**Organizácia informačnej bezpečnosti**

Dáta a informácie sú v dnešnej dobe pre organizácie dôležité a pre mnohé z nich doslova natoľko kritické, že od ich kvality závisí samotná podstata ich činnosti. Zaručenie bezpečnosti dát a informácií je úlohou odboru nazvaného informačná bezpečnosť. Jednou zo základných požiadaviek pre riadenie informačnej bezpečnosti je vhodne zvolený organizačný rámec a stanovenie jednotlivých zodpovedností v oblasti ochrany informačných aktív.

Ak sa organizácia rozhodne vziať pod kontrolu bezpečnosť svojich dát a informácií, je na samom začiatku tejto cesty potrebná identifikácia úloh, ktoré môžu potenciálne súvisieť s ochranou informačných aktív. Následne je dôležité zaručiť, aby zodpovednosť za výkon špecifických bezpečnostných procesov bola jednoznačne priradená konkrétnym pracovným roliam. Prirodzene, nedá sa očakávať, že by organizácia bezprostredne presmerovala väčšinu zdrojov na bezpečnosť ako činnosť, ktorá nie je typicky jej hlavným produktom. Preto je akceptovateľné, ak sa vedenie spočiatku prikloní k minimalistickému riešeniu, pričom zodpovednosť, pôsobnosť a právomoci je vždy možné upraviť aj neskôr. Samozrejme, všetko je potrebné ošetriť vhodnými politikami. O tých však budem podrobnejšie písať v inej časti tejto série článkov.

Čo však znamená termín „organizácia informačnej bezpečnosti“? Zriadenie určitých pracovných rolí nie je ultimátnym cieľom informačnej bezpečnosti a vzhľadom na rôznorodosť činností podnikov by ani nebolo efektívne, aby boli bezpečnostné roly vynucované prostredníctvom legislatívy. Konkrétne roly v bezpečnosti sú vždy závislé od hospodárskeho odvetvia, v ktorom organizácia pôsobí, a aj od miery jej závislosti od kvality spracúvaných informácií.

### Zodpovednosť vedenia

Informačná bezpečnosť by sa mala stať štandardnou súčasťou prevádzkových procesov organizácie, aby ochrana informácií nebola len formálne deklarovaná, ale aby bolo možné zabezpečiť jej reálne vykonávanie v každodennej praxi. Začlenenie bezpečnosti do prevádzkových procesov si vyžaduje dobrú spoluprácu zo strany vedenia spoločnosti, manažmentu IT, bezpečnostného manažmentu, personálu zodpovedného za samotnú informačnú bezpečnosť, vlastníkov informačných systémov, vlastníkov prevádzkových procesov, ale aj dodávateľov služieb.

Začať je potrebné u štatutárneho vedenia, ktoré riadi spoločnosť a koná v jej mene. Pokiaľ má organizácia úprimný záujem o ochranu kritických informácií, záväzok štatutárov podporovať informačnú bezpečnosť je základom pre implementáciu a trvalo udržateľný rozvoj procesu ochrany citlivých informačných aktív. Štatutári sú v zmysle zákona povinní vykonávať svoju funkciu s odbornou starostlivosťou a v záujme spoločnosti a jej spoločníkov (zákon používa aj širší pojem „náležitá starostlivosť“). Konečná zodpovednosť za ochranu majetku spoločnosti, vrátane ochrany informačného majetku, spočíva vždy na štatutárnom vedení organizácie. Táto zodpovednosť sa samozrejme týka aj zodpovednosti za riziká, ktoré pôsobia na informačné aktíva. Základnou pracovnou rolou v informačnej bezpečnosti paradoxne nie je bezpečnostný manažér ani špecialista informačnej bezpečnosti. Jednoznačne hlavnú rolu v procese informačnej bezpečnosti má štatutárne vedenie organizácie. Prinajmenšom by mala byť štatutárnym vedením schválená bezpečnostná stratégia a súbor bezpečnostných politík – to je jediný postup, ktorý zaručí, že politiky sa stanú záväzné pre všetkých zamestnancov, ako aj pre relevantné tretie strany. Štatutárne vedenie by sa tiež malo v pravidelných intervaloch začať zaujímať o stav informačnej bezpečnosti organizácie, napríklad formou správy, ktorú si nechá spracovať a predložiť od manažéra, ktorému je zverené riadenie procesu. Možnosťou je aj objednanie nezávislého posúdenia alebo auditu, ktoré vypracuje externá, odborne spôsobilá osoba. Povinnosť preveriť účinnosť prijatých bezpečnostných opatrení prostredníctvom auditu kybernetickej bezpečnosti určuje prevádzkovateľom základných služieb aj zákon č. [69/2018 Z. z.](https://www.bezpecnostvpraxi.sk/form/goto.ashx?t=26&p=4804197&f=3) o kybernetickej bezpečnosti.

