Systém řízení informační bezpečnosti

PROČ ŘÍDIT INFORMAČNÍ BEZPEČNOST?

Každá organizace potřebuje pro svoje fungování využívat prostředky – aktiva, ať už jde o informace, informační systémy nebo lidské zdroje. Tato aktiva jsou součástí našeho každodenního světa, který není ideální, a proto jsou i tato aktiva nedokonalá. Obsahují slabiny, které mohou být potenciálně zneužité. Kombinace pravděpodobnosti výskytu negativní události (zneužití slabiny) a jejímu dopadu se nazývá rizikem.

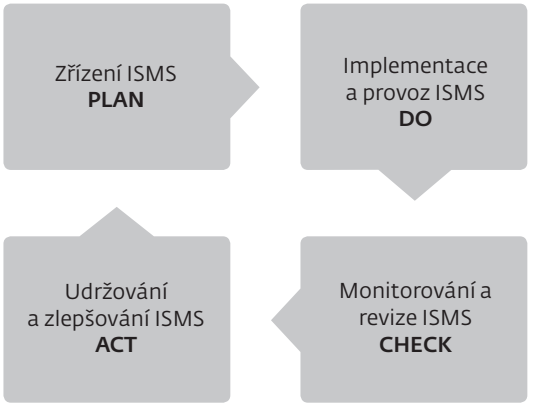
Systém řízení informační bezpečnosti (Information Security Management Systém – ISMS) podle ISO 27000 je založený na řízení rizik. To znamená, že organizace postupně eliminuje rizika v souladu s jejími obchodními potřebami, platnou legislativou a normami, které se zavazují splnit. Doplňkovou výhodou je následné zlepšení firemního prostředí i mimo bezpečnost, například v:

- IT (vypracování inventáře aktiv, zlepšení dostupnosti, zavedení procesů pro reakci na bezpečnostní incidenty a management patchů, ...).
- Oblasti lidských zdrojů (program budování povědomí o informační bezpečnosti).
- Právních vztazích se zaměstnanci a externími subjekty (plnění zákonných požadavků, identifikace služeb, NDA, ...).

Protože většina norem, které se týkají informační bezpečnosti, pokrývá částečně nebo úplně její jednotlivé oblasti, i samotný ISMS se překrývá s některými normami (SOX, SAS 70,...). Takže jestli Vaše organizace potřebuje prokázat soulad s více normami, implementace kompletního ISMS je vhodnou platformou pro spojení jednotlivých norem. Nezanedbatelnou výhodou nasazení systému řízení informační bezpečnosti podle ISO 27000 je možnost certifikace a provázání s ISO 9000.

CO JE SYSTÉM ŘÍZENÍ INFORMAČNÍ BEZPEČNOSTI?

ISMS je součástí celkového systému řízení organizace. Představuje základnu pro řízení bezpečnostních rizik, jejímž cílem je zřídit, implementovat, provozovat, monitorovat, revidovat, udržovat a zlepšovat informační bezpečnost v organizaci (zdroj: ISO/IEC 27001:2005). Podobně jako ostatní systémy řízení definované ISO normami pracuje ISMS v cyklu činností, tzv. PDCA cyklu.



Jednotlivé etapy PDCA cyklu směřují k vybudování efektivního systému řízení informační bezpečnosti:

- Zřízení ISMS / Plan – sepsání politiky a cílů ISMS, procesů a procedur pro řízení rizik a zlepšování informační bezpečnosti tak, aby byly výsledky v souladu s firemní kulturou a obchodními cíli společnosti.
- Implementace a provoz ISMS / Do – implementace politiky ISMS, opatření, procesů a procedur.
- Monitorování a revize ISMS / Check – ohodnocení (pokud možno měřitelné) fungování procesů a předložení reportu managementu organizace.
- Udržování a zlepšování ISMS / Act – přijetí preventivních a nápravných opatření s cílem neustálého zlepšování ISMS.

JAK VÁM MŮŽEME POMOCI?

ESET Services nabízí v rámci ISMS následující služby:

- Implementace ISMS na klíč – pomoc s vypracováním bezpečnostního projektu na zavedení ISMS nebo jen jeho části (např. analýzy rizik, ...). Náplň tohoto programu se liší od organizace k organizaci. Závisí i na rozsahu ISMS a schopnosti zavést některé části vlastními silami. Proto je tato služba na vyžádání. Protože ESET není certifikačním orgánem, případný certifikační audit je zabezpečený externím subjektem.
- Pravidelné konzultace pro CISO (Chief Information Security Officer) – pro zabezpečení optimálního nastavení ISMS nebo implementaci některých bezpečnostních opatření, poskytuje společnost ESET konzultace prostřednictvím vlastních certifikovaných specialistů. Pro Vaše zaměstnance pověřené řízením IT bezpečnosti nabízíme možnost předplatit si zvolený počet konzultačních hodin nebo dní. Ty mohou čerpat kdykoliv v průběhu roku, kdy Vám budou naši konzultanti poskytovat svoje know-how.
- Outsourcing funkce CISO – v případě, že Vaše společnost hledá dedikovaného specialistu pro zavedení ISMS, případně pro řízení bezpečnosti, poskytujeme možnost využít našeho konzultanta jako externího CSO. Ten bude řídit informační bezpečnost ve smyslu normy ISO/IEC 27001:2005, přičemž implementace ISMS není podmínkou.

HLAVNÍ VÝHODY

Implementace ISMS na klíč

- Příprava organizace na ISMS certifikaci nebo pomoc při realizaci některých činností v PDCA cyklu.
- Pomoc při nastavení cílů a výběru vhodných opatření.
- Minimalizování vlastních lidských zdrojů.
- Zaškolení personálu, aby byl po certifikaci připravený převzít řízení informační bezpečnosti.

Pravidelné konzultace pro CSO

- Pomoc v náročnějších činnostech a procesech.
- Nezávislý názor na problematiku.

Outsourcing funkce CSO

- Řízení informační bezpečnosti dle ISO 27000.
- Snižování nákladů společnosti (odpadá potřeba zaměstnat specialistu na řízení bezpečnosti).
- V případě požadavku certifikace.

O ESET Services: Společnost ESET, založena v roce 1992, je světovým výrobcem bezpečnostního softwaru pro domácí i firemní zákazníky. Rozšiřování portfolia služeb vyústilo v roce 2008 do akvizice společnosti Šetrnet, české společnosti s dlouholetými zkušenostmi v oblasti IT a bezpečnosti. V roce 2009 byla vytvořena divize ESET Services, která poskytuje outsourcing bezpečnosti a consulting pro malé a střední podnikatele, ale také pro velké firemní zákazníky. Výhradní zaměření na služby informační bezpečnosti sleduje maximální přínos v této oblasti. Zázemí společnosti ESET, globálně uznávaného dodavatele bezpečnostních řešení a důraz na odbornost pracovníků ESET Services je garancí kvality poskytovaných služeb.