

Politika bezpečnostní

Politika bezpečnostní stanovuje základní principy a východiska pro řízení bezpečnosti ve společnosti. Vymezuje oblasti a zásady ochrany, způsob ochrany jednotlivých oblastí (bezpečnostní nástroje) a osoby odpovědné za ochranu jednotlivých oblastí (bezpečnostní management).

Bezpečnostní politika je nezbytná pro realizaci všech standardů, směrnic, procedur a opatření, které rozhodují o tom, jak jsou aktiva včetně citlivých informací spravována, chráněna a distribuována uvnitř i vně společnosti a jejich informačních systémů. Vedle výsledků analýzy rizik informační bezpečnosti politika vytyčuje hlavní směry, ve kterých je třeba řízení bezpečnosti v organizaci dále rozvíjet.

Rozsah politiky

Předmětem politiky je trvalá ochrana všech aktiv společnosti, které se ve společnosti mohou nacházet nebo k nim má společnost přístup.

Vedení společnosti se zavazuje v souladu se strategií společnosti k neustálému zlepšování systému řízení bezpečnosti a všech souvisejících procesů uplatňovaných v jednotlivých oblastech ochrany.

Oblastmi ochrany v tomto systému řízení bezpečnosti rozumíme:

- Ochrana a zajištění byznys kontinuity
- Ochrana provozu – kontinuita provozu
- Ochrana hmotného majetku
- Ochrana nehmotného majetku
- Bezpečnost lidských zdrojů
- Ochrana produktů a služeb

Východiska politiky

Pojetí současného řízení bezpečnosti informací v organizaci vychází z následujícího modelu dokumentace:

- Politika bezpečnostní
- Strategické cíle na příslušný kalendářní rok
- Bezpečnostní postupy – soubor konkrétních bezpečnostních témat (postupy, pravidla, doporučení) pro zajištění pokynů ze strany managementu ve vztahu k systému bezpečnosti informací a zaměstnancům společnosti.

Pro zajištění neustálé vhodnosti, přiměřenosti a efektivnosti, je zvolený model dokumentace přezkoumáván v pravidelných intervalech nebo tehdy, pokud dojde v organizaci k významným změnám.

Bezpečnost aktiv a IS společnosti je věcí všech zaměstnanců. Všichni zaměstnanci se podílejí na zodpovědnosti za ochranu a dohled nad informacemi, které se vytvářejí, zpracovávají, přijímají nebo odesílají na jejich pracovišti a v jejich projektu. Pod pojem bezpečnost dále zahrnujeme soukromí uživatelů, důvěryhodnost a integritu informací.

Zásady politiky

Vrcholové vedení společnosti se zavazuje v oblasti bezpečnosti k dodržování následujících zásad:

1. Zajištění byznys kontinuity

- Zajistit prediktivní řízení kapacit lidských zdrojů a finanční zdroje, včetně potřebných rezerv, pro plnění všech závazků v dostatečné kvalitě se zajištěním neustálé kontinuity.

2. Ochrana provozu – kontinuita výrobních procesů

- Zajistit autorizovaný provoz všech systémů společnosti s eliminací nebo minimalizací následků případných bezpečnostních incidentů.
- Vyhodnocovat následky bezpečnostních incidentů a uplatňovat nápravná opatření k zamezení jejich opakování stanovením vyhodnotitelných programů a cílů.
- Informační systémy, aplikace, sítě a další prostředky využívané pro nakládání s informacemi (v jakékoli podobě) musí být schopné odolat nebo být obnovitelné v případě uplatnění hrozeb porušení jejich důvěrnosti, integrity nebo dostupnosti.

3. Ochrana hmotného majetku

- Zajistit trvale ochranu majetku a místa, kde společnost poskytuje služby svým zákazníkům trvalým zlepšováním úrovně havarijních a bezpečnostních plánů, jako prevenci před ekonomickými ztrátami, mimořádnými a krizovými událostmi. Ochrana životů a zdraví má vždy přednost před ochranou majetku.

4. Ochrana nehmotného majetku

- Zachovávat a trvale chránit informační aktiva společnosti, tzn. vše, co má pro společnost nějakou hodnotu z pohledu informační bezpečnosti.
- Maximální pozornost věnovat ochraně soukromí uživatelů (osobních údajů), důvěryhodnosti a integritě informací.

5. Bezpečnost lidských zdrojů

- Znat rizika a pravidelným proškolením a nacvičováním havarijních situací jako nedílné součásti přípravy, zajistit prevenci zaměstnanců před těmito riziky.
- Zajistit a požadovat, aby všichni zaměstnanci získali odpovídající povědomí o bezpečnosti.

6. Ochrana produktů a služeb

- Zajistit bezpečnost zaváděných produktů a služeb společnosti odpovědným plněním požadavků všech platných zákonných norem, regulatorních požadavků a předpisů.
- Zároveň se důsledně věnovat ochraně před zneužitím komunikačních služeb.

