Výbor pro digitalizaci, IT a Otevřený kraj
Zastupitelstva Plzeňského kraje

Číslo zasedání	17
Datum konání	13. 3. 2024 – 15.30 hod.
Místo konání	KÚPK, zasedací místnost č. 143
Zapisovatel	Aneta Vaňousová

Prezence

Přítomni	předseda: JUDr. Milan Chaloupka, MBA, LL.M. členové: Ing. Martin Barták, MBA Mgr. Karel Filipčík Lucie Pernglau David Soukup Pavel Šrámek Milan Brož Martin Dittrich Ing. Jan Štěpán Ing. Vlastimil Hebr
Nepřítomni	Jiří Novák
Hosté	**Mgr. Matyáš Kubík** – vedoucí právního oddělení, CNPK, p. o. **Doc. RNDr. Milan Berka, CSc.** – bezpečnostní manažer

Program

1. Zahájení
2. Formální náležitosti (schválení programu, volba ověřovatele zápisu)
3. **Mgr. Matyáš Kubík** – vedoucí právního oddělení, CNPK, p. o.
   Téma: Meet the buyer2024“

   Doc. RNDr. Milan Berka, CSc. – bezpečnostní manažer
   Téma: „informace k novele Zákona o kybernetické bezpečnosti a jeho implementace“
4. Různé, diskuse
5. Závěr

Zápis z jednání

Číslo	Text
1	**Zahájení** Předseda výboru, JUDr. Milan Chaloupka, MBA, LL.M., přivítal přítomné členy vč. hostů a zahájil 17. zasedání Výboru pro digitalizaci, IT a Otevřený kraj ZPK.
2	**Formální náležitosti** a) výbor byl usnášeníschopný (9/11) b) program jednání byl jednomyslně schválen (9/11) c) ověřovatelem zápisu byl zvolen pan Ing. Martin Barták (9/11)
3	**Mgr. Matyáš Kubík** – vedoucí právního oddělení, CNPK, p. o. Téma: „Meet the buyer 2024“ V úvodu své prezentace, po krátkém představení, informoval Mgr. Kubík o průběhu akce: Centrální nákup představil plán VZ na r. 2024. Ředitelka CNPK Mgr. et. Bc. Jana Dubcová hovořila o spolupráci s MMR v rámci podpory rozvoje veřejného zadávání a sdílela obecné informace k novele ZZVZ, DNS. Následně zmínila Videonávod – jak podat nabídku v E-ZAK.

	Stavební VZ přednesl vedoucí odboru investic a majetku JUDr. Michal Bouřa, VZ z oblasti zdravotnictví – Zdeněk Švanda, předseda představenstev nemocnic PK a VZ z oblasti dopravy náměstek hejtmana pro oblast dopravy pan Pavel Čížek. Plán všech VZ pro rok 2024 na stránkách CNPK. Přítomna byla i média - ZAK TV - reportáž, Česká tisková kancelář (ČTK), Český rozhlas. Kapacita sálu naplněna – 90 účastníků z řad zástupců dodavatelů, stavební firmy, dodavatelé zdravotnických přístrojů a dodavatelé centrálně soutěžených komodit. K dispozici bude videozáznam na YouTube pro dodavatele, jejichž účast byla z kapacitních důvodů odmítnuta. Dále bude záznam z akce k dispozici na webu CNPK a LinkedIn účtu CNPK. P. Kubík hodnotil za Centrální nákup akci kladně. Dle jeho slov splnila očekávání dodavatelů, kteří sami preferují MTB formou osobního setkání před online formou, akci považují za jedinečnou svého druhu, a slibují svou účast na akci i v nadcházejících letech. Většina zúčastněných dodavatelů se hlásí do VZ a polovina z nich projevila zájem o školení CNPK pro dodavatele. Předseda výboru JUDr. Chaloupka vznesl dotaz ohledně možnosti využití větších prostor ke konání nadcházejících ročníků? Mgr. Kubík odpověděl, že vzhledem k plné kapacitě jistě.
	Doc. RNDr. Milan Berka CSc. – bezpečnostní manažer <u>Téma:</u> „Informace k novele Zákona o kybernetické bezpečnosti a jeho implementace“ Doc. Berka v úvodu podal informaci k historii vývoje bezpečnosti informací: Důležité jsou především normy a jejich implementace z let 2004 - 2005 : - BS 7799 rok 2002 Systém řízení bezpečnosti informací - ISO 17799 rok 2005 - ISO 27 000 rok 2009 - Systém řízení bezpečnosti informací (Information Security Management System - ISMS) - ISO/IEC 27001 – Systémy řízení bezpečnosti informací – Požadavky, - ISO/IEC 27002 – Soubor postupů pro opatření bezpečnosti informací, - ISO/IEC 27003 – Směrnice pro implementaci ISMS, - ISO/IEC 27004 – Řízení bezpečnosti informací – Měření,

- ISO/IEC 27005 – Řízení rizik bezpečnosti informací,
- ISO/IEC 27014 – Správa a řízení bezpečnosti informací,
- ISO/IEC 27031 – Havarijní plánování a kontinuita,
- ISO/IEC 27035 – Řízení incidentů bezpečnosti informací, aj.

Doc. Berka zmiňuje, že přesnější definice jsou v anglických verzích jednotlivých norem.

Dále uvádí další předpisy:

- Evropské směrnice eIDAS, NIS, …
- Další normy ISO – 9 000, 20 000, 15 408 a další
- Evropské normy - ETSI 419 211, 303 645 a další – odkazují se na ISO normy.
- Relevantní zákony a vyhlášky
- Zákon č. 181/2014 Sb. O kybernetické Bezpečnosti
- Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních kybernetických bezpečnostních incidentů.
- 315, 316 z r. 2021 – Clouodové služby

V rámci PK – CamelNET. Dále informuje že CNPK nespadá pod zákon – VZ. Krizové řízení – součástí portálu PK.

Povinné osoby:

- Poskytovatelé služeb elektronických komunikací a subjekty zajišťující síť elektronických komunikací
- Významné sítě
- Kritická informační infrastruktura (KII)
- Významné informační systémy (VIS)
- Provozovatelé základních služeb (PZS)
- Poskytovatelé digitálních služeb
- Orgán veřejné moci využívající služeb poskytovatelů cloud computingu (Vyhláška č. 315 a 316/2021 Sb. - ISO 27018)

Oblastmi základních služeb jsou: energetika, doprava, bankovnictví, infrastruktura finančních trhů, zdravotnictví, vodní hospodářství, digitální struktura a chemický průmysl.

Povinnými osobami dle nového zákona jsou střední nebo velké podniky popřípadě výhradní poskytovatel níže uvedených služeb ve členském státě EU.

Oblastmi jednotlivých služeb jsou: doprava, finance, zdravotnictví, vodárenství, poskytování digitálních služeb (elektronické komunikace, cloud computingové služby, datová centra, on-line tržiště, sociální sítě, vyhledávače),

doručování zásilek, nakládání s odpady, výroba a distribuce chemických látek, výroba a distribuce potravin, výroba zdravotnických prostředků, počítačů, strojů, elektrických zařízení či dopravních prostředků či výzkumu.

15:56 – příchod – p. Šrámek

V další části prezentace informoval Doc. Berka o zkušenostech z KÚPK:

- analýza rizik před BP
- vysvětlení pojmů (Integrita, Důvěrnost a dostupnost informací)
- personální zabezpečení – v praxi obecně formou testování informovanosti
- fyzická bezpečnost – bezpečnost prostředí – znemožnění přístupu nepovolaných osob k jednotlivým zařízením, zdrojům a aktivům.
- bezpečnost a správa komunikace a procesů (správa komunikace procesů a řízení přístupu).
- antivirová ochrana (nejzranitelnější jsou systémy na bázi MS Windows).
- zabezpečení médií (evidence, dodržování sdílení interních dokumentů, skartace a evidence pohybu dokumentu).
- šifrování a elektronická podpis (správa podpisů – pouze proškolení operátoři (platnost 1 rok). Žádosti o prodloužení certifikátů – Helpdesk).
- identifikace a autentizace uživatele (Průkazem zaměstnance a vizuální kontrolou, elektronickým podpisem uživatele (Digitálním certifikátem), čipovou kartou – bezpečnostním předmětem QSCD, digitálním certifikátem aplikace, názvem účtu a heslem (3 měsíční platnost hesla a pravidla k jeho tvorbě jsou problémem).