### Riadenie a výkon bezpečnostných procesov

Zatiaľ čo štatutárne vedenie má svoje úlohy v dlhodobom, strategickom riadení organizácie, za reálny každodenný výkon prevádzkových a podporných procesov sú zodpovední príslušní manažéri na taktickej a operatívnej úrovni riadenia. Pre názornejšie vysvetlenie jednotlivých úrovní riadenia, kľúčových rolí, vzťahov a toku manažérskych informácií v oblasti informačnej bezpečnosti môže dobre poslúžiť schéma navrhnutá medzinárodnou Asociáciou auditu a kontroly informačných systémov (ISACA) v rámci metodiky zvanej COBIT:



Z tejto schémy vyplýva, že pod štatutárnou úrovňou existujú dve ďalšie úrovne riadenia v informačnej bezpečnosti – taktická (vedenie informačnej bezpečnosti) a operatívna (bezpečnostné operácie alebo bezpečnostná prevádzka). Toto rozdelenie je dôležité najmä vzhľadom na model praktického výkonu bezpečnostných procesov. Zodpovednosti organizácie v informačnej bezpečnosti sú totiž dané bez ohľadu na to, či výkon procesov informačnej bezpečnosti organizácia zabezpečuje sama alebo prostredníctvom dodávateľa. V zmysle dobrej praxe je odporúčané, aby riadenie bezpečnosti zostalo „doma“, t. j. pod úplnou kontrolou spoločnosti. Zaručiť kvalitný výkon bezpečnostných procesov, najmä vzhľadom na mieru prácnosti a vysoké požiadavky, ktoré sú kladené na kvalifikáciu a zručnosti zainteresovaného personálu, však môže byť pre organizáciu mimoriadne náročnou úlohou. Nie je preto ničím výnimočným, ak si spoločnosť objedná vykonávanie špecifických odborných činností v informačnej bezpečnosti dodávateľským spôsobom, pričom si ponechá plný dohľad nad ich riadením.

### Hlavné úlohy v procese usporiadania informačnej bezpečnosti

Ako bolo spomenuté, prvým krokom, ktorý je potrebné vykonať pri zavádzaní informačnej bezpečnosti, je identifikácia všetkých činností, ktoré môžu potenciálne súvisieť s ochranou informačných aktív, a stanovenie zodpovednosti za výkon špecifických bezpečnostných procesov. Je potrebné najmä definovať aktíva a pracovné procedúry spojené s každým jednotlivým systémom a stanoviť osoby zodpovedné za každé aktívum a každý proces. Detaily týchto zodpovedností by mali byť potom zdokumentované v bezpečnostných politikách. Pri stanovení zodpovednosti za aktíva a procesy je nutné myslieť na to, aby boli jasne určené a dokumentované stupne prístupových a schvaľovacích oprávnení v kontexte jednotlivých aktív. Zároveň sa však nesmie zabudnúť na zásadu, že konfliktné povinnosti a zodpovednosti majú byť vzájomne oddelené, aby sa znížila možnosť neoprávnenej kompromitácie informačných aktív organizácie. V praxi to znamená, že žiadna jednotlivá osoba by nemala mať možnosť pristupovať, upravovať alebo používať informačné aktíva bez predchádzajúcej autorizácie a overenia identity. Spustenie udalosti musí byť oddelené od jej autorizácie – tomuto princípu sa hovorí segregácia právomocí, niekedy tiež „komisionálnosť“ alebo „princíp štyroch očí“.

