Věc: Poptávka digitálních služeb pro členy Komory daňových poradců ČR

Komora daňových poradců ČR realizuje záměr zprostředkovat svým členům nabídku škálovatelných digitálních služeb za zvýhodněných podmínek. Je přitom mít na zřeteli skutečnost, že jednou z klíčových potřeb daňových poradců (dále jen DP) je zákonem uložené zachování mlčenlivosti, pod níž spadá i ochrana dat a údajů o klientech. Současně je DP uložena povinnost získávat některé informace v rámci plnění povinností dle zákona proti praní špinavých peněz (tzv. AML zákon).

Tato poptávka je cílena na služby určené především pro samostatné daňové poradce a malé nebo maximálně středně velké společnosti. V rámci rozsáhlého průzkumu, který byl proveden na jaře roku 2023, o takové služby projevilo zájem téměř 50 % oslovených. Služby mohou být nabízeny jednotlivě nebo jako kompletní „balíčky“.

Daňoví poradci se mohou proti kybernetickým rizikům pojistit, ovšem za předpokladu naplnění podmínek, které stanovil zajistitel a které spočívají v péči o hardware a software při dodržování základních bezpečnostních pravidel, ale také v udržování úrovně informovanosti a povědomí o digitálních hrozbách a rizicích. Tyto podmínky zajistitele jsou zahrnuty do doplňkových a nadstandardních služeb uvedených dále.

1. Základní služby

1.1. Cloudové úložiště

- **Zabezpečené cloudové úložiště** – specifikem daňových poradců je povinná mlčenlivost ze zákona a s tím související potřeba ochrany klientských údajů a písemností. Výhodou by proto byla možnost údaje (nebo jejich část) šifrovat.
- **Řízený přístup k úložišti pro X uživatelů** – zabezpečení přístupu před neoprávněnými osobami, definice práv v typickém členění (číst, psát, mazat).

1.2. Distanční plnění povinností dle AML

Cílem je možnost na vyžádání obdržet informace o fyzické nebo právnické osobě v rozsahu požadovaném pro identifikaci a kontrolu klienta dle zákona č. 253/2008 Sb. AML, a to bez fyzické přítomnosti prověřované osoby (viz §8a AML zákona).

2. Doplňkové služby

Jedná se o správu hardware a software daňově poradenské kanceláře a také o pravidelné (např. čtvrtletní) poskytování aktuálních informací.

2.1. Vzdálená správa / kontrola IT

Jedná se o instalaci, udržování a kontrolu HW a SW v pravidelných intervalech, včetně písemného výstupu v podobě osvědčení stavu. Hlavními komponenty jsou:

- antivirus, anti-spyware, anti-malware (profesionální nástroje, ne volně dostupné bezplatné a obdobné verze)
- zabezpečení všech přístupových bodů pro internet firewallem, který je minimálně jednou měsíčně kontrolován a případně nastaven / konfigurován

IČO: 44995059
DIČ: CZ44995059
Bankovní spojení:
UniCredit Bank Czech Republic and Slovakia, a.s.
č.ú. 2107491443/2700
IBAN: CZ4327000000002107491443
BIC: BACXCZPPXXX

Sídlo:
Kozí 4
602 00 Brno
Tel.: +420 542 422 311
E-mail: kdp@kdpcr.cz
Internet: www.kdpcr.cz
ID datové schránky: ng6adi3

- kontrolní procesy zaměřené na SW a Aplikace po ukončení životnosti, nebo s ukončenou podporou (End of Life / End of Support) s cílem identifikovat uvedený SW / Aplikace a minimalizovat rizika vyplývající z ukončení supportu
- kontrola zabezpečení přenosných zařízení – ochrana heslem, doporučeno používat vícefaktorové ověřování

2.2. Pravidelné školení / informování

Jedná se o pravidelné poskytnutí aktuálních informací, např. v podobě meetingu nebo bulletinu. Informace se týkají:

- požadavků dle předpisů o ochraně osobních údajů v souladu s příslušnou legislativou, novinky na poli ePrivacy, regulace AI ad.
- povědomí o oblasti IT bezpečnosti, především rizika phishingu, otevírání příloh v emailech, aktuálních hrozeb a rizik apod.
- pravidel bezpečného prohlížení webu, používání sociálních sítí, zadávání platebních údajů
- požadavků na užívání hesel (síla, pravidelná obměna), případně využívání nástrojů v podobě správce hesel

3. Nadstandardní služby

Představují nadstavbové služby, které uvedl zajistitel jako podmínku pro sjednání rozšířeného rozsahu pojistného krytí.

3.1. Vypracování / udržování dokumentace

Jedná se o zhotovení (přizpůsobení) dokumentace určené ke stanovení postupů v případě incidentu z oblasti kybernetických rizik. Konkrétně by šlo o:

- Plán postupů chování v případě bezpečnostního incidentu (v oblasti IT rizik) nebo narušení bezpečnosti údajů (směrnice pro případ incidentů)
- Plán na zachování / obnovení provozu (zaměřená na IT a cyber rizika) – Business continiuity plan, Business recovery plan

3.2. IT audit z pohledu rizik

Pravidelně (minimálně jednou měsíčně) posilování bezpečnosti systému (hardening) všech serverů a pracovních stanic. Pravidelné odstraňování zbytečného softwaru, loginů, služeb.

V případě zájmu o poskytování výše uvedených služeb, zašlete stručné informace na adresu elektronické pošty **neuzil@kdpcr.cz**. Uveďte prosím základní údaje o rozsahu nabízených služeb např. vyplněním přiložené tabulky.

Kvantitativní profily daňových poradců OSVČ a malých společností (průměr) :

OSVČ

Parametr	1 rok	5 let
Potřebný cloudový prostor pro archivaci v GB	2 GB	12 GB
Počet digitálních písemností	3 000	16 000
Počet uživatelů s přístupem	1	1
Počet udržovaných písemností	20	120

MALÁ FIRMA

Parametr	1 rok	5 let
Potřebný cloudový prostor pro archivaci v GB	7	35
Počet digitálních písemností	10 000	50 000
Počet uživatelů s přístupem	5	5
Počet udržovaných písemností	100	500

STŘEDNÍ FIRMA

Parametr	1 rok	5 let
Potřebný cloudový prostor pro archivaci v GB	1000	3000
Počet digitálních písemností	100 000	400 000
Počet uživatelů s přístupem	20	50
Počet udržovaných písemností	1000	5000

Pozn. Udržováním písemností se rozumí zajištění jejich dlouhodobé použitelnosti v elektronické podobě s využitím pečetí, časových razítek apod.

S pozdravem

MVDr. Milan Vodička
vedoucí Sekce informačních technologií
člen Prezidia KDP ČR

Příloha:
Příloha k poptávce digitálních služeb

IČO: 44995059
DIČ: CZ44995059
Bankovní spojení:
UniCredit Bank Czech Republic and Slovakia, a.s.
č.ú. 2107491443/2700
IBAN: CZ4327000000002107491443
BIC: BACXCZPPXXX

Sídlo:
Kozí 4
602 00 Brno
Tel.: +420 542 422 311
E-mail: kdp@kdpcr.cz
Internet: www.kdpcr.cz
ID datové schránky: ng6adi3