



MANAGEMENT / AKČNÍ PLÁN

Bezpečnostní plán na 90 dní

Výchozí model pro firmu, která potřebuje uspořádat první kroky. Harmonogram přizpůsobte dopadu rizik a dostupné kapacitě.

Dny 1-15 / Zjistit stav

Vyberte důležité služby, odpovědné lidi a dostupné podklady. Oddělte prokázaná zjištění od domněnek. Zaznamenejte naléhavé problémy, které nemohou čekat.

Dny 16-30 / Rozhodnout

Proberte s vedením dopady a varianty. Vyberte omezený počet priorit, přiřadte vlastníky, zdroje a způsob ověření. Každý úkol musí být dostatečně konkrétní pro předání.

Dny 31-60 / Zavést opatření

Sledujte provedení, závislosti a blokace. Změny plánujte s provozem a IT. U nového pravidla určete, koho se týká a jak se o něm dozví.

Dny 61-90 / Ověřit a upravit

Zkontrolujte důkazy dokončení, otevřené výjimky a potřebu opakovaných testů. Shrňte, co se zlepšilo, co není ověřeno a o čem musí vedení rozhodnout.

Rytmus řízení / Udržet odpovědnost

Na krátké pravidelné poradě projděte nejdůležitější úkoly a změny. Nehodnoťte pokrok jen počtem uzavřených položek; ptejte se na skutečný dopad do provozu.



PRACOVNÍ LIST

Jednostránkový plán pro vedení

Vyplňte pro vlastní firmu. Do veřejných formulářů neposílejte citlivé údaje ani přístupové informace.

Cíl programu / garant / období	
První tři priority / vlastníci	
Potřebné kapacity a rozhodnutí	
Důkaz dokončení každé priority	
Termíny kontrol / otevřené výjimky	

Otázky před uzavřením

Co se musí změnit pro zákazníka nebo provoz?

Kdo rozhodne, když opatření narazí na termín nebo rozpočet?

Udržujte plán v praxi prostřednictvím Active Defense.

<https://www.cybersafety.cz/active-defense/>

Autor pracovního materiálu: CyberSafety. Vlastní otázky a šablony pro interní práci. Rozsah přizpůsobte organizaci; nejde o potvrzení souladu s předpisy.