Aby sa zabezpečila reálna zodpovednosť v oblasti informačnej bezpečnosti, je potrebné, aby určené osoby disponovali príslušnou kvalifikáciou a aby sa umožnil taký rozvoj zručností, ktorý bude sledovať vývoj technológií a znalostí. To platí univerzálne – na vlastných zamestnancov aj na dodávateľov. Ako som vyššie uviedol, v dobe závažného nedostatku kvalifikovanej pracovnej sily je bežnou praxou vykonávať špecifické odborné činnosti dodávateľským spôsobom, formou tzv. outsourcingu. Dodávatelia a tretie strany v takomto modeli prichádzajú do styku s informačnými aktívami organizácie mnohokrát na úplne totožnej úrovni ako interní zamestnanci. Z toho dôvodu je dôležitou úlohou aj dokumentovanie, koordinácia a dohľad nad aspektmi informačnej bezpečnosti vo vzťahoch s dodávateľmi.

Z hľadiska organizácie informačnej bezpečnosti je vhodné nezabudnúť na bezpečnostné riziká v projektoch. Projektový manažment by mal obsahovať aj princípy bezpečného dizajnu, bezpečnostného testovania a bezpečnej implementácie systémov a procesov. To je nakoniec už aj zákonnou požiadavkou, keďže napr. všeobecné nariadenie EÚ o ochrane údajov (GDPR) vyžaduje, aby prevádzkovateľ už v čase určenia prostriedkov spracúvania prijal primerané technické a organizačné opatrenia so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou, ktoré spracúvanie predstavuje pre práva a slobody fyzických osôb (tzv. princíp „protection by design“ prekladaný ako „špecificky navrhnutá ochrana údajov“).

### Alokácia zodpovedností

Nie je možné vyčerpávajúcim spôsobom pomenovať všetky roly a ich zodpovednosti v oblasti informačnej bezpečnosti. Implementácia týchto procesov v dostatočnom rozsahu a kvalite je netriviálna úloha, ktorá môže trvať aj mnoho mesiacov či rokov.

Povedzme však, že typickou pracovnou rolou, ktorá je priamo spätá s procesmi informačnej bezpečnosti, je bezpečnostný manažér alebo manažér informačnej bezpečnosti. Vo väčších podnikoch sa tiež zvyknú používať anglické ekvivalenty: Chief security officer (CSO) alebo Chief information security officer (CISO). Tieto skratky sú známe najmä kvôli medzinárodne uznanému systému skratiek typu „CxO“, typicky používaných v prostredí veľkých korporácií. Nespornou výhodou tohto „CxO“ názvoslovia je nezávislosť od organizačnej štruktúry. Takýto názov roly žiadnym spôsobom ani len nenaznačuje, kde v organizačnej štruktúre sa rola nachádza.

CSO (alebo CISO) je zodpovedný za výber a manažment tímu informačnej bezpečnosti, definovanie technických a netechnických bezpečnostných politík, štandardov, postupov a usmernení, za riadenie rizík v informačnej bezpečnosti, stanovenie a vyhodnocovanie príslušných metrík, za podporu vlastníkov procesov v oblasti bezpečnosti informačných aktív, implementáciu a prevádzkovanie podporných nástrojov na dosiahnutie súladu so stanovenou stratégiou informačnej bezpečnosti a za preskúmavanie a monitorovanie súladu. Samozrejme, k manažérskym povinnostiam CSO a CISO patrí aj riadenie vyšetrovania a nápravy incidentov v oblasti informačnej bezpečnosti. A v neposlednom rade je jeho úlohou aj organizácia kampaní na zvýšenie povedomia o bezpečnosti pre zamestnancov, s cieľom zlepšiť kultúru bezpečnosti v organizácii.

Ako však už bolo spomenuté, zaručenie bezpečnosti informačných aktív nie je výhradnou úlohou bezpečnostného manažéra, keďže bezpečnosť sa týka všetkých prevádzkových a podporných procesov organizácie. Za ich riadenie sú zodpovední príslušní manažéri na taktickej a operatívnej úrovni riadenia a základné zásady informačnej bezpečnosti by mali byť povinní dodržiavať všetci zamestnanci a tretie strany v každodenných bežných činnostiach.