7. Informovanost

- Předávat informace zákazníkům, dodavatelům a ostatním právnickým a fyzickým osobám vyskytujícím se ve společnosti i v jejím okolí o rizicích, stanovených opatřeních a jejich žádoucím chování.

Nástroje politiky

K nástrojům bezpečnostní politiky patří cokoli, co je schopno s vynaložením určitých nákladů snížit nebo vyloučit nebezpečí újmý vzniklé na straně společnosti.

1. Klasifikace informací

- Cílem klasifikace je rozdělení všech informací, se kterými společnost pracuje, do tříd dle stupně jejich důvěrnosti. Z toho pak vyplývá způsob nakládání s těmito informacemi a jejich nosiči (osoby oprávněné k manipulaci, způsob skladování, způsob skartace ...) a jejich ochrana.

2. Prevence úniku dat

- Soubor technologických a organizačních opatření, zavedených ke snížení rizika úniku vybraných typů informací, které vyžadují ze své povahy vyšší úroveň regulace nebo ochrany (důvěrné informace, osobní údaje, data chráněná ze zákona), jejichž zpřístupnění (únik) velmi pravděpodobně způsobí škodu (finanční, reputační apod.).

3. Systém pro podporu řízení bezpečnosti

- Jedná se o centrální sběrný systém, který zpracovává všechny bezpečnostní incidenty a rizika v organizaci (narušení bezpečnostních politik, trestně právní události, rizika trestně právního jednání atd.). Výsledkem je pak adekvátní reakce na příslušné incidenty, případné vyčíslení způsobených škod, zastupování organizace v trestním řízení, přijímání protipatření a návrh preventivních postupů.

4. Zabezpečení zaváděných produktů a služeb

- Jedná se o prvotní posouzení zaváděné služby nebo produktu (obchodního záměru) z pohledu bezpečnosti již ve fázi přípravy a vývoje prováděním bezpečnostních testů apod.

5. IT ochrana

- Úkolem IT ochrany je zajistit požadovanou úroveň v charakteristikách – dostupnost, integrita a důvěrnost odpovídajících systémů, aplikací a dat vlastních i zákaznických, včetně poskytovaných cloudových služeb. Jedním z prvků IT ochrany je řízení a správa uživatelských účtů a oprávnění na základě principu „need to know“.

6. Fyzická ochrana

- Fyzická ochrana jako nástroj obsahuje veškerá fyzická zabezpečení provozu, hmotného majetku i osob. Mezi prostředky fyzické ochrany organizace patří prvky technické ochrany, speciální technické ochrany, požární a, mechanické ochrany.

7. Personální ochrana

- Jedná se o zajištění povinností, práv a bezpečnosti práce zaměstnance podle požadavků platných právních předpisů (zejména Zákoníku práce, Listiny základních práv a svobod) a ochranu zaměstnanců formou pravidelných školení, vybavení a zajištění pracovních podmínek. Součástí personální ochrany je neustálý rozvoj bezpečnostního povědomí zaměstnanců a jejich profesní kvalifikace.

8. Krizové řízení

- Krizové řízení lze definovat jako systém a metody řešení krizových situací. Krizové řízení je tvořeno širokým spektrem činností, mezi něž patří zejména plánování, podpora rozhodování v mimořádných/krizových situacích, simulace krizových situací a jejich řešení, civilní nouzové plánování, monitorování, modelování a analýza situací.

9. Firemní kultura a dokumentace z pohledu bezpečnosti

- Zaměstnanci jsou seznamováni nejen s firemní kulturou, ale zároveň s Etickým kodexem a dalšími dokumentovanými informacemi v rámci společných i individuálních školení, jejichž výsledkem je osobní rozvoj zaměstnanců a jejich seznámení se zákonnými, interními a obecně platnými bezpečnostními pravidly.

10. Hlášení neetického (podvodného) jednání

- Společnost má stanoveny mechanismy pro ochranu oznamovatelů před podvodným jednáním. Všichni zaměstnanci mohou tyto postupy použít pro nahlášení neetického (podvodného) jednání.

11. Monitorování a přezkoumávání služeb dodavatelů

- Bezpečnostní požadavky na dodavatele služeb jsou definovány v rámci uzavíraných smluv. Kvalita služeb a míra dodržování jednotlivých požadavků musí být průběžně monitorovány a pravidelně přezkoumávány.

12. Ochrana osobních údajů

- Společnost má zřízenou funkci Pověřence pro ochranu osobních údajů. Bezpečnostní pravidla se zaměřují na zpracování a ochranu osobních údajů ve vztahu ke všem subjektům údajů, tj. klientům nebo potenciálním klientům společnosti, obchodním partnerům společnosti a zaměstnancům společnosti.