ŘÍZENÍ BEZPEČNOSTI INFORMACÍ ISMS

S RŮSTEM STRATEGICKÉHVÝZNAMU INFORMAČNÍCH SYSTÉMŮ SE JEDNÍM Z KLÍČOVÝCH ÚKOLŮ MANAGEMENTU KAŽDÉ ORGANIZACE STÁVÁ ZAJIŠTĚNÍ BEZPEČNOSTI INFORMACÍ V NICH ULOŽENÝCH.

Systém řízení bezpečnosti informací (ISMS – Information Security Management System) představuje doporučený přístup pro vytvoření takového prostředí v organizaci, které zajistí potřebnou ochranu informací před hrozbami. Zavedení ISMS zahrnuje návrh a implementaci procesů vedoucích k řízení informační bezpečnosti, implementaci potřebných opatření, kontrole jejich efektivity a jejich následné neustálé udržování a zlepšování.

[PROČ ZAVÁDĚT ISMS]

Zavedení ISMS je vhodné tehdy, pokud je potřeba chránit data organizace, zákazníků či občanů, zdokonalit zabezpečení informací v podniku či organizaci nebo zajistit kontinuitu činností organizace v případě havárie nebo bezpečnostního incidentu. Důvodem zavádění ISMS může být i rozhodnutí efektivněji vynakládat prostředky a směrovat je do míst s významnými riziky. V neposlední řadě se řízením informační bezpečnosti musí zabývat organizace, které potřebují vyhovět legislativním a regulačním požadavkům.
Následnou certifikací systému řízení bezpečnosti informací může organizace prokazovat svým zákazníkům důvěryhodnost, získat konkurenční výhodu a dostát podmínkám účasti v některých výběrových řízeních.

[PŘÍSTUP A ZKUŠENOSTI]

Provádíme nejen návrh procesů pro všechny uvedené fáze, ale také analýzu rizik, návrh bezpečnostní politiky a další bezpečnostní dokumentace, hodnocení, projektování a implementaci bezpečnostních opatření. Naše nabídka služeb zahrnuje i audit bezpečnosti a havarijní plánování. Ke každému zákazníkovi přistupujeme zcela individuálně a pro zavedení systému řízení bezpečnosti informací aplikujeme poznatky nejlepší praxe.

VLASTNOSTI A VÝHODY

- Vytvoření prostředí zajišťujícího informační bezpečnost a ochranu soukromí
- Snížení rizik souvisejících s nedostupností, únikem či ztrátou informací
- Optimalizace nákladů na zajištění bezpečnosti informací úměrně k hodnotě aktiv
- Úspora nákladů související s odstraňováním následků bezpečnostních incidentů
- Zvýšení povědomí a odpovědnosti zaměstnanců
- Prokázání úsilí k zajištění ochrany informací zákazníkům, partnerům, nadřízeným orgánům a veřejnosti
- Získání konkurenční výhody
- Zlepšení image společnosti

Naši konzultanti jsou kvalifikovanými experty s mezinárodně uznávanými certifikáty (CISM, CISA, CISSP) a jsou prověřeni pro styk s utajovanými informacemi od stupně utajení Důvěrné až po Přísně tajné. Disponují dlouhodobými zkušenostmi získanými v rámci projektů realizovaných u různých zákazníků státní i soukromé sféry.

[POUŽÍVANÉ STANDARDY]

Při návrhu ISMS pracujeme podle následujících standardů:

- ČSN ISO / IEC 27001, který specifikuje požadavky na to, jak v organizaci správně ustanovit, zavést, monitorovat, udržovat a zlepšovat systém pro řízení bezpečnosti informací.
- ČSN ISO / IEC 27002, jenž poskytuje podrobný přehled konkrétních bezpečnostních opatření, jejichž zavedení musí organizace zvážit při budování ISMS.
- ČSN ISO /IEC 27005, který definuje zásady řízení rizik informační bezpečnosti.

[NEUSTÁLÉ ZLEPŠOVÁNÍ]

Poskytujeme profesionální poradenské služby v celém řetězci kroků, jež řízení bezpečnosti informací obsahuje. V rámci implementace ISMS nastavujeme i procesy zajišťující neustálé zlepšování.

Návrh systému řízení

V této fázi je stanoven rozsah systému řízení bezpečnosti, definována bezpečnostní politika, navržen systém řízení rizik včetně provedení vyhodnocení rizik a jsou vybrána opatření pro snížení rizik.

Zavedení systému řízení

V této fázi jsou zavedena bezpečnostní opatření a definovány procesy a postupy, včetně monitorování jejich účinnosti. Je vytvořen plán kontinuity a postupy reakce na bezpečnostní incidenty.

Ověřování systému řízení

V definovaných intervalech je posuzována funkčnost a efektivita procesů a opatření. Jsou prováděny interní audity, přehodnocována rizika a je přezkoumáván systém řízení bezpečnosti informací.

Nápravná a preventivní opatření

Na základě výsledků předchozí fáze jsou prováděna nápravná a preventivní opatření.

[Nabízené služby]

Skupina ICZ nabízí následující služby související se zavedením a provozem systému řízení bezpečnosti informací.

Analýza

V rámci této skupiny služeb nabízí ICZ zhodnocení stavu řízení bezpečnosti v organizaci a návrh potřebných kroků.

Zavedení/revize systému řízení bezpečnosti

V oblasti systému řízení bezpečnosti nabízí ICZ služby vypracování, resp. revize stávajícího systému řízení bezpečnosti informací v organizaci a provedení, resp. aktualizaci analýzy rizik. Při realizaci nabízené služby budou zohledněny požadavky řady norem ISO/IEC 27000.

Návrh bezpečnostních opatření

V rámci této služby nabízí ICZ na základě zjištěného aktuálního stavu bezpečnostních opatření a výsledků analýzy rizik návrh nových, resp. revizi stávajících bezpečnostních opatření na úrovni celé organizace. Při návrhu bude maximálně vycházet ze stávajícího stavu a bude využívat již existující opatření.

V rámci této služby také nabízí konzultace, případně úpravy dokumentace, související s přechodem na novou verzi normy ISO/IEC 27002.

Implementace bezpečnostních opatření

V této oblasti ICZ nabízí jak služby vlastní implementace opatření (organizačních i technických), tak i konzultační služby v rámci implementace opatření tradičními dodavateli zákazníka.

Jednotlivá opatření mohou nabývat různých forem dle možností a požadavků zákazníka – od čistě organizační formy, přes formu opensource nástrojů, až po komerční enterprise řešení. Zde je ICZ připravena zohlednit možnosti a potřeby zákazníka a nabídnout odpovídající formu opatření.

Podpora

Aby byl zavedený systém řízení bezpečnosti informací funkční, musí být podporován sérií činností a procesů.

V případě, že zákazník nemá dostatek kvalifikovaného personálu, je ICZ připravena nabídnout služby konzultací, školení, outsourcingu vybraných rolí, hodnocení stavu bezpečnosti IS (interní audit IS) a svěřené správy nebo provozní podpory implementovaných technologií.

[PRUŽNOST]

Výše uvedené služby je Skupina ICZ připravena kombinovat podle aktuálních potřeb zákazníka.

OBCHODNÍ KONTAKT

ICZ a.s. Na hřebenech II 1718/10
140 00 Praha 4
TEL.: +420 222 271 111
FAX: +420 222 271 112
EMAIL: marketing@i.cz