Manažéri sú (alebo mali by byť) zodpovední za každodenné uplatňovanie politík informačnej bezpečnosti. Sú povinní zabezpečiť, aby v súlade s politikami boli zavedené vhodné technické a organizačné opatrenia a aby ich všetci pracovníci riadne uplatňovali a používali. Priebežne by mali vytvárať podmienky na to, aby boli zamestnanci informovaní o svojich povinnostiach podľa príslušných bezpečnostných politík. Mali by monitorovať plnenie opatrení s cieľom posúdiť ich súlad s bezpečnostnými cieľmi a bezpečnostnou stratégiou a zabezpečovať zdroje a podporu potrebné na zaručenie primeranej ochrany informačných aktív v rámci oblasti ich pracovnej zodpovednosti.

Vlastníci procesov, to sú typicky tí manažéri, ktorí zodpovedajú za ochranu konkrétnych významných informačných aktív. Pravdaže, vlastníci môžu delegovať úlohy týkajúce sa bezpečnosti informácií na iných manažérov alebo iných zamestnancov, ale naďalej im zostáva zodpovednosť za riadne vykonávanie súvisiacich úloh. Zodpovední sú za klasifikáciu informácií a výkon ochrany informačných aktív v zmysle určeného klasifikačného stupňa, monitorovanie dodržiavania požiadaviek na ochranu ovplyvňujúcich ich informačné aktíva, špecifikáciu vhodných bezpečnostných opatrení. V spolupráci s CSO alebo CISO je úlohou vlastníkov procesov aj povoľovanie prístupu k informačným aktívam v súlade s klasifikačným stupňom a zabezpečovanie pravidelného overovania prístupov k systémom v ich gescii.

Najrozšírenejšou rolou v informačnej bezpečnosti sú používatelia informačných technológií, t. j. zamestnanci, zamestnanci dodávateľov, brigádnici alebo zamestnanci vykonávajúci práce na dohodu. Všetci sú zodpovední za dodržiavanie platných politík informačnej bezpečnosti, ak sú tieto relevantné pre ich pracovné roly. Pracovníci sú zodpovední za ochranu všetkých informačných aktív, ktoré im boli zverené pre výkon príslušnej pracovnej roly.

### Výnimky

Niet zrejme takej ľudskej činnosti, ktorá by bola zvládnutá dokonalým spôsobom a ktorá by si v dlhodobom horizonte nevyžadovala žiadne zmeny. Podnikové procesy sú obzvlášť náchylné na potrebu zmien, čo je dané najmä rozvojom trhu. Zmeny procesov však vždy ovplyvnia aj úroveň informačnej bezpečnosti – väčšinou, žiaľ, negatívne.

Pragmaticky uvažujúci bezpečnostný manažér by mal vopred rátať s faktom, že žiadne opatrenie nie je absolútne a že pre niektoré opatrenia bude v istých prípadoch potrebná určitá miera benevolentnosti. Malo by byť v jeho záujme nastaviť vhodné pravidlá pre schvaľovanie výnimiek. Tieto pravidlá neskôr zaručia zachovanie príslušnej úrovne bezpečnosti aj v prípade, že je potrebné rýchlo reagovať na zmenené okolnosti a umožnia udržať primeranú efektivitu opatrení aj v prípade vopred neplánovaných nutných odchýlok od štandardu. Navrhované výnimky, o ktorých sa bezpečnostný manažér domnieva, že by mohli významne negatívnym spôsobom ovplyvniť riziká spojené s informačnou bezpečnosťou, môžu byť v závislosti od závažnosti rizika postúpené na schválenie štatutárnemu vedeniu.

### Zaradenie bezpečnosti v organizačnej štruktúre

Na to, kde by mala byť informačná bezpečnosť zaradená v štruktúre spoločnosti, nie je žiadna norma ani univerzálne odporúčanie. Táto otázka je totiž závislá od mnohých faktorov. Predovšetkým veľkosť organizácie a odvetvie, v ktorom organizácia pôsobí, ovplyvňujú rozhodnutie o tom, kde v úrovni riadenia sa bude nachádzať bezpečnostný manažér a jeho tím. Popíšme si aspoň teoreticky, aké sú možnosti umiestnenia pozície CSO/CISO v kontexte IT procesov organizácií.

