**Implementácia bezpečnostných opatrení**

Bezpečnosť a rovnako aj implementácia bezpečnostných opatrení je cyklický a nikdy nekončiaci proces. A tak k nim treba aj pristupovať. Cyklickosť bezpečnosti a cyklickosť implementácie bezpečnostných opatrení najlepšie popisuje a vystihuje tzv. Demingov model (PDCA – plan-do-check-act), ktorý znázorňuje jednotlivé fázy implementácie bezpečnostných opatrení a ich neustále sa opakovanie. Ak si teda predstavujete implementáciu bezpečnostných opatrení ako jednorazový proces alebo jednorazovú aktivitu, ste na omyle. Na ich plánovaní, vykonaní, neustálom overovaní a zlepšovaní treba v rámci každej jednej organizácie neustále pracovať.



Obr.č.1: Demingov model PDCA

Na to, aby sme v rámci organizácie dosiahli primeranú a náležitú ochranu informačných aktív, je nevyhnutná komplexná fáza plánovania. V rámci plánovania pri riešení kybernetickej a informačnej bezpečnosti odporúčame vybrať si rámec (framework) alebo štandard **1** podľa ktorého bude organizácia postupovať. Od prijatia zákona o kybernetickej bezpečnosti **2** (ďalej len „Zákon“), ktorý nadobudol účinnosť 1. apríla 2018, je tento rámec daný všeobecne záväzným právnym predpisom, z ktorého je potrebné vychádzať. Ide najmä o povinnosť prijať bezpečnostné opatrenia alebo primerané bezpečnostné opatrenia. Prijať bezpečnostné opatrenia sa v úplnom alebo primeranom rozsahu vzťahuje na ústredné orgány podľa [§ 4 písm. a)](https://www.bezpecnostvpraxi.sk/form/goto.ashx?t=27&p=4804459&f=2) Zákona **3** (aplikuje bezpečnostné opatrenia), iné orgány štátnej správy podľa [§ 4 písm. b)](https://www.bezpecnostvpraxi.sk/form/goto.ashx?t=27&p=4804460&f=2) Zákona **4** (prijímajú a dodržiavajú vhodné a primerané bezpečnostné opatrenia podľa [§ 20](https://www.bezpecnostvpraxi.sk/form/goto.ashx?t=27&p=4804668-4804691&f=2)Zákona), ako aj na [prevádzkovateľov základnej služby](https://www.bezpecnostvpraxi.sk/form/goto.ashx?t=40&p=13679358)  (prijímajú a dodržiavajú všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa [§ 20](https://www.bezpecnostvpraxi.sk/form/goto.ashx?t=27&p=4804668-4804691&f=2) a sektorové bezpečnostné opatrenia, ak sú prijaté) a v neposlednom rade aj na [poskytovateľov digitálnej služby](https://www.bezpecnostvpraxi.sk/form/goto.ashx?t=40&p=13679358)  (prijímajú a dodržiavajú vhodné a primerané bezpečnostné opatrenia na účely riadenia rizík súvisiacich s ohrozením kontinuity digitálnej služby a procesu riešenia kybernetických bezpečnostných incidentov).

Bezpečnostnými opatreniami sa podľa [§ 20](https://www.bezpecnostvpraxi.sk/form/goto.ashx?t=27&p=4804668-4804691&f=2) Zákona a na účely tohto Zákona rozumejú úlohy, procesy, roly a technológie v troch základných oblastiach (organizačná, personálna a technická), ktorých cieľom je zabezpečenie kybernetickej a informačnej bezpečnosti počas životného cyklu sietí a informačných systémov. Bezpečnostné opatrenia sa realizujú v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov a v súlade s bezpečnostnými štandardmi v oblasti kybernetickej a informačnej bezpečnosti, pričom klasifikácia informácií a kategorizácia sietí a informačných systémov sa vykonáva na základe významnosti, funkcie a účelu informácií a informačných systémov s ohľadom na dôvernosť, integritu, dostupnosť, kvalitu služby a kontrolnú činnosť.

Bezpečnostné opatrenia je potrebné prijímať s cieľom predchádzania kybernetickým a informačným bezpečnostným incidentom a minimalizovania vplyvov kybernetických a informačných bezpečnostných incidentov na kontinuitu prevádzkovania služby. Bezpečnostné opatrenia sú všeobecné určené pre všetky siete a informačné systémy a sektorové, ktoré sa realizujú na základe špecifík kategorizácie sietí a informačných systémov ústredného orgánu v rozsahu svojej pôsobnosti podľa [prílohy č. 1](https://www.bezpecnostvpraxi.sk/form/goto.ashx?t=27&p=4805011-4805149&f=2) a v súlade s bezpečnostnými štandardmi v oblasti kybernetickej a informačnej bezpečnosti.

