RIADENIE BEZPEČNOSTI INFORMÁCIÍ ISMS

S RASTOM STRATEGICKÉHO VÝZNAMU INFORMAČNÝCH SYSTÉMOV SA JEDNOU Z KĽÚČOVÝCH ÚLOH MANAŽMENTU KAŽDEJ ORGANIZÁCIE STÁVA ZAISTENIE BEZPEČNOSTI INFORMÁCIÍ.

Systém riadenia bezpečnosti informácií (ISMS – Information Security Management System) predstavuje základný prístup pre vytvorenie takého prostredia v organizácii, ktoré zaistí potrebnú ochranu informácií pred hrozbami. Zavedenie ISMS zahŕňa návrh a implementáciu procesov vedúcich k riadeniu informačnej bezpečnosti, implementácii potrebných opatrení, kontrole ich efektivity a ich následné neustále udržovanie a zlepšovanie.

[PREČO ZAVÁDZAŤ ISMS]

Zavedenie ISMS je vhodné vtedy, ak je potrebné chrániť dáta zákazníkov či občanov, zdokonaliť zabezpečenie informácií v podniku alebo zaistiť kontinuitu činností organizácie v prípade bezpečnostného incidentu. Dôvodom zavádzania ISMS môže byť aj rozhodnutie efektívnejšie vynakladať prostriedky a smerovať ich do miest s významnými rizikami. V neposlednom rade sa riadením informačnej bezpečnosti musia zaoberať organizácie, ktoré potrebujú vyhovieť legislatívnym a regulačným požiadavkám.

Následnou certifikáciou systému riadenia bezpečnosti informácií môže organizácia preukazovať svojim zákazníkom svoju dôveryhodnosť, získať konkurenčnú výhodu a splniť podmienky účasti v niektorých výberových konaniach.

[PRÍSTUP A SKÚSENOSTI]

Vykonávame nielen návrh procesov pre všetky uvedené fázy, ale taktiež analýzu rizík, návrh bezpečnostnej politiky a ďalšej bezpečnostnej dokumentácie, hodnotenie, projektovanie a implementáciu bezpečnostných opatrení. Naša ponuka obsahuje aj audit bezpečnosti a havarijné plánovanie. Ku každému zákazníkovi pristupujeme maximálne individuálne a na zavedenie systému riadenia bezpečnosti informácií aplikujeme najlepšiu prax.

VLASTNOSTI A VÝHODY

- Vytvorenie prostredia zaisťujúceho informačnú bezpečnosť a ochranu súkromia
- Zníženie rizík súvisiacich s nedostupnosťou, únikom či stratou informácií
- Optimalizácia nákladov na zaistenie bezpečnosti informácií úmerne k hodnote aktív
- Úspora nákladov súvisiaca s odstraňovaním následkov bezpečnostných incidentov
- Zvýšenie povedomia a zodpovednosti zamestnancov
- Preukázanie úsilia o ochranu informácií zákazníkom, partnerom, nadriadeným orgánom a verejnosti
- Získanie konkurenčnej výhody
- Zlepšenie imidžu spoločnosti

Naši konzultanti sú kvalifikovanými expertmi s medzinárodne uznávanými certifikátmi (CISM - Certified Information Security Manager) a sú preverení na styk s utajovanými informáciami od stupňa utajenia Dôverné až po Prísne tajné. Disponujú dlhodobými skúsenosťami získanými v rámci projektov realizovaných u rôznych zákazníkov štátnej aj súkromnej sféry.

[POUŽÍVANÉ ŠTANDARDY]

Pri návrhu ISMS pracujeme podľa nasledujúcich štandardov:

- ČSN ISO/IEC 27001, ktorý špecifikuje požiadavky na to, ako v organizácii správne ustanoviť, zaviesť, monitorovať, udržiavať a zlepšovať systém na riadenie bezpečnosti informácií.
- ČSN ISO/IEC 27002, ktorý poskytuje podrobný prehľad konkrétnych bezpečnostných opatrení, ktorých zavedenie musí organizácia zvážiť pri budovaní ISMS (zákon č. 181/2014 Zb. o kybernetickej bezpečnosti a najmä nadväzujúca štandardizačná vyhláška č. 316/2014 Zb. o kybernetickej bezpečnosti).