Existujú tri kľúčové atribúty, podľa ktorých sa líšia riadiace pozície v organizačných štruktúrach: línia riadenia (t. j. línia reportingu), rozsah právomocí a úroveň centralizácie.

**Riadiaca línia** súvisí so spôsobom, ktorým sa delegujú úlohy, ako sú schvaľované úlohy a vykonaná práca. Definuje, na ktorej „priečke rebríka“ sa má konkrétne oddelenie alebo rola nachádzať.

**Rozsah právomocí** stanovuje, kto pod koho organizačne patrí a aký je rozsah úloh, za ktoré zodpovedá konkrétne oddelenie alebo rola.

**Úroveň centralizácie** je odpoveďou na otázku, kde sa prijímajú konečné rozhodnutia. Centralizovaná štruktúra je vtedy, ak konečné rozhodnutia prijíma jeden určený subjekt v organizácii. A decentralizovanou štruktúrou sa dá nazvať taká, ak sa konečné rozhodnutia prijímajú v rámci tímu zodpovedného za vykonávanie tohto rozhodnutia alebo v rámci viacerých subjektov často začlenených aj naprieč organizáciou.

V nasledujúcej tabuľke sú stručne zhrnuté možné spôsoby organizácie bezpečnosti vo vzťahu k IT. Ide pravdaže o zjednodušujúci výklad. Ako som už uviedol, konkrétne riešenie organizácie informačnej bezpečnosti v podniku je zložitou úlohou, ktorá sa nedá vykonať na počkanie a určite nie bez predchádzajúcej analýzy.

V poslednom stĺpci tabuľky je uvedená skratka ISMS, resp. vyspelosť ISMS, čo je skratka pre systém riadenia informačnej bezpečnosti (z angl. „Information Security Management System“). Je to súbor pravidiel pre manažérsky systém bezpečnosti pokrytý radou medzinárodných technických noriem ISO/IEC 27000.

Vyspelosť procesov sa zvykne určovať podľa metodiky CMMI (z angl.: „Capability Maturity Model Integration“). Model bol pôvodne vytvorený v SEI Software engineering institute v USA, a to na základe systému ISO 9000 s aplikovaním overených praktík v oblasti vývoja softvéru. Vyspelosť procesov sa uvádza v piatich stupňoch:

**Úroveň procesu „počiatočný“** – proces je vykonávaný ad hoc, bez vopred stanovených aktivít a procedúr, závislý na individuálnom prístupe a na konkrétnych osobách.

**Úroveň procesu „opakovateľný“ –**proces je ustanovený, prebieha väčšinou rovnakým spôsobom, procesná disciplína sa opiera o predchádzajúce výsledky, chýba dokumentácia, metrika a optimalizácia.

**Úroveň procesu „formalizovaný“ –**proces je ustanovený, prebieha rovnakým spôsobom, je zdokumentovaný a štandardizovaný, organizácia má prehľad o vstupoch a výstupoch procesu, proces je integrovaný do ostatných procesov, chýba metrika a  optimalizácia.

**Úroveň procesu „riadený“** –  proces je plne kontrolovaný, obsahuje potrebné formálne prvky, meraná je jeho účinnosť a produktivita, výstupy sú systematicky vyhodnocované.

**Úroveň procesu „optimalizovaný“** – plne kontrolovaný, obsahuje potrebné formálne prvky, meraná je jeho účinnosť a produktivita, proces je priebežne optimalizovaný na základe kvantitatívnej spätnej väzby.