Bezpečnostné opatrenia sa prijímajú na základe odporúčaní medzinárodne akceptovaných štandardov kybernetickej a informačnej bezpečnosti alebo iných vecne obdobných postupov a metód so zreteľom na najnovšie poznatky a pri súčasnom identifikovaní rizík, zraniteľností a požiadaviek regulácie v rámci sektora prevádzkovateľa základnej služby podľa [prílohy č. 1](https://www.bezpecnostvpraxi.sk/form/goto.ashx?t=27&p=4805011-4805149&f=2) Zákona. Bezpečnostné opatrenia, ktorých cieľom je zabezpečenie kybernetickej a informačnej bezpečnosti počas životného cyklu sietí a informačných systémov, je potrebné prijať predovšetkým pre oblasť:

1. organizácie informačnej bezpečnosti,
2. riadenia aktív, hrozieb a rizík,
3. personálnej bezpečnosti,
4. riadenia dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,
5. technických zraniteľností systémov a zariadení,
6. riadenia bezpečnosti sietí a informačných systémov,
7. riadenia prevádzky,
8. riadenia prístupov,
9. kryptografických opatrení,
10. riešenia kybernetických bezpečnostných incidentov,
11. monitorovania, testovania bezpečnosti a bezpečnostných auditov,
12. fyzickej bezpečnosti a bezpečnosti prostredia,
13. riadenia kontinuity procesov.

Subjekty, ktoré majú povinnosť aplikovať bezpečnostné opatrenia, si môžu zvoliť vlastný konkrétny spôsob ich realizácie. Inými slovami, obsah a štruktúra bezpečnostnej dokumentácie, v ktorej sa popisuje prijímanie a dodržiavanie bezpečnostných opatrení, je stanovená vyhláškou Národného bezpečnostného úradu č. [362/2018 Z. z.](https://www.bezpecnostvpraxi.sk/form/goto.ashx?t=26&p=4985417&f=2), ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „Vyhláška o bezpečnostných opatreniach“) a vychádza, resp. je odvodená od požiadaviek a odporúčaní dobrej praxe (best practice) v súlade s ISO / IEC 27001, ISO / IEC 27002, COBIT a iné, pričom konkrétny spôsob ich realizácie môže byť odvodený z princípov niektorého z rámcov riadenia bezpečnostnej architektúry, ako napríklad Sherwood Applied Business Security Architecture (SABSA), resp. TOGAF9. Dôležité je, aby bol cieľ určený vyhláškou o bezpečnostných opatreniach naplnený a zásady a princípy definované v nej dodržané.

Okrem oblastí uvedených v [§ 20 ods. 3](https://www.bezpecnostvpraxi.sk/form/goto.ashx?t=27&p=4804671-4804684&f=2) Zákona a podrobne popísaných v [§ 5 až § 17 vyhlášky](https://www.bezpecnostvpraxi.sk/form/goto.ashx?t=27&p=4985475-4985695&f=2) o bezpečnostných opatreniach musia bezpečnostné opatrenia zahŕňať najmenej procesy a postupy súvisiace s detekciou, evidenciou a riešením kybernetických a informačných bezpečnostných incidentov, a to minimálne:

1. detekciu kybernetických a informačných bezpečnostných incidentov,
2. evidenciu kybernetických a informačných bezpečnostných incidentov,
3. postupy riešenia a riešenie kybernetických a informačných bezpečnostných incidentov,
4. určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,
5. pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických a informačných bezpečnostných incidentov a centrálneho systému včasného varovania.

Alfou a omegou implementácie bezpečnostných opatrení v organizáciách je schválenie bezpečnostnej dokumentácie, v ktorej sa popíše, ako sa bezpečnostné opatrenia budú prijímať a dodržiavať a ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu. V zmysle vyššie uvedeného Demingovho modelu PDCA nie je ani prijatie a schválenie bezpečnostnej dokumentácie jednorazová aktivita. Bezpečnostná dokumentácia musí byť pravidelne preskúmavaná a revidovaná tak, aby ju organizácia udržiavala aktuálnu, a teda zodpovedajúcu realite a bezpečnostným požiadavkám. Čo sa týka obsahových náležitostí, obsah a štruktúru bezpečnostnej dokumentácie podrobne upravuje [§ 2 vyhlášky](https://www.bezpecnostvpraxi.sk/form/goto.ashx?t=27&p=4985431-4985448&f=2) o bezpečnostných opatreniach.

