/DIS 45001:2016 ***Systémy manažérstva BOZP.*** Požiadavky s návodom na použitie *(Occupational health and safety management systems -- Requirements with guidance for use)*
- STN EN ISO 14001:2015 ***Systémy manažérstva životného prostredia.*** Požiadavky s pokynmi na použitie *(Environmental management systems -- Requirements with guidance for use)*
- STN ISO/IEC 27000:2014 (36 9789), Informačné technológie. Bezpečnostné metódy. ***Systémy riadenia informačnej bezpečnosti.*** Prehľad a slovník.
- STN EN ISO 22301 Ochrana spoločnosti. ***Systémy manažérstva plynulosti podnikania***. Požiadavky (ISO 22301:2012)
- ISO 55002:2014 ***Manažérske systémy. Manažérstvo aktív.*** Návod.
- ISO/DIS 34001.3 ***Systém manažérstva bezpečnosti.*** Riadenie a prostriedky ochrany pred podvodmi.

Napriek tomu, že pre systém manažérstva bezpečnosti organizácie nie je zatiaľ stanovená špecifická medzinárodná norma ISO, je možné v organizáciách uvedený článok, spracovaný podľa prílohy SL, využiť na plánovanie vytvorenia systému manažérstva bezpečnosti. Ďalšie časti PDCA cyklu pri riešení systému manažérstva bezpečnosti organizácie budú uvedené v novom článku.

GRANTOVÁ PODPORA

Príspevok bol spracovaný v rámci projektu VEGA 1/0787/14.

LITERATÚRA

[1] BELAN, Ľ. 2015. *Bezpečnostný manažment: Manažérstvo bezpečnosti.* EDIS UNIZA. 200 s. ISBN 978-80-554-1163-7.

[2] *ANNEX SL (ISO Guide 83).*