Ak premietneme vyššie uvedenú teóriu do tabuľky, je týmto spôsobom možné rozlíšiť medzi niekoľkými typmi organizačného usporiadania bezpečnostných rolí.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Typ bezpečnosti** | **Líniareportingu** | **Rozsah právomocí** | **Úroveňcentralizácie** | **Segregácia právomocí** | **Predpokladanávyspelosť ISMS** |
| **Ignorovaná**(t.j. žiadne bezpečnostné roly) | – | – | – | – | 0 – ISMS nie jezavedený |
| **Minimálna**(čiastočné poverenia bezpečnostnými funkciami) | – | Čiastočný | Decentralizovaná | Najhorší scenár | 0 – ISMS nie jezavedený |
| **Formálna**(manažér IT je zároveň bezpečnostným manažérom) | Formálna rola | Identickýs manažérom IT | Centralizovaná | Neexistuje | 1 – ISMS„počiatočný“ |
| **Základná**(manažér informačnej bezpečnosti ovplyvňuje IT, reportuje manažérovi IT) | Nejasná | Identickýs manažérom IT | Čiastočnecentralizovaná | Slabá | 2 – ISMS„opakovateľný“ |
| **Agilná**(manažér informačnej bezpečnosti ovplyvňuje IT, reportuje bezpečnostnému manažérovi. Bezpečnostný manažér reportuje manažérovi IT) | Slabá | Nedostatočný | Čiastočnecentralizovaná | Čiastočná | 3 – ISMS„formalizovaný“ |
| **Riadená**(Vytvorené oddelenie bezpečnosti, bezpečnostný manažér reportuje manažérovi IT) | Udržateľná | Dostatočný | Centralizovaná | Udržateľná | 4 – ISMS„riadený“ |
| **Integrovaná**(Vytvorené oddelenie bezpečnosti, zriadené nezávislé oddelenie bezpečnostných operácií, bezpečnostný manažér reportuje manažérovi IT) | Dostatočná | Dostatočný | Centralizovaná | Dobrá | 5 – ISMS„optimalizovaný“ |
| **Nezávislá inštitucionálna**(Vytvorené oddelenie bezpečnosti, zriadené nezávislé oddelenie bezpečnostných operácií, bezpečnostný manažér reportuje v nezávislej riadiacej línii, prípadne priamo štatutárnemu vedeniu) | Optimálna | Široký | Centralizovaná | Najlepší scenár | 5 – ISMS„optimalizovaný“ |

Iste si v tabuľke všimnete, že niektoré atribúty organizačného usporiadania bezprostredne určujú vyspelosť systému riadenia informačnej bezpečnosti v organizácii.

Napríklad, ak bezpečnostný manažér podlieha štatutárnemu vedeniu bez ďalšieho manažérskeho stupňa, vníma sa to ako prejav priameho záujmu vedenia o informačnú bezpečnosť. Štatutárnemu vedeniu to umožňuje podporovať a strategicky riadiť informačnú bezpečnosť v súlade s príslušnou legislatívou a reguláciami. Ak bezpečnostný manažér má mandát od najvyššieho vedenia, požiadavky bezpečnosti môžu byť vhodne zosúladené naprieč celou organizáciou. Na nižších manažérskych úrovniach sú požiadavky bezpečnosti implementované prostredníctvom špecifických vnútorných predpisov príslušnej organizačnej jednotky. V podnikateľskom prostredí je pri tomto usporiadaní člen predstavenstva tzv. „sponzor“ a bezpečnostný manažér je vlastníkom rozpočtu informačnej bezpečnosti.

Ak je bezpečnosť nezávislá od IT, prináša to ďalšie výhody. Predovšetkým je tým zaručená segregácia právomocí, čo sekundárne umožní vytvoriť pozíciu osoby zodpovednej za ochranu osobných údajov (Data Protection Officer - DPO), prípadne aj kumuláciou s niektorou z bezpečnostných rolí. Nemožno tiež nespomenúť, že informačná bezpečnosť a komfort IT služieb sú v nepriamej úmere, čo znamená, že vo vzťahu bezpečnosť verzus prevádzka IT viac ako inde platí slovenské príslovie „bližšia košeľa ako kabát“. Pri nezávislom umiestnení bezpečnosti však požiadavky bezpečnosti nie sú podriadené požiadavkám prevádzky IT ani vývoja SW, a tým sa umožní vykonávanie nezávislého posudzovania IT rizík a kybernetických bezpečnostných rizík.

Aké plynú obmedzenia a nedostatky z absencie rolí informačnej bezpečnosti? Predovšetkým – neexistuje jednotné riadenie bezpečnosti a procesy bezpečnostných operácií sú implementované nedostatočne alebo vôbec.