[MODEL PDCA]

Poskytujeme profesionálne poradenské služby v celom reťazci krokov, ktoré riadenie bezpečnosti informácií obsahuje. V prípade implementácie ISMS podľa normy ČSN ISO/IEC 27001 postupujeme podľa uvedeného štandardu ISO 27001.

Fáza „Plánuj"

Plánovanie predstavuje základ budovania systému riadenia informačnej bezpečnosti. V tejto fáze je stanovený rozsah systému riadenia bezpečnosti, definovaná bezpečnostná politika, navrhnuté riadenie rizík vrátane ich vyhodnotenia a sú vybraté opatrenia na zníženie rizík.

Fáza „Rob"

Fáza „Rob" zahŕňa zavedenie a využívanie bezpečnostných opatrení, procesov a postupov vrátane monitorovania ich účinnosti. Jej súčasťou je tiež vytvorenie plánu kontinuity a postupov reakcie na bezpečnostné incidenty.

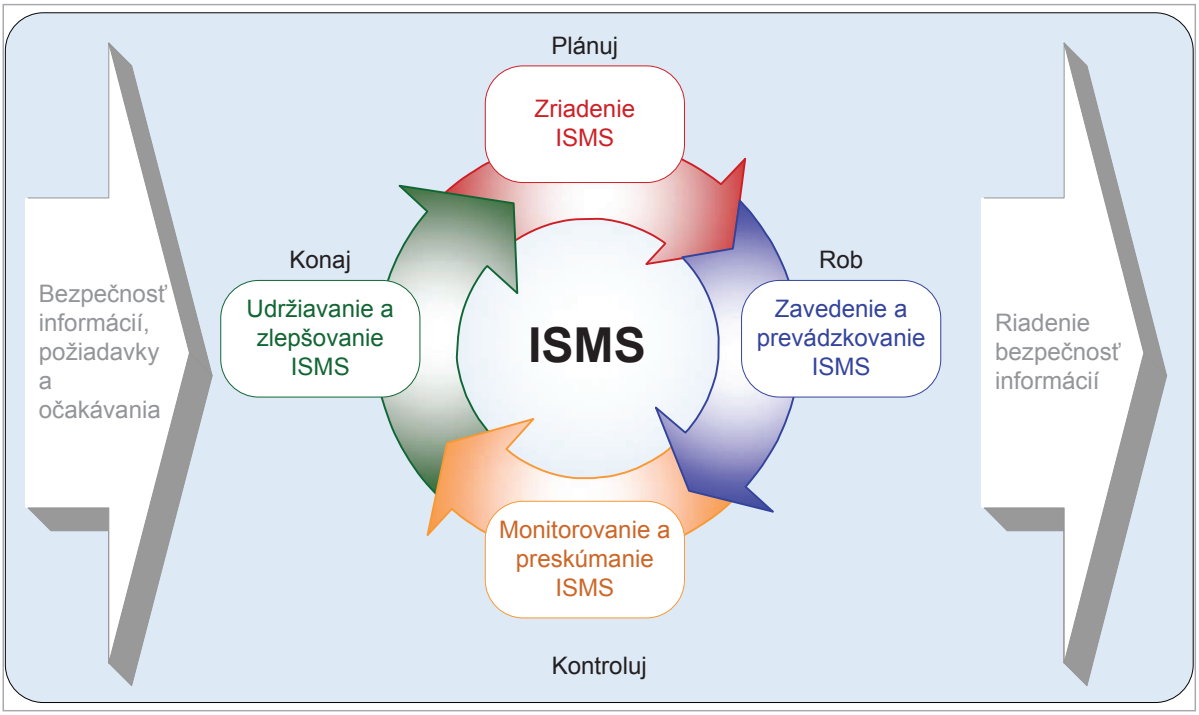
Fáza „Kontroluj"

V tejto fáze je posudzovaná funkčnosť a efektivita procesov a opatrení. Sú vykonané interné audity, prehodnotené riziká a je preskúmaný systém riadenia bezpečnosti informácií.

Fáza „Konaj"

Na základe výsledkov predchádzajúcej fázy sú vykonané nápravné a preventívne opatrenia.

■ Schéma modelu PDCA



OBCHODNÝ 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