ŘÍZENÍ BEZPEČNOSTI INFORMACÍ ISMS

S RŮSTEM STRATEGICKÉHO VÝZNAMU INFORMAČNÍCH SYSTÉMŮ SE JEDNÍM Z KLÍČOVÝCH ÚKOLŮ MANAGEMENTU KAŽDÉ ORGANIZACE STÁVÁ ZAJIŠTĚNÍ BEZPEČNOSTI INFORMACÍ.

Systém řízení bezpečnosti informací (ISMS – Information Security Management System) představuje základní 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 nebo zajistit kontinuitu činností organizace v případě 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 obsahuje i audit bezpečnosti a havarijní plánování. Ke každému zákazníkovi přistupujeme zcela individuálně a pro zavedení systému řízení bezpečnosti informací aplikujeme nejlepší praxi.
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.

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 o ochranu informací zákazníkům, partnerům, nadřízeným orgánům a veřejnosti
- Získání konkurenční výhody
- Zlepšení image společnosti

[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 (zákon č. 82/2018Sb. o kybernetické bezpečnosti a zejména navazující standartizační vyhláška č. 316/2014 Sb. o kybernetické bezpečnosti).

[MODEL PDCA - KONTINUÁLNÍ ZLEPŠOVÁNÍ]

Poskytujeme profesionální poradenské služby v celém řetězci kroků, jež řízení bezpečnosti informací obsahuje. V rámci implementace ISMS nastavujeme i procesy zajišťující kontinuální zlepšování, v této oblasti typicky reprezentované PDCA cyklem

Fáze „Plánuj"

Plánování představuje základ budování systému řízení informační bezpečnosti. V této fázi je stanoven rozsah systému řízení bezpečnosti, definována bezpečnostní politika, navrženo řízení rizik včetně jejich vyhodnocení a jsou vybrána opatření pro snížení rizik.

Fáze „Dělej"

Fáze „Dělej" zahrnuje zavedení a využívání bezpečnostních opatření, procesů a postupů včetně monitorování jejich účinnosti. Její součástí je rovněž vytvoření plánu kontinuity a postupů reakce na bezpečnostní incidenty.

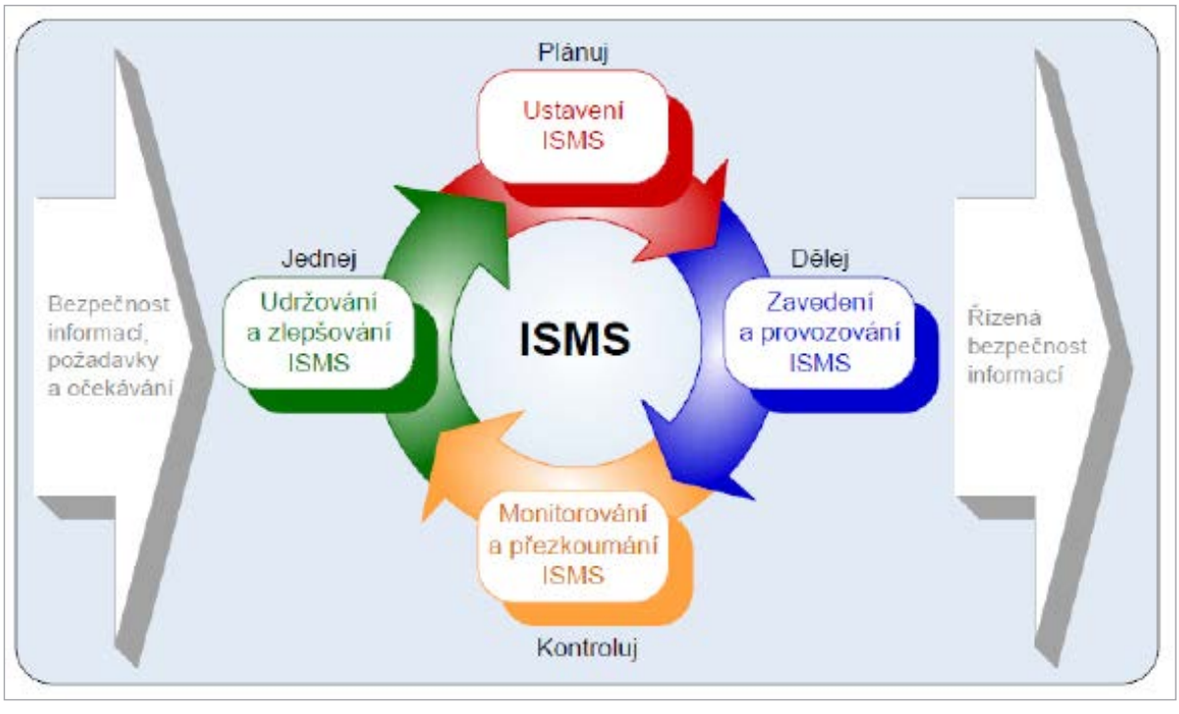
Fáze „Kontroluj"

V této fázi je posouzena funkčnost a efektivita procesů a opatření. Jsou provedeny interní audity, přehodnocena rizika a je přezkoumán systém řízení bezpečnosti informací.

Fáze „Jednej"

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

Schéma modelu PDCA



OBCHODNÍ KONTAKT

ICZ a.s. Na hřebenech II 1718/10
140 00 Praha 4
TEL.: +420 222 271 111
FAX: +420 222 271 112
E-MAIL: marketing@iczgroup.com