Bezpečnostná dokumentácia musí obsahovať aj schválenú bezpečnostnú stratégiu kybernetickej a informačnej bezpečnosti a bezpečnostné politiky kybernetickej a informačnej bezpečnosti. Bezpečnostná stratégia vychádza z výsledkov analýzy rizík a obsahuje predovšetkým ciele a základné princípy na dosiahnutie účelu zabezpečenia kybernetickej a informačnej bezpečnosti. Bezpečnostná stratégia je následne podkladom na prijatie bezpečnostnej politiky kybernetickej a informačnej bezpečnosti, ktorá sa vytvára pre strategickú úroveň riadenia, čiže pre vedenie organizácie. Politiku kybernetickej a informačnej bezpečnosti treba chápať ako vrcholový dokument, ktorý obsahuje strategické bezpečnostné ciele a požadovanú úroveň bezpečnosti. Je v nej potrebné zdôrazniť zodpovednosť vedenia za bezpečnosť organizácie a zároveň určiť aj rozsah jej aplikácie (či platí pre celú organizáciu, alebo len jej časť). Vyhláška o bezpečnostných opatreniach umožňuje, aby bezpečnostná stratégia mohla byť prijatá priamo aj vo forme bezpečnostnej politiky kybernetickej a informačnej bezpečnosti. Súbor politík informačnej bezpečnosti schvaľuje vedenie organizácie a mal by sa vydať a oznámiť všetkým zamestnancom, ako aj relevantným tretím stranám. Taktiež ani politika ako súčasť bezpečnostnej dokumentácie nie je jednorazová aktivita. Musí byť stanovená periodicita jej preskúmavania a jej aktualizácie, preskúmavaná musí byť v plánovaných intervaloch, resp. bezodkladne vždy pri výskyte významných zmien.

Zodpovednosť za komplexné riešenie kybernetickej a informačnej bezpečnosti musí „ležať na pleciach“ vrcholového vedenia organizácie. Samotné úlohy, ktoré z tejto činnosti vyplývajú, musia byť delegované na manažéra kybernetickej bezpečnosti. Manažér kybernetickej a informačnej bezpečnosti zodpovedá za organizovanie systému riadenia kybernetickej a informačnej bezpečnosti a jeho úloha je kľúčová pre správne nastavenie fungovania systému riadenia kybernetickej a informačnej bezpečnosti. Manažér kybernetickej a informačnej bezpečnosti musí mať možnosť predkladať návrhy a oznamovať informácie v oblasti kybernetickej a informačnej bezpečnosti priamo štatutárnemu orgánu organizácie a zároveň musí byť nezávislý od riadenia prevádzky a vývoja služieb informačných technológií. Jeho povinnosťou bude informovať vedenie o činnostiach vyplývajúcich z výkonu úlohy, teda najmä o stave systému riadenia kybernetickej bezpečnosti.

Riešenie, resp. nedostatočné riešenie informačnej a kybernetickej bezpečnosti môže mať veľký dosah na celkové fungovanie organizácie. Úlohou vedenia organizácie je najmä zabezpečiť, aby sa na jednej strane k manažérovi kybernetickej bezpečnosti dostávali všetky relevantné informácie, no na strane druhej, aby bola kybernetická bezpečnosť presadzovaná naprieč všetkými dôležitými procesmi, projektmi a činnosťami organizácie a aby všetci zamestnanci (vedúcich pracovníkov nevynímajúc) podporovali aktivity súvisiace s kybernetickou aj informačnou bezpečnosťou.

Aby bolo možné zavedený systém bezpečnosti udržiavať funkčný a neustále ho zlepšovať, je potrebné periodicky preskúmavať jeho efektívnosť. V správach z preverenia manažér kybernetickej a informačnej bezpečnosti pripravuje aj návrhy opatrení na zlepšenie. Je žiadúce ho schváliť manažmentom, pripraviť zdroje a plán implementácie schválených opatrení. Týmto sa proces implementácie bezpečnostných opatrení a budovania systému kybernetickej a informačnej bezpečnosti v rámci organizácie uzatvára a plynule prechádza opäť do plánovania, vytvorenia, implementácie a ďalšieho preverovania bezpečnostných opatrení.

Súvisiace právne predpisy ZZ SR

* [69/2018 Z. z.](http://www.epi.sk/zz/2018-69) Zákon o kybernetickej bezpečnosti
* [362/2018 Z. z.](http://www.epi.sk/zz/2018-362) Vyhláška, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení