ELEKTRONICKÁ KOMUNIKACE A KYBERBEZPEČNOST

Odpovědný člen rady kraje	Radní pro resort ekonomiky, majetku, investic, veřejných zakázek a informatiky
Garant	Ředitel krajského úřadu

Prioritní oblast	VEŘEJNÁ SPRÁVA
Vazba na strategický a specifický cíl Koncepce	ZRYCHLIT / UŠETŘIT
Vazba na specifický cíl Koncepce	1.4 ZKRÁCENÍ ČASU PRO ADMINISTRATIVNÍ PROCESY A ÚSPORA NÁKLADŮ DÍKY DIGITALIZACI V RÁMCI ÚŘADU
	1.5 ZKRÁCENÍ DOBY PRO NALEZENÍ POTŘEBNÝCH INFORMACÍ PRO RYCHLEJŠÍ KOMUNIKACI UŽIVATELŮ A ÚŘADU
	3.2 ZVÝŠENÍ PROCENTA VEŘEJNÝCH SLUŽEB A OTEVŘENÝCH DAT, KTERÉ MOHOU ZÍSKAT OBČANÉ PROSTŘEDNICTVÍM WEBU MOBILNÍHO TELEFONU

VIZE

- Bezpapírový úřad.
- Zkvalitnění interních administrativních procesů při zpracování a vyhledávání informací.
- Zjednodušení a zpřístupnění komunikačních možností veřejnosti s úřadem / rozšíření nabídky elektronických služeb pro otevřenost občanům.
- Snížení rizik a minimalizace negativních dopadů útoků, hrozeb a neočekávaných incidentů u významných informačních systémů.

STRUČNÝ POPIS SOUČASNÉHO STAVU A ZDŮVODNĚNÍ

Práce s dokumenty v papírové podobě se stává u mnoha agend zátěží, která se projevuje finančně, časově i v organizaci práce. Krajský úřad denně zpracovává množství informací, které sám vytváří nebo mu jsou doručeny. Nejenže roste počet dokumentů, zároveň rostou požadavky na jejich evidenci a na následné operace s nimi.

Interní procesy krajského úřadu jsou zpracovávány v rozdílných informačních systémech. Část procesů je elektronizována plně, jiná část procesů je digitalizována pouze částečně v určité fázi životního cyklu dokumentu a jsou zde i procesy, které jsou zatím stále řešeny pouze papírovou formou.

Komunikace mezi občany a krajským úřadem lze vést elektronicky, nicméně občan nemá přehled o stupni nebo stavu vyřízení své záležitosti uvnitř úřadu.

Na výše uvedené navazuje i potřeba kontinuální, adekvátní kybernetické ochrany úřadu, agend a vzdělávání v této oblasti. Byť je tato oblast průběžně řešena – vzdělávací kurzy NÚKIB nebo prověřování souladu kybernetické ochrany s legislativními požadavky, je třeba se jí i nadále věnovat s odpovídající vážností a kapacitou.

AKTIVITY

1/ Elektronická komunikace v rámci úřadu
Základní oblastí aktivit je kontinuální sledování jednotlivých agend úřadu a vyhodnocování potenciálu jejich digitalizace a vzájemné provázanosti – tam kde je to účelné. Je účelné sjednotit evidenční systémy, pokud je to možné vzájemně je provázat a zajistit přístupy jednotlivých pracovníků k potřebným informacím. Předmětem aktivit je zavést: - Elektronickou evidenci v rámci jednotlivých agend. - Předávání výstupů v elektronické formě. - Vzájemné provázání informačních systémů.
Příklady konkrétních projektů
- Zprovoznění upomínkového systému procesů vyřizování žádostí o poskytnutí informací, požadavků na vyjádření ze strany krajského úřadu a podobně. - Elektronické platební poukazy pro platbu faktur. - Digitalizace vnitřní úpravy rozpočtu

2/ Elektronická komunikace úřadu s obyvateli a institucemi

Tato oblast úzce navazuje na oblast předchozí – elektronická komunikace s obyvateli a institucemi může navazovat zejména na úspěšnou digitalizaci agend uvnitř úřadu. Elektronizace veřejné a státní správy neboli eGovernment má veřejnosti usnadnit styk s úřady a zajistit efektivnější fungovaní úřadu. eGovernment má tak lidem zjednodušit komunikaci s úřady bez nutnosti fyzické návštěvy.
Na straně úřadu elektronická komunikace formalizovanými kanály usnadňuje zaevidování daných podání a možnost sledování průběhu jejich vyřízení. Snižuje se tak riziko administrativní chybovosti.

Příklady konkrétních projektů

- Zajištění online sledování podaných dokumentů a žádostí na Liberecký kraj vč. automatických odpovědí jako potvrzení přijetí dokumentu či žádosti úřadem.
- Připojování příspěvkových organizací a obcí Libereckého kraje ke spisové službě
- Spuštění objednávkových systémů pro sjednání času schůzky a vyřízení záležitostí na úřadě.
- Vytvoření platebního portálu / elektronický systém pro snadnou platbu za poplatky a služby.

3/ Zajišťování kybernetické bezpečnosti

Vedle zajištění co nejširšího nasazení automatizace a elektronizace je potřeba zohlednit rizika kyberútoků a ztráty dat. Krajský úřad zajišťuje kyberbezpečnost na základě předpisů a legislativy, nicméně vzhledem ke zvyšujícím se rizikům by měla být tato agenda vždy o krok napřed – kontinuální proces zhodnocení rizika týkající se dat a informací v elektronické podobě a zajišťování zvýšené kyberbezpečnosti na úroveň, která bude umět předcházet i náročnějším útokům a omylům a chránit veškerá data zpracovávaná krajským úřadem. K tomu je nezbytné zajistit plnění cílů systému řízení bezpečnosti informací a poskytnutí potřebných zdrojů personálních, finančních i technických. Kybernetická bezpečnost musí být začleněna též do metodik řízení projektů.
Řešení kybernetické bezpečnosti je důležité jak v rámci samotného krajského úřadu, tak i v jednotlivých krajských organizacích.

Příklady konkrétních projektů

- Průběžné zvyšování povědomí zaměstnanců o rizicích a zásadách bezpečného chování v souvislosti s rozšiřováním elektronických agend, aplikací, dat apod. a v souvislosti s vývojem, četností a charakterem útoků.
- Průběžné prověřování úrovně a stavu zabezpečení v souvislosti s vývojem hrozeb.
- Průběžné zavádění vyšších standardů bezpečnostních opatření.
- Projektové řešení zvýšení kybernetické bezpečnosti významných informačních systémů a informačních systémů v prostředí krajského úřadu zavedením nových funkcionalit HW a SW prvků provozní infrastruktury kraje zejména v oblasti kontroly provozu informačních technologií a datové komunikace včetně detekce nestandardních stavů a útoků

PARTNERSTVÍ A SPOLUPRÁCE

- Vzdělávací instituce (Juniorní centrum kybernetické bezpečnosti, SŠ, TUL)
- Města a obce
- Organizace zřizované městy a obcemi (školy, spolky)
- Příspěvkové organizace LK
- NÚKIB

INDIKÁTORY

- Počet nově digitalizovaných procesů krajského úřadu.
- Počet činností krajského úřadu, kde je nastaveno online sledování.
- Počet organizací nově připojených ke spisové službě.
- Počet vzdělávacích akcí pro zaměstnance ke zvýšení kybernetické bezpečnosti.
- Počet subjektů zapojených do komunikace s veřejností prostřednictvím Platebního portálu.