Obmedzenie nastáva aj pri pokuse o kumuláciu niektorých bezpečnostných rolí s  IT rolami. Problémom je najmä nedostatok špecifických vedomostí a zručností. IT špecialisti sa, pochopiteľne, sústredia primárne na svoje vlastné pracovné úlohy a v takom prostredí nie je možné očakávať, že sa vyvinie dostatočná spôsobilosť v oblasti ochrany informácií. Kumulácia rolí spôsobí aj pracovné preťaženie, čo následne vedie k problémom v prioritizácii úloh (má administrátor v prípade incidentu najprv riešiť návrat systémov do štandardného stavu alebo digitálnu forenznú analýzu?). Ak by aj organizácia mala takých zručných IT špecialistov, ktorí by zvládli dvojjedinú rolu, prinajmenšom nastane jasné porušenie princípu segregácie právomocí. Na druhej strane – príliš rozdrobené individuálne povinnosti zamestnancov oddelenia bezpečnosti by následne viedli k nejasnej línii riadenia, k problémom so zodpovednosťou za pridelené úlohy a v oblasti kybernetickej bezpečnosti tým typicky aj k nižšej vyspelosti procesu riešenia kybernetických bezpečnostných incidentov.

Aká organizačná štruktúra je teda najvhodnejšia? Opätovne zopakujem: univerzálne riešenia organizačnej štruktúry nejestvujú. Berúc však do úvahy reálnu dobrú prax, dá sa aspoň naznačiť, ktorá zo štruktúr sa môže hodiť pre niektorý typ organizácie viac alebo  menej.

Pre veľké komerčné organizácie, ktoré sú závislé od informačných aktív (napríklad banky, telekomunikační operátori, energetické a vodárenské podniky alebo veľké výrobné podniky), je vhodné sústrediť sa na vytvorenie „integrovanej bezpečnosti“ alebo „nezávislej inštitucionálnej bezpečnosti“. Tieto dva typy štruktúr zaručia efektívnu koordináciu medzi jednotlivými doménami bezpečnosti a zosúladenie s požiadavkami normy ISO/IEC 27001 „Bezpečnostné metódy – Systém riadenia informačnej bezpečnosti – Požiadavky“. Najmä vhodnú integráciu fyzickej a objektovej bezpečnosti, riadenia kontinuity činností, riešenia podvodov, ochrany osobných údajov a ďalších. Pri týchto dvoch usporiadaniach bezpečnosti sú jasne definované a alokované zodpovednosti, zaručená je segregácia právomocí a je vytvorený jednotný kontaktný bod pre všetky otázky súvisiace s bezpečnosťou vrátane kontaktu s relevantnými autoritami, regulátormi trhu, štátnou mocou a odbornými organizáciami. Je tiež veľmi dôležité, že v tomto type usporiadania je možné najúčelnejším spôsobom riadiť náklady spojené s bezpečnosťou.

Pre malé a stredne veľké podniky (tzv. segment „SME“) je vhodným usporiadaním „riadená bezpečnosť“ alebo „agilná bezpečnosť“. Tieto pokrývajú aspoň hlavné domény bezpečnosti, pričom neskôr sa manažérsky systém môže priebežne vylepšovať. Pri týchto dvoch usporiadaniach bezpečnosti sú čiastočne definované základné zodpovednosti, segregácia právomocí je na dostatočnej udržateľnej úrovni a je vytvorený jednotný kontaktný bod pre hlavné bezpečnostné otázky, najmä riešenie kybernetických bezpečnostných incidentov.

Organizácia informačnej bezpečnosti je však skutočne iba prvým krokom k stavu, v ktorom je možné vyhlásiť, že manažujete informačnú bezpečnosť vašej organizácie. K dosiahnutiu súladu so zákonnými požiadavkami a dosiahnutiu takej úrovne ošetrenia bezpečnostných rizík, v ktorej bude vaša organizácia odolná aspoň voči aktuálne známym hrozbám, vás čaká ešte množstvo ďalšej práce.

[§ 20 zákona č. 69/2018 Z. z.](https://www.bezpecnostvpraxi.sk/form/goto.ashx?t=29&p=4804671-4804672&f=2)

[§ 5 vyhlášky č. 362/2018 Z. z.](https://www.bezpecnostvpraxi.sk/form/goto.ashx?t=29&p=4985475-4985485&f=2)