Harmonogram prvního týdne ISM aneb pět pracovních dnů na počátku života firemního ISMS

Poznámka úvodem: Místo ISM bude v dalším textu použita zkratka CRP (Common Responsible Person), tedy společná odpovědná osoba – a té je určen následující text jako jednoduchý doplněk postupu pro vytvoření příručky systému řízení informační bezpečnosti.

Den první: Nastavení & pravomoci

Než se pustíte do jakékoliv technické práce, buďte si jisti pevnými základy.

- **Sejděte se s odpovědným vedoucím (AM)**: a ujistěte se, že máte jeho podporu – bez podpory top managementu nebude ISMS fungovat. Případně nechť AM rovnou podepíše prohlášení o bezpečnosti nebo politiku informační bezpečnosti.
- **Ponořte se do předpisů**: Projděte si **IS.I.OR.200** (Systém řízení) pro pochopení právních závazků vyššího vedení.
- **Určete složku**: Vytvořte bezpečnou centrální „knihovnu ISMS“ (v souladu s firemními zvyklostmi například na sdíleném disku anebo skutečné desky s pořadači v polici), kde budou žít potřebné dokumenty.

Den druhý: Lov v šedé zóně IT (Odhalení aktiv)

Nemůžete chránit to, o čem nemáte tušení, že existuje.

- **Projděte se firmou**: Promluvte si s piloty a mechaniky a hlavně se ptejte: „*Jaký software nebo aplikace skutečně využíváte při své práci?*“ **Pokuste se** především **najít zejména „skrytá“ aktiva**: Například ověřte, zda se jako EFB používají soukromé tablety, nebo zda se plánuje v soukromých skupinách na WhatsAppu, nebo se údržba sleduje pomocí excelových tabulek, které nejsou na oficiálním serveru atp.
- **Otevřete seznam aktiv**: Je čas zaplnit první sloupec **Registru rizik**.

Den třetí: Bezpečnostní souvislosti (Zhodnocení míry rizik)

Part IS se týká výhradně **bezpečnosti letectví**.

- **Cvičení „Co kdyby“**: Pro všechna aktiva, nalezená předchozího dne, si položte otázku: „*Pokud tento software/aplikaci vymažu, anebo pokud mi od zítra bude dávat špatné informace, může být let nebezpečný (nebo ovlivní to řízení letové způsobilosti)?*“
- **Protřiďte výsledky**: Jestliže je odpověď „Ne“ (například firemní marketingové „webovky“), přesuňte aktivum na seznam s nižší prioritou. Pokud je odpověď „Ano“ (např. EFB nebo CAMO software), jde o **kritické aktivum**.

Den čtvrtý: Čas na podání rukou

Zejména malé organizace silně závisejí na externích dodavatelích.

- **Identifikujte klíčové partnery**: Sestavte seznam poskytovatelů IT služeb, prodejců software pro plánování letů (Jeppesen, ForeFlight…) anebo software pro řízení údržby.
- **Prověřte smlouvy**: Obsahují bezpečnostní doložku? Máte u dodavatelů kontaktní osobu, které můžete volat, pokud jsou „hacknuti“ *oni*?
- **Sestavte seznam dodavatelů**: Bude obsahovat čísla na nouzovou podporu pro plán reakce na incident.

Den pátý: Rychlé výsledky & Analýza slabých míst

Skončete týden s jasnou představou, co se bude dít dál.

- **Kontrola vícefaktorového ověřování (MFA)**: Mají všichni MFA na svých e-mailových adresách? Pokud ne, nechť je toto v příštím týdnu vaše priorita č. 1. Je to nejlevnější a nejefektivnější bezpečnostní opatření, jaké můžete udělat.
- **Naplánujte první briefing**: Stanovte datum pro 15minutovou schůzku všech, na které představíte formulář hlášení.
- **Harmonogram**: Vytvořte jednoduchý časový plán na 3 měsíce na dokončení Příručky a Prohlášení o použitelnosti.

Pro-tipy pro CRP

Nesnažte se být IT géniem, buďte raději **bezpečnostním detektivem**. Vaším úkolem je zajistit, že digitální nástroje používané vaší firmou budou dostatečně důvěryhodné na to, aby udržely letadlo ve vzduchu (nebo abyste zachovali jeho letovou způsobilost).