  Dle názoru Doc. Berky je lepší variantou náhodně generované heslo nebo biometrická či certifikovaná forma.

- vzdálený přístup – nutnost zažádat přes Helpdesk
- bezpečnostní událost a incident – informaci možno předat prostřednictvím Helpdesku (IT), e-mailem nebo telefonicky takovou formou aby byla využita služba, která není předmětem daného incidentu.

Následně informuje o možné dotaci na kybernetickou bezpečnost:

- podání žádosti od 30. 4. 2024
- NPO – výzvy č. 40 – 43: Kybernetická bezpečnost pro kraje, obce, OSS a zdravotnická zařízení
- ukončení realizace: 31. 12. 2025,
- maximální uznatelné výdaje: 50 mil. Kč (na 1 žádost),
- dotace: 100 % (bez DPH),
- způsobilý uchazeč: poskytovatel zdravotní péče podle zákona (veřejný vždy, soukromý, pokud má uzavřenu smlouvu o SOHZ), případně zřizovatel. Obce, kraje, OSS + SPO.

	Podporované aktivity: - Služby v oblasti bezpečnostního auditu a ISMS. - Dostupnost a bezpečnost dat – servery, disková pole. - Bezpečnost sítí – firewall, segmentace, moderní wi-fi 7. - Nástroj pro ověřování identity uživatelů a řízení přístupových oprávnění. - Antivirová ochrana - Certifikované audity – cca 100 tis. (provádí se po 3 letech) - Interní audity – každý rok Pro firmy: - výzva průběžná s alokací 0,5 mld. Kč, - dotace: 30 % - 40 %, - způsobilý žadatel: malé a střední podniky, celá ČR (mimo Prahu), - dotace 250 tis. až 200 tis. EUR v režimu de minimis Z dotace lze podpořit níže uvedené projekty: - Provozní, vnitropodnikové IS (ERP, CRM, MIS, BI…). - Logistické a skladové technologie (robotická přeprava zboží v areálu) a návazné - SW. - Vnitropodniková konektivita (aktivní a pasivní prvky sítě, nezbytná měřicí technika - a instalační materiál) a zajištění distančního přístupu zaměstnanců. - Kybernetická bezpečnost - Jednorázová školení zakončena certifikací - BIM a CDE systémy pro vytváření digitálních modelů ve stavebnictví a příbuzných - oborů. - Vytvoření digitálního dvojčete či obdobné studie, která by verifikovala uskutečnění procesu digitální transformace. Předseda výboru JUDr. Chaloupka se dotazoval na možné sankce za nedodržení NIS 2? Doc. Berka uvedl, že sankce jsou likvidační. V rámci implementace daného zákona je ještě rok či více. Je zde možnost kurzů pro firmy zajišťující správu. V případě nedodržení výše uvedeného přijde dotčenému subjektu nejprve upozornění a následná výzva k nápravě až poté by se řešila možná sankce.
4	**Diskuse, různé** Do diskuse se nikdo nepřihlásil.

5	**Závěr** Pan předseda poděkoval všem přítomným za účast, připomněl termín dalšího zasedání (tj. 15. května) a jednání v 16: 24 hod. ukončil.

Zápis byl vyhotoven dne 18. 3. 2024

Aneta Vaňousová	Ing. Martin Barták	JUDr. Milan Chaloupka, MBA, LL.M.
zapisovatel	**ověřovatel**	**předseda výboru**