Specifikace postupů vytvoření recovery plánů/plánů obnovy

Požadavky na vytvoření plánů obnovy

Úvodní analýza

Pro vytvoření kvalitních plánů obnovy předpokládáme vytvoření úvodní analýzy. Součástí této analýzy bude:

- Zhodnocení stávající analýzy rizik
- Validace kritických aktiv
- Analýza IT infrastruktury
- Vydefinování potřebných scénářů pro finální tvorbu plánů obnovy

Obecný incident response

Předmětem je dodání dokumentovaného procesu incident response. Proces bude reflektovat best-practise v této oblasti za účelem zajištění rychlé identifikace narušení bezpečnosti dat nebo kybernetického útoku, minimalizace jeho následků, omezení škod a odstranění příčin, aby se snížilo riziko budoucích incidentů. Součástí incident response procesu budou zejména RACI matice povinností a odpovědností všech zaměstnanců, řešitelů incidentů, IT oddělení, manažerů bezpečnosti a vrcholového vedení organizace. Incident response bude obsahovat i komunikační matici pro případ eskalace a řešení incidentů. Součástí incident response procesu bude i workflow pro řešení incidentů pokrývající oblasti identifikace incidentu, stanovení dopadů, řešení incidentu a reporting.

Strategie obnovy infrastruktury

Předmětem bude dodání dokumentu Strategie obnovy. Jedná se o dokument, který bude pokrývat strategii obnovy a obnovení kritických funkcí IT infrastruktury po výskytu události nebo incidentu.

Součástí strategie obnovy musí být:

- zohlednění posouzení rizik pro tvorbu, vznik a revizi plánů obnovy,
- metodika stanovení cílů obnovy systému po výskytu události nebo incidentu,
- pravidla a postupy zálohování IT infrastruktury,
- pravidla aktivace plánů obnovy plánů.

Součástí strategie obnovy bude dále specifikace rolí, odpovědností a pravomocí v rámci aktivace plánů obnovy a řešení incidentů. Strategie obnovy bude obsahovat i pravidla pro neustálé zlepšování strategie obnovy.

Detailní plány obnovy infrastruktury

Předmětem je dodání plánů obnovy IT infrastruktury v počtu maximálně 7 plánů. Každý plán obnovy bude obsahovat následující strukturu:

- Popis cílů plánu obnovy
- Seznam kontaktů na klíčové osoby včetně externích pracovníků
- Komunikační matice klíčových osob a eskalační procedury
- Seznam triggerů – událostí, které vedou ke spuštění plánu obnovy
- Aktivace týmů pro řešení plánu obnovy
- Detailní identifikace aktiv IT infrastruktury pro kterou je plán obnovy relevantní
    - Identifikace IT infrastruktury, které se plán obnovy týká

    - Seznam IT aktiv
    - Klíčové kontakty – výrobce, uživatelé, administrátoři
- Detailní postup kroků v případě aktivace plánu obnovy
- Záznam vykonaných činností
- Požadavky na zpětné vyhodnocení účinnosti a efektivnosti plánu obnovy po vyřešení incidentu