Výstupní audit kybernetické bezpečnosti – specifikace činností a podmínek

Výstupní audit kybernetické bezpečnosti (dále jen „audit“) představuje nezávislé a objektivní posouzení kybernetického zabezpečení organizace. Cílem auditu je identifikace slabých míst v infrastruktuře a ověření shody nastavených opatření s aktuálně platnou legislativou v oblasti kybernetické bezpečnosti a s požadavky poskytovatele dotace na projekt „Rozvoj kybernetické bezpečnosti města Trutnova“, registrační číslo projektu CZ.31.2.0/0.0/0.0/23_093/0008360.

1. Metodika a legislativní rámec

Audit je realizován v souladu s následujícími předpisy a normami:

- **Zákon č. 264/2025 Sb.**, o kybernetické bezpečnosti.
- **Vyhláška č. 410/2025 Sb.**, o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.
- **Směrnice NIS2** a **ENISA ECSF** (European Cybersecurity Skills Framework).
- Standardy řady **ISO/IEC 27000**.

2. Rozsah auditu

Předmětem auditu jsou následující oblasti:

- **Síťová infrastruktura:** Zabezpečení perimetru (firewall), kontrola zabezpečení vnitřní sítě, kontrola segmentace a zabezpečení bezdrátových sítí.
- **Koncová zařízení a servery:** Bezpečnost operačních systémů a nastavení antivirové ochrany.
- **Identita a přístup:** Zabezpečení doménové infrastruktury, správa administrátorských účtů a politika hesel.
- **Záloha dat a kontinuita činnosti:** Kontrola nastavení záloh, kontrola zabezpečení souborů záloh a ověření dostupnosti služeb.
- **Komunikace a logování:** Zabezpečení elektronické pošty a kontrola nastavení logování bezpečnostních událostí.
- **Fyzická a organizační bezpečnost:** Fyzická bezpečnost IT infrastruktury a úroveň školení kybernetické bezpečnosti.

3. Požadavky na součinnost objednatele

- přístup (dálkový, případně i fyzický, a to výhradně v pracovní době městského úřadu a po předchozí domluvě),
- nepřímé zapojení (zodpovídání dotazů).

4. Povinnosti dodavatele

- dodavatel je povinen zahájit svoji činnost k obstání díla bez zbytečného odkladu po dni vystavení objednávky,

- dodavatel je při provádění díla povinen postupovat pečlivě, dle svých nejlepších znalostí a schopností, přičemž je při své činnosti povinen sledovat a chránit oprávněné zájmy objednatele, postupovat v souladu s jeho pokyny a dle platných dotačních pravidel pro výzvu č.41 NPO (výzva č. 41 - Kybernetická bezpečnost - obce),
- dodavatel je povinen zajistit utajení důvěrných informací získaných při plnění objednávky způsobem obvyklým pro utajování takových informací, není-li výslovně sjednáno jinak; tato povinnost platí bez ohledu na ukončení účinnosti objednávky, tj. předání díla,
- dodavatel se výslovně zavazuje chránit a zachovávat mlčenlivost o všech datech získaných nebo přístupných v informačním systému objednatele nebo i jinak, zejména o osobních údajích (ve smyslu NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)) a utajovaných skutečnostech podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů; dodavatel se zavazuje takové informace nezneužít ve svůj prospěch nebo ve prospěch jiného.

5. Výstupy auditu

Proces je zakončen předáním auditní zprávy v elektronické podobě v PDF a na žádost objednatele i 1x v tištěné podobě.