



Redakční otázky k tématu

AUDITY A ISO NORMY

odborného on-line magazínu ICT SECURITY – www.ictsecurity.cz

Nadpis článku:

Na ISMS je třeba nahlížet jako na dlouhodobou investici, která se musí vyplatit.

Autor odpovědí:

Jaroslav Mareček, produktový specialista a auditor ISMS, COMGUARD a.s.

1) Jak správně a přesně vyčíslit přínosy auditů a zavádění norem ISO?

Zavedení a udržování certifikovaného ISMS dle ISO 27001 může mít podle našich zkušeností různé efekty. Je to konkurenční výhoda uplatnitelná v rámci výběrových řízení (např. na outsourcing správy) i image posilující záležitost. Zásadní oblastí je eliminace ztrát vyplývajících z bezpečnostních incidentů, kterým předchází systematizované řízení bezpečnostních rizik (např. ne/dostupnost e-shopu). ISMS může pomoci zamezit pokutám, které vyplývají z prohřešků vůči legislativě (např. ochrana důvěrných informací) či z neshody s oborovými normami (např. PCI DSS). Navíc organizace získá morální právo pro vyžadování stejného přístupu i u svých partnerů. To všechno by neměl být problém pro jakoukoli organizaci kvantifikovat a tedy vyčíslit přínosy auditů a zavádění norem ISO. Důležité je, že tyto přínosy musí v dlouhodobém horizontu převýšit náklady spojené s ISMS, jinak nebude mít reálnou podporu top managementu, která je alfou a omegou jeho fungování. ISMS = investice.

2) S jak velkou pracovní i časovou náročností je nutné při zavádění ISO norem počítat?

Obvykle se jedná o měsíce. Náročnost časovou i pracovní výrazně eliminuje reálná podpora vedení společnosti a existence funkce bezpečnostního manažera v organizaci.

3) Jak obtížné je nasadit ISO normy do prostředí, která s nimi zatím nemají zkušenosti?

Obvyklým postupem je navázání na stávající systém řízení jakosti dle ISO 9001 (QMS), což velmi usnadňuje zavádění ISMS, např. díky existujícímu systému řízení dokumentů apod. Logika ISO norem je v mnohém velmi podobná, proto si myslím, že pokud ISMS nepředchází QMS, je zavedení ISMS 2x tak náročné.

4) Jak výrazný posun v kvalitě bezpečnosti představuje certifikace dle CSN ISO/IEC 27001? Pro koho je vhodná?

ISO 27001 je normou typu „best practices“, jejíž zavedení (+ certifikace ISMS) samo o sobě nic neřeší, pokud systém není skutečně používán a vynucován :-). Je jedním z nejvhodnějších návodů na to, jak dobře řídit bezpečnost informací a na nic při tom nezapomenout. Vhodná je pro všechny organizace, kterým přinese



adekvátní efekt (viz otázka č. 1). Konkrétnější odpověď snad ani není možná, každá organizace si to musí umět spočítat sama.

5) Lze smysluplný audit provést i s interními zdroji, nebo je za každých okolností kvůli „provozní slepotě“ využívat externích služeb?

Na základě našich zkušeností doporučujeme i pro interní audity externí auditory. Konfrontace názorů vlastních zaměstnanců s experty z konzultantských firem vdechuje celému systému život a udržuje ho v reálných mantinelech.