

ANALÝZA RIZIK

Informační bezpečnost je aktuálním problémem každé společnosti a úspěchy či neúspěchy v této oblasti mají významný vliv nejen na samotnou výkonnost firmy, ale také na její image a důvěryhodnost na trhu.

Kvalitní implementaci předchází důkladná analýza

Zavedení bezpečnostního systému předchází analýza rizik, poté je možné zpracovat plán informační bezpečnosti a úspěšně jej zavést do běžné praxe. Společnost FreeDivision díky své komplexní nabídce služeb v oblasti bezpečnosti klientům zajistí nejen analýzu rizik, ale i všechny následné kroky při zajištění informační bezpečnosti. Včetně případné kompletní revize bezpečnostních prostředků a zavedení nových bezpečnostních opatření „na klíč“.

Třífázový projekt

Analýza rizik je rozvržena do tří základních etap. Začíná samotným zpracováním analýzy rizik, zhodnocením aktuálního stavu bezpečnosti. Ve druhé fázi vzniká bezpečnostní politika a bezpečnostní projekt. Bezpečnostní politika na úrovni představuje soubor zásad, opatření a postupů pro zajištění informační bezpečnosti. Jako plán implementace slouží bezpečnostní projekt, podle kterého je možné navržená opatření zavést do běžného chodu firmy.

Ve třetí etapě jde o zavedení zásad a cílů stanovených bezpečnostní politikou do praxe. Naši specialisté poskytují především metodickou

podporu, vlastní implementaci zajišťují pracovníci klienta. Kromě metodické podpory zajistíme i technické služby v oblasti bezpečnosti, školení a případnou aktualizaci bezpečnostní politiky.

Komplexní pokrytí firemních činností

Analýza rizik zkoumá slabiny a hrozby ve všech oblastech činnosti klienta, které mohou představovat bezpečnostní riziko. Naši specialisté přezkoumají soulad s legislativními požadavky (např. dodržování či porušování autorského zákona v souvislosti s legálním softwarem). Zaměří se i na organizační aspekty při řízení informační bezpečnosti a přístupu třetích stran (odběratelé, dodavatelé, spolupracovníci). Přezkoumají bezpečnost při práci se softwarem a hardwarem. Důležitá je i analýza technologií pro komunikaci interní i externí, stejně jako šifrovacích a dešifrovacích prostředků při komunikaci.

Analýza rizik zahrnuje i přezkoumání fyzické bezpečnosti (např. řízení přístupu do místnosti s výpočetní technikou) a personální bezpečnosti. Analyzujeme také fungování správy provozu IT. Analýza rizik zahrnuje i pravidla pro změny v bezpečnostním systému a kontrolní mechanismy,

tedy pravidelnou revizi bezpečnostní politiky, interní audity a další podoblasti.

VÝHODY

Minimalizace rizik bezpečnostních hrozeb

- Neoprávněného přístupu
- Neoprávněné manipulace s daty
- Vyzrazení citlivých dat
- Zničení dat
- Počítačových virů
- Útoků z internetu

Vyjasnění práv a povinností

- Při práci s výpočetní technikou
- Při manipulaci s klasifikovanými daty

Kontrola, prevence, legislativní soulad

- Spolehlivé kontrolní a monitorovací mechanismy
- Včasné odhalení bezpečnostních incidentů
- Předcházení bezpečnostním problémům
- Soulad s legislativními požadavky (např. Autorský zákon, Zákon o ochraně osobních údajů)

